InstaSafe
Cloud. Secure. Instant.

INSTASAFE WINDOWS AUTHENTICATION

InstaSafe Windows Authentication

InstaSafe Windows Authentication provides protection from account compromise through the use of weak or stolen passwords by adding an additional layer of security to existing security postures – whether they were obtained through phishing or brute force attacks.

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 Windows Authentication 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:

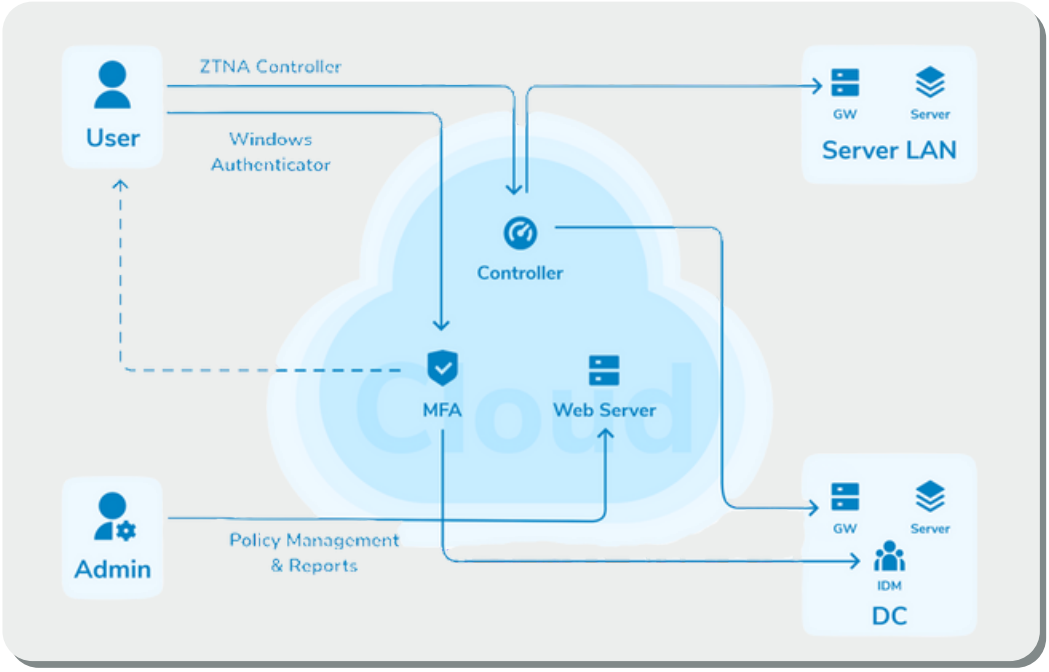
The first question pertains to your identity verification. The second pertains to a mobile device or a laptop with an email you have that can help validate your identity. The third pertains to a password or code that you know. A combination of multiple authentication factors results in a more secure 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 successfully exploit these vulnerabilities.

Introducing InstaSafe Windows MFA

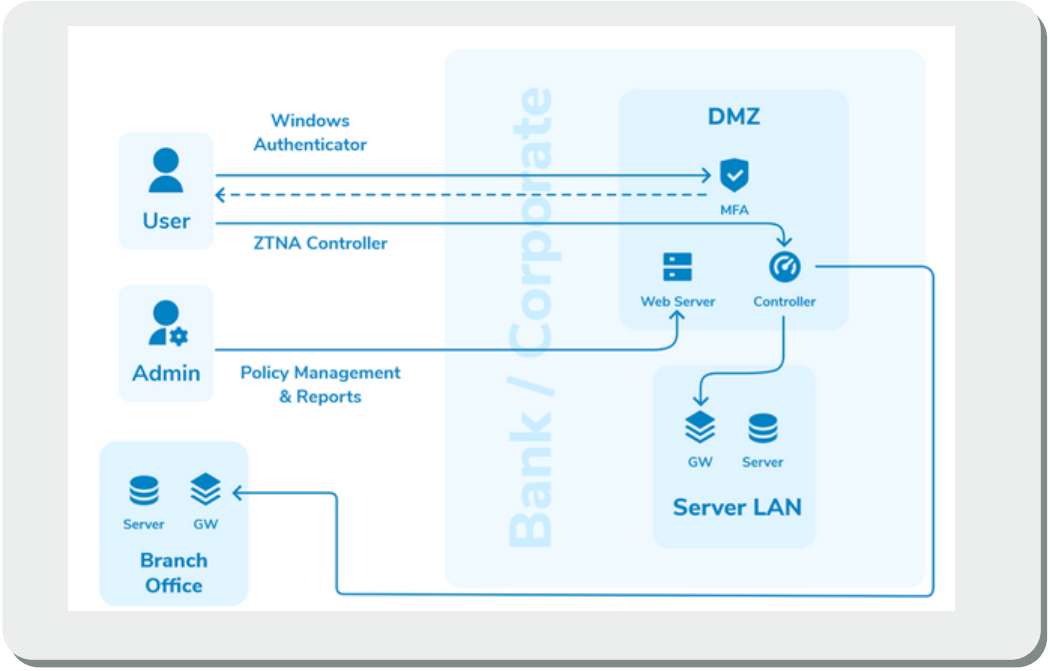
MFA powered by InstaSafe adds an additional layer of cloud-enabled Multifactor Authentication system to your security infrastructure to secure networks from account compromise.

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

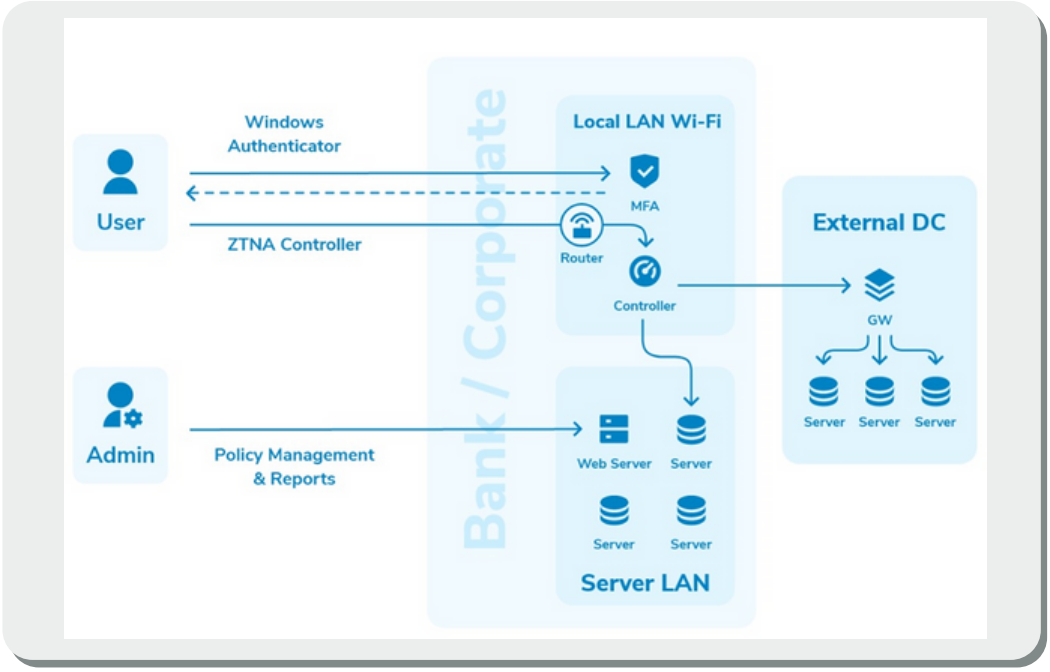
The InstaSafe Windows Authentication does this by communicating with the Centralized InstaSafe Console . The InstaSafe Console can manage multiple kinds of second factors for the domain users, ranging from classical OTP soft tokens, one time codes via SMS/Email, Smartphone Apps to the Google Authenticator. A User will need to authenticate their identity with their Windows password, and additionally with their token as the second factor.



Scenario 1: Cloud Deployment



Scenario 2: On-premise Deployment



Scenario 3: NAC Deployment

Use cases

1. MFA for windows login

Workflow:

1. User logs in to the windows with AD Domain user name and password.
2. Windows will prompt for MFA, User needs to enter the PASSCODE from InstaSafe Authenticator.
3. User login successful and user can work on the desktop/laptop.

2. MFA for windows login with secure access

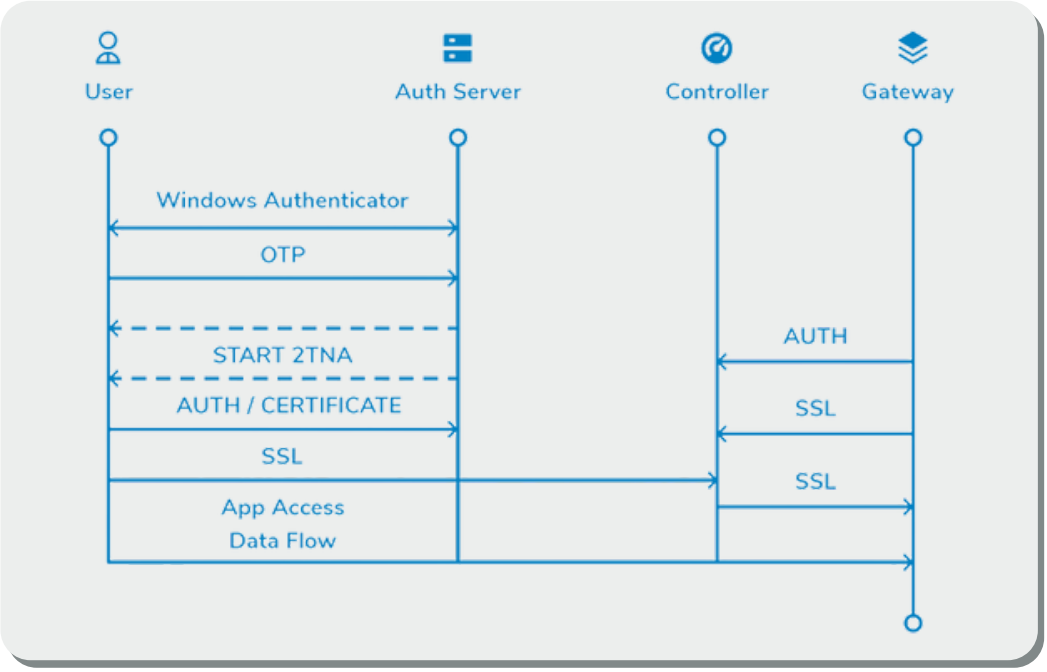
Workflow:

1. User logs in to the windows with AD Domain user name and password.
2. Windows will prompt for MFA, User needs to enter the PASSCODE from InstaSafe Authenticator.
3. User login successful and user can work on the desktop/laptop.
4. User can access all the allowed applications from outside of the office without need of VPN.

3. MFA for windows login with NAC

Workflow:

1. User logs in to the windows with AD Domain user name and password.
2. Windows will prompt for MFA, User needs to enter the PASSCODE from InstaSafe Authenticator.
3. InstaSafe app identifies whether a user is logging in from allowed devices or not.
4. InstaSafe app will verify the device compliance status, like AV status, AV last update, Domain name check, Hotfix status. If any one of the rules is not matching, the user will not be able to login to the machine.
5. User can access all the allowed applications from outside of the office without need of VPN.



Workflow

InstaSafe's Windows MFA is designed to secure your applications by employing a second source of validation, like a phone or token, to verify user identity before granting access. InstaSafe's simplified and secure workflow ensures a streamlined experience for your users. With flexible options for on premise or cloud deployments, InstaSafe seamlessly integrates with your technology stack.

Certificate Based Authentication

InstaSafe's Windows MFA is designed to secure your applications by employing a second source of validation, like a phone or token, to verify user identity before granting access. InstaSafe's simplified and secure workflow ensures a streamlined experience for your users. With flexible options for on premise or cloud deployments, InstaSafe seamlessly integrates with your technology stack.

Authentication Type	ISA Agent Connection	Password Verification	2FA	Security Checks*
Password + Certificate	On Demand	Yes	Yes (If configured)	Yes (If configured)
Certificate	Always-On (Auto Connect)	No	No	Yes (If configured)

**Security checks include Device Binding, Geo-Location Binding and Device Checks (NAC)*

While the InstaSafe Agent itself would not prompt for credential authentication in Always-On mode, users would still need to authenticate themselves with their domain credentials in order to login to the domain profile on their systems. As Always-on performs a non-interactive login, authentication is performed based on user and device certificates. For more security and compliance requirements where MFA is mandatory, always-on should not be enabled.

The InstaSafe Windows MFA feature is essentially an integration that implements MFA as part of the Windows Login, thereby providing an improved security posture for users connecting via Always-On mode. In addition, the Windows MFA also serves like SSO, wherein a user needs to authenticate just once in order to login to the Windows system as well as connect the InstaSafe Agent.

Benefits of InstaSafe Multifactor Authenticator

- Flexible Cloud based or On premise Deployment options for simplified implementation
- Designed to seamlessly support existing security stack and provide an unparalleled user experience
- Designed to support and manage multiple types of second factors, from soft tokens, one time SMS/Email Codes, to Google Authenticator
- Multi Tiered, Hyperscalable backend, suited for deployments across organizations of any size
- Access Policies offering a wide range of second factor delivery methods, with automatic failover for guaranteed code delivery regardless of user location or connectivity
- Support for a wide range of applications and systems
- Protects and secures RDP Access to Servers

InstaSafe's support for multiple factors of authentication and automatic failover ensure a seamless admin experience and a frictionless user experience. What your organisation ends up with is a hyper-scalable, flexible authentication system that secures your systems and servers. Authentication. Simplified.

FAQ

How are messages and API communications protected?

- All communications with the server are encrypted with TLS 1.2. However, to support a web proxy, Mutual-TLS is not implemented here. Mutual-TLS would require both client and server certificates to initiate a TLS session.

How are keys generated and protected?

- 2048-bit RSA keys are generated when the app is rst run and are unique to that installation. Only the public key is transported to the server.

- Private keys are stored using the protected storage mechanisms available through the mobile operating system. This is a recent add to the Android platform and is used where available.

What happens if a user's credentials are stolen, and the attacker attempts to use them when the user is in a trusted location? Will automation let the attacker in?

- Absolutely not. In order for automation to occur, the same user must perform the same action on the same service, from the same browser, in a trusted location. In this case, since the attacker does not control the user's browser, when the attacker attempts to use the credentials, the user will receive a notification. The user can then block the request.

What happens if a user is in a trusted location, but attempts to authenticate from a new browser/app?

- If the trusted location does not match its previously approved browser/app, the new request from the new browser/app will be treated as an untrusted location. As such, InstaSafe Authenticator will prompt the user to approve or deny the request.

What happens if a user is in a trusted location, but the mobile device cannot identify the location and/or location services are unavailable?

- In cases where location services are unavailable, InstaSafe Authenticator will treat the location as an untrusted location. As such, InstaSafe Authenticator will prompt the user to approve or deny the request.

What happens if a user does not have data connectivity (no Wi-Fi, no data)?

- In cases where users have no connectivity, users may use the verification code (time-based one-time password) associated with the connection. The TOTP syncs at the time of account connection with InstaSafe Authenticator and can be used in situations where no signal is available. This solution also applies to scenarios when users are on a plane without Wi-Fi.

REPORTING

Real-time Visibility

Productivity charts display instant visibility on compliance with defined policies. Query authentication activity in real-time by user, IP address, geo-IP data, login outcome, authentication client type. See exactly which users are authenticating to which systems, services and applications.

Report Builder

Administrators can define their own reports based on available field names and criteria. Reports can be saved and then exported to CSV or PDF. Audit reports can be searched using criteria including time, user, IP address, geo-IP data, successful or failed login and client type.

Scheduling and Alerting

Link reports to schedules and optionally only receive a report when there is content (alert mode). Alert on failed logins, specific users, etc.

Log Retention and Auto-archiving

MFA log data is archived automatically after 30 days and available to download from the portal for a period of 12 months. Longer retention periods are available.

MANAGEMENT

User Synchronization

Active Directory synchronization service ensures changes to Active Directory are replicated.

Web Interface

Fully integrated with the InstaSafe Centralized Console.

DEPLOYMENT

Backend

Highly scalable fully redundant and 100% cloud based delivered from multiple data centers.

Authentication Clients

Easy to install agents deployed on MFA protected on-premise services in order to connect to the cloud backend.

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 /instasafe