HELP GUIDE

Step-Up Authentication

Heighten security measures for high-risk transactions.

AUTHENTICID

Protecting against fraud threats throughout the user journey poses a significant challenge. Insufficient systems and vulnerabilities in processes provide an opportune playground for fraudsters. However, by implementing step-up authentication, the risk of a breach by a malicious actor is minimized, thereby strengthening your overall security posture.

What is Step-Up Authentication?

Step-up authentication is the process by which users are asked to provide additional proof of identity before accessing resources or performing specific actions in an application or system. Step-up authentication is usually implemented as part of an authentication process that matches the assurance level of authentication with the risk level of any request, which balances user friction and system security.

How does Step-Up Authentication Improve the Client Experience?

Step-up authentication aims to enhance the user experience by implementing additional verification **only** when it's absolutely essential. Unlike standard static multi-factor authentication, which necessitates extra steps for every sign-in or specific action, step-up authentication primarily strengthens security measures in high-risk scenarios.

Consequently, for most routine actions, users can enjoy a smooth and seamless experience without the need for cumbersome security measures. However, in situations involving more sensitive procedures like modifying personal information or conducting substantial transactions, users can appreciate the heightened level of safeguarding, reassuring them that their accounts and data remain secure.

AUTHENTICID

Where is Step-Up Authentication Used?

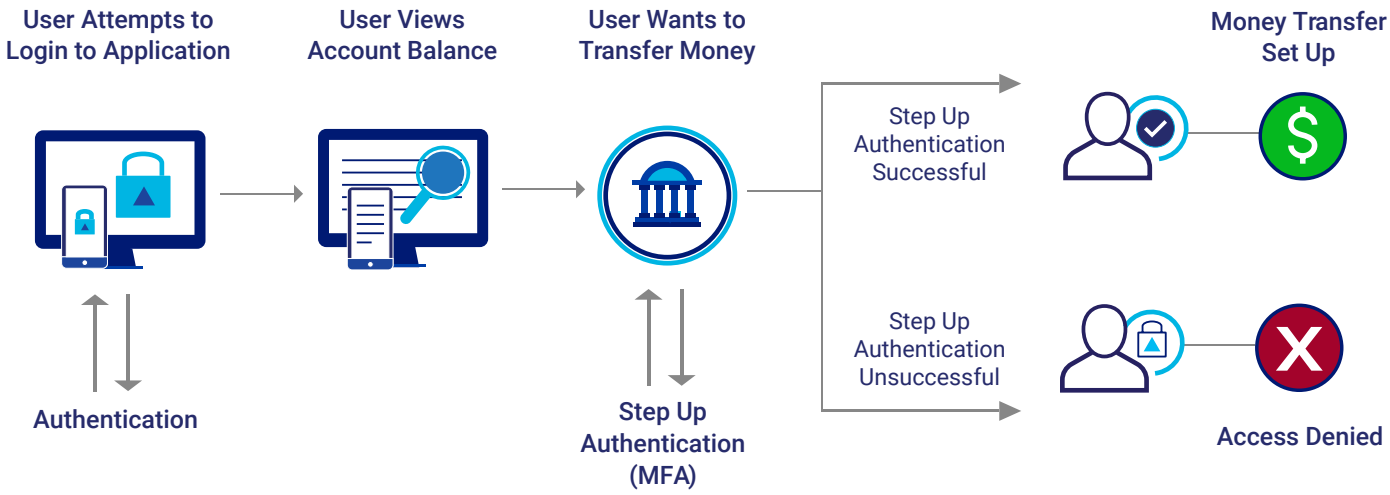
Use step-up authentication to ensure that access to the most sensitive resources, data, or actions has a stronger authentication mechanism. When implemented, step-up authentication can provide a seamless user experience while protecting both identities and your organization. There are a number of activities that can trigger step-up authentication:

Trigger Events

Wrong Login Credentials	When a user has multiple entries of incorrect login credentials, step-up authentication can be triggered via sending a link via text or email to reset a password or by requiring biometric verification.
Changing Account Details	Requests to change contact information or personal information on user accounts, or if a user is logging in from a new location, can require step-up authentication to keep accounts and identities safe.
Major Financial Transaction Attempts	In financial institutions, basic, low-risk user actions most likely do not require additional authentication measures. But when a customer attempts to make a larger-than-normal purchase or withdrawal, or an attempt to transfer funds, step-up authentication can be triggered to prove you are the owner of the account.
Access to Sensitive Company Data	Users may have different levels of access for system or company resources, and accessing a more sensitive data set or company-altering data can trigger this process.
Data Viewing vs. Data Editing	Providing a user the ability to view versus edit their data or credentials can trigger step-up authentication if the data is at higher risk of fraud or identity theft.
Privilege Content Access	Membership and payment-based resources can use step-up authentication for materials access, especially for online publications or subscription services.
Unfamiliar Login Location	Users logging in from an unusual location or a location they haven't been to can trigger step-up authentication, especially if a transaction is involved.

AUTHENTICID

Step-Up Authentication (Sample Workflow)



What Industries Should Use Step-Up Authentication?

Step-up authentication should be used in any industry that has a high-risk of identity fraud coupled with sensitive resources. These industries include finance, healthcare, government services, and ecommerce.

Organizations can use step-up authentication to meet compliance requirements or follow internal security policies.

How is Step-Up Authentication Different from Multi-Factor Authentication?

Multi-factor authentication (MFA) is when users are asked to provide multiple forms of authentication to prove their identity when higher levels of assurance are required. Since step-up authentication requires users to produce an additional form of authentication, it thus utilizes MFA and MFA techniques.

Use step-up authentication with MFA for additional layers of authentication.

AUTHENTICID

Step-up authentication balances enterprise security with necessary, high-risk accessibility for users.

How Can Step-Up Authentication be Implemented?

Step-up authentication can be enabled using a number of authentication methods. They are typically divided into three categories:

Something you know: (Knowledge) A piece of information only you should know, like a password or PIN.
Something you have: (Possession) A unique object only you should have access to, like a phone or token.
Something you are: (Inherence) Something that identifies who you are, like a fingerprint or facial recognition.

1 KNOWLEDGE FACTOR

Something you know

Password

Security Question

2 POSSESSION FACTOR

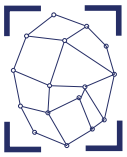
Something you have

Smartphone

Hardware Token

3 INHERENCE FACTOR

Something you are



Facial Recognition

Fingerprint

Not all authentication methods are created equal. Each method carriers a different security level. Utilizing facial biometric authentication, otherwise known as a taking a selfie, in combination with liveness detection typically offers a higher level of security. This combination can ensure the person taking the selfie is actually present and stop the most sophisticated spoofing attempts.

To learn more about identity verification and next-gen authentication tools, visit AuthenticID.com or schedule a demo.