Review: Seven 2FA Apps

Review: Seven 2FA Apps

We've tested 7 two-factor authentication apps. We need something that can be used across the organization.

Disclaimer: We have no affiliation with the companies mentioned. This article is based solely on our independent research findings. There are no affiliate marketing links provided below for your convenience. The apps are listed in alphabetical order.

How we write our reviews: For an impartial and comprehensive review, all apps undergo thorough testing:

- Real-time usage in actual projects.
- Evaluation by different team members across various countries.
- Testing on different devices and operating systems.
- A minimum of two weeks, typically four, trial periods.
- The article undergoes peer review by team members before being sent to the app's publisher for final review.

Background:

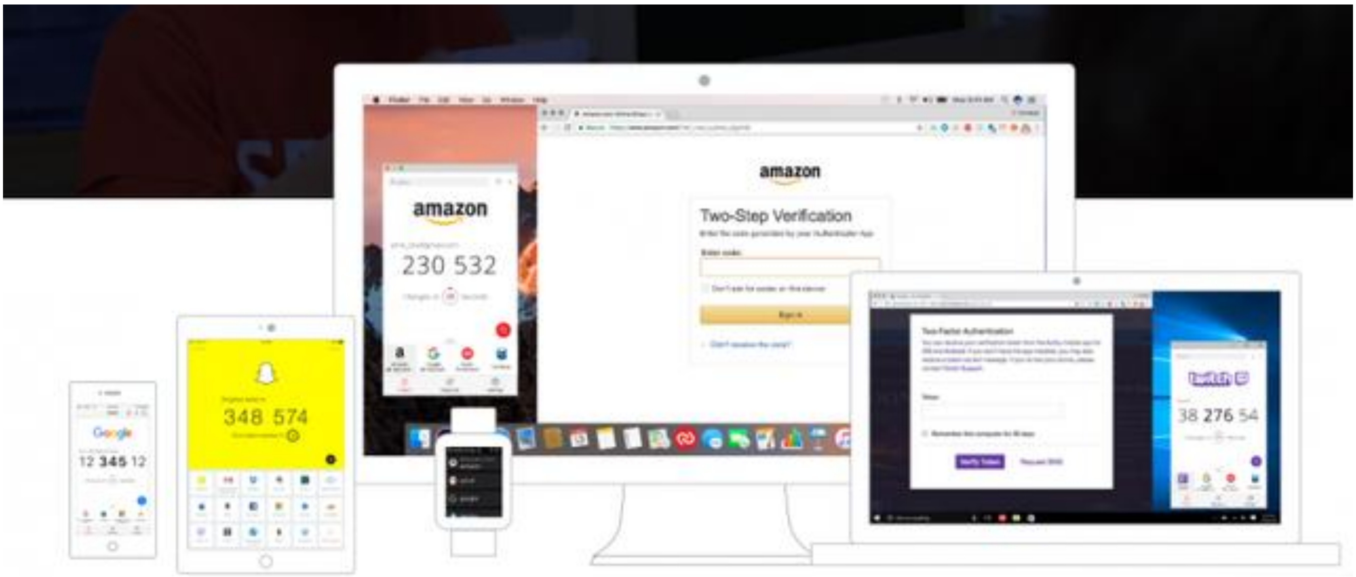
Two-factor authentication (2FA) enhances device or system security by requiring two verification steps, surpassing the vulnerability of a single login-password. While 2FA commonly involves one-time passwords via text messages, this method can pose security risks. It's akin to adding two padlocks to a door: the login-password acts as one padlock, and an additional method serves as the second. Although more padlocks can enhance security, it also extends the door-opening process, emphasizing the importance of starting with at least two.

Our specifications sheet:

- Ensure broad platform coverage (Windows, iOS, Android OS, Clouds, social media like Facebook, Twitter).
- Provide diverse 2FA options, including email authentication apps and hardware keys.
- Prioritize offline functionality.
- Allow disabling of less secure SMS 2FA, voice messages, and fingerprint options prone to interception or brute-force attacks by hackers and state-sponsored criminals.

01-Authy.

Authy is a free application designed to capture 2FA tokens from widely used web services. It also serves as a client for the Twilio 2FA API, streamlining the implementation of two-factor authentication for companies such as CloudFlare, Twitch, and SendGrid.



Website: https://authy.com

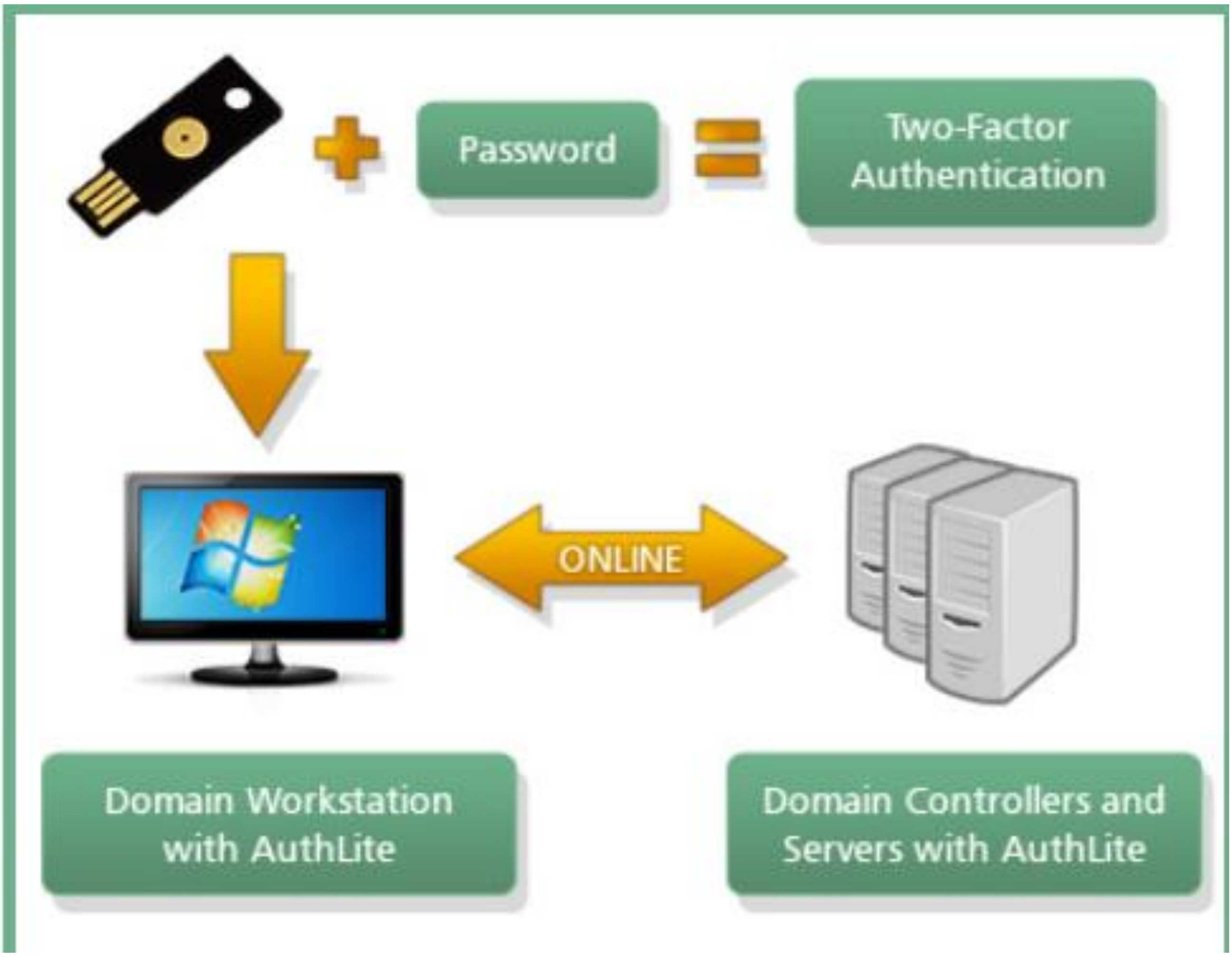
1.1 Pros:

- Authy is available on common platforms like iOS and Android, with a desktop client for Windows and Mac OS, and Linux support forthcoming.
- It captures 2FA tokens from popular services such as Facebook, Google, and Twitter
- Offering guides at authy.com/guides.
- The app collaborates with the Twilio 2FA API, providing codes and push-based authentication.
- Multiple device authentication is supported, allowing use across various devices. In case of loss or retirement, deauthorization and reauthorization are swift, via SMS/voice or more secure app methods.
- Backup tokens functionality prevents access loss if the authorized device is misplaced.
- The app allows disabling of SMS and voice call authentication, provides offline authentication, and ensures easy installation.

1.2 Cons:

- The app offers free use with services like Twitter and Snapchat. However, implementing a full 2FA solution in your application incurs costs. The pricing is budget-friendly, with the first 100 authentications per month being free. Beyond that, you can opt for a pay-as-you-go model at $0.045 USD per authentication. For 300 authentications monthly, the cost is $13.5 USD.

02-Authlite.


Password
Two-Factor Authentication
ONLINE
Domain Workstation with AuthLite
Domain Controllers and Servers with AuthLite

Website: http://www.authlite.com

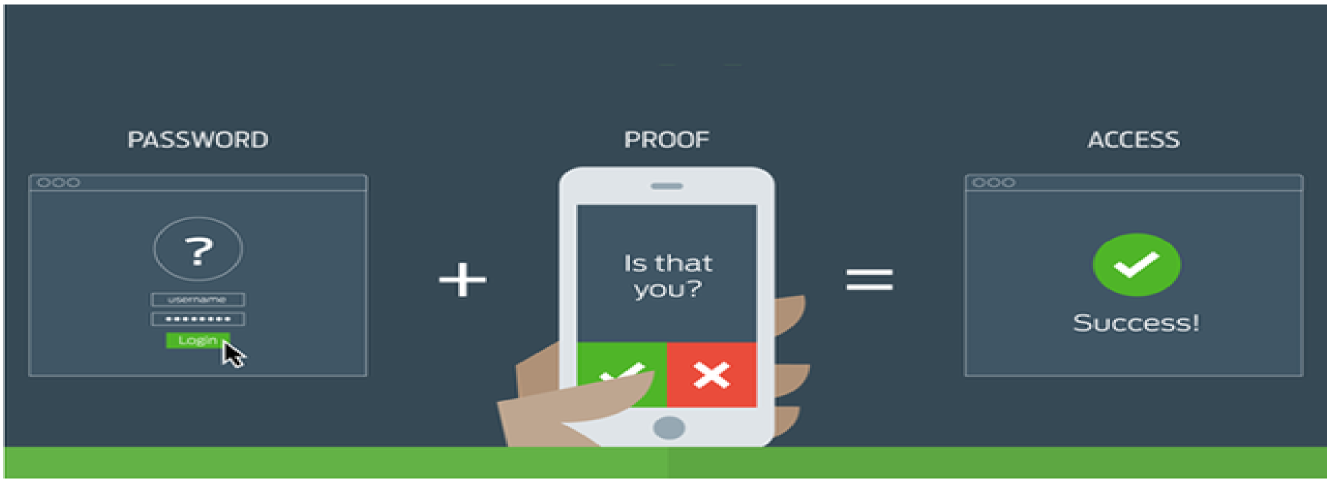
2.1 Pros:

- AuthLite offers offline authentication capabilities and supports any OATH token, including smartphone soft token apps like Google Authenticator. This flexibility can potentially reduce costs compared to using YubiKey devices. Especially for larger user volumes, AuthLite's pricing is significantly lower than $48 per user. It can enforce two-factor authentication for any authentication linked to Active Directory, including systems using ADFS for federation into AD.

2.2 Cons:

AuthLite is a lightweight solution with a narrow focus on specific authentication types: Windows authentication, RDP authentication, and VPN. For two-factor authentication, a Yubikey USB stick is required. However, this may not be practical, as it poses the risk of being lost, potentially resulting in device access loss. The price is relatively high compared to the features offered, at 48 USD per user for a lifetime license and an additional 30 USD for the Yubico Key Token, totaling 70 USD.

03-Duo.



Website: https://duo.com

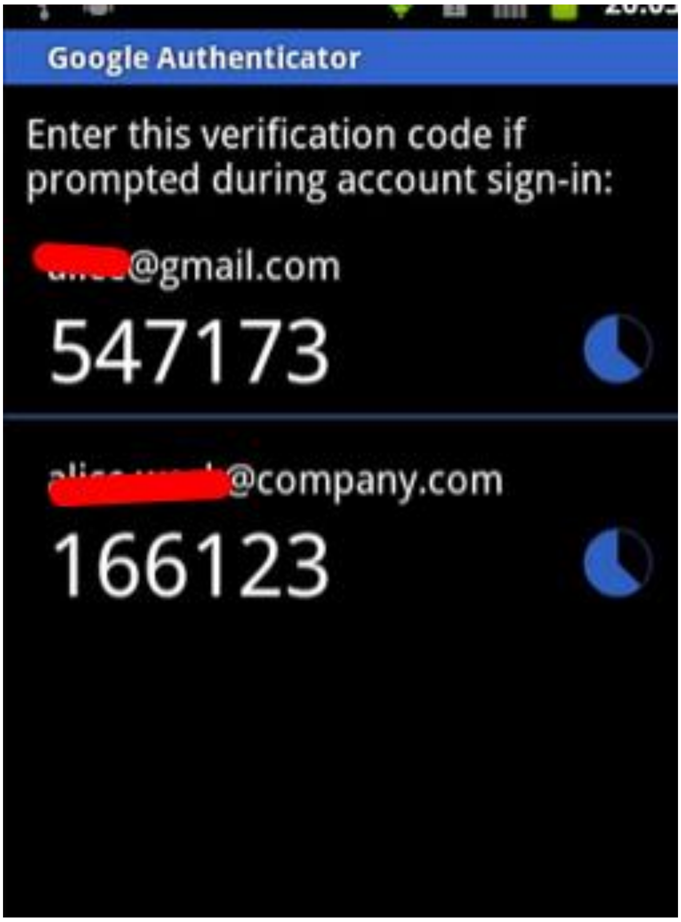
3.1 Pros:

It sounds like the application you're describing has comprehensive support across various platforms like Windows, VPN, SSH, and Cloud. It boasts a robust centralized user console for efficient user and device management. In cases of lost, stolen, or retired devices, deauthorization can be quickly executed from any authorized device. The system offers multiple authentication methods and allows users to disable SMS or voice call authentications as needed. This flexibility enhances security and usability across different scenarios.

3.2 Cons:

It seems the application is missing support for mobile operating systems like Android and iOS when it comes to 2FA. The pricing for the package designed for use in high-risk countries is quite high, at 6 USD per user per month. Furthermore, there's feedback from the support team indicating that "offline authentication" doesn't work optimally because devices need to be connected to the internet for it to function properly. These factors suggest potential limitations and considerations for users looking into this solution.

04-Google Authentication.



Google Authenticator

Enter this verification code if prompted during account sign-in:

[redacted]@gmail.com

547173

[redacted]@company.com

166123

Website: https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2

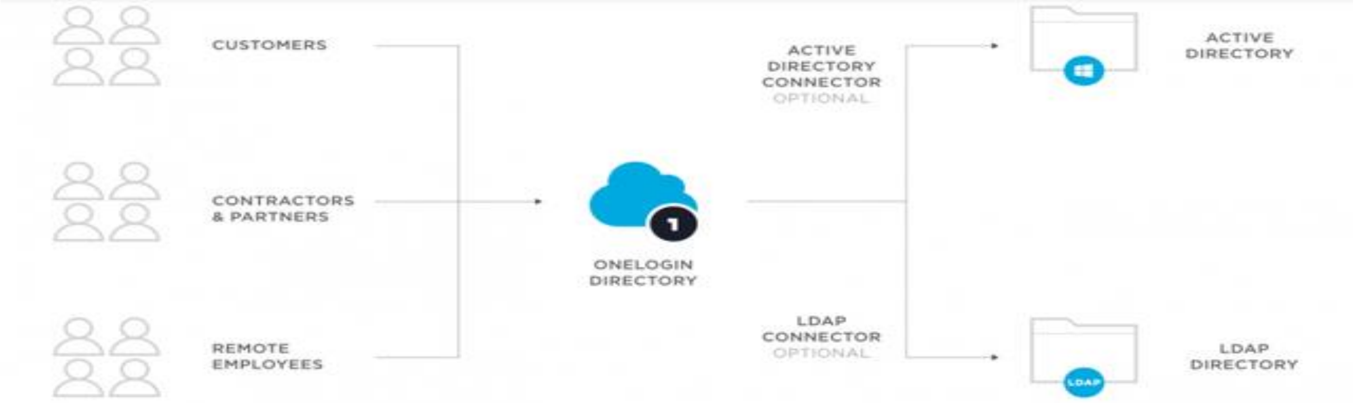
4.1 Pros:

The system offers 2-Step Verification through SMS text message or Voice call. It allows code generation using a mobile device and supports offline authentication through the Google Authenticator app, ensuring receipt of codes even without an internet connection or mobile service. The service is available for free.

4.2 Cons:

The authentication tool is utilized for signing into various accounts, including Google, Facebook, Tumblr, Dropbox, vk.com, and WordPress. For Windows logins, a third-party application integrated with Google Auth must be sought. Limited to one device per account, it lacks a backup recovery option in case of mobile loss or confiscation by law enforcement.

05-Onelogin.



Website: https://www.onelogin.com

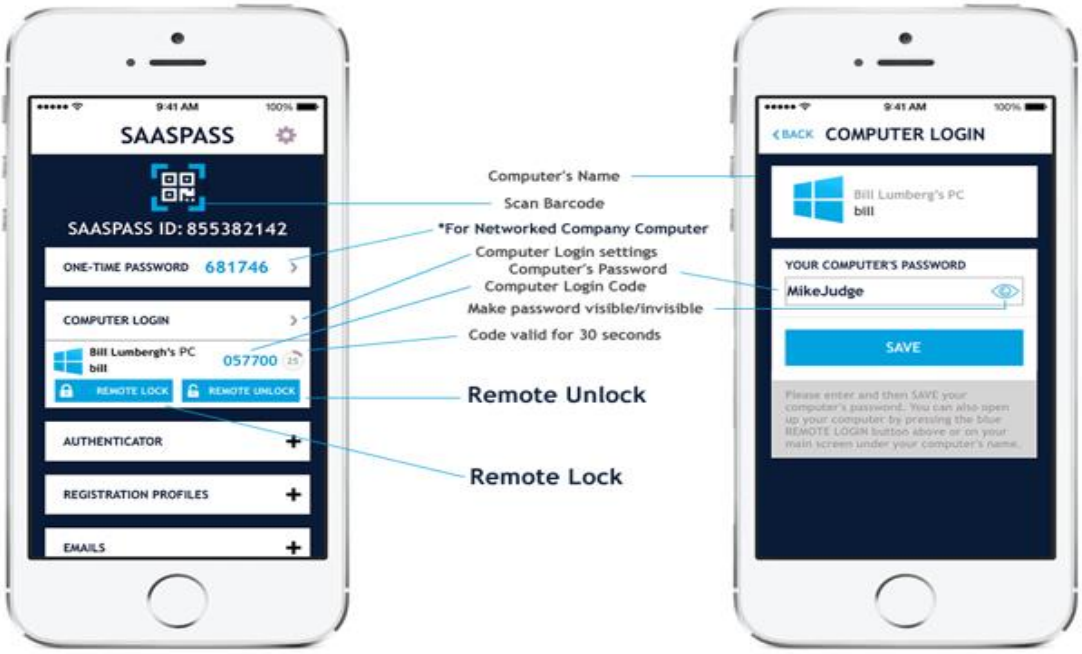
5.1 Pros:

Price is affordable.
It has a centralized reporting for the users 48 USD/year.

5.2 Cons:

This solution operates as a centralized IT system, requiring an in-house IT staff and integration with an Active Directory, achievable with a single click. However, for our globally dispersed agents without a centralized setup, this becomes a drawback. The availability of offline authentication is not explicitly mentioned. It appears to primarily support desktop operating systems (Windows and Mac OS) and applications.

06-SAASPASS.



Website: https://saaspass.com

6.1 Pros:

It covers a wide array of platforms, requiring a smartphone for operation, including iPhone, Android, Apple Watch, Android Wear, Blackberry, Windows Phone, Java ME, iPad, iPad Mini, Android Tablet, Windows Tablet, Mac OSX, Windows OS, Mac Mini, Wearables, Google Glass, and Kindle. This solution supports multiple platforms and applications for 2FA, facilitating authentication across devices. Swift deauthorization is possible for lost, stolen, or retired devices, and it offers token backup to prevent access loss. With multiple authentication methods like Touch ID, it allows disabling SMS, voice call, and fingerprint authentication. Offline authentication is also supported. The pricing is more affordable compared to other solutions, with free and paid packages starting around 20 USD/year and 40 USD/year respectively. Installation is straightforward.

07-Yubico (Yubikey).

Website: https://www.yubico.com

7.1 Pros:

This solution spans various platforms, including Windows desktops (with Linux support coming soon), iOS, Android OS, selected cloud storages, and web platforms like Facebook and Twitter. It facilitates multiple device logins and offers offline authentication. The cost is budget-friendly, approximately 50 USD per USB token (Yubikey). Installation is straightforward.

7.2 Cons:

This solution relies solely on USB authentication using Yubikey. If the Yubikey is lost, stolen, or confiscated by the government, there is a significant risk of losing access to both applications and devices such as computers and mobiles. Unfortunately, there is no option to backup tokens.

8. Conclusion:

Two-factor authentication significantly mitigates threats by necessitating more than just password access, making it unlikely for attackers, including state criminals, to possess the associated physical device. The added layers of authentication enhance system security.

Among the mentioned apps, all excel in providing an extra layer of protection. They support mobile tokens, offer diverse flexible authentication methods, and undergo additional analysis for some. Differences emerge in pricing, packaging, multi-device installation, offline authentication, app support, user-friendliness, and SMS option disablement. Considering these factors, SAASPASS stands out as the primary solution, followed by Authy as the secondary choice.