One Identity Starling Two-Factor Authentication

Administration Guide

Starling Two-Factor Authentication Administration Guide
Updated - November 2019

Contents

Starling Two-Factor Authentication

Introduction to Starling Two-Factor Authentication

Accessible from the Starling site (https://www.cloud.oneidentity.com/), this service uses advanced two-factor authentication capabilities to further protect your resources. Starling Two-Factor Authentication is able to do so without overly restricting your user's authentication options and also allows for quick responses to any authentication issues your users may have through an easy-to-use interface.

Starling Two-Factor Authentication can be used alongside a number of One Identity products thus allowing for you to take advantage of a hybrid cloud solution, and can also be tailored to fit your needs through the use of the following on-premises components: AD FS Adapter, Desktop Login, HTTP Module, and RADIUS Agent.

IMPORTANT: In order to use Starling Two-Factor Authentication you need a Starling organization and account. For more information, see the Starling documentation (https://support.oneidentity.com/starling-two-factor-authentication/hosted/technical-documents).

IMPORTANT: In order to use Starling Two-Factor Authentication some additional software and hardware requirements must be met. For more information, see Additional hardware and software requirements.

NOTE: To view the documentation or contact support while using Starling Two-Factor Authentication click the  button.

Supported browsers

The following browsers are supported when accessing the Starling service.

Table 1: Supported desktop browsers

Browser	Minimum OS/Platform	Version
Internet Explorer	Windows 7	11
Google Chrome	Windows 10 Mac OS X Yosemite	Latest
Mozilla Firefox	Windows 8.1	Latest
Microsoft Edge	Windows 10	Latest
Safari	Mac OS X Yosemite	See OS/Platform

Table 2: Supported mobile browsers

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

Navigating Starling Two-Factor Authentication using a mobile device

Along with the main Starling portal, Starling Two-Factor Authentication is compatible with mobile devices. Use the  button at the top of your screen to display the navigation bar options and account information. Also, be aware that due to space constraints some tables may be condensed when viewed in portrait mode to only display key columns and some features may not be available.

Additional hardware and software requirements

Features available within Starling Two-Factor Authentication have additional requirements beyond those necessary for Starling overall (for more information, see the *Starling User Guide*).

Starling Two-Factor Authentication application requirements

Table 3: Application requirements

Application type	Link
Desktop (64-bit only)	https://2fa.cloud.oneidentity.com/install
Android	https://play.google.com/store/apps/details?id=com.starling.twofactor
iOS	https://itunes.apple.com/app/starling-2fa/id1205700916

Hardware token requirements

Table 4: Hardware token requirements

Token type	Specifications
OATH-HOTP	• CSV Each line must use the following column order: NOTE: Examples: • `{serial},{secretKeyTxt},{oathMovingFactorSeed}` • `{serial},{secretKeyTxt},,,,{timeInterval}` • Serial number • Secret key in decrypted hexadecimal format NOTE: The following columns are only required if the default value is incorrect. Columns left empty are automatically read as the default value. • Counter (HOTP only, default 0) • Algorithm type (default HOTP) • Response length (default 6) • Time interval (TOTP only, default 30) • PSKC • If unencrypted, secret must be in decrypted base 64 encoded string. • If encrypted, either AES (Advanced Encryption Standard) or 3DES (Triple Data Encryption Algorithm) is supported, the file key is required. Supported hash algorithms: • HMAC-SHA1

Token type	Specifications
	• HMAC-MD5 • HMAC-SHA256 • HMAC-SHA384 • HMAC-SHA512
TOTP	NOTE: The token code is valid for approximately 5 minutes. • CSV Each line must use the following column order: NOTE: Examples: • `{serial},{secretKeyTxt},{oathMovingFactorSeed}` • `{serial},{secretKeyTxt},,,,{timeInterval}` • Serial number • Secret key in decrypted hexadecimal format NOTE: The following columns are only required if the default value is incorrect. Columns left empty are automatically read as the default value. • Counter (HOTP only, default 0) • Algorithm type (default HOTP) • Response length (default 6) • Time interval (TOTP only, default 30) • PSKC: NOTE: Vasco v12 PSKC is supported, but not Vasco v11 PSKC. • If unencrypted, secret must be in decrypted base 64 encoded string. • If encrypted, either AES (Advanced Encryption Standard) or 3DES (Triple Data Encryption Algorithm) is supported, the file key is required. Supported hash algorithms: • HMAC-SHA1 • HMAC-MD5 • HMAC-SHA256 • HMAC-SHA384

Token type	Specifications
	• HMAC-SHA512 • DPX • NOSTATIC

Azure Active Directory integration requirements

Table 5: Application requirements

Permission	Specification
Account requirements	• Internal Privileged Role Administrator or internal Global Administrator Azure Active Directory account. • Subscription to a premium Azure Active Directory edition.

Integrating client products with Starling Two-Factor Authentication

There are two methods client products (such as Password Manager and One Identity Safeguard) are able to use to integrate with Starling Two-Factor Authentication. Check the documentation for the client product for more information on which integration option is available.

- Subscription key method: This method requires the **Subscription key** (available on the Dashboard page of Starling Two-Factor Authentication) be used to configure your on-premises client product to connect with Starling Two-Factor Authentication.
- Join method: This method requires the on-premises client product be joined to Starling Two-Factor Authentication without the use of a subscription key. For information on this process specific to your client product, contact Support or Sales for more information on joining with Starling.

  If you are joining Starling Two-Factor Authentication via a purchased Hybrid subscription, see the on-premises product's documentation for information on the join process. You can also find information and video tutorials on this process on the One Identity Hybrid Subscription knowledge base.

The Starling Two-Factor Authentication service

Once you have created a Starling organization, you can add the Starling Two-Factor Authentication service to that organization. The types of subscriptions available for Starling Two-Factor Authentication are:

- Paid subscription
- Hybrid subscription
- Trial subscription

Paid subscription

A Starling Two-Factor Authentication subscription can be purchased by a Starling organization. A paid subscription provides you with full access to the product (including the on-premises components) for the length of your contract and a set number of user licenses. This type of subscription can also be combined with the Hybrid subscription (which provides unlimited licenses for your hybrid product) in order to gain full access to all features of Starling Two-Factor Authentication. For information on the on-premises Starling Two-Factor Authentication components (AD FS Adapter, Desktop Login, HTTP Module, and RADIUS Agent), see the Starling Two-Factor Authentication documentation.

For information on purchasing a subscription to the Starling Two-Factor Authentication service, use the **More Information** button associated with the service.

NOTE: Contact Sales or Support to cancel a paid subscription.

Hybrid subscription

A Starling Two-Factor Authentication subscription can be purchased by a Starling organization via One Identity Hybrid Subscription (which is available for purchase alongside eligible on-premises products such as One Identity Safeguard and Password Manager). A Hybrid subscription provides you with unlimited licenses for your hybrid product, but does not include access to the on-premises components of Starling Two-Factor Authentication. This type of subscription can also be combined with a paid subscription (which provides access to the on-premises components) in order to gain full access to all features of Starling Two-Factor Authentication.

For information on purchasing a subscription to the Starling Two-Factor Authentication service, use the **More Information** button associated with the service.

NOTE: Contact Sales or Support to cancel a Hybrid subscription.

Trial subscription

Services available for trial can be subscribed to for a limited period of time before they require a full subscription. This allows you to view and test the product before making a longer term commitment to using the service. If you do not decide to upgrade your subscription, you will lose access to Starling Two-Factor Authentication. However, if you decide to upgrade to a paid subscription at a later date, the Starling Two-Factor Authentication service will be restored in the same condition it was in when it expired.

Starting a service trial

Once logged in to Starling you can trial the Starling Two-Factor Authentication service.

To start a service trial

1. Sign in to Starling.
2. On the Starling home page, locate the Starling Two-Factor Authentication service and click **Trial**.
3. In the dialog, select your country from the drop-down list. This field only appears the first time you add a service to your organization.
4. If applicable, a second field will appear in which you must select your state or province from the drop-down list. This field only appears the first time you add a service to your organization.
5. Click **Confirm**.

   The service will be added to the **My Services** section and be available for use until the trial period has ended. The number of days left in your trial is indicated by a countdown on the service access button on the Starling home page. At any point in the trial you can use the **More Information** button associated with the service to find out how to purchase the product.

Ending a service trial

The number of days left in your trial is indicated on the service access button. Once your trial period has ended the service will no longer be accessible. Please use the contact information associated with the service to inquire about purchasing options.

Inviting an administrator to a service

The following procedure applies to organization administrators. It is designed to allow additional administrators to be added and to allow a new administrator to be invited to a service in cases where the last administrator assigned to that service has left the organization.

To invite an administrator to a service

1. From the Starling home page, click the button associated with the service to which you want to invite a new administrator.
2. Select **Invite Administrator**.
3. Depending on the type of account, the following methods can be used for inviting a new administrator to the service:
    - To invite an administrator:
        a. Enter the name and email address of the user.
        b. Click **Invite**. An invitation to the service will be sent to the user.
    - To invite an administrator with an Azure AD work account:

        NOTE: This option is only available for organization administrators with an Azure AD work account.

        a. Click the drop-down menu field.
        b. In the blank search box, begin typing the name of the user. When you have located the user, select them from the list.
        c. Click **Invite**. An invitation to the service will be sent to the user.

Managing multiple Starling organizations

Starling users have the option of adding additional collaborators to their Starling Two-Factor Authentication service (Adding additional collaborators). In cases where an invited collaborator has already created a Starling organization, they can switch between organizations from within Starling.

To switch between Starling organizations

1. From within the Starling Two-Factor Authentication service, click the button in the title bar to open a drop-down menu listing the names of the organizations to which you have access.
2. Select the name of the organization to which you want to switch. The Starling Two-Factor Authentication service will update to display the information associated with the organization listed in the title bar.

2

Getting started

Using the Starling Two-Factor Authentication service

Once you have added the Starling Two-Factor Authentication service to your One Identity Starling organization, as either a trial, hybrid, or paid subscription, you have full access to the Starling Two-Factor Authentication service.

To navigate through the service use the title bar along the top of the site, which contains the following links:

-  : If multiple organizations are associated with your account, this button (displaying the name of the organization you are currently viewing) appears and opens a drop-down menu that allows you to move between organizations. For more information, see Managing multiple Starling organizations.
-  : This button (displaying the first name of the account owner) opens a drop-down menu that allows you to select one of the following options:
  - **My Services**: Clicking this link takes you to the One Identity Starling home page.
  - **Sign out**: Clicking this link signs you out of One Identity Starling.
-  : This button opens a dialog displaying notifications related to your account.
-  : This button opens a drop-down menu that allows you to select one of the following options:
  - **Documentation**: Clicking this link opens a new tab with the Starling Two-Factor Authentication Administration Guide.
  - **Support**: Clicking this link opens a new tab with the Starling Two-Factor Authentication Support site.
-  : This button opens a drop-down menu that allows you to select one of the following options:

- **2FA Settings**: Clicking this link opens the Settings page for Starling Two-Factor Authentication.
- **Starling Settings**: Clicking this link opens the settings page where you can manage your entire Starling account. For more information, see the *One Identity Starling User Guide*.

The main pages available within Starling Two-Factor Authentication are listed in the navigation bar, which is located beneath the title bar:

- Dashboard page: This is the home page of Starling Two-Factor Authentication and provides insight into your service. Helpdesk collaborators see a limited version of this page.
- Collaborators page: This page is used to add additional collaborators to your Starling Two-Factor Authentication service. Primary Administrators have full access and permissions on this page, whereas Administrators will require a secondary approval from another Administrator or Primary Administrator before their changes will take effect.
- Users page: This page is used for managing the user accounts associated with your Starling Two-Factor Authentication service. Helpdesk collaborators are able to access this page to generate temporary response codes for users.
- Approvals page: This page is used for managing the approvals required when an Administrator makes changes to the collaborators or the subscription key.
- Integrations page: This page is used for integrating Azure Active Directory with your Starling Two-Factor Authentication service.
- Hardware Tokens page: This page is used for managing the hardware tokens associated with your Starling Two-Factor Authentication service. Helpdesk collaborators are able to access a limited version of this page.
- Settings page: This page is used to customize the settings used by Starling Two-Factor Authentication (General Settings tab) and the Starling 2FA app (Token UI Settings tab).
- Downloads: This page is used to download the Starling 2FA application and the Starling Two-Factor Authentication on-premises components.

Dashboard page

Upon opening Starling Two-Factor Authentication, you will be directed to the **Dashboard** page. The **Dashboard** page provides an overview of your subscription.

The following information is displayed on the **Dashboard** page:

Calls

This tile displays the number of calls made in the current month regardless of whether the authentication was successful.

SMS

This tile displays the number of codes sent in the current month regardless of whether the authentication was successful.

Authentications

This tile displays the number of successful authentications (excluding push notifications) in the current month.

Service usage graph

This graph reflects the **Calls**, **SMS**, and **Authentications** tile information for the previous 13 months of the subscription.

License Details

This pane provides the following licensing information for your Starling Two-Factor Authentication service. The information contained in this pane changes depending on the type of subscription you have:

Hybrid subscription

- **License Status**: This field displays the current status of your Starling Two-Factor Authentication subscription. An alert will appear if one of your subscriptions (paid or Hybrid) has expired while the other is still active.
- **Licensed Users**: This field displays the total number of available user licenses for trial or paid subscriptions. Hybrid subscriptions allow for unlimited licenses for your hybrid products (and the number of authenticated hybrid users is indicated in the **Hybrid Subscription Users** field), however you may also have an active paid subscription which limits the number of licenses for your non-hybrid products.

  IMPORTANT: If your Hybrid subscription expires while your paid subscription is still valid, you will need to ensure your total number of **Consumed User Licenses** is equal to or less than your **Licensed Users**.

- **Consumed User Licenses**: This field displays the total number of user licenses currently consumed for a paid or trial subscription, and must be equal to or less than your purchased licenses (**Licensed Users** count).

  NOTE: If you have switched to a Hybrid subscription, as each user authenticates to a hybrid-enabled product they will switch to being counted as **Hybrid Subscription Users** rather than **Consumed User Licenses**. Some users will automatically be switched to the **Hybrid Subscription Users** count since they had previously authenticated via a hybrid-enabled product.

- **Created**: This field displays the date and time the subscription was created.
- **Expires**: This field displays the date and time the subscription will expire.

- **Hybrid Subscription**: This field indicates whether or not there is a Hybrid subscription. You can have both a paid and Hybrid subscription active at the same time.
- **Hybrid Subscription Expires**: This field displays the date and time the Hybrid subscription will expire.
- **Hybrid Subscription Users**: This field displays the total number of users that have authenticated to a hybrid-enabled client product.

Paid subscription

- **License Status**: This field displays the current status of your Starling Two-Factor Authentication subscription.
- **Licensed Users**: This field displays the total number of available user licenses.
- **Consumed User Licenses**: This field displays the total number of user licenses currently consumed for a paid subscription, and must be equal to or less than your purchased licenses (**Licensed users** count).
- **Created**: This field displays the date and time the subscription was created.
- **Expires**: This field displays the date and time the subscription will expire.
- **Hybrid Subscription**: This field indicates whether or not there is a Hybrid subscription. You can have both a paid and Hybrid subscription active at the same time.

Trial subscription

- The number of days left in your trial is indicated at the top of the pane.
- **Licensed Users**: This field displays the total number of available user licenses.
- **Consumed User Licenses**: This field displays the total number of user licenses currently consumed. The number of consumed licenses must be equal to or less than the number of available licenses (**Licensed users** count).
- **Created**: This field displays the date and time the trial was created.
- **Expires**: This field displays the date and time the trial will expire.
- **Hybrid Subscription**: This field indicates whether or not there is a Hybrid subscription.

Subscription Details

This pane provides the following information on the Starling Two-Factor Authentication subscription:

- **Id**: This field displays your subscription Id. This may be requested by Support if you contact them for assistance with your subscription.

Subscription Key

This expandable tile contains the key needed to integrate a client product with Starling Two-Factor Authentication. For information on using this key with your client product, contact Sales or Support. A new key can only be generated every 24 hours.

Primary Administrators and Administrators can use the **Create New Key** button to generate a new key (although Administrators will require approval for the new key) for any reason. After a new key is generated, the old key will remain valid for 24 hours.

3

Collaborators

Introduction to Collaborators

Starling Two-Factor Authentication allows users to add collaborators to their service (as Primary Administrator, Administrator, or Helpdesk) based on the type of access required for the user. Adding additional collaborators is optional and can be done at any time using the Collaborators page.

The following roles are available for your collaborators:

- Primary Administrator: This role allows you full access to all parts of the Starling Two-Factor Authentication service and allows you full configuration capabilities. There must always be at least one Primary Administrator associated with the service.
- Administrator: This role allows you full access to the Starling Two-Factor Authentication service. However, Administrators will require approval from another Administrator or Primary Administrator when they make changes to the collaborators for the service or generate a new subscription key.
- Helpdesk: This role provides limited access to the Starling Two-Factor Authentication service. Specifically, Helpdesk users have access to the Users page, Hardware Tokens page, and a limited view of the Dashboard page. Helpdesk users are responsible for managing users, including issuing temporary access tokens.

Collaborators page

The **Collaborators** page is displayed when **Collaborators** is clicked in the navigation bar. The **Collaborators** page is used for adding and managing the collaborators currently associated with the Starling Two-Factor Authentication service. Primary Administrators have full access and permissions on this page, whereas Administrators will require a secondary approval from another Administrator or Primary Administrator before their changes will take effect.

The following options appear on this page:

Invite Collaborator

Clicking this button opens the **Invite Collaborator** dialog so you can add new collaborators to your Starling Two-Factor Authentication service. For more information, see Adding additional collaborators or Adding additional Azure AD work account collaborators.

Refresh

Clicking this button refreshes the table.

This field is used to search for a user based on their name or email. To use the search functionality, start typing in the field. The table will automatically update to display results that match.

The following information and options appear in the table on this page:

Name

This displays the name specified in the collaborator invite.

Email

This displays the email address associated with the collaborator.

Role

This displays the role currently assigned to the collaborator. The available roles are:

- **Primary Administrator**: This role allows you full access to all parts of the Starling Two-Factor Authentication service and allows you full configuration capabilities. There must always be at least one Primary Administrator associated with the service.
- **Administrator**: This role allows you full access to the Starling Two-Factor Authentication service. However, Administrators will require approval from another Administrator or Primary Administrator when they make changes to the collaborators for the service or generate a new subscription key.
- **Helpdesk**: This role provides limited access to the Starling Two-Factor Authentication service. Specifically, Helpdesk users have access to the Users page, Hardware Tokens page, and a limited view of the Dashboard page. Helpdesk users are responsible for managing users, including issuing temporary access tokens.

Status

This displays the status of the collaborator. When a collaborator is added they will be marked as **Invited** until the invitation has been accepted, at which point the **Status**

column will update to display **Registered**. If an Administrator has selected to remove a collaborator, a status of **Pending Removal** will appear until the request has been approved or rejected.

The ⋮ button appearing for a collaborator contains the following options depending on the current status of the collaborator.

- **Edit Role**: Available for a confirmed collaborator, selecting this option opens the **Edit Role** dialog where you can make changes to the selected role. Administrators that make edits to a collaborator require approval from another Administrator or Primary Administrator. For more information, see Editing roles.
- **Remove Collaborator**: Available for a confirmed collaborator, select this option to remove the collaborator from Starling Two-Factor Authentication. Administrators that select to remove a collaborator require approval from another Administrator or Primary Administrator. For more information, see Removing collaborators.
- **Resend Invitation**: Available for an invited collaborator, selecting this option resends the invitation to the selected collaborator if they have not yet accepted. For more information, see Resending collaborator invitation.
- **Cancel Invitation**: Available for an invited collaborator, selecting this option cancels the invitation to the selected collaborator if they have not yet accepted. For more information, see Canceling collaborator invitation.

NOTE: You are unable to manage your own collaborator account. If you are the only Primary Administrator for the account then only another Primary Administrator can remove or edit your role. Coordinate with other administrators before making edits to their roles to avoid removing each other as administrators.

Managing collaborators

The following sections provide information on managing collaborators for the Starling Two-Factor Authentication service.

- Adding additional collaborators
- Adding additional Azure AD work account collaborators
- Editing roles
- Removing collaborators
- Resending collaborator invitation
- Canceling collaborator invitation

Adding additional collaborators

Collaborators are optional and can be added at any time. For information on adding a collaborator from your Azure AD account, see Adding additional Azure AD work account collaborators.

NOTE: Administrators require a secondary approval from another Administrator or Primary Administrator before their changes will take effect.

To add additional collaborators

1. On the **Collaborators** page, click **Invite Collaborator**.
2. In the **Invite Collaborator** dialog, click the **Role** field to select the role that will be assigned to the new collaborator:
    - **Primary Administrator**: This role allows you full access to all parts of the Starling Two-Factor Authentication service and allows you full configuration capabilities. There must always be at least one Primary Administrator associated with the account.
    - **Administrator**: This role allows you full access to the Starling Two-Factor Authentication service. However, Administrators will require approval from another Administrator or Primary Administrator when they make changes to the collaborators for the service or generate a new subscription key.
    - **Helpdesk**: This role allows you limited access to the Dashboard for managing users, Hardware Tokens page, and to the Users page to generate temporary response codes.
3. Enter the name and email address for the new collaborator.
4. Click **Invite**.
5. An email will be sent with a link to either register a new account that has access to your organization or, if the recipient has already registered with Starling using this email address, a notification that they now have access to your organization's Starling Two-Factor Authentication service. They will be marked as **Registered** (already registered users) or **Invited** (new Starling users) until the invitation has been accepted (at which point the **Status** column will update to display **Registered**).

    NOTE: Users associated with multiple organizations can switch between Starling subscriptions once they have logged in (Managing multiple Starling organizations).

    NOTE: Until an invite has been accepted, the following options are available:
    - **Resend Invitation**: Selecting this option will resend the invitation.
    - **Cancel Invitation**: Selecting this option will cancel the invitation. The invited user will not be notified that the invitation was canceled; however, when logging in they will be unable to access the service.

Adding additional Azure AD work account collaborators

Collaborators are optional and can be added at any time. For information on adding a collaborator from outside your Azure AD account, see Adding additional collaborators.

To add additional Azure AD work account collaborators

1. On the **Collaborators** page, click **Invite Collaborator**.
2. In the **Role** field, select the role that will be assigned to the new collaborator:
    - **Primary Administrator**: This role allows you full access to all parts of the Starling Two-Factor Authentication service and allows you full configuration capabilities. There must always be at least one Primary Administrator associated with the service.
    - **Administrator**: This role allows you full access to the Starling Two-Factor Authentication service. However, Administrators will require approval from another Administrator or Primary Administrator when they make changes to the collaborators for the service or generate a new subscription key.
    - **Helpdesk**: This role provides limited access to the Starling Two-Factor Authentication service. Specifically, Helpdesk users have access to the Users page, Hardware Tokens page, and a limited view of the Dashboard page. Helpdesk users are responsible for managing users, including issuing temporary access tokens.
3. Click in the **Search for collaborator** field and begin typing in the empty field to filter the available collaborators.
4. Click the name of the collaborator you want to add to populate the field.

    NOTE: If the collaborator cannot be found or is not associated with your Azure AD tenant, click **Unable to find collaborator** and enter the name and email address of the user you would like to add as a collaborator to your organization.

5. Click **Invite**.
6. An email will be sent with a link to either register a new account that has access to your organization or, if the recipient has already registered with Starling using this email address, a notification that they now have access to your organization's Starling Two-Factor Authentication service. They will be marked as **Registered** (already registered users) or **Invited** (new Starling users) until the invitation has been accepted (at which point the **Status** column will update to display **Registered**).

    NOTE: Users associated with multiple organizations can switch between Starling subscriptions once they have logged in (Managing multiple Starling organizations).

NOTE: Until an invite has been accepted, the following options are available:

- **Resend Invitation**: Selecting this option will resend the invitation.
- **Cancel Invitation**: Selecting this option will cancel the invitation. The invited user will not be notified that the invitation was canceled; however, when logging in they will be unable to access the service.

Editing roles

The following procedure explains how to edit a collaborator's assigned roles.

NOTE: Administrators require a secondary approval from another Administrator or Primary Administrator before their changes will take effect.

To edit roles for a collaborator

NOTE: It can take up to 15 minutes for changes to take effect for currently logged in users.

1. On the **Collaborators** page, locate the collaborator whose role you want to edit.
2. Once you have located the collaborator to edit, click the ⋮ button associated with their account.
3. Select **Edit Role**.
4. In the **Edit Role** dialog, make any necessary changes.
5. Click **Save** to save your changes and return to the **Collaborators** page.

Removing collaborators

If a collaborator is no longer needed, you can remove them from the Starling Two-Factor Authentication service.

NOTE: Administrators require a secondary approval from another Administrator or Primary Administrator before their changes will take effect. However, a collaborator pending removal will be redirected to an error page should they attempt to access Starling Two-Factor Authentication. Once the secondary approval occurs, the removed collaborator will no longer see the Starling Two-Factor Authentication service listed.

NOTE: You are unable to manage your own collaborator account. If you are the only Primary Administrator for the account then only another Primary Administrator can remove or edit your role. Coordinate with other administrators before making edits to their roles to avoid removing each other as administrators.

To remove collaborators

1. On the **Collaborators** page, locate the user you want to delete as a collaborator.
2. Once you have located the collaborator to edit, click the ⋮ button associated with their account.
3. Select **Remove Collaborator**.
4. In the confirmation dialog, click **Yes** to remove their access to your subscription of Starling Two-Factor Authentication.

Resending collaborator invitation

If an invited collaborator has not accepted their invitation or their invitation was deleted, you can resend the email invitation.

To resend collaborator invitations

1. On the **Collaborators** page, locate the invited collaborator you will be resending an invitation to.
2. Once you have located the collaborator, click the ⋮ button associated with their account.
3. Select **Resend Invitation**.

   A new invitation will be sent to the collaborator.

Canceling collaborator invitation

If an invited collaborator is no longer needed, you can rescind their collaborator invitation from the Starling Two-Factor Authentication service before they accept the emailed invitation.

To cancel collaborator invitations

1. On the **Collaborators** page, locate the invited collaborator whose invitation you will be canceling.
2. Once you have located the collaborator, click the ⋮ button associated with their account.
3. Select **Cancel Invitation**.
4. In the confirmation dialog, click **Yes** to remove their access to your subscription of Starling Two-Factor Authentication.

   The previously invited user will not be notified that the invitation was canceled; however, when logging in they will be unable to access the service.

4

Users

Introduction to Users

Once a client product joins with Starling Two-Factor Authentication, users are automatically added to the **Users** page as they authenticate via the client product. From this page you can view and manage the users currently associated with the Starling Two-Factor Authentication service.

Users page

The **Users** page is displayed when **Users** is clicked in the navigation bar. The **Users** page is used for managing the users currently associated with the Starling Two-Factor Authentication service.

The following buttons appear at the top of this page:

Add

Clicking this button opens the **Add User** dialog so you can add new users to your Starling Two-Factor Authentication service without waiting for them to authenticate via your client product. However, there is no way to sync unique users added to Starling Two-Factor Authentication with the client product and they will be unable to authenticate if they are not also in the client product. This means you must ensure any users manually added to Starling Two-Factor Authentication are identical to existing users within your client product. For more information, see Adding additional users.

Import Users

Clicking this button opens the **Import Users** dialog so you can add multiple users at the same time using a CSV file. However, there is no way to sync unique users added to Starling Two-Factor Authentication with the client product and they will be unable to authenticate if they are not also in the client product. This means you must ensure any users manually added to Starling Two-Factor Authentication are identical to

existing users within your client product. For more information, see Importing users with a CSV file.

Delete

Activated once one or more users are selected in the table, you can delete the selected user from the table by clicking this button. There is a 30 day window to restore the account from the **Users** page after a user has been deleted. If a user marked for deletion authenticates during those 30 days then they will be restored automatically while also pulling in any updated user data, and if the user does not authenticate after being marked for deletion then they will be deleted and no longer count towards your consumed licenses. For more information, see Deleting users.

Disable

Activated once one or more user accounts are selected in the table, clicking this button disables the user account so that it cannot be used nor will it be counted towards your consumed licenses. For more information, see Disabling a user account.

Enable

Activated once one or more disabled user accounts are selected in the table, clicking this button enables a previously disabled user account so that it can be used and will be counted towards your consumed licenses. For more information, see Enabling a user account.

Restore

Activated once one or more users marked for deletion are selected in the table, clicking this button restores the user account. For more information, see Restoring users.

Refresh

Clicking this button refreshes the table.

This field is used to search for a user based on their name, email, or mobile number. To use the search functionality, start typing in the field. The table will automatically update to display results that match.

The following information and option appear in the table on this page:

Email

This displays the email address associated with the user.

Name

This displays the name of the user.

Mobile

This displays the mobile number for the user.

Status

This displays the status of the user.

- **Active**: This indicates the user is active and counts towards your consumed licenses.
- **Inactive**: This indicates a user account has been disabled and thus does not count towards consumed licenses.
- **Pending Removal**: This indicates a user account is marked for deletion and thus does not count towards consumed licenses. If the user account is not restored or does not authenticate within 30 days then it will be deleted from Starling Two-Factor Authentication.

Hardware Tokens

This lists the number of hardware tokens assigned to a user. Clicking the link in the field will direct you to a user specific version of the Hardware Tokens page where you can manage tokens for the user. Depending on your collaborator type, the following functionalities are available:

- **Assign**: (Primary Administrators and Administrators only) Select this option to assign the token to a user. For more information, see Assigning a hardware token to a user.
- **Unassign**: (Primary Administrators and Administrators only) Select this option to unassign a token from a user. For more information, see Unassigning a hardware token from a user.
- **Reset**: Select this option to reset the token. For more information, see Resetting a hardware token.
- **Test**: Select this option to test the token. For more information, see Testing a hardware token assigned to a user.

Last Used

This column displays the date the user last successfully authenticated using Starling Two-Factor Authentication.

Clicking the **Temporary response** link associated with a user, generates a code that can be used by the user if they are unable to authenticate using their configured device. For more information, see Generating a temporary response code for a user.

Managing users

The following sections provide information on managing users for the Starling Two-Factor Authentication service.

NOTE: Once added to Starling Two-Factor Authentication, users can be assigned hardware tokens from the Users page. For more information, see Managing hardware tokens.

- Adding additional users
- Importing users with a CSV file
- Deleting users
- Disabling a user account
- Enabling a user account
- Generating a temporary response code for a user

Adding additional users

Although your users will be provisioned on-demand when joining Starling Two-Factor Authentication, you do have the option of manually adding users. However, there is no way to sync unique users with the client product and they will be unable to authenticate through Starling Two-Factor Authentication if they are not also in the client product. This means you must ensure any users manually added to Starling Two-Factor Authentication are identical to existing users within your client product.

To add additional users

CAUTION: Client products not using hardware tokens: It is recommended that you allow users to be provisioned on-demand to ensure they correctly sync up between the client product and Starling Two-Factor Authentication.

Client products using hardware tokens: Because you need to have a hardware token assigned to a user prior to their first authentication attempt with the hardware token, you need to manually add new users to Starling Two-Factor Authentication and assign a token to them. These users must be identical to a user in the client product in order to recognize the user when they first authenticate. If they are not identical then they will be unable to authenticate until the mismatched user records are corrected and the hardware token assigned to the correct record.

1. On the **Users** page, click **Add**.
2. In the **Add User** dialog, enter the email, name (optional), country (this assigns the

country code for the mobile number), and mobile number of the user you would like to add.

> **CAUTION: If the phone number for a manually added user already exists but with a different name or email, then the name and email for the user will be updated. If the same phone number is used in multiple subscriptions then all subscriptions will be updated accordingly.**

3. Click **Save**.

   Once a user has been added, a new token will appear in their Starling 2FA app. If the user has not been provisioned in any Starling Two-Factor Authentication subscription and the General Settings tab option to send SMS is enabled, the new user will also receive instructions on installing the Starling 2FA app.

Importing users with a CSV file

Although your users will be provisioned on-demand when joining Starling Two-Factor Authentication, you do have the option of manually adding users. However, there is no way to sync unique users with the client product and they will be unable to authenticate through Starling Two-Factor Authentication if they are not also in the client product. This means you must ensure any users manually added to Starling Two-Factor Authentication are identical to existing users within your client product.

To import users with a CSV file

> **CAUTION: Client products not using hardware tokens: It is recommended that you allow users to be provisioned on-demand to ensure they correctly sync up between the client product and Starling Two-Factor Authentication.**
>
> **Client products using hardware tokens: Because you need to have a hardware token assigned to a user prior to their first authentication attempt with the hardware token, you need to manually add new users to Starling Two-Factor Authentication and assign a token to them. These users must be identical to a user in the client product in order to recognize the user when they first authenticate. If they are not identical then they will be unable to authenticate until the mismatched records are corrected and the hardware token assigned to the correct record.**

1. On the **Users** page, click **Import**.
2. In the **Import Users** dialog, click **Choose file**.
3. Select a CSV file containing information on each of the users to be added. The file must have a phone number (*<+1 1234567>*, +1 is used if no country code is specified) and email (*<email@domain>*). A display name (*<First Last>*) is optional.
4. Click **Open**.
5. In the Import **Hardware Tokens** dialog, click **Next**.

6. Select the check box associated with the user or users to be imported. Any issues found with users identified in the file will be indicated by a  icon. Hover over the icon for more information as to why the user was not imported.

   CAUTION: If the phone number for a manually added user already exists but with a different name or email, then the name and email for the user will be updated. If the same phone number is used in multiple subscriptions then all subscriptions will be updated accordingly.

7. Click **Import Users**. Each successfully imported user will appear listed on the **Users** page.

   Once a user has been added, a new token will appear in their Starling 2FA app. If the user has not been provisioned in any Starling Two-Factor Authentication subscription and the General Settings tab option to send SMS is enabled, the new user will also receive instructions on installing the Starling 2FA app.

Deleting users

In cases where you have licensed users that are not using the product, users can be marked for deletion within Starling Two-Factor Authentication and given a window of 30 days before being deleted. If a user marked for deletion authenticates during those 30 days then they will be restored automatically while also pulling in any updated user data, and if the user does not authenticate after being marked for deletion then they will be deleted and no longer count towards your consumed licenses

To delete a user

1. In the table on the **Users** page, select the check box associated with each user to be deleted.
2. Click **Delete**.
3. In the confirmation dialog, click **Yes**.

   The users will be marked for deletion. Unless a user is restored or authenticates within 30 days, they will be deleted from Starling Two-Factor Authentication.

Restoring users

The following procedures explain how to manually restore users that have been marked for deletion.

To restore a user

1. In the table on the **Users** page, select the check box associated with each user to be restored.
2. Click **Restore**.
3. In the confirmation dialog, click **Yes**.

   The user will be restored to the state they were prior to being marked for deletion.

Disabling a user account

You can temporarily stop a user from being able to access protected applications by disabling the account from the **Users** page.

To disable a user account

1. In the table on the **Users** page, select the check box associated with each user account to be disabled.
2. Click **Disable**.
3. In the confirmation dialog, click **Yes**.

   The user will be unable to access protected applications until they have been re-enabled. For more information, see Enabling a user account.

Enabling a user account

User accounts that were previously disabled will need to be re-enabled in order to allow them to access protected applications.

To enable a user account

1. In the table on the **Users** page, select the check box associated with each user to be re-enabled.
2. Click **Enable**.
3. In the confirmation dialog, click **Yes**.

   The user account will be restored to the state it was in prior to being disabled.

Generating a temporary response code for a user

A temporary response code can be generated and then sent by an administrator or helpdesk collaborator to a user if they are unable to authenticate using their configured

device. This code should only be sent after the identity of the user has been confirmed.

To generate a temporary response code for a user

1. On the **Users** page, locate the user that requires a temporary response code.
2. In the associated action column, click **Temporary response**.
3. A **Temporary Response** dialog will appear. Send the numerical code to the user so that they can use the code to gain access to their application. The code will only be valid for 15 minutes and you will be unable to return to this dialog once it is closed.
4. Once the user has gained access, click **OK** to close the dialog.

> NOTE: Clicking **Temporary response** for the same user before they have authenticated with the previous code will instantly expire the previously generated code and generate a new code. The user will need to use the most recently generated code within 15 minutes to authenticate.

5

Approvals

Introduction to Approvals

The **Approvals** page is used by Administrators and Primary Administrators to approve changes to the collaborators for the service and to approve newly generated subscription keys. Only those actions taken by an Administrator require approval; Primary Administrators do not require approval from a second administrator.

Approvals page

The **Approvals** page is displayed when **Approvals** is clicked in the navigation bar. The **Approvals** page is used by Administrators and Primary Administrators to approve actions taken by an Administrator that require approval; Primary Administrators do not require approval from a second administrator.

The following button appears above the Approvals table:

Refresh

Clicking this button refreshes the list of approvals.

This field is used to search for an approval based on the creator or collaborator name associated with it. To use the search functionality, start typing in the field. The table will automatically update to display results that match.

The following information and options appear on the Approvals table:

Request to Approve

This is the action that prompted the approval. For example, if an Administrator is adding a new collaborator then this column will show **Add collaborator** and if an

Administrator generates a new subscription key then this column will show **Create New Key**.

Collaborator Name

This is the name of the collaborator that is impacted by the approval request. This column will be empty if the request is related to a subscription key.

Collaborator Role

This is the role of the collaborator for which an approval has been requested. This column will be empty if the request is related to a subscription key.

Created By

This is the name of the collaborator that requested the approval.

Status

This is the state of the approval. The following states may appear:

- **Pending**: This means the approval has been sent but has not been responded to.
- **Confirmed**: This means the approval has been confirmed by an administrator.
- **Canceled**: This means the approval was rejected by an administrator.
- **Failed**: This status appears for subscription key requests that occur while the 24 hour switching period is still in effect for an earlier key request. It indicates the new key request failed and that you must wait until the original 24 hour period has expired before requesting a new subscription key. This status may also appear for a collaborator request and means the approval failed to go through.

Creation Date

This is the date and time the approval was requested.

The ⋮ button appearing for an approval contains the following options depending on the item and your permissions for that item.

NOTE: New Primary Administrators and Administrators are unable to manage pending requests that were created before they were added as a collaborator.

- **Confirm Approval**: Click this button to approve the request. For more information, see Confirm a request.
- **Cancel Approval**: Click this button to cancel the request. For more information, see Canceling an approval request.
- **Resend Approval**: Click this button to resend the request. For more information, see Resending an approval request.

- **Retry Approval**: Click this button to retry sending the request. For more information, see Retrying a failed approval request.
- **Delete Approval**: Click this button to remove a completed request from the **Approvals** page. For more information, see Deleting an approval request.

Managing approvals

The following sections provide information on managing approvals for the Starling Two-Factor Authentication service.

NOTE: New Primary Administrators and Administrators are unable to manage pending requests that were created before they were added as a collaborator.

- Confirm a request
- Resending an approval request
- Canceling an approval request
- Retrying a failed approval request
- Deleting an approval request

Confirm a request

Once a request is determined to be acceptable, a Primary Administrator or Administrator needs to confirm it on the **Approvals** page.

To confirm a request

1. On the **Approvals** page, click the ⋮ button associated with the request that is being confirmed.
2. Click **Confirm Approval**.
3. In the confirmation dialog, click **Yes**.

   The request will be confirmed and the requested changes made.

Resending an approval request

If a request for approval needs to be resent, an Administrator can select to resend the request from the **Approvals** page.

To resend a request

1. On the **Approvals** page, click the ⋮ button associated with the request that is being resent.
2. Click **Resend Approval**.
3. In the confirmation dialog, click **Yes**.

   The request for approval will be resent.

Retrying a failed approval request

If a request for approval fails to go through, an Administrator can select to retry the request from the **Approvals** page.

To retry a request

1. On the **Approvals** page, click the ⋮ button associated with the request that is being resent.
2. Click **Retry Approval**.
3. In the confirmation dialog, click **Yes**.

   Starling Two-Factor Authentication will try to send out a new approval request for the action. If the request fails again, delete the failing request and retry the action that originally required the approval.

Canceling an approval request

Once a request is determined to be unacceptable, a Primary Administrator or Administrator needs to cancel it on the **Approvals** page.

To cancel a request

1. On the **Approvals** page, click the ⋮ button associated with the request that is being canceled.
2. Click **Cancel Approval**.
3. In the confirmation dialog, click **Yes**.

   The request will be canceled and the requested changes will not be made.

Deleting an approval request

Once a request has been approved or canceled, a Primary Administrator or Administrator can remove the request from the **Approvals** page so that it is no longer listed.

To delete an approval request

IMPORTANT: Deleting an approval request only removes a previously responded to request from the listed items. It does not impact the decision that was already made for the request (confirm or cancel).

1. On the **Approvals** page, click the ⋮ button associated with the previously responded to request that is being deleted.
2. Click **Delete Approval**.
3. In the confirmation dialog, click **Yes**.

   The request will no longer appear listed on the **Approvals** page.

5

Integrations

Introduction to Integrations

The **Integrations** page of Starling Two-Factor Authentication is used for integrating Azure Active Directory with your Starling Two-Factor Authentication service. This allows for Azure Active Directory to take advantage of Starling Two-Factor Authentication's advanced two-factor authentication capabilities to further protect your resources.

Integrations page

The **Integrations** page is displayed when **Integrations** is clicked in the navigation bar. The **Integrations** page is used by Administrators and Primary Administrators to integrate Azure Active Directory with your Starling Two-Factor Authentication service.

The following options appear on this page:

My integrations

This section is blank until an Azure Active Directory integration has been configured. Once an integration is completed, the following options will appear after clicking the  button on an Azure Active Directory tile:

- **View JSON**: Selecting this option opens a dialog displaying the JSON data used when adding the integration. You can copy the JSON data from the dialog using the  button. Click **Close** to close the dialog and return to the **Integrations** page.
- **Disconnect**: Selecting this option opens a dialog explaining how to disconnect Azure Active Directory and Starling Two-Factor Authentication. For more information, see Disconnecting Azure Active Directory.

Available integrations

Click the **Azure AD** tile in this section to integrate Azure Active Directory with Starling Two-Factor Authentication. For more information, see Integrating Azure Active Directory.

Integrating Azure Active Directory

Follow these instructions in order to integrate Azure Active Directory with Starling Two-Factor Authentication.

To integrate Azure Active Directory with Starling Two-Factor Authentication

IMPORTANT: A subscription to a premium Azure Active Directory edition is required.

IMPORTANT: You must use an internal Privileged Role Administrator or internal Global Administrator Azure Active Directory account.

1. On the **Integrations** page, click the **Azure AD** tile in the **Available integrations** section.
2. In the **Configure Azure AD integration** dialog, click **Grant permission**.
3. Sign in to your Azure Active Directory account. Once you have completed signing in you will be redirected back to Starling Two-Factor Authentication.
4. Copy the JSON data from the **Configure Azure AD integration** dialog using the  button.
5. In a separate tab or window, open and log in to the Azure portal with the account used in step 3.
6. In the Azure portal, click **All services**.
7. Click **Identity**.
8. Click **Conditional Access**.
9. On the **Conditional Access – Policies** page, click **Custom controls**.
10. On the **Custom controls** page, click the **New custom control** button.
11. Paste the JSON data copied from Starling Two-Factor Authentication in the textbox.
12. Click the **Create** button.
13. Once you have completed the Azure Active Directory changes, return to Starling Two-Factor Authentication and click **Continue** in the **Configure Azure AD integration** dialog.
14. In the Azure portal, click **All services**.
15. Click **Identity**.
16. Click **Conditional Access**.

17. On the **Conditional Access – Policies** page, click the **New policy** button.
18. In the **Name** field, enter a name for the policy.
19. Click **Users and groups**.
20. On the **Users and groups** page, assign any necessary users and groups to the policy.
21. Click the **Done** button.
22. Click **Cloud apps or actions**.
23. On the **Cloud apps or actions** page, assign any necessary cloud applications to the policy.
24. Click the **Done** button.
25. Click **Grant**.
26. On the **Grant** page, select **Grant access**.
27. Select the check box for the 2FA custom control that was created using the JSON data.
28. Click the **Select** button.
29. Enable the policy by switching the toggle to **On**.
30. Click the **Create** button.
31. Return to Starling Two-Factor Authentication and click **Complete** in the **Configure Azure AD integration** dialog. The integration will be listed under the **My integrations** section of Starling Two-Factor Authentication, and the cloud applications assigned to the policy will begin prompting for two-factor authentication.

Disconnecting Azure Active Directory

Follow these instructions in order to disconnect Azure Active Directory from Starling Two-Factor Authentication.

To disconnect Azure Active Directory from Starling Two-Factor Authentication

IMPORTANT: A subscription to a premium Azure Active Directory edition is required.

IMPORTANT: You must use an internal Privileged Role Administrator or internal Global Administrator Azure Active Directory account associated with the instance being disconnected.

1. On the **Integrations** page, click the button associated with the **Azure AD** tile being disconnected.
2. Select **Disconnect**.
3. In a separate tab or window, open the Azure portal and sign in to your account.
4. In Azure Active Directory, click **All services**.

5. Click **Identity**.
6. Click **Conditional Access**.
7. On the **Conditional Access – Policies** page, delete the Starling Two-Factor Authentication policy that is being disconnected.
8. On the **Conditional Access – Policies** page, click **Custom controls**.
9. On the **Custom controls** page, delete the custom control associated with Starling Two-Factor Authentication.
10. Return to Starling Two-Factor Authentication and click **Disconnect**. The integration will no longer appear listed in the **My integrations** section.

Hardware Tokens

Introduction to Hardware Tokens

The **Hardware Tokens** page of Starling Two-Factor Authentication is used for adding and managing the hardware tokens (for example, YubiKey 5 NFC) that are used for authentication by your configured users.

The following hardware token file types are currently usable with Starling Two-Factor Authentication:

IMPORTANT: For information on specific file requirements, see Additional hardware and software requirements.

- CSV
- PSKC
- DPX

Hardware Tokens page

The **Hardware Tokens** page is displayed when **Hardware Tokens** is clicked in the navigation bar. The **Hardware Tokens** page is used to add and manage hardware tokens.

The following buttons appear at the top of the page:

Import

Clicking this button opens the **Import Hardware Tokens** dialog where you can configure a new token for use with Starling Two-Factor Authentication. For more information, see Importing hardware tokens.

Delete

Clicking this button opens the **Delete Token** dialog where you can remove the token from Starling Two-Factor Authentication. For more information, see Deleting

hardware tokens.

Refresh

Clicking this button refreshes the Hardware Tokens table.

This field is used to search for a token based on the manufacturer, serial number, or assigned user. To use the search functionality, start typing in the field. The table will automatically update to display results that match.

The following information and option appear in the table on this page:

Manufacturer

If included in the imported file, this column displays the name of the token manufacturer.

Serial Number

The serial number for the token.

Type

This column displays the type of token.

Response Length

This is the response length for the token.

Assigned To

Clicking the link in this column displays the email, name, and mobile number of the user (or users) the token is currently assigned to within Starling Two-Factor Authentication. This column will display **None** if the token is not currently assigned to a user.

The following configuration options may appear on this drop-down depending on the current state of the token and collaborator type:

- **Assign**: Select this option to assign the token to a user. For more information, see Assigning a hardware token to a user.
- **Unassign**: Select this option to unassign a token from a user. For more information, see Unassigning a hardware token from a user.

- **Reset**: Select this option to reset the token. For more information, see Resetting a hardware token.
- **Test**: Select this option to test the token. For more information, see Testing a hardware token assigned to a user.

Managing hardware tokens

The following sections provide information on managing hardware tokens within the Starling Two-Factor Authentication service.

- Importing hardware tokens
- Assigning a hardware token to a user
- Testing a hardware token assigned to a user
- Resetting a hardware token
- Unassigning a hardware token from a user
- Deleting hardware tokens

Importing hardware tokens

To begin using hardware tokens for authentication with Starling Two-Factor Authentication they must first be imported.

To import hardware tokens

IMPORTANT: Before importing hardware tokens, review the Additional hardware and software requirements.

IMPORTANT: Before using hardware tokens with Starling Two-Factor Authentication, ensure you have followed all installation and configuration requirements from the token manufacturer to ensure tokens are ready for use.

1. On the **Hardware Tokens** page, click **Import**.
2. In the Import **Hardware Tokens** dialog, click **Choose file**.
3. Select the CSV or PSKC file containing the token information. This file should have been generated according to the instructions provided by your token manufacturer and match the file requirements (Additional hardware and software requirements).
4. (Optional) If using an encrypted PSKC file or DPX file you need to enter your file key.
5. Click **Open**.
6. In the Import **Hardware Tokens** dialog, click **Next**.

7. Select the check box associated with the token or tokens to be imported. Any issues found with tokens identified in the file will be indicated by a  icon. Hover over the icon for more information as to why the token was not imported.
8. Click **Import tokens**. Each successfully imported token will appear listed on the **Hardware Tokens** page and can be assigned to a user. For more information, see Assigning a hardware token to a user.

Assigning a hardware token to a user

After being imported (for more information, see Importing hardware tokens), administrators can assign a token to a user through either the **Hardware Tokens** page or the **Users** page.

IMPORTANT: Before using hardware tokens with Starling Two-Factor Authentication, ensure you have followed all installation and configuration requirements from the token manufacturer to ensure tokens are ready for use.

To assign a hardware token to a user from the Hardware Tokens page

1. On the **Hardware Tokens** page, locate the token to be assigned and click the button.
2. Select **Assign**.
3. In the dialog, locate the user to be assigned the token.
4. Click **Assign token**.

   The token will now appear listed as assigned to the user.

To assign a hardware token to a user from the Users page

1. On the **Users** page, locate the user that will be assigned a token and click the link in the **Hardware Tokens** column.
2. You will be redirected to the **User Hardware Tokens** page which is specific to the selected user.
3. Click **Assign**.
4. In the dialog, use the search field to locate the token by name or serial number. Once you have located the correct token, click **Assign token**.

   The token will now appear listed as assigned to the user.

Testing a hardware token assigned to a user

To ensure the token is working correctly with Starling Two-Factor Authentication, administrators and Helpdesk can test the response generated by the token.

IMPORTANT: Before using hardware tokens with Starling Two-Factor Authentication, ensure you have followed all installation and configuration requirements from the token manufacturer to ensure tokens are ready for use.

To test a hardware token from the Hardware Tokens page

1. On the **Hardware Tokens** page, locate the token to be tested and click the ⋮ button.
2. Select **Test**.
3. The user whose token is being tested needs to generate a response with their token. In the **Test Token** dialog, enter the response the user received.
4. Click **Test**.

   NOTE: If the test fails, you can try resetting the token counter (For more information, see Resetting a hardware token).

To test a hardware token from the Users page

1. On the **Users** page, locate the user with the token to be tested and click the link in the **Hardware Tokens** column.
2. You will be redirected to the **User Hardware Tokens** page specific to the selected user. Locate the token to be tested and click the ⋮ button.
3. Select **Test**.
4. The user whose token is being tested needs to generate a response with their token. In the **Test Token** dialog, enter the response the user received.
5. Click **Test**.

   NOTE: If the test fails, you can try resetting the token counter (For more information, see Resetting a hardware token).

Resetting a hardware token

After being imported (for more information, see Importing hardware tokens), if a user is reporting issues with their token being unable to authenticate, you can reset a token if there is an issue with the counter being out of sync.

IMPORTANT: Before using hardware tokens with Starling Two-Factor Authentication, ensure you have followed all installation and configuration requirements from the token manufacturer to ensure tokens are ready for use.

To reset a hardware token from the Hardware Tokens page

1. On the **Hardware Tokens** page, locate the token to be reset and click the ⋮ button.

2. Select **Reset**.
3. In the **Confirm** dialog, click **Yes**. Once a token has been reset, you can test the token to confirm it is working with Starling Two-Factor Authentication (for more information, see Testing a hardware token assigned to a user).

   NOTE: If the token is still having issues you may need to try reprogramming the token and then reimporting the new token file.

To reset a hardware token from the Users page

1. On the **Users** page, locate the user with the token to be reset and click the link in the **Hardware Tokens** column.
2. You will be redirected to the **User Hardware Tokens** page specific to the selected user. Locate the token to be reset and click the ⋮ button.
3. Select **Reset**.
4. In the **Confirm** dialog, click **Yes**. Once a token has been reset, you can test the token to confirm it is working with Starling Two-Factor Authentication (for more information, see Testing a hardware token assigned to a user).

   NOTE: If the token is still having issues you may need to try reprogramming the token and then reimporting the new token file.

Unassigning a hardware token from a user

After being assigned (for more information, see Assigning a hardware token to a user), Primary Administrators can unassign a token from a user through either the **Hardware Tokens** page or the **Users** page. Once a user has been unassigned, they will no longer be able to use the token for authenticating.

To unassign a hardware token from a user from the Hardware Tokens page

1. On the **Hardware Tokens** page, locate the token to be unassigned and click the ⋮ button.
2. Select **Unassign**.
3. In the **Assigned To** dialog, select the check box associated with the user (or users) the token will be unassigned from.
4. Click **Unassign user**.

   The user will no longer be assigned to the token.

To unassign a hardware token from a user from the Users page

1. On the **Users** page, locate the user that will be unassigned from a token and click the

link in the **Hardware Tokens** column.

2. You will be redirected to the **User Hardware Tokens** page specific to the selected user.
3. Select the check box associated with the token (or tokens) to be unassigned.
4. Click **Unassign**.
5. In the **Unassign token** dialog, click **Yes**.

   The token will no longer be assigned to the user.

Deleting hardware tokens

If a token is no longer needed, it can be deleted from Starling Two-Factor Authentication and thus no longer available for authenticating to protected applications.

To delete a hardware token

NOTE: Any users still assigned to a token being deleted will automatically be unassigned from that token.

1. In the table on the **Hardware Tokens** page, select the check box associated with the token (or tokens) to be deleted.
2. Click **Delete**.
3. In the confirmation dialog, click **Yes**.

   The token will be deleted from Starling Two-Factor Authentication.

Settings

Introduction to Settings

The **Settings** page of Starling Two-Factor Authentication is used for configuring and customizing your Starling Two-Factor Authentication application. All changes made on these pages will take effect immediately upon saving. The page consists of two tabs: General Settings tab and Token UI Settings tab

General Settings tab

The **General Settings** tab is displayed by default when **Settings** is clicked in the navigation bar.

The following setting appears in the **Messages** section:

SMS Installation Instructions

Enabled by default, this toggle allows you to select whether to send application installation instructions via SMS to newly added Starling Two-Factor Authentication users. If you have multiple Starling organizations, users will see each token listed separately within their application and not receive a new email with installation instructions.

The following settings appear in the **User Authentication Methods** section:

SMS

Enabled by default, this toggle allows you to select whether SMS will be an available two-factor authentication option for users logging in to a protected application. When enabled, users will be able to receive the requested token response via text message.

Phone Calls

Enabled by default, this toggle allows you to select whether automated phone calls will be an available two-factor authentication option for users logging in to a protected application. When enabled, users will be able to receive the requested token response via an automated phone call.

Interactive Phone Calls

Enabled by default, this toggle allows you to select whether interactive phone calls will be an available two-factor authentication option for users logging in to a protected application. When enabled, users will be able to receive instructions for generating a token response via a phone call.

OTP Length

This field allows you to select the character length (6-8) for one-time passwords. By default this is set to 7 characters.

Once you have completed configuring your Starling Two-Factor Authentication token, click **Save Settings** to save all settings (changes will take effect immediately) or **Reset** to return the token to the last saved settings.

Token UI Settings tab

The **Token UI Settings** tab can be accessed on the **Settings** page. The **Token UI Settings** tab is used for customizing your Starling Two-Factor Authentication token. The current token design is displayed on the right and automatically refreshes as changes are made to the settings.

Token Name

This field is used for setting the token name (by default, **Starling 2FA**). The name must be between 1-30 characters. If you have multiple Starling organizations then it is recommended that you assign a unique name for each to avoid confusion since a user will see each token listed separately within their application.

The following settings appear in the **Token Logo** section:

Main logo

Click the **Upload** button to locate and select the PNG file to use as the main logo. The image in this file must be no more than 588 x 214 pixels and the file size must be under 128kb.

Menu logo

Click the **Upload** button to locate and select the PNG file to use as the menu logo. The image in this file must be no more than 81 x 81 pixels and the file size must be under 64kb.

The following settings appear in the **Token Colors** section:

Label Color

This field is used to select the color of the token label. To edit the label color, click the box on the right side of the field to open a color selector dialog or type the hex color code directly into the field.

Code Color

This field is used to select the color of the token code. To edit the code color, click the box on the right side of the field to open a color selector dialog or type the hex color code directly into the field.

Background Color

This field is used to select the background color of the token. To edit the background color, click the box on the right side of the field to open a color selector dialog or type the hex color code directly into the field.

Timer Color

This field is used to select the color of the token timer. To edit the timer color, click the box on the right side of the field to open a color selector dialog or type the hex color code directly into the field.

Once you have completed customizing your Starling Two-Factor Authentication token, click **Save Settings** to save all settings (changes will take effect immediately) or **Reset** to return the token to the last saved settings.

8

Downloads

Introduction to Downloads

The **Downloads** page is used to access downloads for the Starling 2FA application and on-premises components.

The following downloads are available:

Starling 2FA app

The Starling Two-Factor Authentication application is what is used to generate one-time passwords and receives push notification requests. When installing the application (regardless of platform), the phone number you first use to register is also your unique ID. This means that if you have multiple devices you want to register under the same account, you can install the application on a separate device by instead using the unique ID (the primary device phone number) to keep both devices under the same account.

The application is available at the following links depending on your desired platform:

- **Android**: https://play.google.com/store/apps/details?id=com.starling.twofactor
- **iOS**: https://itunes.apple.com/app/starling-2fa/id1205700916

IMPORTANT: The options for **Windows** and **Macintosh** will begin the download process automatically when the associated **Download** button is clicked.

- **Windows** (64-bit)
- **Macintosh** (64-bit)

You can also use the **Get the app** link (https://2fa.cloud.oneidentity.com/install) to automatically detect which version to install.

On-prem components

The Starling Two-Factor Authentication on-premises components available with a paid subscription are listed in this section. Use the **Download** button associated with

each listed on-premises component to begin the installation process.

The following on-premises components are available:

NOTE: For more information, see the documentation specific to each component (https://support.oneidentity.com/starling-two-factor-authentication/hosted/technical-documents).

- **Starling 2FA RADIUS agent**
- **Starling 2FA AD FS Adaptor**
- **Starling 2FA Desktop Login**
- **Starling 2FA HTTP module**

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 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 at www.YouTube.com/OneIdentity
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product