Р·СЕРВИС

# Двухфакторная аутентификация

для защиты учетных записей пользователей в Р-Сервис

## 1 Общая информация

Р-Сервис поддерживает двухфакторную аутентификацию (2FA) для защиты учетных записей пользователей от компрометации паролей и несанкционированного доступа.

Двухфакторная аутентификация (2FA) является частью встроенного контура безопасности платформы и может использоваться:

- для локальной аутентификации в Р-Сервис;
- совместно с Единым входом (Single Sign-On (SSO));
- как обязательная политика безопасности организации.

После включения двухфакторной аутентификации (2FA) пользователь подтверждает вход двумя независимыми факторами:

- логин и пароль;
- одноразовый код подтверждения.

## 2 Поддерживаемые методы двухфакторной аутентификации (2FA)

Основной метод двухфакторной аутентификации в Р-Сервис — использование **приложений-аутентификаторов с одноразовыми TOTP[1]-кодами**.

Поддерживаются стандартные RFC6238[2]-совместимые приложения, включая:

- Google Authenticator;
- Microsoft Authenticator;
- Authy;
- Яндекс-Ключ;
- Bitwarden;
- другие TOTP-совместимые приложения.

## 3 Процесс включения двухфакторной аутентификации (2FA)

Для активации двухфакторной аутентификации пользователь:

1. Инициирует включение двухфакторной аутентификации (2FA) в настройках безопасности;
2. Получает ссылку подтверждения;
3. Подключает приложение-аутентификатор;
4. Подтверждает настройку одноразовым кодом;
5. Получает ключи восстановления (recovery-коды) для аварийного восстановления доступа.

После успешной активации пользователь получает уведомление о включении двухфакторной аутентификации (2FA).

## 4 Ключи восстановления (recovery-коды)

При включении двухфакторной аутентификации (2FA) система автоматически генерирует набор ключей восстановления (recovery-кодов).

### 4.1 Назначение ключей восстановления (recovery-кодов)

Данные коды используются для восстановления доступа в случаях:

---

[1] TOTP – алгоритм генерации одноразовых паролей.

[2] RFC6238 – программы, реализующие алгоритм TOTP, описанный в соответствующем стандарте.

- потери телефона;
- удаления приложения-аутентификатора;
- недоступности второго фактора;
- аварийного доступа к учетной записи.

### 4.2 Особенности работы

Каждый ключ восстановления (recovery-код) является одноразовым;

- при повторной настройке двухфакторной аутентификации (2FA) старые ключи восстановления (recovery-коды) автоматически становятся недействительными;
- служба поддержки не может восстановить доступ пользователя без ключей восстановления (recovery-кодов).

Р-Сервис рекомендует хранить данные коды в защищенном месте.

### 4.3 Уведомления безопасности

Р-Сервис автоматически уведомляет пользователей о событиях безопасности, связанных с двухфакторной аутентификацией.

Поддерживаются уведомления:

- начало активации двухфакторной аутентификации (2FA);
- успешное включение двухфакторной аутентификации (2FA);
- отключение двухфакторной аутентификации (2FA);
- использование ключа восстановления (recovery-кода) для входа.

Уведомления содержат информацию о событии и помогают оперативно выявлять подозрительную активность.

## 5 Обязательное использование двухфакторной аутентификации (2FA)

Р-Сервис поддерживает принудительное использование двухфакторной аутентификации на уровне аккаунта (пространства).

### 5.1 Политика «Требовать двухфакторную аутентификацию»

При включении политики:

- все пользователи аккаунта (пространства) обязаны использовать двухфакторную аутентификацию (2FA);
- доступ без второго фактора блокируется;
- требование распространяется на всех зарегистрированных пользователей аккаунта (пространства).

Политика может быть активирована только после того, как владелец пространства сам включил двухфакторную аутентификацию (2FA) для своего пространства.

## 6 Интеграция с Единым входом (Single Sign-On (SSO))

Р-Сервис поддерживает интеграцию с корпоративными SSO/SAML[3]-провайдерами.

[3] SAML – открытый стандарт обмена данными аутентификации.

### 6.1 Сценарий 1 – локальная двухфакторная аутентификация (2FA) внутри Р-Сервис.

Пользователь:

1. Проходит аутентификацию через Единый вход (SSO);

2. Дополнительно вводит код двухфакторной аутентификации (2FA) Р-Сервис.

Сценарий используется при необходимости дополнительного уровня защиты внутри платформы.

### 6.2 Сценарий 2 – многофакторная аутентификация (MFA) на стороне внешнего провайдера идентификации.

Пользователь проходит многофакторную аутентификацию (MFA) внутри корпоративного провайдера идентификации:

- Microsoft Entra ID (Azure AD);
- Okta;
- Keycloak;
- ADFS;
- других SAML-провайдеров.

В этом случае Р-Сервис может не запрашивать дополнительный код двухфакторной аутентификации (2FA).

Такой подход соответствует enterprise[4]-практике централизованного управления идентификацией и безопасностью.

## 7 Безопасность и контроль доступа

Механизм двухфакторной аутентификации (2FA) встроен в общий процесс аутентификации платформы и используется совместно с:

- политиками паролей;
- Единым входом (SSO);
- аудитом событий безопасности;
- контролем активных сессий;
- настройками безопасности аккаунта (пространства).

Настройки безопасности и политики двухфакторной аутентификации управляются через консоль «Настройки → Безопасность».

Доступ к настройкам имеют пользователи с соответствующими административными ролями.

[4] Enterprise — крупная корпоративная инфраструктура или среда.