INSTASAFE MULTI-FACTOR AUTHENTICATOR

GUIDE BOOK

InstaSafe Multi Factor Authenticator

Multi-factor authentication (MFA) is a comprehensive strategy for enhancing the security of both physical and logical access. In this approach, users are mandated to provide a combination of two or more distinct authenticators to confirm their identity during the login process. The use of MFA enhances overall security by ensuring that even if one authenticator is compromised, unauthorized individuals cannot fulfill the second authentication requirement, preventing access to the designated physical area or computer system.

The Importance of Multifactor Authentication:

Given the increasing frequency of cyber attacks, there is an indispensable need for maintaining and preserving trust across online setups. With the constant evolution of business processes, the necessity of a defensive strategy that focuses on both identity and data components of security becomes imperative.

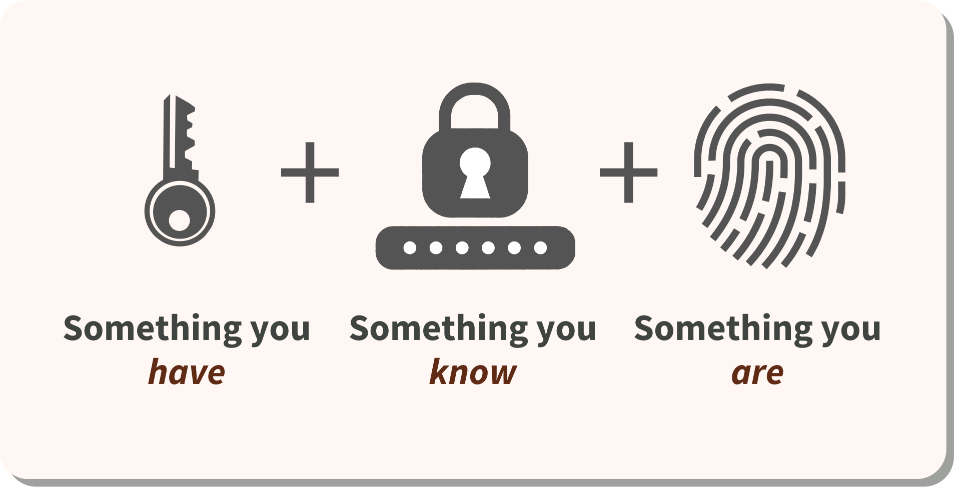
However, with the advent of an increasingly risky business environment, authentication processes have become cumbersome, while not assuring the same level of flexibility with regards to the factors of authentication being deployed.

InstaSafe Authenticator aims to transform the security paradigm through proven authentication capabilities that secure your systems with an additional layer of security, while having features suited for rapid and broad deployment on scale. With a user friendly and flexible authentication interface, companies can improve their security posture and leverage the security benefits of multifactor authentication.

How Multifactor Authentication Works:

Multi-Factor Authentication is based on a set of 3 primary factors:

- Something you are
- Something you have
- Something you know



Something you *have* + **Something you *know*** + **Something you *are***

The first question pertains to your identity verification. The second pertains to a mobile device or a laptop with an email you have that can help validate your identity. The third pertains to a password or code that you know. A combination of multiple authentication factors results in a more secure system. A single layer of authentication like a password becomes a liability since passwords have become so complex that users often tend to use a similar set of passwords for all their credentials, making it easy for hacking techniques like brute force attacks to exploit these vulnerabilities successfully.

InstaSafe MFA methods

InstaSafe Authenticator follows different types of Authentication methods-

- OTP via SMS and Email
- Time-Based OTP
- mPIN
- Biometrics Authentication - Facial and Fingerprint
- Push Notification
- Hardware Token

Instasafe Authenticator capabilities includes:

- *Integrate with Any VPN*: InstaSafe Authenticator can integrate with any VPN or remote gateway
- *FIDO Compliant: compatible with any FIDO compliant security hardware key*
- *Supports major authentication protocols: It supports RADIUS, TACACS, OAUTH and SAML Authentication protocols*
- *Passwordless Authentication: Mobile app with various authentication methods available*

Key InstaSafe Authenticator Features:

Continuous Facial Authentication

User can get authenticated to the application using their live face. Continuous facial authentication further checks the liveness of the user by monitoring the face every 30secs. If the user moves out from the frame of device screen or any third person comes infront of the device screen, the application gets automated logged out. This authentication mechanism is helpful for very sensitive business applications.

FIDO Authentication

FIDO (Fast Identity Online) is an Open and standardized authentication protocols developed by FIDO alliance aims to eliminate the password problem of authentication and Man in the middle attack associated with MFA hacking. FIDO authentication is based on public key crytography. FIDO allows users to sign in using passkeys. Passkeys are stored locally on the devices with the biometric information.

RADIUS Authentication

RADIUS is a client-server networking protocol that enables centralized authentication and authorization for a remote network. InstaSafe controller can act as a RADIUS server while prompting for MFA. Radius supports a variety of authentication methods, including PAP (Password Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol), EAP (Extensible Authentication Protocol), and more.

TACACS Authentication

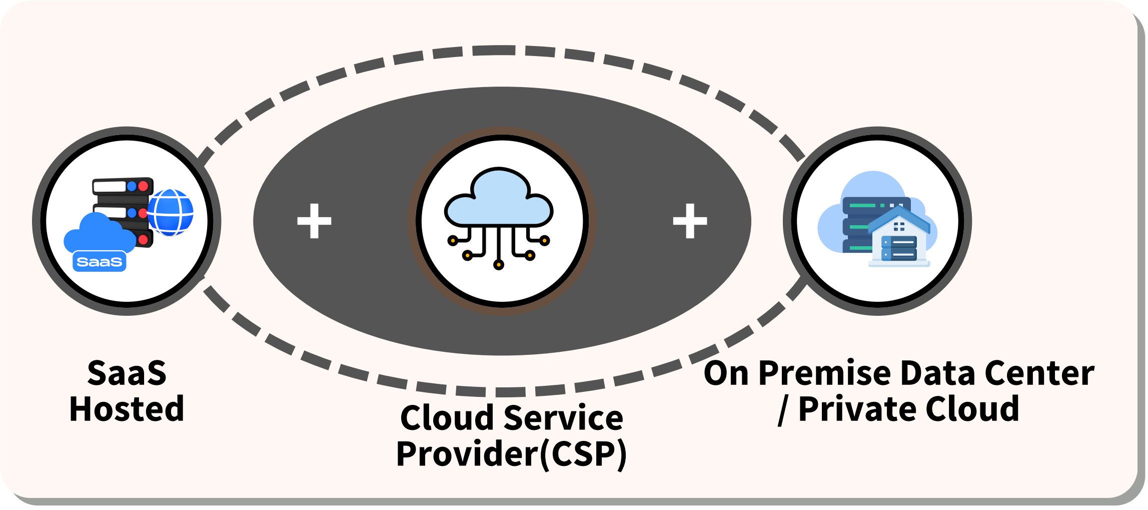
TACACS is a network security protocol that provides centralized authentication, authorization, and accounting services to access network devices and services. TACACS provide additional security feature compared to RADIUS as it uses a separate encryption key for each services. TACACS is associated with CISCO networking equipment and used to secure access to CISCO devices. InstaSafe controller can act as a TACACS server and enable authentication.

Windows Login

Windows Login is a simplified, secure authentication solution that improves the logon security of Windows Desktops, Servers, and Windows Terminal Servers, ensuring a secure login experience for your users. InstaSafe Authenticator can improve security posture by adding an additional factor of authentication when logging into Windows systems.

Deployment Methods

InstaSafe authenticator can be deployed in both public cloud and on-premises data center.


SaaS
+
+
SaaS Hosted
Cloud Service Provider(CSP)
On Premise Data Center / Private Cloud

About InstaSafe

InstaSafe's mission is to secure enterprises from the abuse of excessive trust and privilege access. We empower organizations across to globe in preparing their security infrastructure for digital transformation in a cloud-dominated world. Recognized by Gartner as one of the top representative vendors providing Zero Trust Security, InstaSafe Secure Access, InstaSafe Zero Trust Application Access, and InstaSafe Authenticator follow the vision that trust can never be an entitlement, to offer securely enhanced and rapid access of enterprise applications to users situated anywhere across the globe. We secure 500,000 endpoints for more than 150 customers, spread across 5 continents, with our 100% cloud-delivered solutions, ensuring that our offerings are in line with our mission of being Cloud, Secure, and Instant.

Problems? Talk to us

Let's talk more about how InstaSafe can empower your remote workforce through transformational and seamless security.

✉ sales@instasafe.com   www.instasafe.com

You can connect us at:

/instasafe   /instasafe   /instasafe   /instasafeZT