MFA

PRODUCT DATA-SHEET

Multi Factor Authentication (MFA)

Multi-factor authentication validates user identity with passwords and an additional layer of authentication - we help you customize both these layers.

Google Authenticator
get a time bound 6 digit code from app

miniOrange Authenticator
get a time bound code real time from app

OTP over SMS / Email
receive key to be enterred for authentication

Security Questions
for alternate login methods as well as MFA

Yubikey Hardware Token
USB which generates a key

Microsoft Authenticator
numeric code real time from app

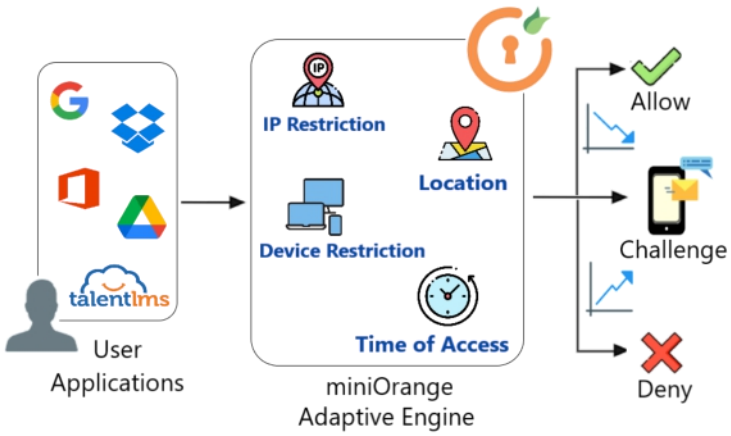
SMS / Email with link
link that can be clicked for authentication

Push Notifications via miniOrange app
user has to click Accept | Deny

+ 5 more

Adaptive Authentication

- **IP Restriction** - admin configures a list of IP addresses to allow or deny access
- **Location Restriction** - admin configures a list of locations where we want to allow end-users
- **Device Restriction** - admin allow end-users to add a fixed number of devices
- **Time Restriction** - admin configures a time zone with Start and End Time



- 15+ Authentication Methods
- Adaptive Authentication supported
- Configurable according to your requirements

miniOrange

We are here to simplify your user identity and security needs, since 2012

Secure IT Right

Restrict 2FA methods for End Users

Admin has privileges to restrict 2FA methods for end-users so that users are only allowed to use particular 2-factor methods. Admin can set the default 2-factor method for users to avoid the extra step where each user can set their own method. Users can only see allowed 2-factor methods on the user dashboard.

Alternate 2fa login methods

Enable forgot phone with security questions , OTP over alternate email. This option can be used at times when users don't have access to the main devices where 2fa is set up. Users can then use the alternate method that they have configured like Security Questions or OTP over Alternate email.

Role based Two Factor Authentication (2FA)

Role-based authentication or role-based 2FA is an approach to restricting system access to authorized users. We provide an option to manage users according to their roles and providing them the necessary access. Admin can enable/disable 2FA for a particular role and for any application.

MFA for VPN - RADIUS Authentication

miniOrange provides 2-factor Authentication on top of VPN Authentication by acting as a RADIUS server.
We can also configure our Authentication product in three possible ways with your RADIUS server :
1. Side by Side
2. Include and Extend
3. Custom RADIUS

MFA For Windows logon and RDP Access

Windows 2FA always verifies identities before allowing access, making it more difficult for unauthorized users to gain access to your Microsoft Windows account. miniOrange Credential Provider can be installed on Microsoft Windows Client and Server operating systems to enable the Two-Factor Authentication to Remote Desktop (RDP) and local Windows Login.

MFA For linux logon and SSH Access

miniOrange Two Factor Authentication (2FA) SSH Module provides a secure way to login into linux servers that enhance the security and makes brute force attacks more difficult.

Two Factor Authentication (2FA) on top of SSH Access, adds an extra layer of security to increase the identity assurance and reduce risk and exposure.

MFA for VDI - Virtual Desktop Infrastructure

Virtual Desktop Infrastructure offers a complete solution for managing and providing access to virtualized desktop environments hosted in the datacenter.

MFA for Virtual Desktop Infrastructure enables organizations to securely simplify administration, reduce operating costs, increase the utilization of existing IT assets, and boost security by moving on from a vulnerable traditional desktop environment to MFA enabled VDI.