Most Popular 2-Factor Authentication (2FA) Compared

Updated August 31, 2016: We have added FreeOTP, Authenticator Plus and SoundLogin!
Please look below for the added Password Managers review and also take a look at our updated comparison table.

Devolutions

GOOGLE AUTHENTICATOR vs AUTHY vs YUBICO vs DUO FREEOTP vs AUTHENTICATOR PLUS vs SOUNDLOGIN

Do you, by any chance, use the same password for more than one website? Do you download software straight from the Internet? Or click on sketchy links in email messages? By doing any of these typical actions, you risk having your password stolen or being hacked. 2FA will prevent this from happening by adding an extra layer of security to your account.

There are 3 well-known factors used for authentication: something you know (a password or passphrase), something you have (your mobile phone or a token), and something you are (your fingerprint). 2FA means the system is using two of these options to authenticate you.

2FA can offer important benefits to enterprises as well as individual users, although the technology can seem complicated and the tools themselves vary. Choosing the right software to fit your needs is a hefty task, so we did some digging around for you and took a closer look at the most popular ones: Google Authenticator, Authy, Yubico, Duo, FreeOTP, Authenticator Plus and SoundLogin.

Some of the features that we look for in a great 2FA application are mobile support, multiple token support, reporting, complexity workflow and FIDO support.

GOOGLE AUTHENTICATOR IS A 2FA MOBILE APPLICATION THAT USES THE TIME-BASED ONE-TIME PASSWORD ALGORITHM (TOTP) AND HMAC-BASED ONE-TIME PASSWORD ALGORITHM (HOTP), FOR AUTHENTICATING USERS.

WHAT WE LOVE

TOTP ALGORITHM: Google Authenticator uses the TOTP algorithm to provide new code every 60 seconds, making it a secure option to generate codes for 2FA.

WORKS WITHOUT INTERNET ACCESS: One of the most appealing features of Google Authenticator is that it doesn't require any sort of internet or cellular connectivity. Since Google Authenticator uses TOTP, the same code will be generated on your mobile device and on the Google side without internet. The matching code gives you access to your account.

HOLDS MULTIPLE ACCOUNTS IN ONE PLACE: Most websites allow you to have more than one account, but won't allow you to use the same mobile number with multiple accounts. To receive your 2FA code, you then have to give different mobile numbers for each. The Google Authenticator application allows you to have codes for all your accounts in one place.

EASY TO USE: Google Authenticator is easy to use and has a simple interface. The application also works in airplane mode and will work on older version of Android. It is less than 2MB in size, so it works easily on all devices, even those with less RAM and storage..

WHERE IT NEEDS IMPROVEMENT

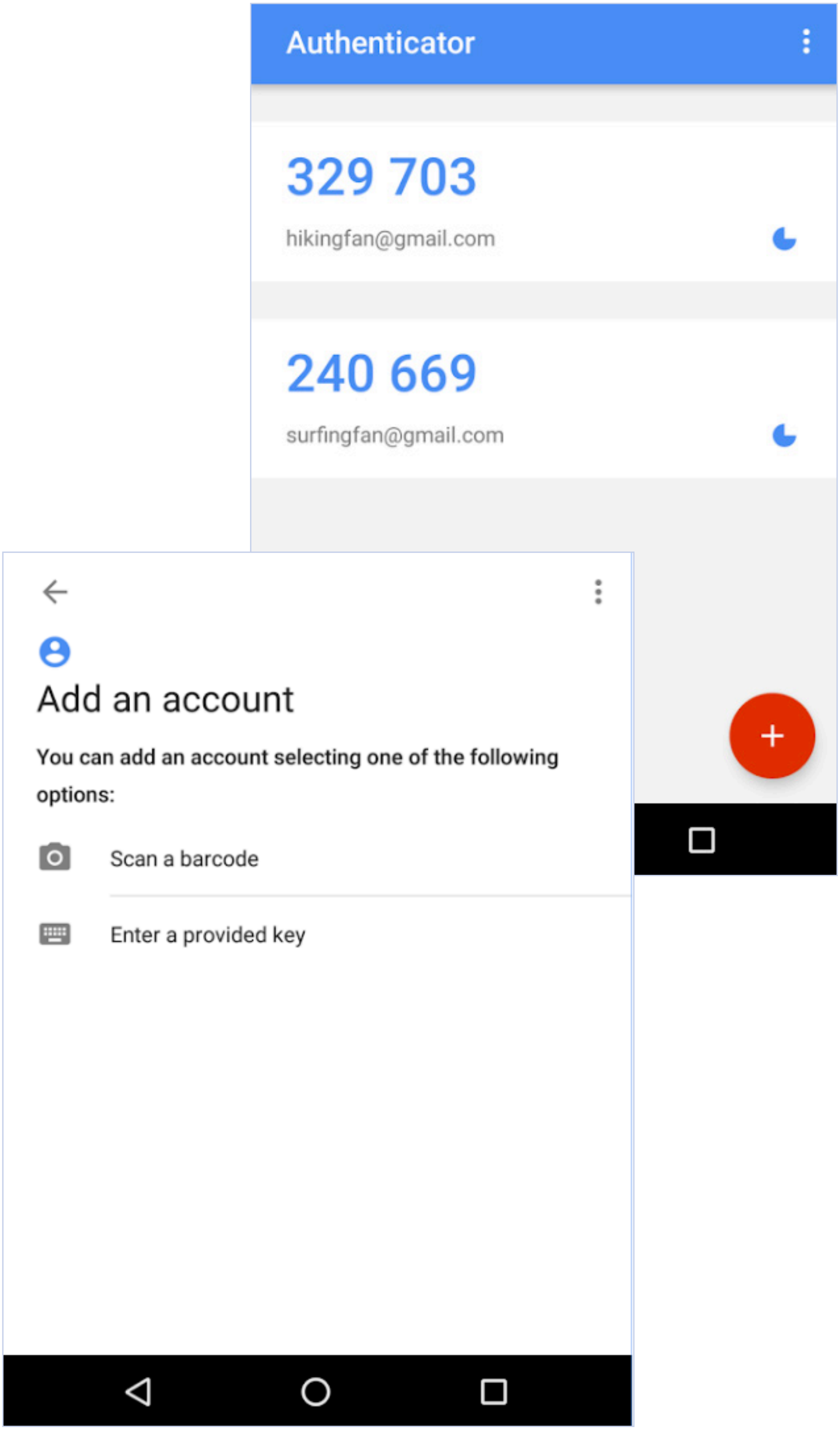
USER INTERFACE: Google Authenticator would benefit from a smoother interface. The new version adds a lot of white space and wasted space, including a lot of scrolling to get where you want to be.

TOO FEW ACCOUNTS ON THE SCREEN: If you only have 4 accounts, then it will work well, but if you have 14 accounts, only 4 of them will occupy the entire screen, making it impossible to view all of your accounts in a glance.

WHO IT'S FOR

Google Authenticator is **mostly for single users**, but it could also **serve industry standards**. It is best suited for users who need an easy app to protect their password on some of the most popular websites.

The application is completely free.



Authenticator

329 703

hikingfan@gmail.com

240 669

surfingfan@gmail.com

Add an account

You can add an account selecting one of the following options:

Scan a barcode

Enter a provided key

GET MORE INFORMATION ON GOOGLE AUTHENTICATOR AT
https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&hl=en

AUTHY

AUTHY MAKES IT EASY FOR ANYONE TO USE THEIR IPHONE, ANDROID OR DESKTOP FOR 2FA WITH ALL THEIR ONLINE ACCOUNTS. CHOOSE BETWEEN 3 DIFFERENT COMBINATIONS OF AUTHENTICATION OPTIONS: AUTHY SOFTTOKEN, AUTHY ONECODE AND AUTHY ONETOUCH.

WHAT WE LOVE

MOBILE AND DESKTOP APPLICATION: If you want to install 2FA on your desktop, Authy is the way to go. The application is supported whether you're using iOS, Android, BlackBerry, Linux, Mac OS or Windows — you could even install the application on your Apple Watch.

SECURITY TOKEN DIRECTLY ON YOUR DESKTOP: Most people use their smartphone as their second factor, which means that you have to copy the security code onto your computer when prompted. Authy makes it easier by inserting the security token directly on your desktop.

SYNC AND BACKUP IN THE CLOUD: Authy allows you to sync and backup your accounts on the Cloud. This saves time, since you no longer have to manually add your accounts to each device and browser.

REMOVE OTHER AUTHORIZED DEVICES: If your phone is stolen or lost, you will be able to remove the lost phone from the devices' list on your desktop application, thereby preventing it from syncing with Authy's servers. Keep in mind, however, that if your phone has been stolen, the thief could still use Authy to generate tokens for any accounts you've already added to it.

WHERE IT NEEDS IMPROVEMENT

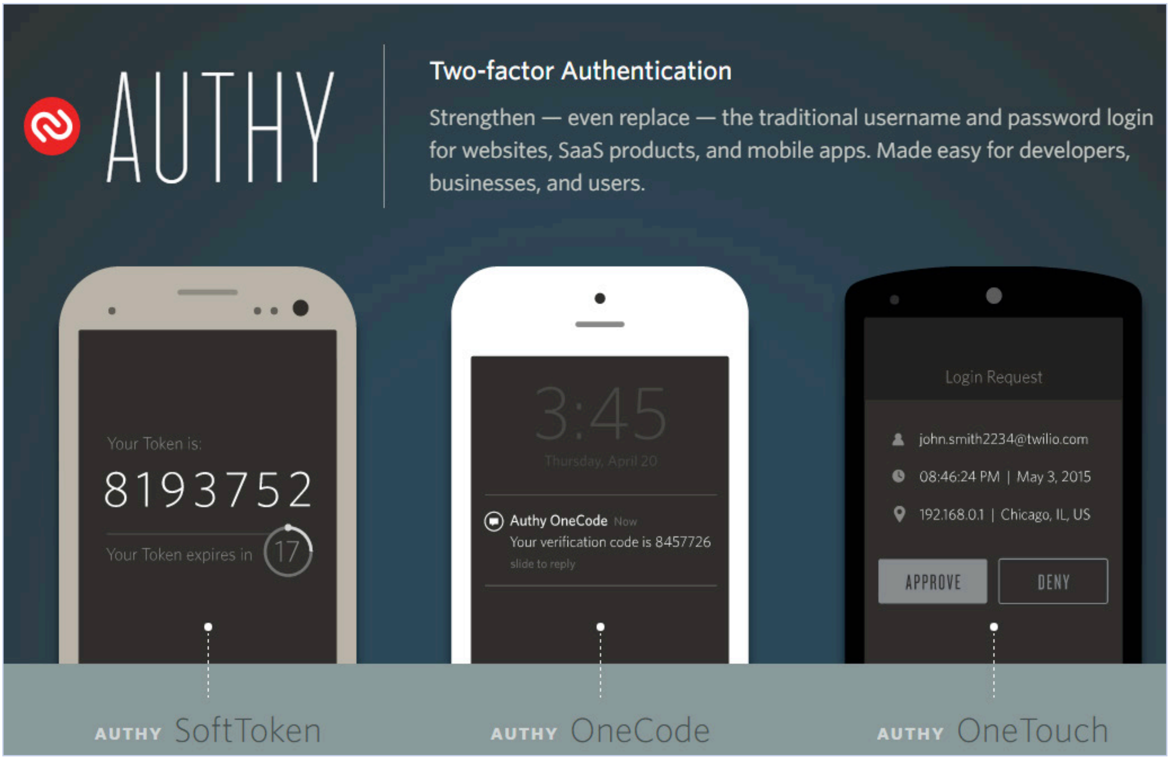
MASTER PASSWORD NOT MANDATORY: Authy hasn't made it mandatory to enter a master password to protect its desktop edition; without protection, this could be a safety concern. Entering a master password upon installation should be mandatory.

INITIAL INVESTMENT OF TIME: Getting Authy up and running takes some time, as you have to set up each of your accounts individually, authorizing the Authy application to generate 2FA tokens for each one.

WHO IT'S FOR

Authy has made it quite easy and manageable to have **2FA for single users, developers and businesses.**

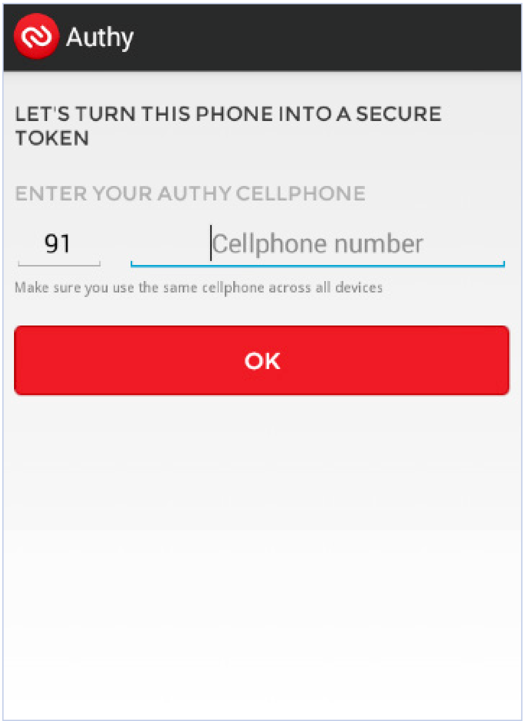
Authy has different pricing depending on which plan – Authentication, Phone verification or Phone intelligence — you choose. They have a **free plan for less than 100 authentications per month or a pay-per-use plan**. You will have to contact them for an Enterprise license price, which will vary depending on volume.



AUTHY

Two-factor Authentication

Strengthen — even replace — the traditional username and password login for websites, SaaS products, and mobile apps. Made easy for developers, businesses, and users.

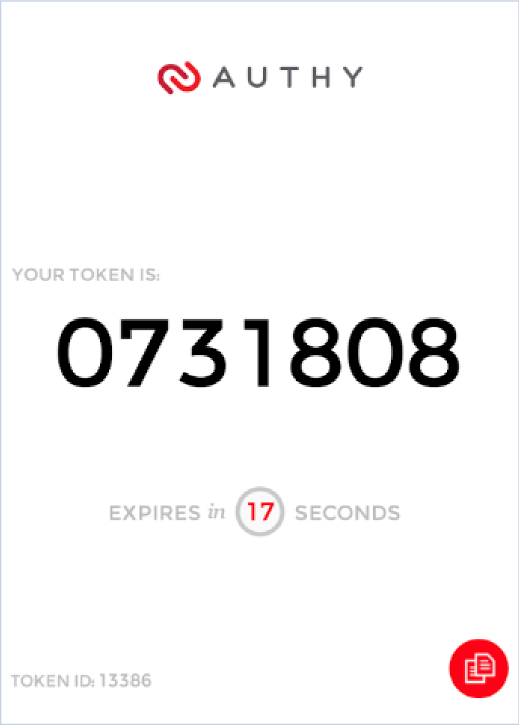


LET'S TURN THIS PHONE INTO A SECURE TOKEN

ENTER YOUR AUTHY CELLPHONE

91 Cellphone number

Make sure you use the same cellphone across all devices



YOUR TOKEN IS:

0731808

EXPIRES *in* 17 SECONDS

TOKEN ID: 13386

GET MORE INFORMATION ON AUTHY AT
https://authy.com/

yubico

YUBICO OFFERS YUBIKEY, WHICH IS A SMALL HARDWARE DEVICE THAT FEATURES 2FA WITH THE SIMPLE TOUCH OF A BUTTON.

WHAT WE LOVE

WORKS INDEPENDENTLY: Hardware keys like YubiKey have the great advantage of not relying on phone or network coverage, or anything else; no matter what, they just do their job.

ONE KEY TO SECURE UNLIMITED APPLICATIONS: There is no limit to the number of applications you can access from a single YubiKey. Just buy it once and use it as much as you want!

EXCELLENT SUPPORT FOR USERS: Yubico offers support via email or online support tickets. They also offer plenty of online support documents, which are available to download, as well as some open source software for developers.

EASE OF USE: YubiKey is incredibly easy to use. With a simple touch, it protects access to your computers, networks and online services. It's robust, small and never needs a battery.

The standard YubiKey USB authentication key starts at $40. Yubico also offers a FIDO U2F Security Key for $18.

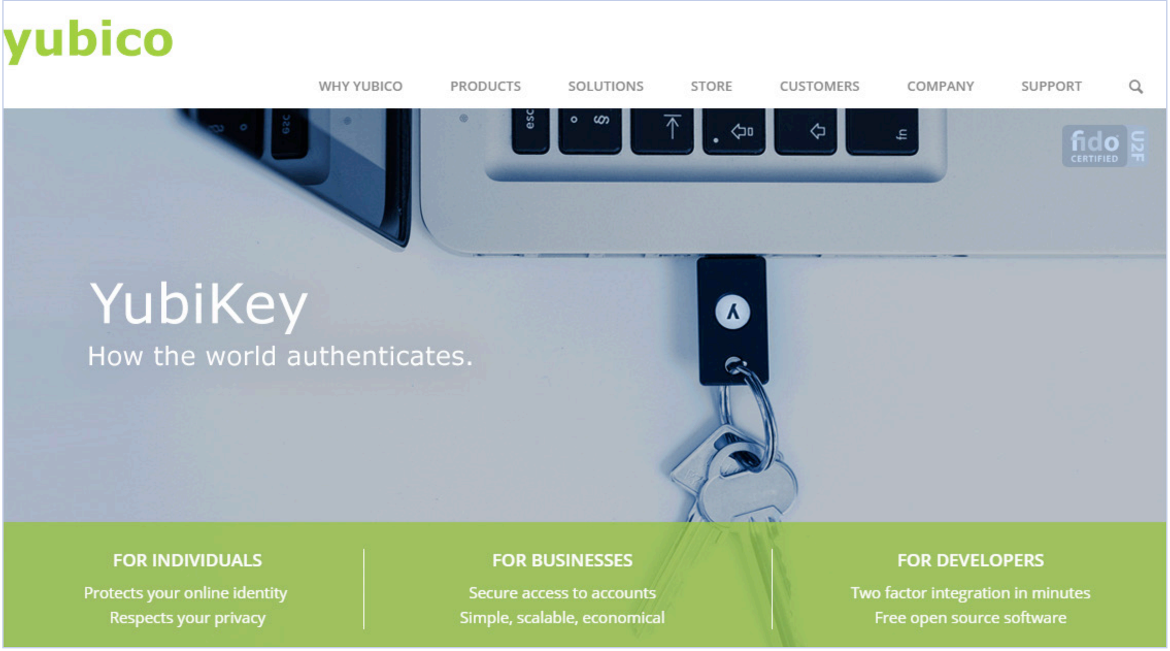
WHERE IT NEEDS IMPROVEMENT

SOME SITES ARE NOT REALLY SUPPORTED BY YUBIKEY: Yubico lists WordPress as being supported but the plugin for WordPress is not developed by Yubico. The plugin was coded by an individual and hasn't been updated in over two years, so it comes up with a security warning in the WordPress Plugin Directory. Yubico also lists Dashlane as being supported, but you will need a Premium or Business account for it to work. If you only have a free Dashlane account, YubiKey will not be supported.

EASY TO LOSE: The YubiKey is pretty small and some people find it hard not to lose one of these tiny gadgets.

WHO IT'S FOR

The YubiKey really is **for anyone and everyone**. It's built **strong enough for large companies**, while remaining **simple enough for single users**. Any organization considering 2FA should take a very close look at Yubico. It would even be the perfect solution for developers since Yubico offers open source software, documentation and tools.



YubiKey

How the world authenticates.

FOR INDIVIDUALS

Protects your online identity
Respects your privacy

FOR BUSINESSES

Secure access to accounts
Simple, scalable, economical

FOR DEVELOPERS

Two factor integration in minutes
Free open source software

GET MORE INFORMATION ON YUBICO AT

https://www.yubico.com/

DUO ENABLES USERS TO SECURE THEIR LOGINS AND TRANSACTIONS BY SELF-ENROLLING AND AUTHENTICATING THROUGH THEIR SMARTPHONES, THE DUO MOBILE APP, A LANDLINE, OR EVEN OFFLINE.

WHAT WE LOVE

ICLOUD BACKUP OF ALL YOUR INFORMATION: When enabling iCloud Backup, your Duo Mobile account information will be automatically backed up on your phone and can then be restored on the same device.

DUO PUSH: With Duo Push, you won't even have to copy numbers anymore. It is an out-of-band authentication method that prevents remote attackers from stealing your password. The app or website sends an authorization request directly to the application on your smartphone, which displays two buttons: Approve and Deny. From there, you simply tap "Approve" on the push notification sent to your phone.

INTEGRATES WITH ALMOST EVERYTHING: Duo 2FA can be integrated into websites, VPNs and Cloud Services. It can work with iPhones, Androids, Windows phones, Blackberries and personal computers..

ENDPOINT SECURITY: For organization, the Duo Platform Edition gives you advanced analytics to help you look into your users' devices and security health. This edition will even flag any out-of-date device software for you, giving you rapid insight into possible security risks.

WHERE IT NEEDS IMPROVEMENT

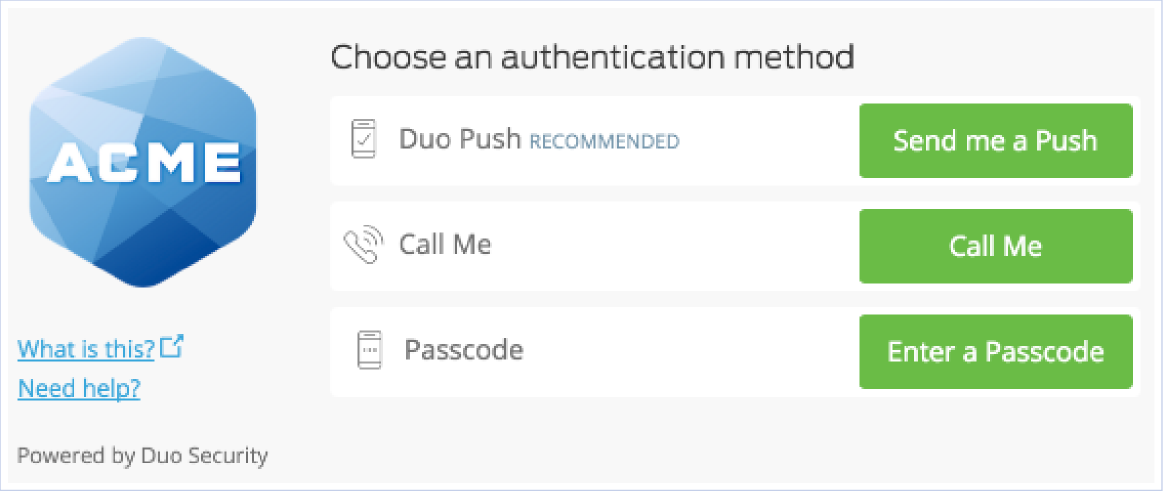
COUNTDOWN CLOCK: Duo could improve by integrating a countdown into their application. This would prevent users from being in the middle of typing the number in, only for it to suddenly change.

CONFIGURATION SYNC BETWEEN DEVICES: At the moment, there is no way to synchronize your configuration between devices. You have to configure each device separately if working with more than one.

WHO IT'S FOR

Duo's customers can easily range from **single users** to **small businesses** to **large corporations**. It is easy to use for the single user but still meets organizational security requirements and has a wide range of options (like Endpoint Security and group management) for larger organizations.

The **Personal license** (2FA for up to 10 users) is **completely free**; the **Business license is $1/user/month**; the **Enterprise license is $3/user/month**; and the **Platform license will cost you $6/user/month**.



Choose an authentication method

Duo Push RECOMMENDED — Send me a Push

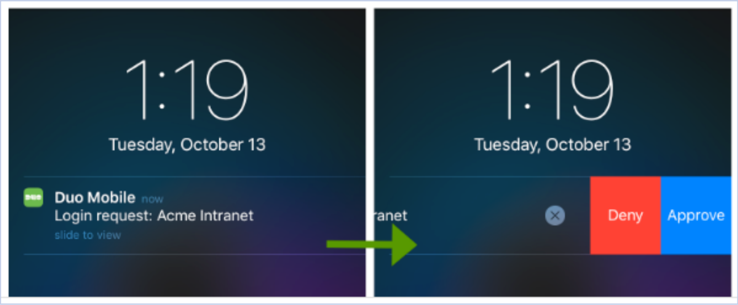
Call Me — Call Me

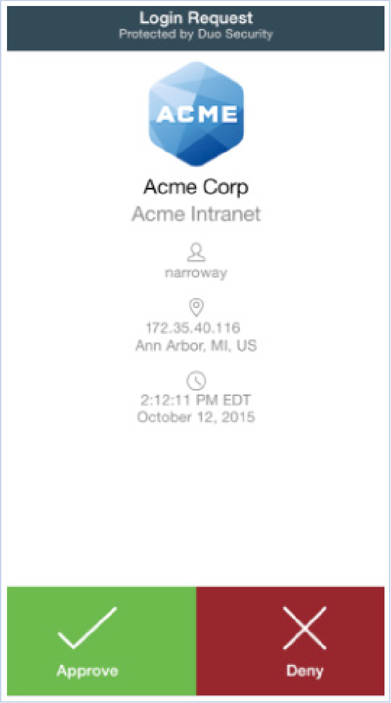
Passcode — Enter a Passcode

What is this?

Need help?

Powered by Duo Security





Login Request
Protected by Duo Security

Acme Corp
Acme Intranet

narroway

172.35.40.116
Ann Arbor, MI, US

2:12:11 PM EDT
October 12, 2015

GET MORE INFORMATION ON DUO AT
https://duo.com/

FreeOTP
Two-Factor Authentication

FREEOTP IS A FREE AND OPEN SOURCE TWO-FACTOR AUTHENTICATION APPLICATION. IT ADDS A SECOND LAYER OF SECURITY FOR YOUR ONLINE ACCOUNTS.

WHAT WE LOVE

EASY TO USE: Easily add tokens by simply scanning a QR-code or by entering the token configuration manually. No need to be tech-savvy to use this application.

FREEOTP IMPLEMENTS OPEN STANDARDS: FreeOTP implements the open standards, meaning there are no necessary proprietary server-side components. FreeOTP offers HOTP and TOTP integration.

LIGHTWEIGHT: Compared to some other 2FA applications that can be up to 6MB, FreeOTP actually takes up less than 500KB.

WORKS ON MULTIPLE ONLINE SERVICES: FreeOTP works great with multiple online services like Facebook, Evernote, Google, and GitHub (to name only a few).

WHERE IT NEEDS IMPROVEMENT

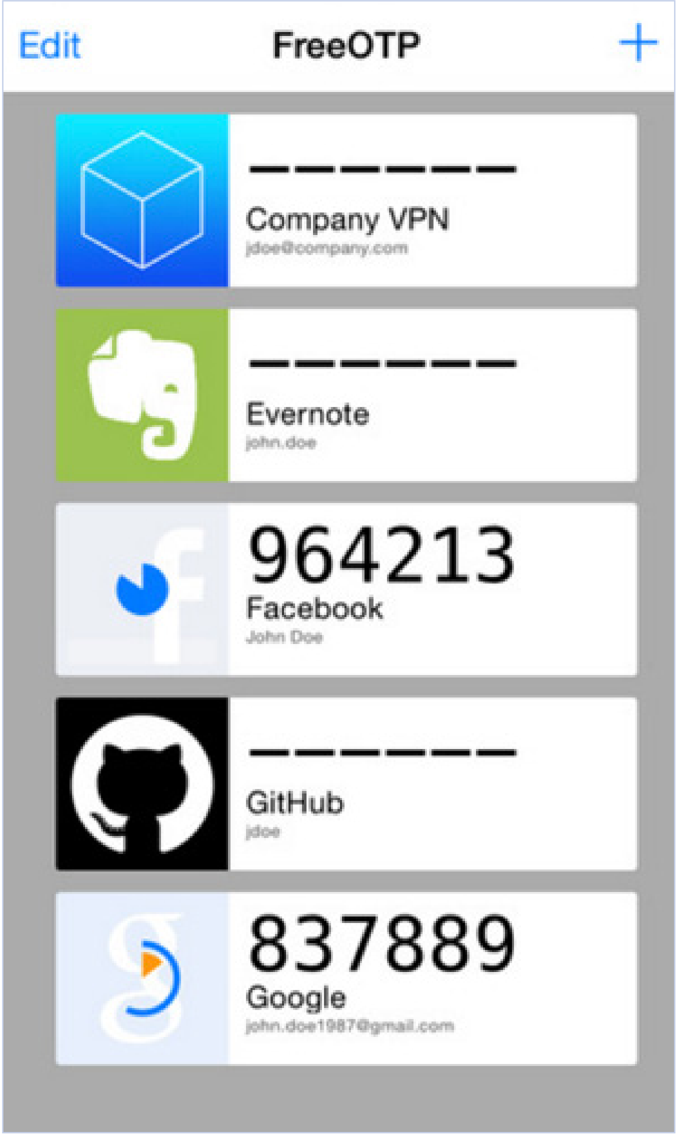
USER INTERFACE: The application definitely has some work to do to catch up with some other 2FA solutions. They would greatly benefit from a smoother interface, as at the moment it is underdeveloped and quite rustic.

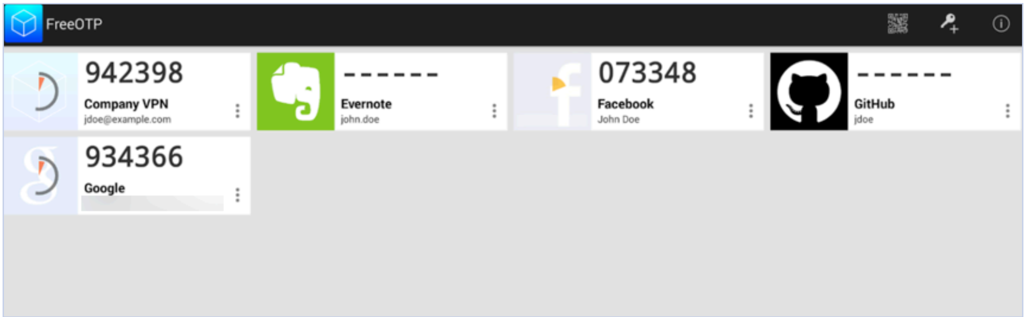
OFFERS NO BACKUP: They offer no backup and restore functionality, making you feel like all your eggs are in the same basket with nothing to keep them safe if something happens.

WHO IT'S FOR

FreeOTP is often used to **replace Google Authenticator**. It is mostly for **single users** and is best suited for users in need of a quick and easy app that's also a lightweight install.

The application is completely free.





GET MORE INFORMATION ON FREEOTP AT

https://freeotp.github.io/

AUTHENTICATOR PLUS OFFERS A HIGHLY SECURE 2FA SOLUTION WITH SEAMLESS SYNCHRONIZATION ACROSS DEVICES.

WHAT WE LOVE

HIGH LEVEL OF SECURITY: The account data is encrypted with 256-bit AES encryption and also a PIN lock for an extra layer of security. The data is encrypted and decrypted locally before any syncing is made – your password never has to leave your device and stays accessible only to you.

SYNC ACROSS DEVICES: Authenticator Plus offers smooth synchronization across multiple devices. The application is available for Android phones, tablets, iPhone, iPad, Android Wear and Apple Watch.

ORGANIZE: Easily position your frequently used accounts on top for quick access, group your different accounts by category and display account logos to find them with a glimpse of an eye.

AUTOMATIC BACKUP / RESTORE: Allows for automatic backup of your data to a cloud solution like Dropbox or Google Drive, which can then be easily restored.

WHERE IT NEEDS IMPROVEMENT

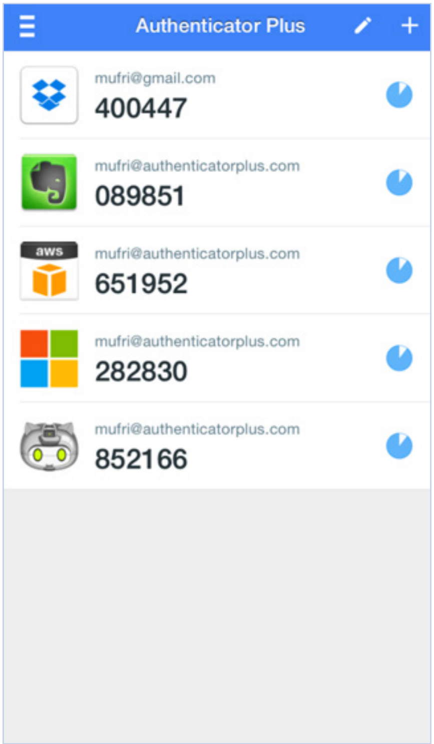
BARCODE SCANNER: Many users have mentioned compatibility issues when using the Authenticator Plus barcode scanner with either the Amazon Fire phone or the Kindle Fire. Authenticator will simply not recognize the barcode scanner.

SUPPORT: Authenticator Plus could highly benefit from more documentation and support.

WHO IT'S FOR

Authenticator Plus is for **everyone** in need of an extra layer of security on their smartphones and tablets. It is **quick and easy to use** for everyone.

They offer a free version but you could choose to pay a one-time fee of **$3,99** to access all the Authenticator Plus's Pro features.



Authenticator Plus

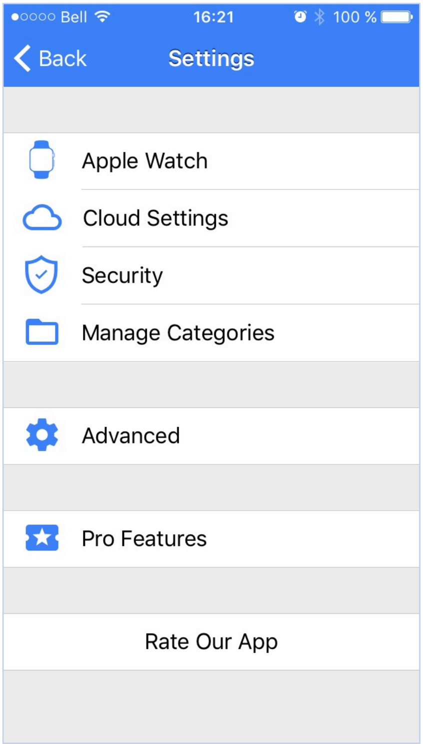
mufri@gmail.com
400447

mufri@authenticatorplus.com
089851

mufri@authenticatorplus.com
651952

mufri@authenticatorplus.com
282830

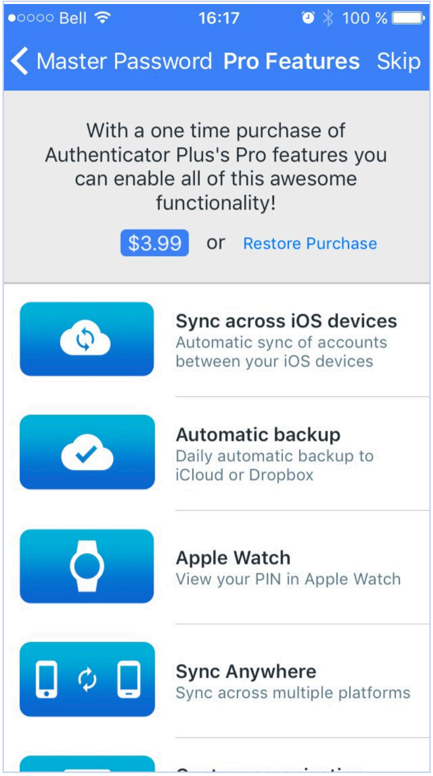
mufri@authenticatorplus.com
852166



< Back Settings

- Apple Watch
- Cloud Settings
- Security
- Manage Categories
- Advanced
- Pro Features

Rate Our App



< Master Password **Pro Features** Skip

With a one time purchase of Authenticator Plus's Pro features you can enable all of this awesome functionality!

$3.99 or Restore Purchase

Sync across iOS devices
Automatic sync of accounts between your iOS devices

Automatic backup
Daily automatic backup to iCloud or Dropbox

Apple Watch
View your PIN in Apple Watch

Sync Anywhere
Sync across multiple platforms

GET MORE INFORMATION ON AUTHENTICATOR PLUS AT

https://www.authenticatorplus.com/

Sound Login

SOUNDLOGIN IS A TWO-FACTOR AUTHENTICATION THAT RELIES ON SOUND TO GENERATE ONE-TIME CODES.

WHAT WE LOVE

EASY-TO-USE: SoundLogin simplifies the 2FA process by relying on an audio frequency. Simply click on the one-time code button on the mobile application which will play a short notification sound containing an encoded OTP. The browser then captures the sound, decodes it and automatically fills in the form on the website. No more manual entering of one-time passwords.

SECURE SOLUTION: Since the OTP is carried out locally by the sound wave, no account data is transferred over the Internet, making it safe from remote attack since no one can intercept your one-time password.

EXTRACT OTP: The application provides the option to extract one-time passwords from SMS messages and then send them to the browser via sound notification automatically or after user confirmation.

INNOVATIVE TECHNOLOGY: The SoundLogin mobile application by itself acts as a Google Authenticator or FreeOTP application, and is fully compatible with these applications. It is a new technology that is still a little glitch, but it's worth looking at for the novelty of alone.

WHERE IT NEEDS IMPROVEMENT

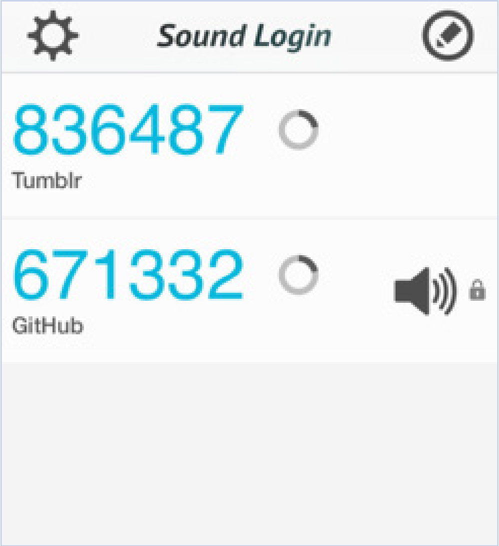
STILL A WORK-IN-PROGRESS: SoundLogin is still pretty rough around the edges. With small glitches and occasional inaccurate code, at the moment it's not ideal to have it as your only 2FA solution.

SUPPORT: They offer no real documentation or support for the application. All they have is a contact form that you have to fill in to get more information about the SoundLogin solution.

WHO IT'S FOR

SoundLogin is for **everyone** who is intrigue by new technology, any single user who loves to try out new gadget will want to give this a try.

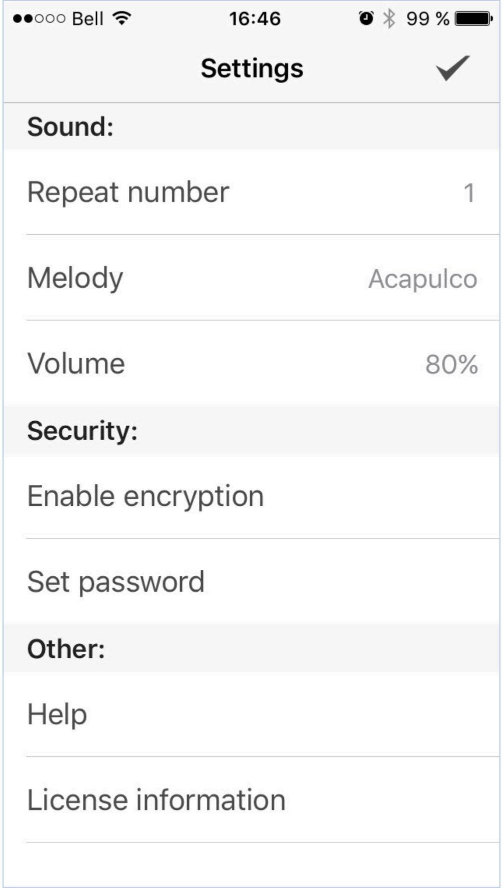
SoundLogin is **completely free** for download on Google play, Amazon or on the App Store.



Sound Login

836487
Tumblr

671332
GitHub



●●○○○ Bell 16:46 99 %

Settings ✓

Sound:

Repeat number 1

Melody Acapulco

Volume 80%

Security:

Enable encryption

Set password

Other:

Help

License information

600526
One-time password is entered automatically
Enter one-time password
* * * * * *
600562
One-time password

SoundLogin app generates code and sends it to your browser

GET MORE INFORMATION ON SOUNDLOGIN PLUS AT

https://www.soundlogin.com/

CONCLUSION

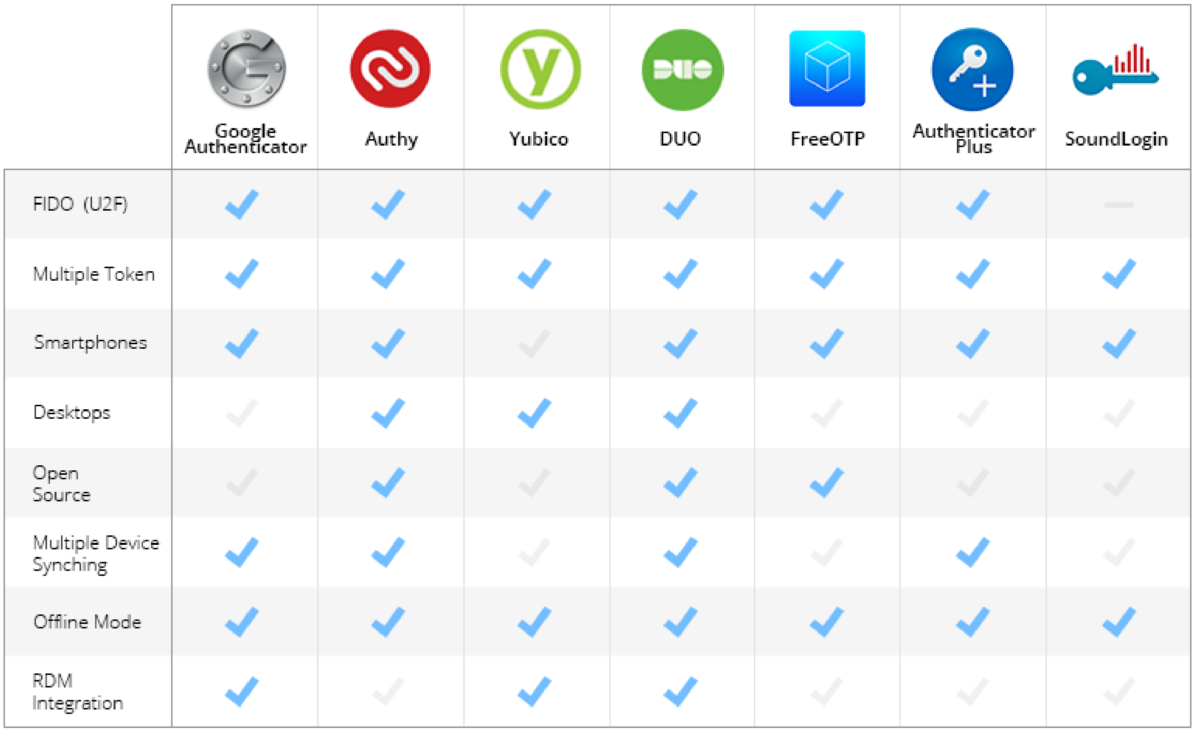
Since 2FA can render hacker attacks much less threatening since accessing passwords is not enough anymore to access your information; and it is pretty unlikely that the attacker would also have the physical device associated with the user account. More layers of authentication makes a system more secure.

Any of these four apps would do a great job in providing that extra layer of protection. All of them support mobile tokens, have different levels of flexible authentication methods, and some will even provide you with advanced analytics. They differ, however, when it comes to pricing, packaging offers, and ability to comprehend and act on the diverse product reports. Surely, these four should be in the starting lineup for any individual or enterprise in the market for a great 2FA.

We concentrated this blog more towards user oriented 2FA, however there are other beasts out there that are more enterprise driven like AuthAnvil or SafeNet only to mention a few. Devolutions Server actually incorporates those solutions such as: AuthAnvil, SafeNet, Azure MFA and Radius. Maybe one day will do a comparison with those ones...maybe...

Let's not forget that 2FA comes in all sizes and flavors and you need to know as much about multifactor authentication as possible before choosing the right one for you.

HERE IS A TABLE FOR A QUICK OVERVIEW OF SOME ADVANCED OPTIONS SUPPORTED BY THE DIFFERENT 2 FACTOR AUTHENTICATION APPLICATIONS.



	Google Authenticator	Authy	Yubico	DUO	FreeOTP	Authenticator Plus	SoundLogin
FIDO (U2F)	✓	✓	✓	✓	✓	✓	—
Multiple Token	✓	✓	✓	✓	✓	✓	✓
Smartphones	✓	✓		✓	✓	✓	✓
Desktops		✓	✓	✓			
Open Source		✓		✓	✓		
Multiple Device Synching	✓	✓		✓		✓	
Offline Mode	✓	✓	✓	✓	✓	✓	✓
RDM Integration	✓		✓	✓			