Acronis

WHITEPAPER

The Important Role of Two-factor Authentication in Cyber Protection for Businesses

Your guide to multilayered defense

By the end of 2021, businesses will be hit by ransomware every 11 seconds. Phishing and spear-phishing continue to be the number one infection vector and administrators are quite often the target. Of course, in many large organizations the administrators that control resources and access to data are well aware of these threats and can avoid this trap. In many small- to medium-businesses it's much more of an issue for admins. And, when admins seem difficult to compromise, cybercriminals can still attack users with higher privileges and then escalate to the admin level where they can do serious, lasting harm.

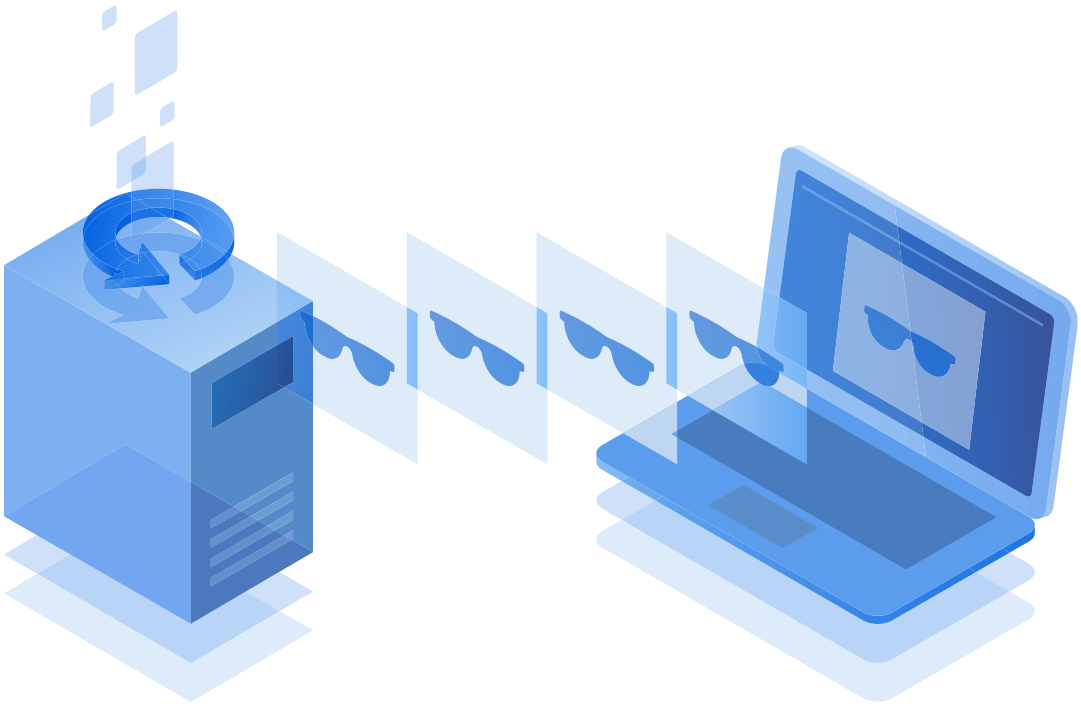
In ransomware incidents and other kinds of extortion attacks (currently one of the most serious threats for businesses) cybercriminals encrypt business critical data and delete the backups that would serve as a method of recovery. They then demand a ransom to decrypt data with the threat that, if the ransom is left unpaid, all the encrypted data, applications, and systems will be deleted. They can do many other malicious things once embedded in an organization's network, but this is one of the most common attack scenarios and it's on the rise – ransomware incidents increased 50% in the second half of 2020 over the first six months.

Ransomware attacks like these typically start with stolen admin access credentials: login and password.

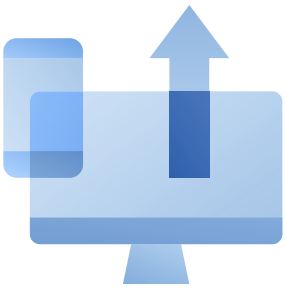
We're assuming here that the company in question follows a good password strategy – passwords are strong and can't be brute-forced unnoticeably. After getting the required credentials, a cybercriminal can access various resources and execute operations to achieve their malicious goal.

While still very common security features, basic login and password credentials are no longer enough to protect business-critical data.

That's why, for the past several years, sensitive data has been protected by two-factor authentication (2FA) access.



What is two-factor authentication and why is it important?



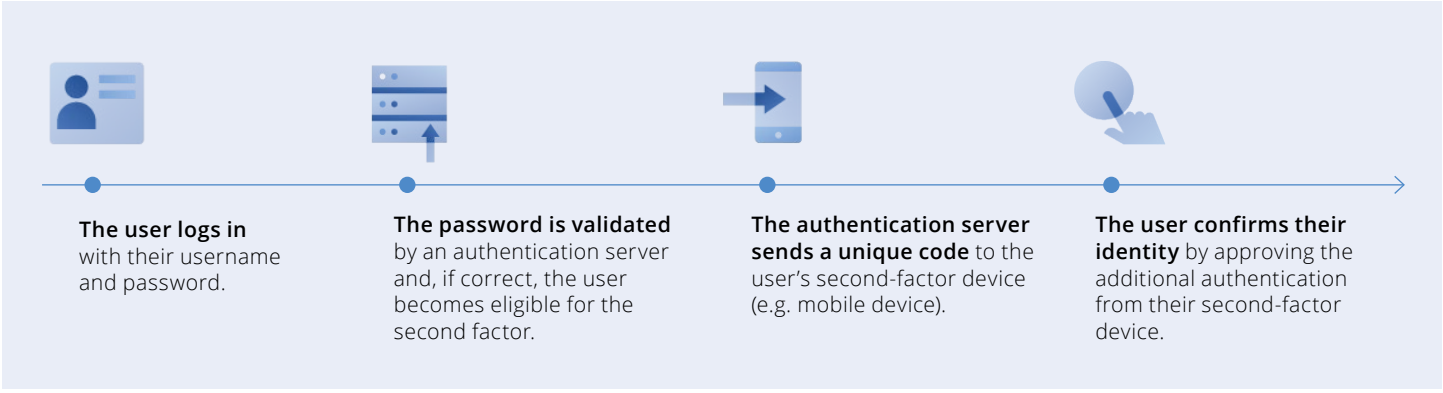
Two-factor authentication is a type of multi-factor authentication that provides extra protection from unauthorized access to your account by checking a user's identity with a combination of two different factors:

- **Something that a user knows (PIN or password)**
- **Something that a user has (token)**
- **Something that a user is (biometrics)**

Anyone who uses online banking, any well-known email provider, messengers, and many other web or mobile services should be familiar with this system. 2FA is widely used in security because it quite effectively neutralizes the risks associated with compromised passwords. If a password is hacked, guessed, or phished as we explained above, it's no longer enough to give a criminal access.

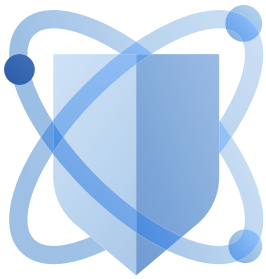
While many second factors can be used, one of the most popular is a Time-based One-Time Password (TOTP). Typically generated by a mobile app, this is a one-time-use password that expires quickly.

When it's used, a 2FA transaction works like this:



As we know, there is no way to guarantee 100% security and 2FA is not an exception. An account can still be vulnerable via hacking through password recovery options, but these options are controlled in a business environment so the vulnerability primarily affects home users. Lost password recovery functionality of any service usually resets your password via email, completely bypassing 2FA. That's why email accounts should always be monitored for messages requesting password changes.

Acronis 2FA combined with multilayered protection saves the day



The Acronis Cyber Cloud platform supports Time-based One-Time Password (TOTP) authentication. If the TOTP authentication is enabled in the system, users will need to enter their traditional password and the one-time TOTP code to access the system. The TOTP code is generated in the authentication application on a user's second-factor device based on the current time and the secret code (QR-code or alphanumeric code) provided by the platform.

Two-factor authentication is set up on the organizational level. You can enable or disable it:

- For your own organization.
- For your child tenant *(only in cases where the support access option is enabled within that child tenant).*

All of your organization's users must install an authentication application on their second-factor devices (mobile phones, laptops, desktops, or tablets). The recommended authenticators:

- Google Authenticator
- Microsoft Authenticator

It's important that users ensure that the time is set correctly on the device with the installed authentication application. Most 2FA apps will only work on one device at a time to add more security to this approach. Acronis engineers are also prepared to defend against brute-force attacks: when an intruder tries to get access to the system by submitting many passwords, with the hope of guessing one correctly.

The brute-force protection mechanism of the Acronis Cyber Cloud platform is based on device cookies. The settings for brute-force protection that are used in the platform are pre-defined:

PARAMETER	ENTERING THE PASSWORD	ENTERING THE TOTP CODE
Attempt limit	10	5
Attempt limit period *(the limit is reset after timeout)*	15 min (900 sec)	15 min (900 sec)
Lockout happens on	Attempt limit + 1 (11th attempt)	Attempt limit
Lockout period	5 min (300 sec)	5 min (300 sec)

Enabling two-factor authentication made easy

Setting up 2FA with Acronis Cyber Cloud is easy. Assuming every user installed Google Authenticator on their phone, admins should do the following:

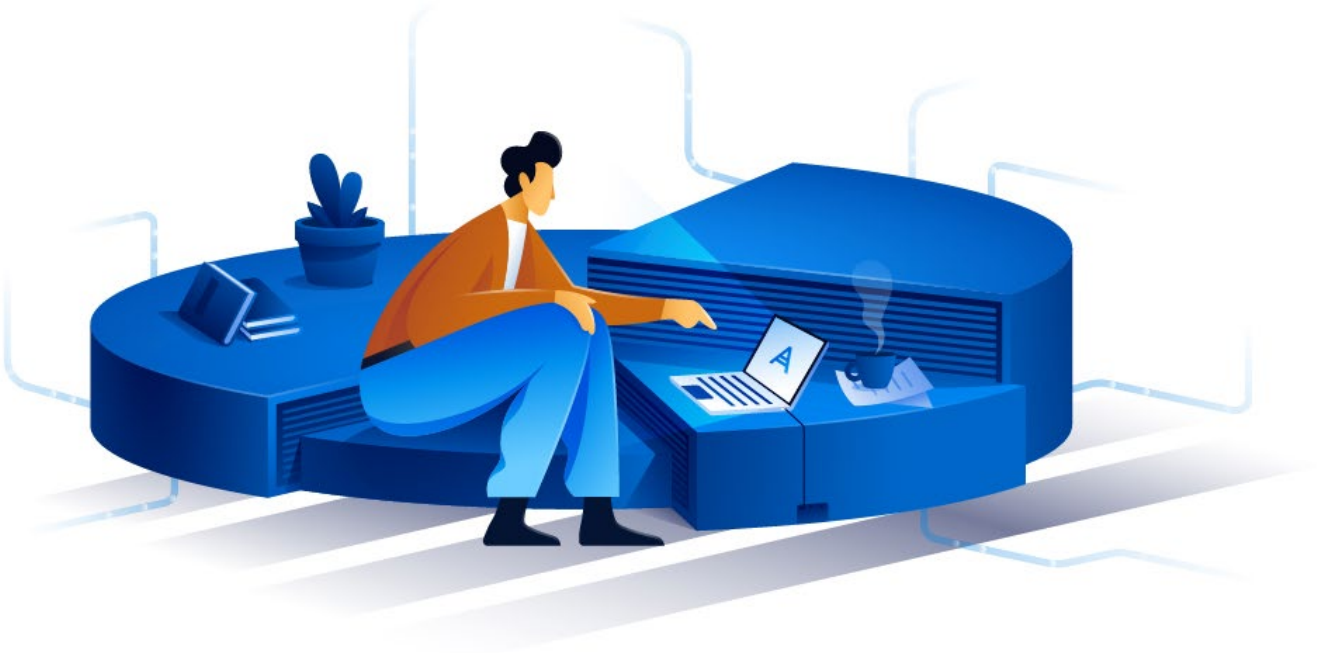
- In the management portal, go to Settings > Security.
- To enable two-factor authentication, turn on the slider. To confirm, click Enable.

After that, users will be prompted to enter the login, password, and TOTP code to log in to the system. On the Users tab, the 2FA status column will appear. You can track which users have set up two-factor authentication for their accounts.

The admin may need to enable two-factor authentication for specific users for whom it was previously disabled.

- In the management portal on the Users tab, find a user for whom you want to change the settings, and then click the ellipsis icon.
- Click Mark as a regular account. As a result, the user will have to set up two-factor authentication or provide the TOTP code when entering the system.

Before enabling it for every user, you may want to pilot it on selected ones if you have concerns.



An important part of a multilayered defense

While Acronis Active Protection protects users of Acronis Cyber Cloud, Acronis Cyber Backup, and Acronis True Image from ransomware, it's important to understand that this technology alone isn't enough to combat all the cyberthreats that face business and home environments if security measures like two-factor authentication and access restriction aren't in place. If cybercriminals are able to compromise an admin who controls security posture settings, Acronis Active Protection can be maliciously disabled for user machines and, potentially, data may be encrypted after that.

Acronis Active Protection is a multilayered security technology that not only detects ransomware through behavioral heuristics, but also analyzes the stack trace of executable Windows processes with the help of a machine learning model with self-defense capabilities. These capabilities prevent malicious actors from disabling or compromising Acronis agent processes running under the Windows operating system.

2FA adds another essential layer of protection here, which ensures that Acronis Active Protection can work properly and minimizes the chance of an entire organization hack thanks to the 2FA authenticator app on users' mobile devices.