DATASHEET

Multi-Factor Authentication Manager (MFA)

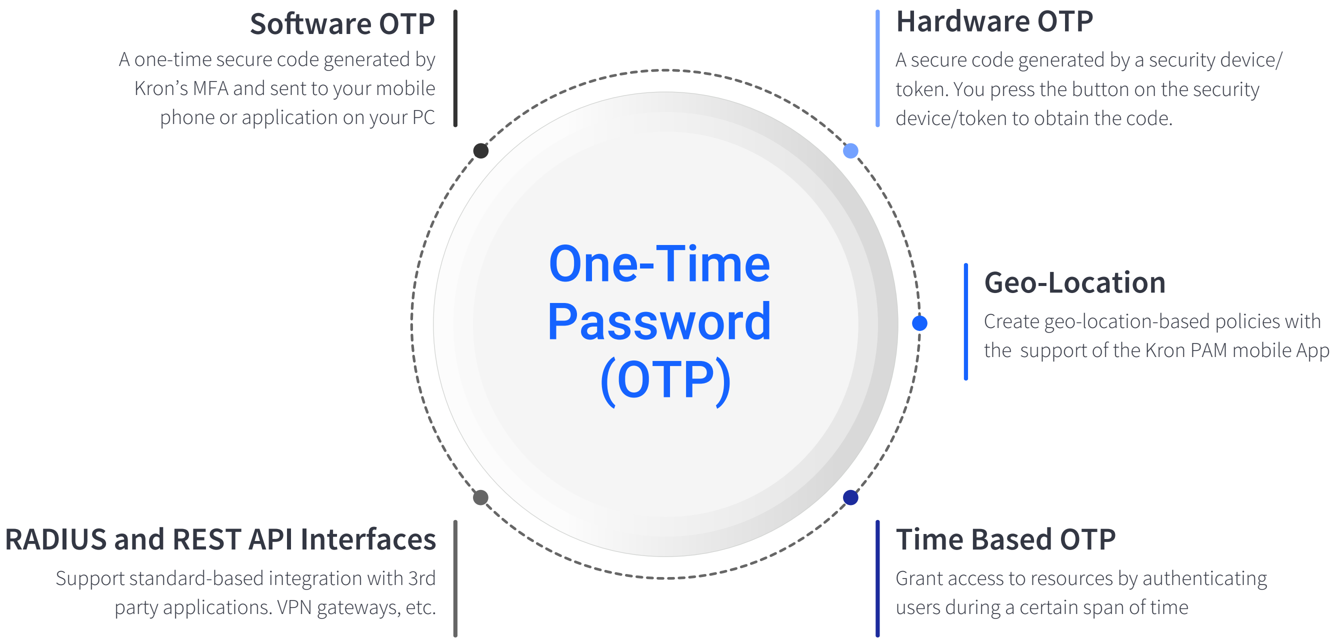
Enhance Your Authentication Process

There are thousands of different types of accounts in an enterprise infrastructure; personal accounts (of employees, contractors, etc.), local administrative accounts, privileged user accounts, domain administrative accounts, emergency accounts, service accounts, and application accounts. **You may train your employees on cyber security and implement multiple technical preventive actions, but accounts are still (and will continue to be) hacked/leaked/compromised.**

For example, socially engineered malware and phishing attacks are the most common **attack types** and there is nothing much you can do other than training employees, but they will still accidentally be victims of such attacks. Whatever preventive actions you take, you must have a plan B to prevent **compromised** accounts/identities from accessing the enterprise's critical data/assets.

While accessing critical systems during the authentication process, Kron PAM's MFA combines **two different authentication factors** to complete the login process and to achieve a greater level of security: User credentials, and a secure code (token) generated by the Kron PAM MFA Manager, Kron PAM Mobile App or a Hardware Token.

Second Layer of Security to **Verify your Identity**



Software OTP
A one-time secure code generated by Kron's MFA and sent to your mobile phone or application on your PC

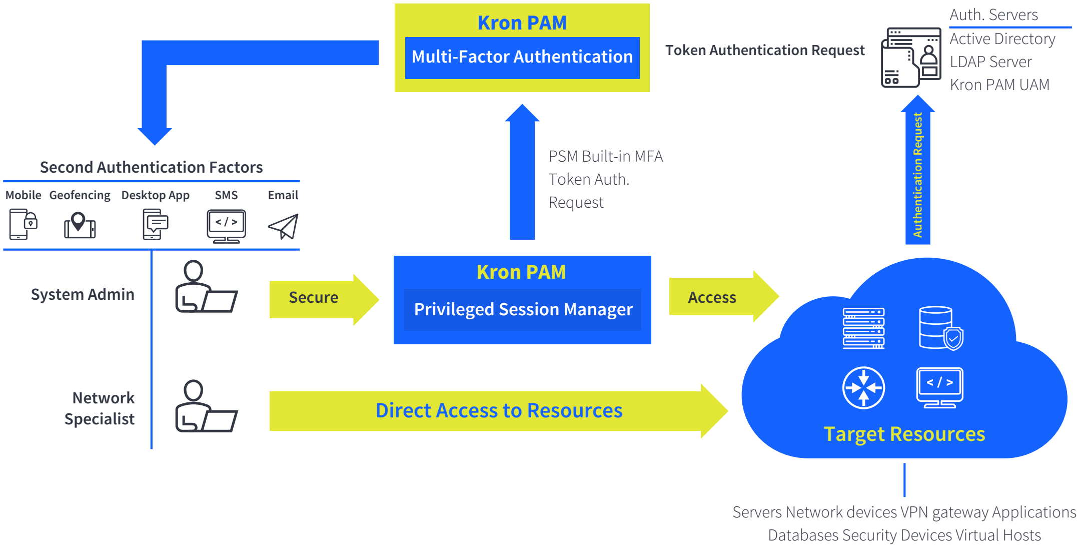
Hardware OTP
A secure code generated by a security device/token. You press the button on the security device/token to obtain the code.

Geo-Location
Create geo-location-based policies with the support of the Kron PAM mobile App

RADIUS and REST API Interfaces
Support standard-based integration with 3rd party applications. VPN gateways, etc.

Time Based OTP
Grant access to resources by authenticating users during a certain span of time

How The MFA Manager Works?


Kron PAM
Multi-Factor Authentication
Token Authentication Request
Auth. Servers
Active Directory
LDAP Server
Kron PAM UAM
Second Authentication Factors
Mobile
Geofencing
Desktop App
SMS
Email
PSM Built-in MFA Token Auth. Request
Authentication Request
System Admin
Secure
Kron PAM
Privileged Session Manager
Access
Network Specialist
Direct Access to Resources
Target Resources
Servers Network devices VPN gateway Applications
Databases Security Devices Virtual Hosts

How the Adaptive MFA Manager Works

Step 1

The user connects to the target host directly or via the Kron PAM PSM and enters the username & password.

Step 2

The target host checks the user credentials with the defined authentication server. The Authentication server asks for a second authentication through the Kron PAM MFA Manager.

Step 3

The Kron PAM MFA Manager generates a secure code (token) (one-time use only), and either sends the token to the user (via SMS/email/mobile app) or the user generates the same token offline on its mobile app.

Step 4

The user enters the secure code (The secure codes are generally reset every 30 seconds).

Step 5

The target host sends the token to the Kron PAM MFA Manager.

Step 6

The Kron PAM MFA Manager checks whether the received token is correct or not; if yes, access is granted.

Feature & Benefits

Multi-Factor Authentication enables you to strengthen the protection of vital resources by drastically reducing the chances of various security attacks, including identity theft, phishing, online fraud and more. Even if an employee's account is compromised, it is still not possible to access the enterprise's critical assets/ resources, unless the employee's mobile phone (or email account) is stolen as well.

The MFA Manager provides another level of security, even if the password is weak or **non-expiry.**

Kron PAM's MFA Manager **provides** you with broad authentication methods and features, allowing customers to define different types of use cases, **security levels,** and attack vectors. The MFA Manager supports both online (SMS, Email and Kron PAM Mobile App) and offline (Kron PAM Mobile App and hard token) token authentication.

The Kron PAM MFA Manager supports hardware-based authentication, which is a technique for user authentication that relies on a dedicated physical device **(such as a token)** held by an authorized user, in addition to a basic password, to grant access to critical resources. In a hardware-based authentication method, these devices produce a unique secure code to get access for a limited time. The combination of the secure code and the password constitute a multi-factor authentication system.

Kron PAM's MFA Manager comprises another type of two-factor authentication method called out-of-band authentication. With this method, the authentication process requires a secondary verification through a secure code delivered over an independent communication tunnel (SMS or e-mail) in addition to the user credentials.

The Kron PAM MFA Manager also supports software-based authentication that enables users to access the secure code of a secondary **verification process through** a software application on the user's computer, smart-phone, or mobile device.

Password sharing becomes irrelevant because any passwords shared with colleagues are useless by leveraging the **Kron PAM MFA** solution.

Auto lock user account when an employee terminates employment (integration with the enterprise Active Directory or LDAP is required).

The MFA Manager enables **geo-location** and time restrictions for secure access.

The Kron PAM MFA Manager also enables two-factor authentication for external apps, and provides standard-based integration with RADIUS and **REST API** interfaces with external applications (VPNs, firewalls, email servers and others).

The MFA Manager is **pre-integrated** with other Kron PAM modules.