Okta User Guide

1. Introduction

With the help of a technical identity, the software Okta enables employees as well as external persons who require a Ringier account to log in securely to the connected IT services. As a result, all Ringier identities are protected and monitored according to state-of-the-art security standards. This Okta User Guide explains all important processes and functionalities in and around Okta.
Furthermore, the following aids are available to the users:

Specifically for the roll-out in June 2022:

- Okta Quick Guide for Users (with a Windows device from RBS IT)
- Okta User Quick Guide (with a Mac device from RBS IT)
- Okta User Quick Guide (without a device from RBS IT/macOS 10.14)
- General Okta FAQ
- Instructions Okta Verify App (iOS)
- Instructions Okta Verify App (Android)

For new IT accounts:

- Okta Quick Guide for Users (with a Windows device from RBS IT)
- Okta User Quick Guide (with a Mac device from RBS IT)
- Okta User Quick Guide (without a device from RBS IT/macOS 10.14)

Answers to frequently asked questions (FAQ) can be found here. Okta also provides further comprehensive instructions in the Okta Help Center.

2. About Okta

Among Okta's advantages:

- Secure credentials that allow access to multiple applications, saving valuable time on repeated accesses
- Additional security features and functions such as various multi factor authentication methods
- Secure mobile device verification
- Simple, transparent biometric authentications

Okta also enables easy, fast, and secure logins to connected IT services through its convenient and user-friendly dashboard.

You can use the Okta Dashboard (see chapter 6) anywhere, anytime:

- reset your password directly on the login page..
- change your password once you are logged in.
- unlock your account.
- change your multi factor authentication methods.

3. Access

Okta can be accessed via the following link: https://ringier.okta.com/

The registration on the Okta platform is done by means of:

- **Username:** Your business email address
- **Password:** Your single sign-on password

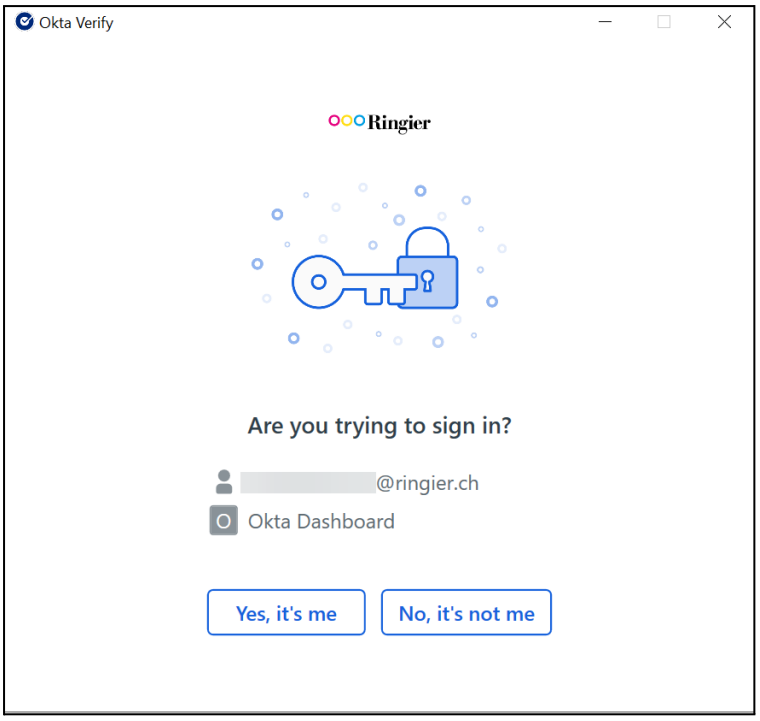
If the user name is not known, the Ringier IT Helpdesk (helpdesk@ringier.ch or +41 62 746 33 33) should be contacted. In case of a forgotten password, the «Forgot password?» link at the bottom of the Okta login page can be used to generate a new password. If the link is not available, the Ringier IT Helpdesk (helpdesk@ringier.ch or +41 62 746 33 33) will be happy to help.

4. Initial registration

Using three to six simple steps, you initially log in to the Okta platform using the quick guides linked under 1. Introduction and set up the security methods. To open the Okta platform, click the following link in your default browser (ideally Chrome): https://ringier.okta.com/

5. Okta Verify

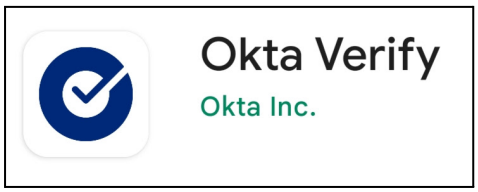
Okta Verify is an application that is available for the client, but also for mobile devices. Once set up, the app always launches when you select «Sign in with Okta FastPass» or «Use Okta FastPass». You'll then be prompted to authenticate each time:



5.1. Okta Verify on client (notebook, desktop, etc.)

Okta Verify is pre-installed on devices from RBS IT. Mac devices with the Mojave OS (10.14) version are an exception: Okta Verify cannot be installed on these devices.

5.2. Okta Verify as an app on the smartphone (mobile device)



Android: https://play.google.com/store/apps/details?id=com.okta.android.auth&gl=US
iOS: https://apps.apple.com/us/app/okta-verify/id490179405

Initially, install the «Okta Verify» app from Okta Inc. on your smartphone. You can find it in the respective app store. After installation, the app will guide you step by step through the necessary settings. Please note:

1. The account type to be selected in the app is «Organization».
2. «Use biometrics» is recommended by RBS IT.

Detailed instructions on how to set up the app can be found here:

- iOS: https://help.okta.com/eu/en-us/Content/Topics/end-user/ov-setup-ios.htm
- Android: https://help.okta.com/eu/en-us/Content/Topics/end-user/ov-setup-android.htm

The app «Okta Verify» from Okta Inc. on your smartphone allows you to authenticate using Okta FastPass and also to generate an authentication code. This is required, for example, when logging in to Amazon WorkSpaces (AWS).

Further, you can access the Okta Dashboard directly from the app. A tutorial can be found here:

- iOs: https://help.okta.com/eu/en-us/Content/Topics/end-user/ov-launch-dashboard-ios.htm
- Android: https://help.okta.com/eu/en-us/Content/Topics/end-user/ov-launch-dashboard-android.htm

6. Okta Dashboard

The Okta Dashboard is a platform that provides secure access to all connected services. It can be accessed via the following link: https://ringier.okta.com/

The dashboard can also be accessed on mobile devices via the Okta Verify application (see chapter 5). Access to all connected services is based on single sign-on (SSO) technology.

The dashboard can be used to manage the Okta account and organize or request services. The following activities can be performed on the dashboard:

6.1. Security methods

Multi factor authentication (MFA) is ensured through the various security methods. The following methods can be set up with Okta:

- Okta Verify: See chapter 5
- Security Key or Biometric (Security Key or Biometric Authenticator like Windows Hello, Touch ID, Face ID etc.): Okta describes step by step how to set it up.
- Google Authenticator: Install the app «Google Authenticator» on your smartphone and set it up.
- Phone (text message or call): Is subject to a charge and is only set up in justified cases with the consent of the cost center manager(s). Please contact the IT Helpdesk.
- Security Question: Choose a question whose answer you can remember well.

All security methods can be set up or changed as follows:

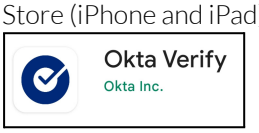
1. In the Dashboard, go to Settings (click on the arrow in the top right-hand corner).
2. Scroll to the section "Security method".
3. The various security methods are listed there and can be configured or removed, meaning deleted.

Important settings and specific changes are listed in detail below.

6.1.1. Okta Verify app on the smartphone

Setting up the Okta Verify app on your smartphone is strongly recommended by RBS IT:

1. Go to «Settings in the Dashboard.
2. Scroll to the «Security Methods» section.
3. Under «Okta Verify» you can see whether Okat Verify is already set up and on which smartphone.
4. Click on «Set up another» to set up the Okta Verify app on your smartphone.
5. Follow the steps described in the browser. The ***Okta Verify*** app has the following icon in the App Store (iPhone and iPad) or from Google Play (Android devices):



6. Follow the steps described in the app:
   - Select ***Organisation*** as the account type.
   - Scan the ***QR code*** (generated when selecting the Okta Verify method in the browser).
7. «Activate biometric data» is recommended by Ringier IT.
8. This completes the setup of the app.

6.1.2. Update security question

You can update your security question as follows:

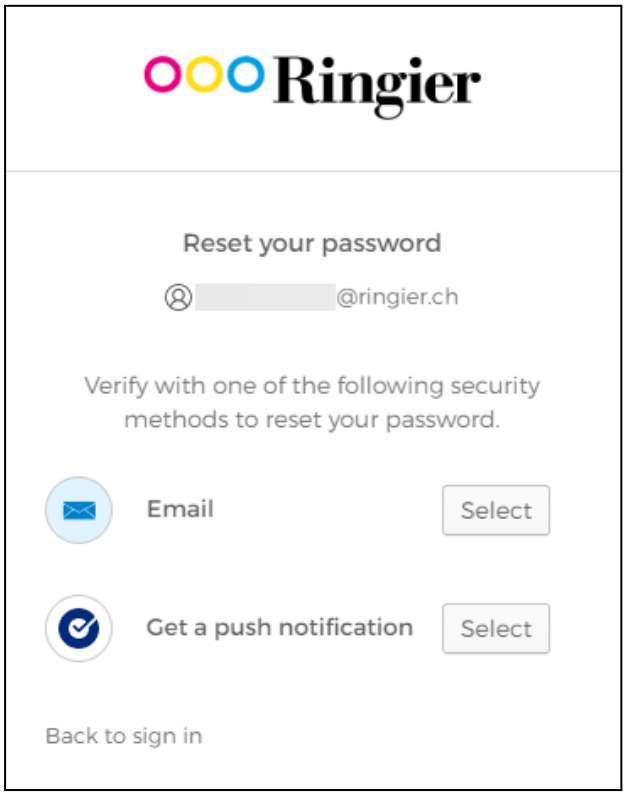
1. Go to Settings in the dashboard.
2. Scroll to the section «Security Methods».
3. Click the «Remove» button next to «Security Question».
4. Confirm that you really want to remove the security question.
5. Log in to Okta again.
6. At «Security Question» click the «Set up» button and set up your security question again.

6.1.3. Password

6.1.3.1. Reset password

If the password is forgotten, it can be reset independently:

1. Open in browser: https://ringier.okta.com/
2. Enter your username and click «Next».
3. Select the security method «Password».
4. Choose the method how you want to reset your password:



5. Follow the instructions in the smartphone or browser.

6.1.3.2. Change password

The password can be changed via «Settings» (click on *User Name* in the upper right corner) > «Change Password».

6.1.3.3. Password policy

Okta refuses to use weak and known passwords. The exact password requirements are listed in the Okta Dashboard in the section «Change Password».
A password is valid for a maximum of 180 days for a standard account and 90 days for a privileged account. 10 days before expiration, Okta alerts that the password needs to be changed soon.

6.2. Unlock account

Okta notifies the user of a locked account via email. You can use Okta to unlock your account on your own (this requires your security question):

1. Open in the browser: https://ringier.okta.com/
2. Click «Unlock account?» at the bottom of the page.
3. Enter your username and choose a security method by clicking «Select» at the desired method.
4. Follow the further instructions.

6.3. Add section

Up to five sections can be created in the Okta Dashboard:

1. Open in the browser: https://ringier.okta.com/
2. Click «Add section (+)» in the left sidebar.
3. Enter a name for the new section. For example: Personal applications.

6.4. Apps

6.4.1. Change the order of apps

The order of the apps can be changed as desired:

1. Open in the browser: https://ringier.okta.com/
2. Click and hold the desired app icon.
3. Drag the app to the desired location and release. (The app can also be moved to another section).

Note: Apps can be moved from any section except the «Recently Used».

6.4.2. Find apps

Apps can also be accessed directly from the «Search your apps» box at the top of the dashboard.

6.4.3. Find recently used apps

The section «Recently Used» is only displayed if more than 12 apps are listed in the dashboard. For RBS IT, this number of apps is not expected to be reached until 2023. This section displays up to 6 apps that you have recently accessed.
The section «Recently Used» can also be removed if necessary:

1. Go to Settings in the dashboard.
2. Scroll down to the section «Recently Used» and click on «Edit».
3. Uncheck the «Enable recently used apps» checkbox and click «Save».

6.5. Display language

The display language can be changed as desired:

1. Go to Settings in the dashboard.
2. Scroll to the section «Display Language».
3. Click on «Edit».
4. Select the desired language.
5. Click on «Save».

7. Special cases

7.1. Amazon WorkSpaces

Amazon WorkSpaces (AWS) requires the Time-based One-time Password algorithm (TOTP) as a security method. This is a method for generating time-limited codes. Such an authentication code can be generated with the app «Okta Verify» - see chapter 5.2.. Alternatively, the app «Google Authenticator» can be used - see chapter 6.1..

7.2. Shared Mailboxes

Description follows.

7.3. Accounts without email addresses

The Ringier login ID is to be used under user name.

7.4. Technical accounts

If a service does not support MFA, then an exception can be requested via the IT Helpdesk with justification.