Getting Started:

One-Time Passwords for Raxak Protect™

A quick walk-through guide to using One-Time Passwords (OTP) for Raxak Protect

Introduction

One-Time Passwords (OTPs) provide an extra layer of security for password-based login. It combines passwords (what you know) with a hardware device or smart-phone based token (what you have) to provide increased security against password theft.

Last updated: May 2025 (for Release 5.2.1 or later of the Cloud Raxak portals)

Sections in this Guide

1 Audience

This guide is intended for users of the Raxak Protect console who log in using either a local or an LDAP/Active Directory username and password, who are looking for an additional layer of security.

The Raxak Protect portal itself is accessible to **all user types** (Security Admins, Regular Admins, Privileged Users, Regular Users, and Interim Users; please see the **Getting Started: Key Concepts** guide for user type descriptions).

2 Prerequisites

Please read the Getting Started: New User Guide if you have not yet done so. This Getting Started guide assumes that your IT environment is already set up to use the Cloud Raxak portals. This guide also assumes that you know your login information, user type, and portal URL, and are comfortable using Raxak Protect through the GUI interface.

If you need clarification on any of the concepts or terms used in this guide at any point, please see the **Getting Started: Key Concepts** guide for basic descriptions.

Note that all trademarks (e.g., Azure, AWS, and such) belong to their respective holders.

3 What are One-Time Passwords

A **one-time password** (OTP), also known as one-time PIN or dynamic password, is a password that is valid for only one login session or transaction, on a computer system or other digital device. OTPs avoid a number of shortcomings that are associated with traditional (static) password-based authentication; and our implementation also incorporate two-factor authentication by ensuring that the one-time password requires access to something a person has (such as a smart-phone with a pre-initialized authenticator app) as well as something a person knows (the traditional password).

OTP generation algorithms typically make use of pseudorandomness or randomness, making prediction of successor OTPs by an attacker difficult, and also cryptographic hash functions, which can be used to derive a value but are hard to reverse and therefore difficult for an attacker to obtain the data that was used for the hash. This is necessary because otherwise it would be easy to predict future OTPs by observing previous ones.

4 Getting an Authenticator App

Raxak Protect implements time-based OTPs (also known as TOTP; specified in the IETF RFC 6238). Multiple free or open source smart-phone apps support TOTP including Google Authenticator (described here as an example). Other apps that support TOTP are summarized in Section 8 below.

Google Authenticator is a software-based authenticator by Google that implements two-step verification services using the Time-based One-time Password Algorithm (TOTP; specified in RFC 6238), for authenticating users of software applications. When logging into a site supporting Authenticator, Authenticator generates a six- to eight-digit one-time password which users must enter in addition to their usual login details.

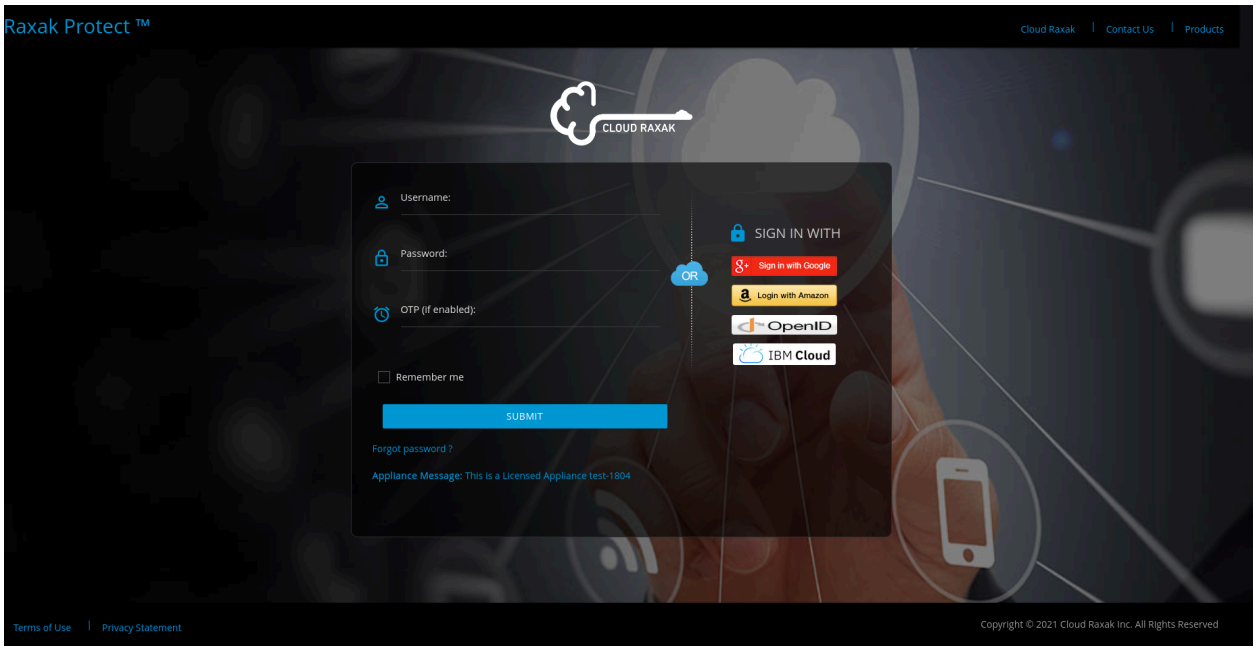
Google Authenticator is available on all standard app stores including the Google Play Store or the Apple Store.

5 Enabling OTP for a User

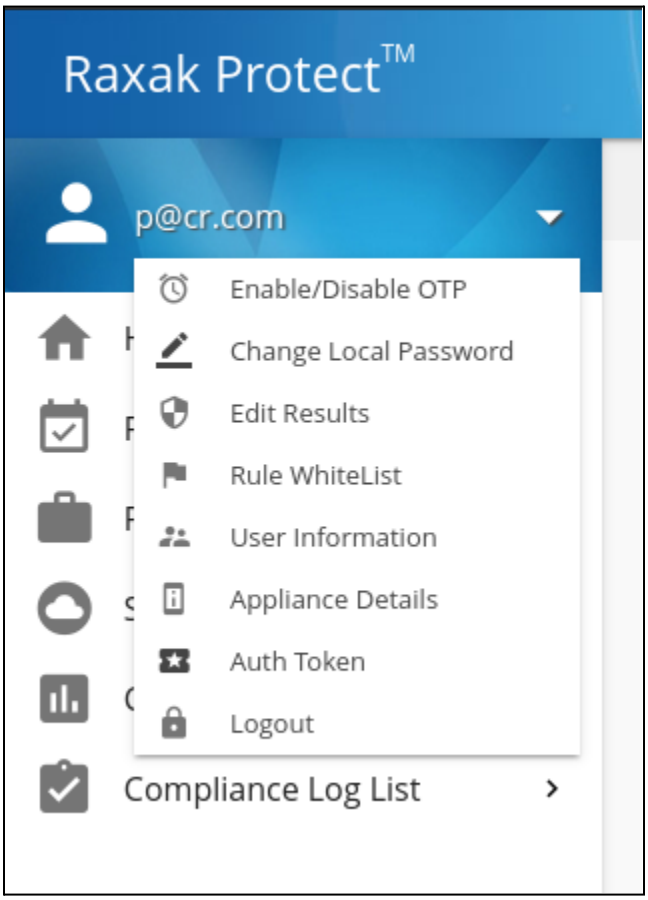
Note: For security reasons, OTP can only be enabled by each user for their own use. It can only be enabled for logging in with username/password, not for OAuth based logins (e.g., Login with Google or Amazon).

To enable OTP usage, you must first have a username/password associated with the account. For creating user accounts, see the guide Getting Started: Raxak Manage. By default OTP is disabled for all users.

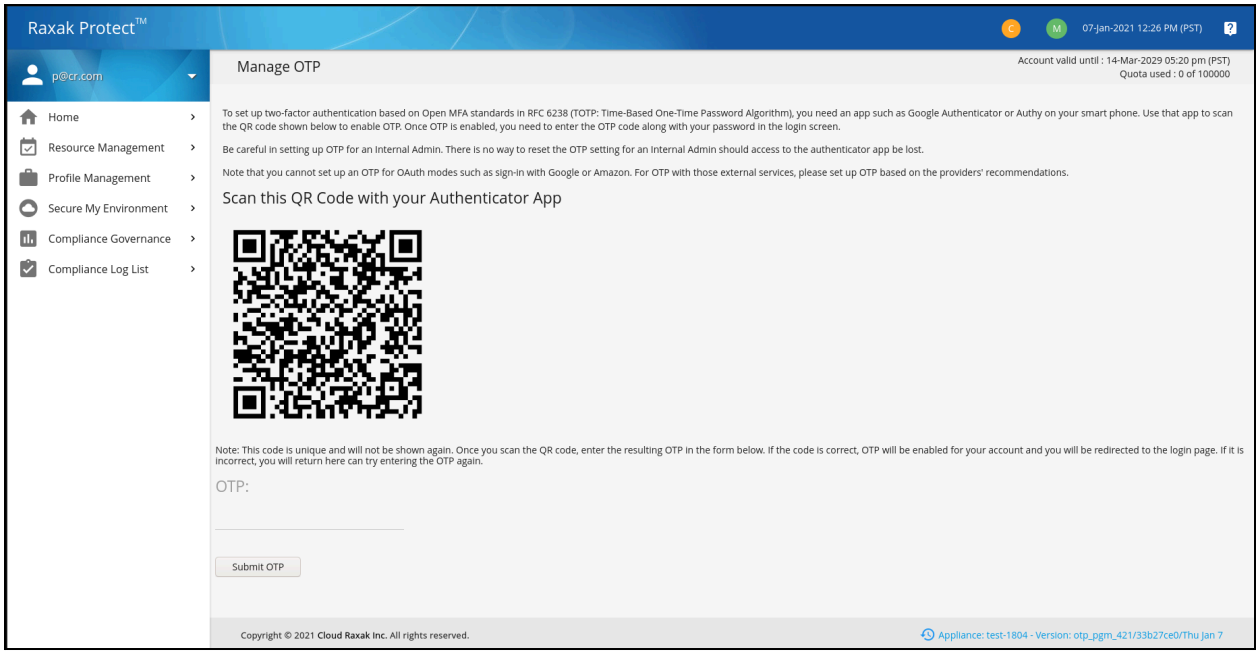
Log in to the Raxak Protect console with just your username and password on the standard login screen. Leave the OTP field blank.



Then, use the dropdown menu next to the username above the left navigation bar to select the **Enable/Disable OTP** menu item.



If the user does not have OTP enabled, you will see a screen as shown below. If the OTP is already enabled, you will be able to disable it as shown in the next section.



Use your authenticator app (e.g., Google Authenticator) to scan the QR code displayed on the screen. This code encodes your username, the appliance name, and the secret that is used for synchronizing your app with the OTP authentication back-end. Once the code is scanned, your app will indicate that the transaction is complete and start showing you time-based OTP codes.

The username and appliance name will be visible in the created Authenticator entry to allow you to keep track of different Raxak Protect accounts. For example, the Microsoft Authenticator entry looks like this:

Cloud Raxak (Raxak Protect (test-1804):p@cr.com)

where test-1804 is the name of the test appliance that created the code, and p@cr.com is the username for the account. Of course, your appliance name and username will be different.

Below the QR code is a form for entering an OTP generated by your Authenticator app. Fresh OTPs are generated and displayed every 30 seconds. Enter the current OTPs into the form and press **Submit OTP** within the validity period of that OTP code.

Note that OTP is not successfully enabled for your account until you complete this step. You must validate to the system that you have an Authenticator app that has been synchronized with the system before OTP is enabled for login.

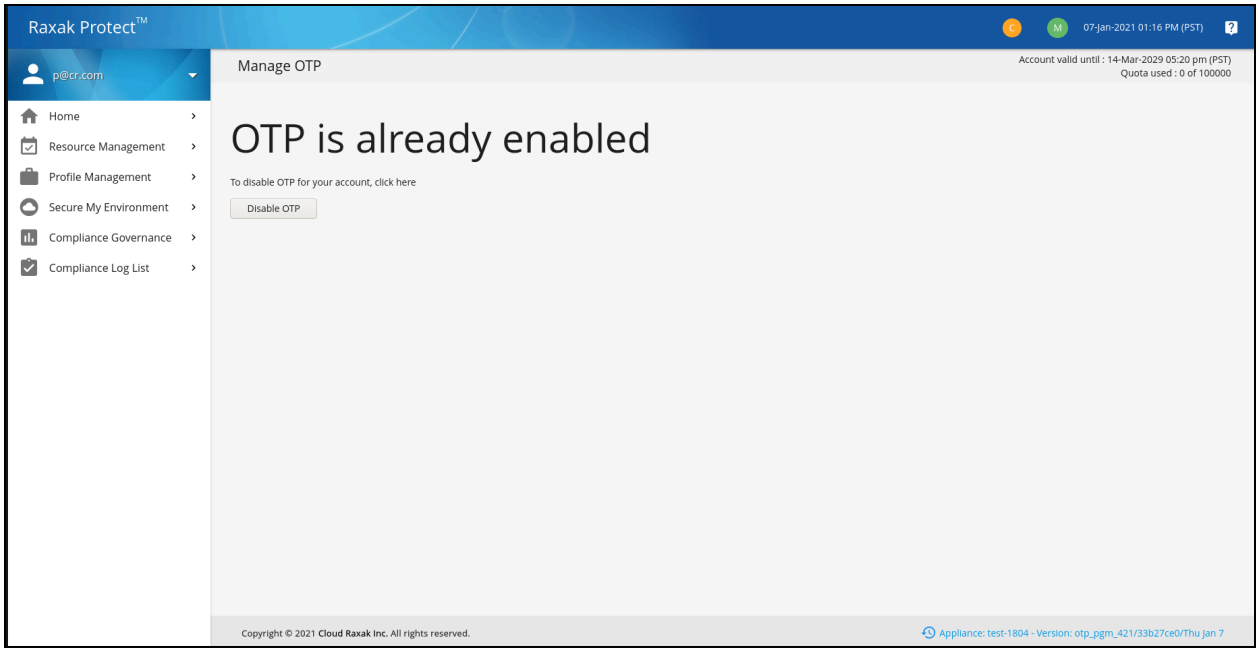
Once you enter the OTP and submit it for verification, one of two outcomes happen.

- If the OTP is correct and within its validity period, you will get a pop up message indicating success and you will immediately be redirected to the login page where you will have to re-authenticate with your username, password, and a fresh OTP.
- If the OTP is incorrect, you will get a pop up message indicating failure and you will remain on the Manage OTP page where you can try again with either re-scanning the QR code or re-entering the next valid OTP code.

Note that the same QR code will never be displayed again for security reasons. If for any reason you lose access to your Authenticator app, there is no way to reactivate the OTP on a different device until OTP is first deactivated on your account (See Section 7)

6 Disabling OTP for Your Own Account

If OTP is enabled for your account and you login and proceed to the **Enable/Disable OTP** menu item, you will see the following screen:



Clicking on **Disable OTP** will disable OTP for your account. You will remain logged in and will be redirected to the Dashboard screen. Unless you re-activate OTP you will not have to enter an OTP password at your next login. Remember to delete the OTP entry from your Authenticator app since it is no longer needed.

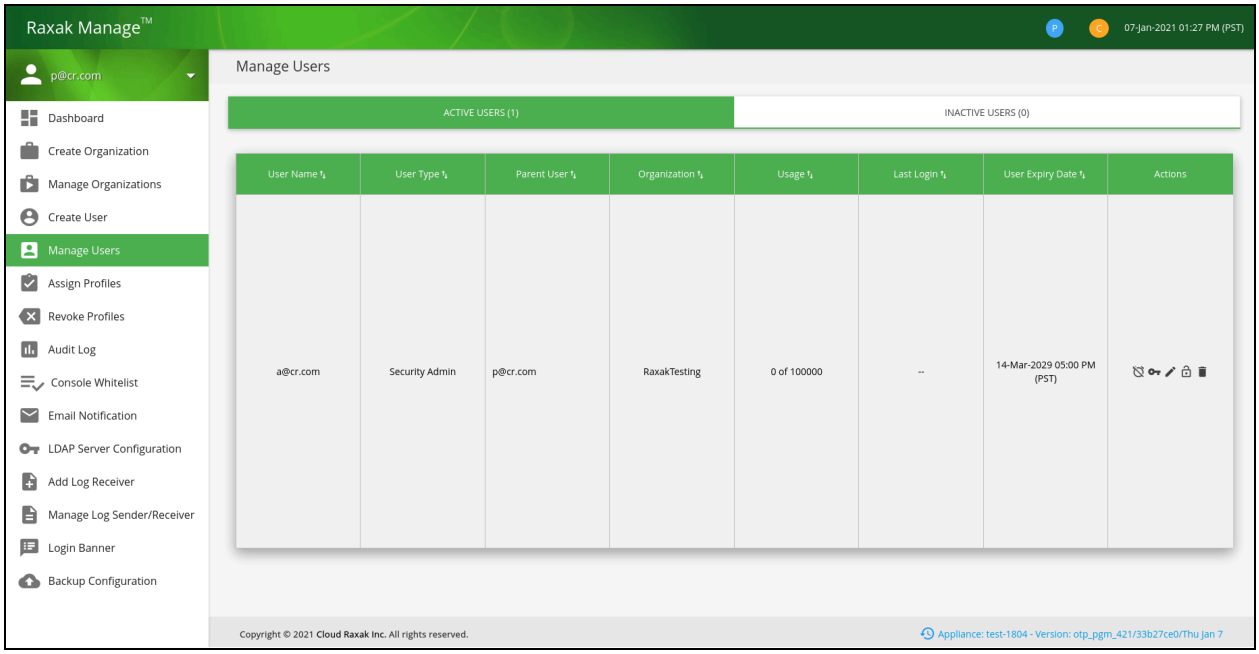
7 Disabling OTP for Other Users

If you have OTP enabled and then lose access to the synchronized Authenticator device, the only way for you to log in again is to have a suitable parent or the Appliance's Internal Admin disable your OTP.

For security reasons, only a direct parent who also has OTP enabled or an Internal Admin can disable OTP on a user account. This protects the system from compromised passwords.

Note also that if an Internal Admin has OTP enabled and loses access to the synchronized Authenticator device, only another Internal Admin can disable the OTP. If there is only one Internal Admin, please contact Cloud Raxak for help since this condition cannot be addressed via the Appliance console.

To disable OTP, you need the Internal Admin or a parent with OTP enabled and access to the **Raxak Manage** portal. In the Raxak Manage portal, navigate to the Manage Users page through the left navigation pane. Users with OTP enabled will show up with the icon in the **Actions** column as shown below. If the logged in user does not have the authority to disable OTP for the listed user, the icon will be grayed out.



Clicking on the icon will show a pop-up with the option to disable the user's OTP. Once disabled, the user can then log in without having to supply a OTP.

8 Compatibility Tests

As of January 11, 2021 Raxak Protect's OTP system has been tested with the following OTP apps. All these apps are available on the Google Play Store for the Android platform as well as the Apple App Store for the iPhone platform.

Icon	Mobile App	Vendor	Comments
	Authy	Twilio	Allows cloud-based backup of your codes. Three-way protection.
	FreeOTP Authenticator	Red Hat	Open source but fewer features than the competition.
	Authenticator	Microsoft	Second layer of protection with screen unlock or fingerprint integration.
	Google Authenticator	Google	Commonly available and may be pre-installed on many Android devices.

Most technical websites periodically publish reviews of OTP apps as well. Since the Raxak Protect OTP solution follows the published IETF standards, it should be compatible with all major app offerings. For example, see a recent review from Android Authority with other less well known but functional apps that can be used.

If you find that your favorite app has compatibility issues with the Raxak Protect implementation, please report it to Cloud Raxak.