GRIDINSOFT

HELP CENTER

OFFICIAL SUPPORT GUIDE

M

Multi-Factor Authentication (MFA): Methods and Setup

Learn which authentication factors count as MFA, why passkeys and security keys resist phishing, and how to set up recovery safely.

PUBLISHER

Gridinsoft Support

UPDATED

Oct 8, 2026

READ TIME

4 min

CONTENTS

In this guide

01 The three authentication factor categories

02 MFA methods from strongest to weaker

03 What is an MFA code?

04 How to enable MFA safely

05 MFA fatigue and phishing-proxy attacks

06 Passkeys, passwordless login, and MFA

07 MFA deployment for organizations

08 What to do after an unexpected MFA prompt

09 MFA is a layer, not a complete defense

Multi-factor authentication (MFA) requires evidence from at least two different factor categories before granting access. It reduces the chance that a stolen password alone can compromise an account.

Two steps are not always two factors. A password plus a security question both rely on information the user knows. Strong MFA combines independent factors and protects enrollment, recovery, and session tokens as carefully as the login itself.

01 The three authentication factor categories

- **Something you know:** a password or PIN.
- **Something you have:** a security key, registered phone, smart card, or authenticator.
- **Something you are:** a biometric characteristic used through a trusted device.

Location, device health, and behavior can influence risk decisions, but they are not automatically independent authentication factors.

02 MFA methods from strongest to weaker

FIDO2/WebAuthn security keys and properly implemented passkeys use public-key cryptography bound to the legitimate site, making them resistant to ordinary credential-phishing pages. Certificate-based smart cards can also provide strong phishing resistance.

Authenticator-app codes are broadly useful but can be relayed through a live phishing proxy. Push notifications are vulnerable to approval fatigue unless the user verifies context; number matching is safer than a simple approve button. SMS and voice codes improve on password-only access but face SIM-swap, interception, and social-engineering risks.

03 What is an MFA code?

An **MFA code** is a short, usually one-time verification code used as one step of a multi-factor login. It may be generated by an authenticator app or delivered by text, email, or a hardware token. The code is not the whole MFA system and should never be given to someone who calls,

messages, or emails asking for it.

A code proves possession of the device or channel only for that challenge. It can still be stolen by a real-time phishing page, so security keys and passkeys provide stronger phishing resistance when available.

04 How to enable MFA safely

1. Start with primary email, password manager, financial, cloud, and administrator accounts.
2. Open the service through a bookmark or typed address, not an enrollment link from email.
3. Register at least two strong authenticators when supported.
4. Store recovery codes offline in a protected location.
5. Remove old phone numbers, devices, app passwords, and unused authenticators.
6. Test recovery before an emergency and enable login alerts.

05 MFA fatigue and phishing-proxy attacks

Attackers may send repeated push requests and call the victim pretending to be support. Deny any request you did not initiate and report it; repeated prompts can mean the password is already known. A phishing proxy can capture a password, one-time code, and resulting session cookie in real time. Phishing-resistant authentication prevents the authenticator from signing in to the attacker’s look-alike domain.

06 Passkeys, passwordless login, and MFA

A passkey is a credential based on public-key cryptography and unlocked on a device, often with a PIN or biometric. Whether a passkey satisfies one or multiple factors depends on its implementation and the service’s policy. “Passwordless” describes the user experience, not automatically the assurance level. Protect account recovery and synced passkey accounts with equally strong controls.

07 MFA deployment for organizations

Require MFA for remote access, email, cloud consoles, and privileged actions; prioritize phishing-resistant methods for administrators and sensitive users. Block legacy authentication paths that bypass MFA, monitor enrollment changes and failed challenges, and issue managed recovery procedures. Keep emergency accounts tightly controlled, monitored, and tested.

08 What to do after an unexpected MFA prompt

Deny the request, do not share a code, and open the service independently. Change the password if it may be exposed, revoke active sessions, review recovery details and registered authenticators, and check for malicious forwarding rules or connected apps. Contact support through an official channel if access was lost.

09 MFA is a layer, not a complete defense

MFA cannot prevent every session theft, malicious OAuth grant, compromised endpoint, or insider action. Combine it with unique passwords, secure recovery, device updates, least privilege, and monitoring. Even a weaker second factor is generally better than password-only access, but migrate high-risk accounts to phishing-resistant methods.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com