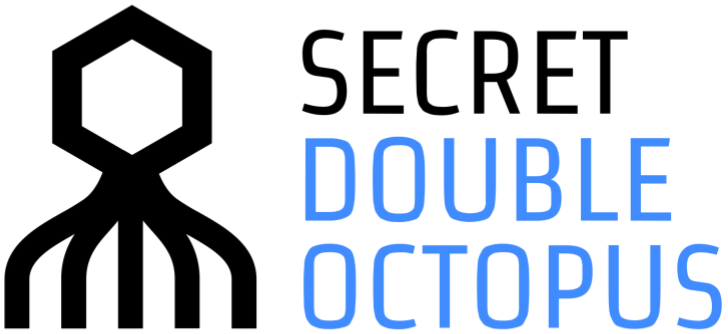
AUGUST 27, 2020



Octopus Authenticator Installation and Operation Guide Version 3.11.0

Preface

This document describes the Secret Double Octopus Authenticator solution, the procedures, and functionalities for installation and operation of Octopus Authenticator Mobile App in the following order:

- Phase 1 – Octopus Authenticator App installation
- Phase 2 – User's system enrollment
- Phase 3 – Octopus Authentication example scenarios

General

Secret Double Octopus liberates users from the pain of passwords. Using this app, users don't need to manage passwords and can enjoy a consistent login experience throughout their work day. Organizations gain the benefits of high assurance and credential control across domain accounts, VPN, cloud applications and legacy apps.

System Overview

The mobile device seems to be the ideal authenticator. However, first generation attempts at this suffer from a single point of failure. One example was the reliance on SMS for authentication, proven to be easily hackable, but the same is true for all another current approach (keys, push notification, etc.). Secret Double Octopus introducing the industry's first authenticator with multi-shield authentication for devices and users. Secret Double Octopus is flexible to support any backend applications, VPN or clouds services, and focus on the most seamless user experience possible.

Security

Resilient, Multi-Shield device authentication

Secret Double Octopus presents a unique Secret Sharing cryptographic algorithm, resilient to unlimited computing power, authenticates the device by multiple routes, thus avoiding a single point of hacking.

No OTP for hackers to hijack

OTP is vulnerable to hijacking both en-route to the mobile device and when typed in the browser session.

Complete Multi-Factor with Biometrics, IAM

Octopus Authenticator utilizes biometric systems such as TouchID and FIDO, as well as identity access management systems, like Active Directory, to conduct complete multi-factor verification in a single solution.

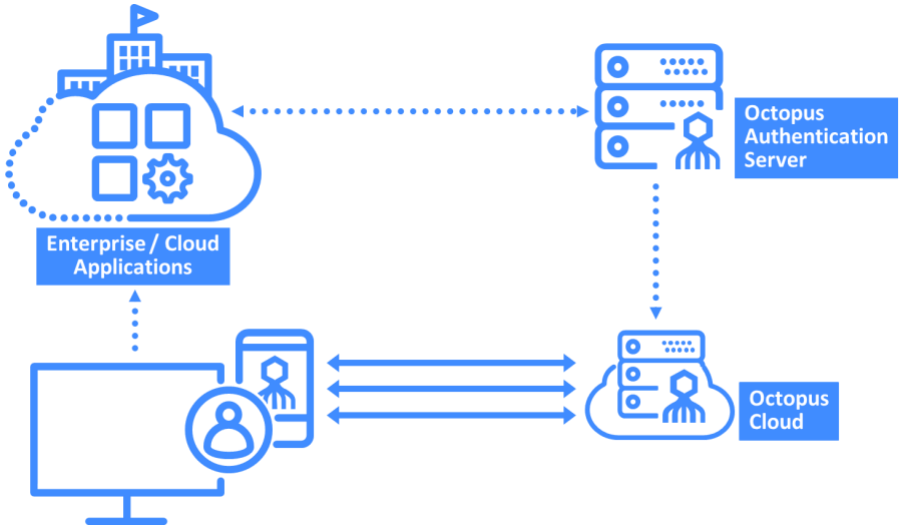
Avoid MiTM Attacks and SSL Manipulations

A random AES256 key is delivered using Secret Sharing to the device for symmetric encryption, eliminating MITM and eavesdropping attacks.

Hardened Mobile App

Octopus Authenticator Mobile App includes the following protections against cyber-attacks: Binary Obfuscation, Root/Jailbreak detection, Anti-Tampering, Code Injection Protection, Device ID Pinning, MiTM protection, Backup protection, Encrypted file system

System Architecture



STEP 1 – Octopus Authenticator App Installation

Participating Devices:

i. iOS mobile devices with iOS 10 and above (iPhone 5 or later. Recommend iPhone 5s or later, for use of fingerprint scanning)
ii. Android devices with Android 5 and above

To download the Octopus Authenticator App, please refer to Apple AppStore or Google Play.

STEP 2 – User Enrollment

Octopus Authenticator App requires pre-enrollment to allow using it to approve authentication and to approve transactions. The enrollment process is simple and secured to enroll a user with a specific device.

1. User receives an enrollment invitation email, generated by the system admin.
2. The invitation email includes the following information:
    a. Link to download the application (AppStore and Google Play).
    b. Enrollment QR Code
    c. Manual code
    d. Enrollment link (Use only when clicking on mobile email)
3. To enroll follow one of the enrollment options:
    a. Enroll via the mobile browser; follow the link specified in the invitation email.
    b. Enroll with the QR code; scan the QR code using the Octopus Authenticator App.
    c. Enroll manually; enter the manual code using the Octopus Authenticator App.
    d. Open the invitaion email on the mobile and click the “Enroll” link which open the Octopus Authenticator directly and enroll.

Note: For security reasons, the enrollment code will expire after a period. Please make sure to enroll within this timeframe. In case your code expires before you enroll, please contact Secret Double Octopus support team for a new enrollment code.

4. Upon the first enrollment, the user will receive a successful enrollment notification.

Invitation Email example:

SECRET DOUBLE OCTOPUS

Hi [redacted]

We would like to welcome you to the Octopus Authenticator, a simple and highly secure system for validating your identity to various applications and networks.

Your next step is to download the Octopus Authenticator to your mobile device, and identify yourself to the system using the instructions below. Once that is completed, the Octopus Authenticator will notify you when an application or network requires your identification, and you will confirm or reject with a single tap.

Step 1: Download and install Octopus Authenticator

Get it on Google play Download on the App Store

Step 2: Follow one of the enrollment options below:

To enroll directly with the Octopus Authenticator follow this link: Enroll

To enroll with QR code scan the following using the Octopus Authenticator application:

To enroll manually use the following code: ***04a51fa2e56e4cfeb643698470e78ebd***

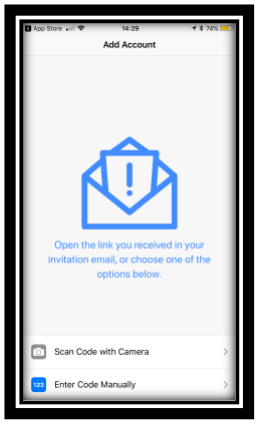
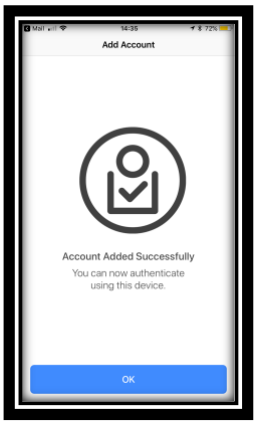
For any assistance please contact: support@doubleoctopus.com or your system admin.

The Invitation will expire in 10 minutes, Please make sure to enroll within this timeframe.

Keep Safe,
Secret Double Octopus

Octopus Authenticator App Enrollment Flow

The diagram below demonstrates one out of three enrollment options, using a QR code enrollment

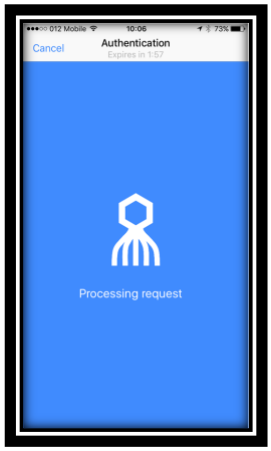
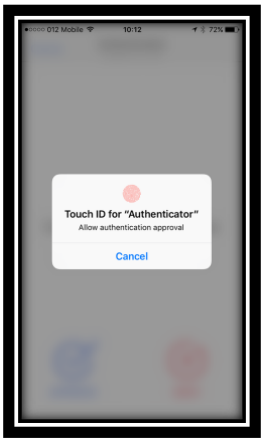
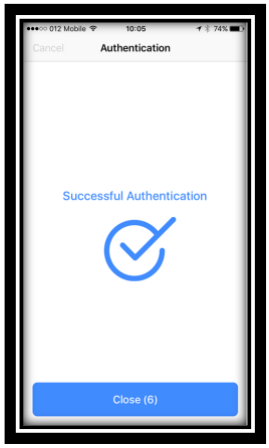
1	2	3	4
			

STEP 3 – Authentication Scenarios

Once users enroll a device, they can use it to authenticate to the participating services. For each such service, the user receives a push notification with an approval request. Once the user approves the authentication, the Octopus Authentication Server sends the response back to the service.

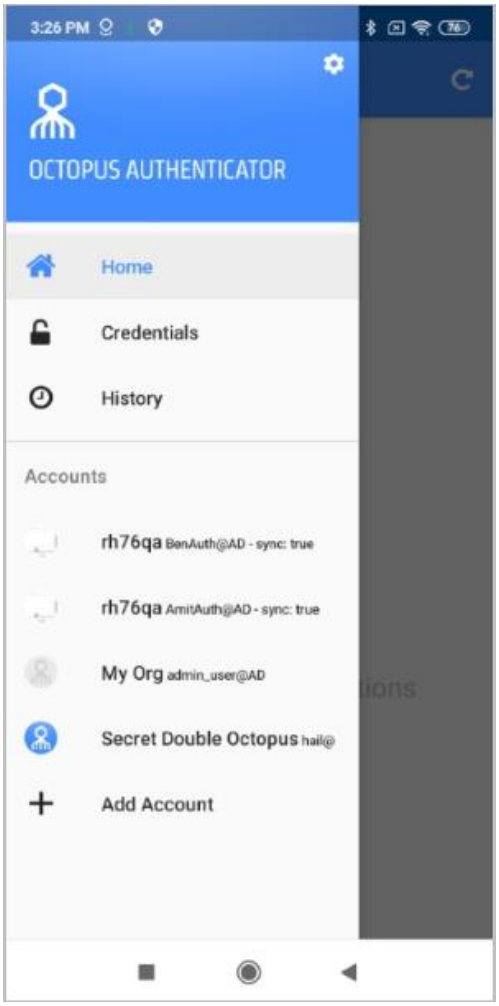
Note: The identification field (email, username) is required for each service.

The following diagram shows an example of a service authentication flow.

1	2	3	4
			

Mobile App Menu

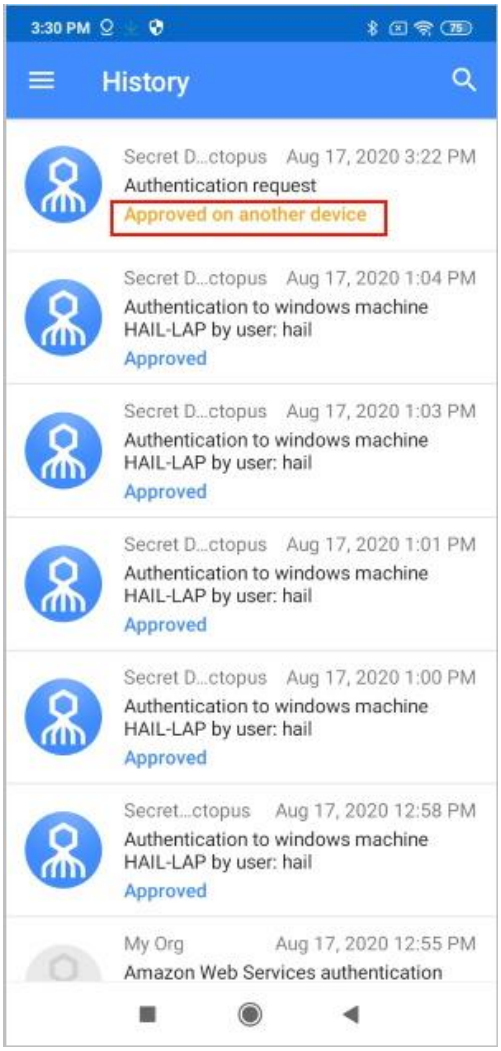
Most of the app navigation takes place from the menu screen. From here, users can view authentication history, lists of generated credentials and account information.



Authentication History

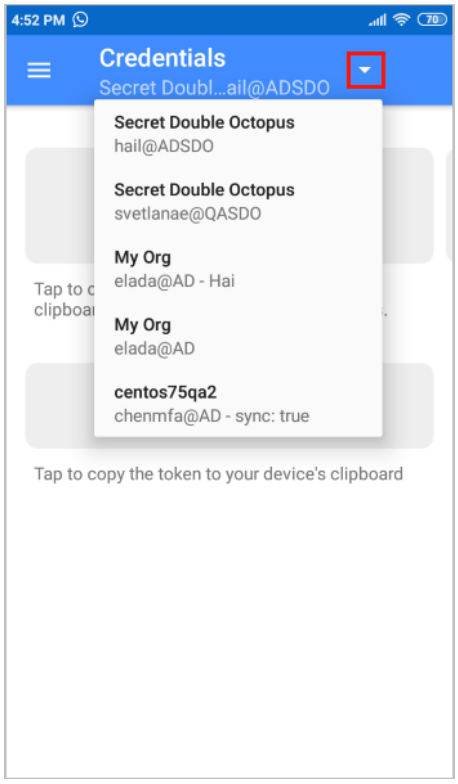
The **History** screen displays details about previous authentication requests, including their status (e.g., **Approved**).

For users with more than one device, the Authenticator app is immediately updated when an authentication request is approved or denied on another device.

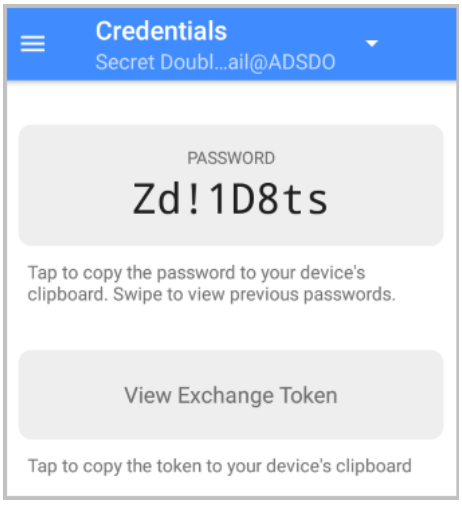


Account Credentials

The **Credentials** screen allows users to view and work with passwords and tokens that have been generated for their account(s). Users who have more than one account specify the relevant account by opening the list at the top of the page and tapping the account.

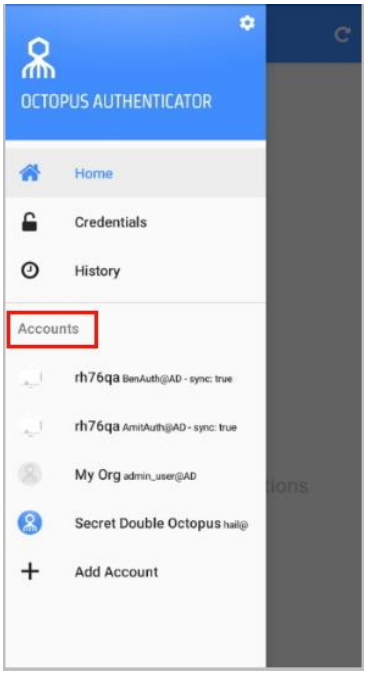


Users can then copy the credentials, or swipe to navigate to previously issued passwords.

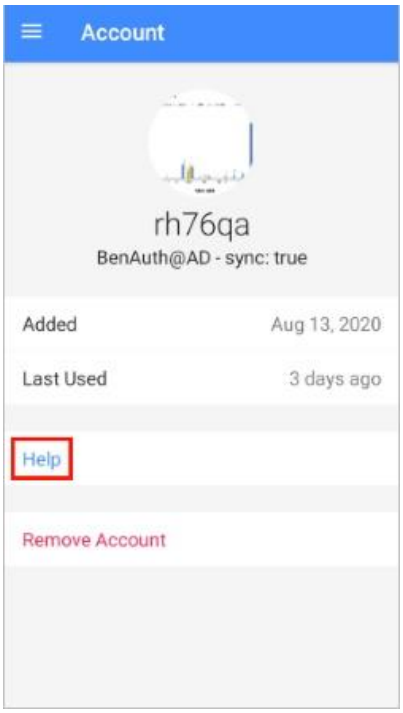


Account Information and Troubleshooting

Users access the **Account** page by tapping the relevant account in the menu's **Accounts** list.



The **Account** page provides basic information about the account as well as a link to the **Help** screen.



To assist communication with support teams and facilitate rapid resolution of any issues that users encounter, the **Help** screen displays the Octopus Authenticator version and various other details.

The **Feedback** portion of the **Help** screen allows users to easily report issues. When users tap **Report Problem**, a report which includes account details and a log file, is automatically generated. When users send the report by email, the subject line is prefilled and the company support email appears automatically in the CC list.