Array

Array IDpass Identity Solution

DATASHEET

Array IDpass, a passwordless strong authentication solution safeguards your digital identity enabling seamless and highly secure authentication in the evolving digital world.

With the increasing complexity and sophistication of cyber threats, passwordless authentication has emerged as a crucial solution for organizations in today's digital landscape. Setting a strong and secure passwords has become paramount to safeguarding our online identities.

Password related issues such as forgotten or reused passwords across multiple accounts, or account lockouts, result in significant help desk costs for organizations which poses a significant security risk, as compromised passwords can lead to unauthorized access. Industries, such as finance, healthcare, and government, have strict regulatory requirements for data protection and user authentication. Thus, the need for secure and scalable authentication becomes crucial. Passwordless authentication eliminates these risks by removing the dependency on passwords altogether.

Array IDpass Identity Solution addresses the limitations of traditional password-based methods, enable secure account and system access for employees and users with a robust Multi-Factor Authentication (MFA) solution enabling highly secure and faster interactions with sensitive data and applications from anywhere. Our solution offers improved security, user experience, compliance, and scalability while mitigating risks associated with password-related vulnerabilities and effectively combats phishing attempts.

By deploying Array IDpass Identity Solution, organizations can significantly enhance their security posture by leveraging more robust authentication methods such as biometrics, cryptographic keys improving user experience, meet regulatory requirements leading to cost savings in terms of helpdesk resources and infrastructure.

FIDO Alliance

The FIDO Alliance (Fast Identity Online Alliance) is a global industry consortium focused on developing open, scalable, and interoperable authentication standards to address the challenges of traditional password-based authentication.

FIDO (Fast Identity Online) was released as an open standard by the FIDO alliance. It is a set of open, standardized protocols that enable phishing-resistant, passwordless authentication aimed at improving identity authentication and strengthening account security providing simpler, stronger, and more secure authentication mechanisms for online services, applications, and devices on the internet.

The primary objective of FIDO is to eliminate traditional password authentication methods, as passwords are often weak, prone to being guessed, easily stolen, or cracked and susceptible to various attacks such as phishing and credential theft leading to account breaches.

FIDO employs a combination of cryptographic keys, biometrics, and secure hardware to verify the user's identity. FIDO offers an authentication method based on public/private key encryption known as "public key cryptography." Users can utilize smartphones, USB security keys, or biometric technologies such as fingerprints or facial recognition for identity verification. FIDO Members include Google, Apple, Microsoft, Intel, Amazon, etc.

Traditional MFA Weakness

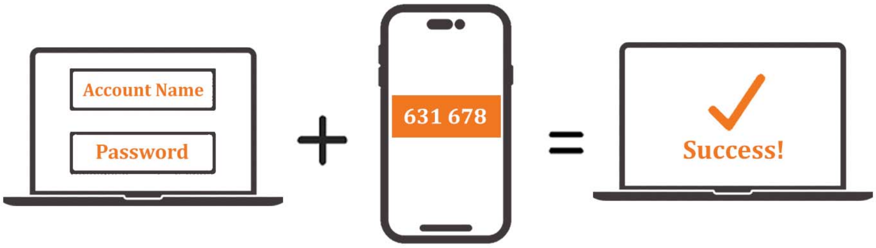
- Phishing Attacks: Traditional MFA methods can be susceptible to phishing attacks where malicious actors trick users into revealing their credentials or MFA codes through deceptive emails or websites.
- Account Takeovers: Despite having MFA in place, determined attackers can still exploit vulnerabilities in the authentication process, such as SIM swapping, social engineering, or exploiting weak SMS-based authentication.
- User Experience Challenges: Traditional MFA methods can introduce friction and inconvenience for users, leading to poor adoption rates and workarounds that compromise security.
- Single Point of Failure: If a single factor, such as a password, is compromised, traditional MFA methods may not provide sufficient protection.

Array IDpass Key Benefits

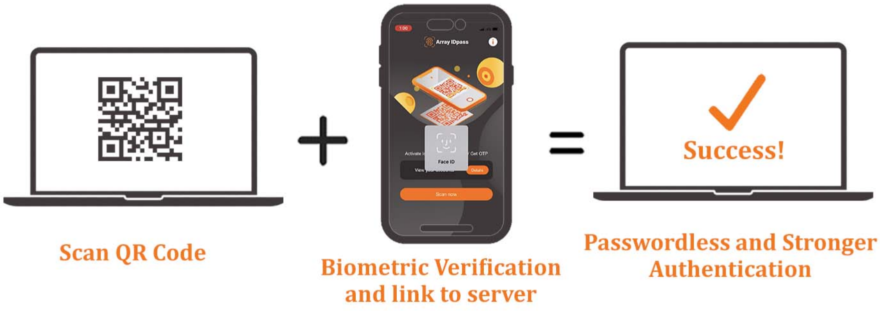
- Prevent phishing attacks, identity theft, fraud and unauthorized account takeovers with advanced security measures.
- Deliver enhanced user experience when logging into different systems, ensuring a smoother and more intuitive process. Easy to integrate with various system such as M365, VPN, VDI, Firewall, etc.
- Passwordless strong authentication solution helps organizations adherence to regulatory frameworks like the General Data Protection Regulation (GDPR) or the Payment Card Industry Data Security Standard (PCI DSS).
- International FIDO certified solution

How Array IDpass work?

Traditional MFA

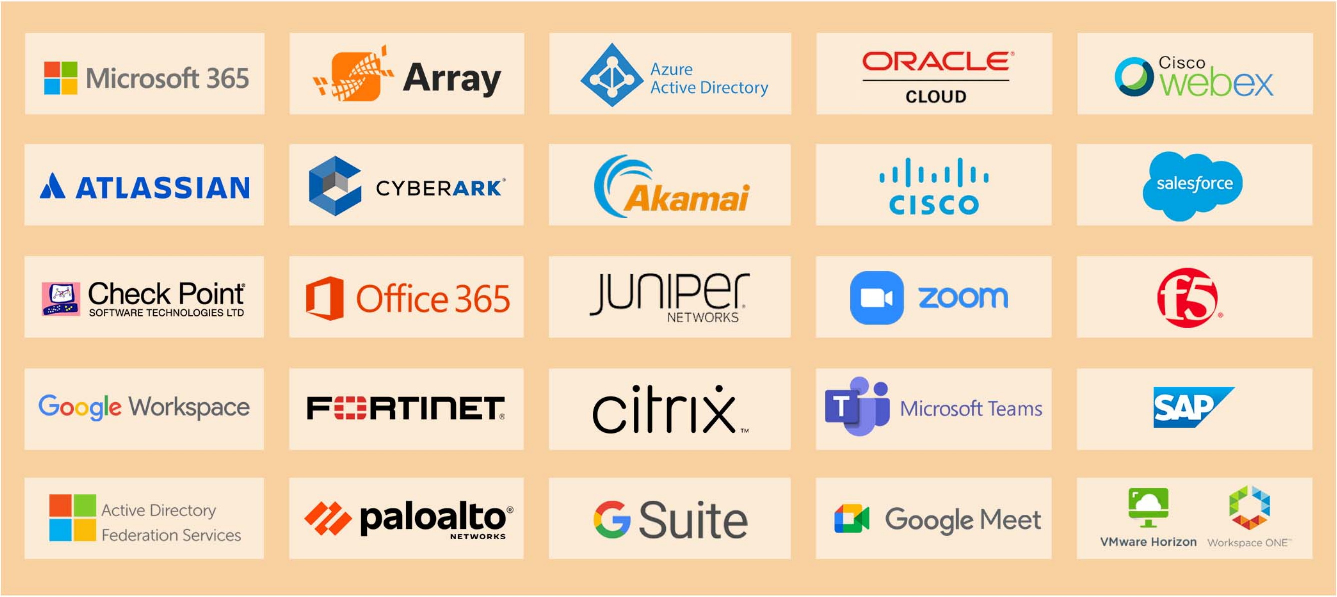


Array IDpass Solution


Array IDpass
Face ID
Scan now
Success!
Scan QR Code
Biometric Verification and link to server
Passwordless and Stronger Authentication

Easy to integrate with various system

Array IDpass support commonly adopted authorization and single sign-on specifications in the industry, such as OAuth 2.0, SAML, RADIUS, allowing integration with various enterprise applications, including major OEM application services.



Array IDpass Features

Array IDpass, Your identity guardian, Best tool for identity authentication service

Easy to use and fast to log in: Simply scan the QR Code for biometric recognition to log in.

Affordable cost and with expert help to do implementation.

Multiple application scenarios: Windows/Linux OS login, VPN, VDI remote login.

Able to integrate up to 25 original software, such as Google Workspace, Microsoft 365, Cisco Webex and more.

Array IDpass Identity Solution Mechanism Components

User Verification: Array IDpass employs various user verification methods, including biometrics (such as fingerprints or facial recognition) and user-present devices (such as security keys or smartphones), to establish user identity securely.

Public Key Cryptography: Array IDpass relies on public key cryptography to ensure the confidentiality and integrity of authentication transactions. Each Array IDpass device generates a unique key pair: a private key stored securely on the device and a public key registered with the online service.

Registration: During registration with an online service that supports Array IDpass authentication, the user's device creates a new key pair. The public key is securely registered with the service while the private key remains on the device and is never shared.

Authentication: When the user attempts to authenticate with the online service, the Array IDpass device proves possession of the private key by signing a challenge generated by the service. The signed challenge is then sent back to the service for verification.

Cryptographic Assertion: The signed challenge, along with other information, is cryptographically processed to create a secure assertion. This assertion verifies the user's identity and is used to grant access to the service.

By employing public key cryptography and secure user verification methods, Array IDpass enables strong authentication while eliminating the need for passwords. Array IDpass mechanism enhances security, reduces the risk of phishing and credential theft, and provides a seamless user experience.

Advantages of Array IDpass

- Enhanced Security: Passwords are often vulnerable to various security threats, including brute-force attacks, phishing and password reuse. Array IDpass eliminates these risks by leveraging stronger authentication factors such as biometrics, security keys, or other hardware tokens.

- Reduced Credential Theft: Since Array IDpass login does not rely on passwords, the risk of credential theft through methods like keyloggers or password guessing is significantly reduced. This helps protect sensitive data and systems from unauthorized access.

- Simplified User Experience: Array IDpass login streamlines the authentication process, making it more user-friendly and convenient. Users no longer need to remember complex passwords or go through the hassle of frequent password resets. This improves productvity and user satisfaction.

- Elimination of Password-related Issues: With Array IDpass, common password-related issues like forgotten passwords or account lockouts become irrelevant. This reduces the burden on IT support teams and saves time and resources.

- Compliance and Regulations: Many industries and regulatory frameworks require strong authentication measures to protect sensitive data. Array IDpass login helps organizations meet these compliance requirements by implementing robust authentication methods.

Why Array IDpass?

Array IDpass complies with international FIDO standards. The FIDO Server (supporting both FIDO UAF and FIDO2) and FIDO UAF SDK have both conforms to internationally recognized FIDO standards.

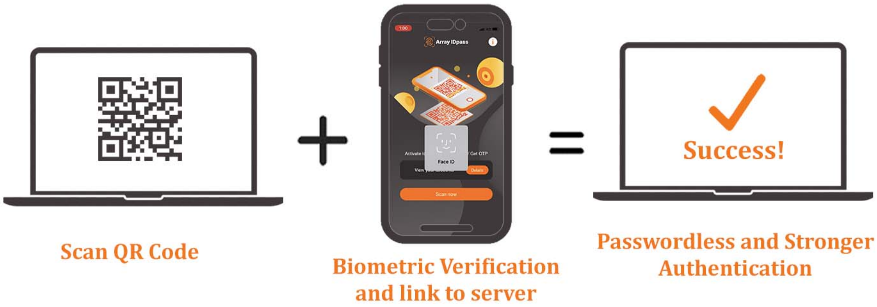
Array IDpass provides an on-premise solution that offers enhanced security compared to other products that solely provide SaaS (Software-as-a-Service) solutions.

Array IDpass offers superior security and an enhanced user experience at an affordable cost when compared to traditional Multi-Factor Authentication (MFA) solutions.

Our solution is easy to integrate with various system and is compatible with various platforms and devices, including desktops and mobile devices.

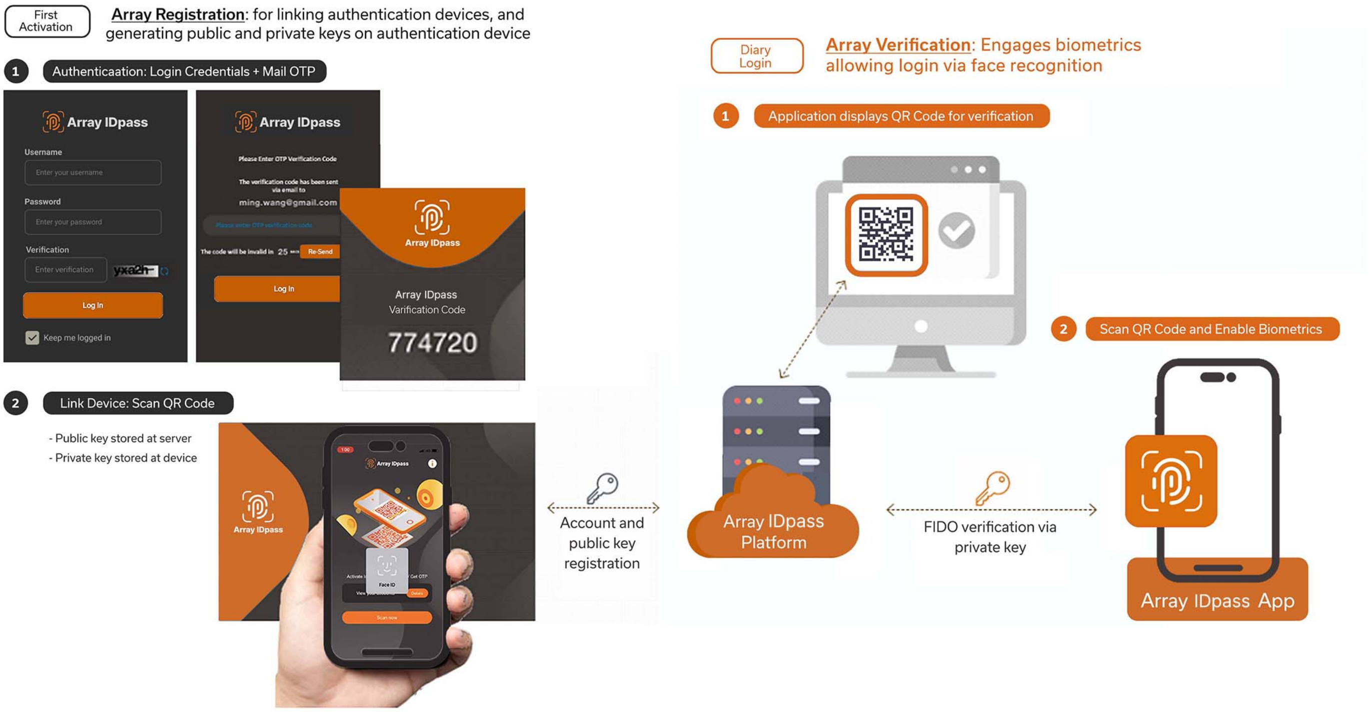
Our solution can integrate more than 25 original software, such as Google Workspace, Microsoft 365, Cisco Webex, etc. Array IDpass can seamlessly integrate if the system supports SAML or OIDC.

Authentication Flow


Success!
Scan QR Code
Biometric Verification and link to server
Passwordless and Stronger Authentication

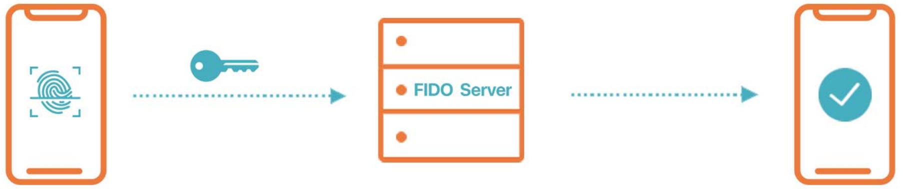
Traditionally, users were required to manually enter their account name/password along with an SMS or email OTP to access the system. With Array IDpass, users can effortlessly scan the system's QR code and utilize biometric verification, such as Face ID, to seamlessly log into multiple systems

Registration Flow


First Activation
Array Registration: for linking authentication devices, and generating public and private keys on authentication device
1
Authenticaation: Login Credentials + Mail OTP
Array IDpass
Username
Enter your username
Password
Enter your password
Verification
Enter verification
yxa2h
Log In
Keep me logged in
Array IDpass
Please Enter OTP Verification Code
The verification code has been sent via email to
ming.wang@gmail.com
Please enter OTP verification code
The code will be invalid in 25
Re-Send
Log In
Array IDpass
Array IDpass
Varification Code
774720
2
Link Device: Scan QR Code
- Public key stored at server
- Private key stored at device
Array IDpass
Array IDpass
Face ID
Scan now
Account and public key registration
Diary Login
Array Verification: Engages biometrics allowing login via face recognition
1
Application displays QR Code for verification
2
Scan QR Code and Enable Biometrics
Array IDpass Platform
FIDO verification via private key
Array IDpass App

Array offers the option to set up an enrollment server at the client's location, allowing it to integrate with Active Directory (AD). During the registration process, the company can send a registration email containing a link to all its staff members. Staff members can easily scan the QR code to associate their mobile devices with their profiles. Subsequently, they can access various systems using their mobile devices.

FIDO Mechanism



1 The User undergoes Passwordless Authentication

- The user undergoes passwordless authentication,such as biometrics verification or pattern locks.
- After the user passes the authentication, the private key is used to generate a signatures.

2 FIDO Server Signature verification

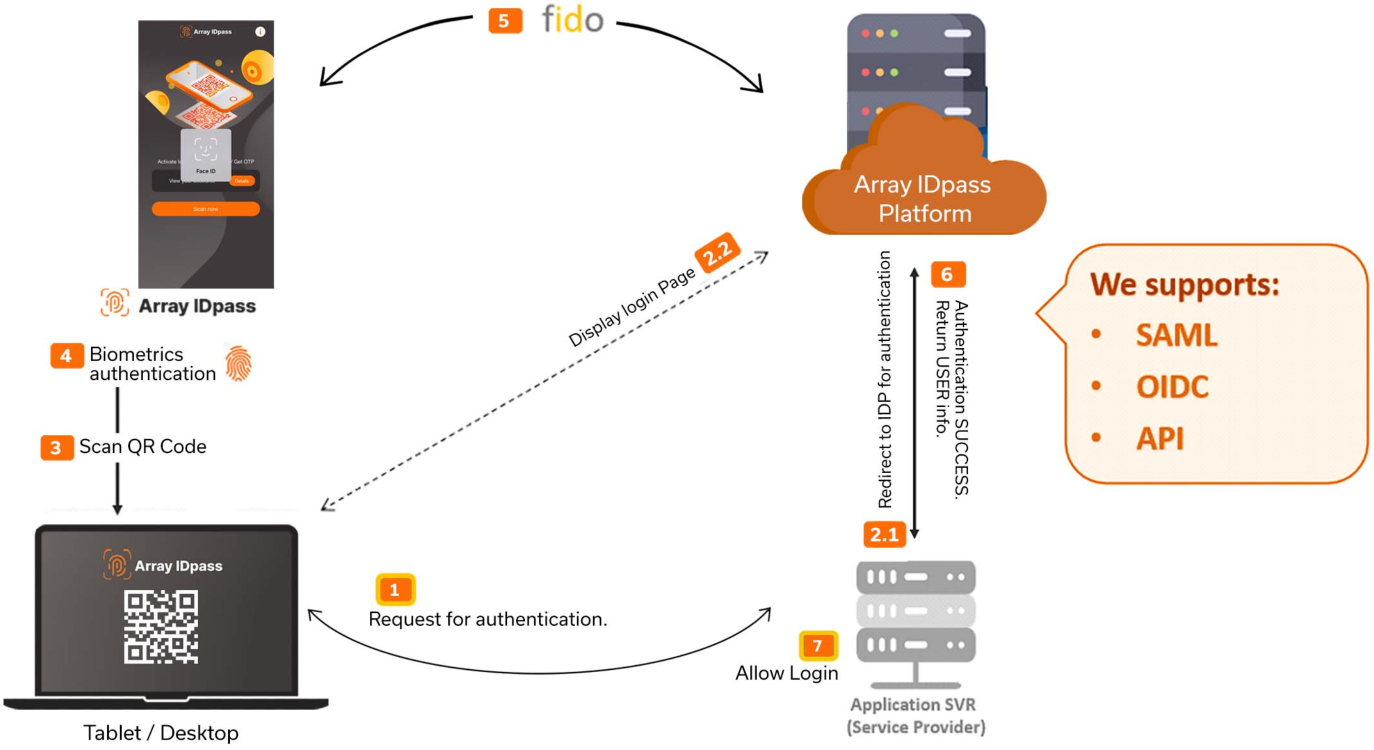
- The signature is sent to FIDO Server and the signature is verifiled based on the previously agreed public key.
- FIDO Server notifies service middle-platform user of the passing of identity verification.

3 Complete verification

- The middle platform of a website sends data to the user's browser.

Array IDpass support commonly adopted authorization and single sign-on specifications in the industry, such as OAuth 2.0, SAML, RADIUS, allowing integration with various enterprise applications, including major OEM application services.

Array IDpass Architecture



Array IDpass Daily Scenarios

1 **Windows Login**

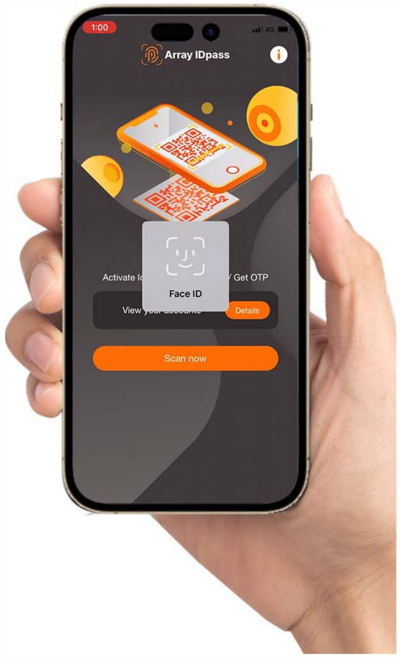
- OS Password-less Login
- Introduce MFA strong authentication, and improve user experiences

2 **VPN/Wi-Fi Access**

- VPN/VOi are common cyberattack targets, by leverage FIDO preventing systems from phishing, brutal force dictionary attacks.

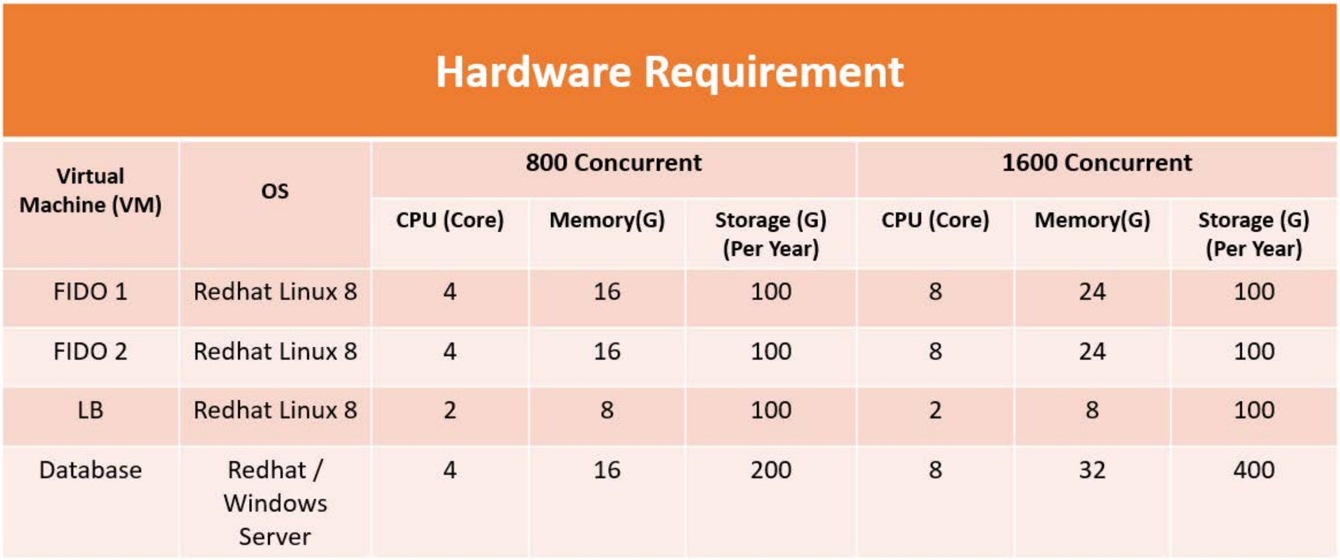
3 **Web/Mobile Application Access**

- May integrate with other SSO protocol. Safe and easy to use.
- QR Code Login prevents leaving user account footprint on devices, secure account safety and privacy.



Array IDpass support commonly adopted authorization and single sign-on specifications in the industry, such as OAuth 2.0, SAML, RADIUS, allowing integration with various enterprise applications, including major OEM application services.

Array IDpass Hardware Requirement



Hardware Requirement

Virtual Machine (VM)	OS	800 Concurrent			1600 Concurrent		
		CPU (Core)	Memory(G)	Storage (G) (Per Year)	CPU (Core)	Memory(G)	Storage (G) (Per Year)
FIDO 1	Redhat Linux 8	4	16	100	8	24	100
FIDO 2	Redhat Linux 8	4	16	100	8	24	100
LB	Redhat Linux 8	2	8	100	2	8	100
Database	Redhat / Windows Server	4	16	200	8	32	400

For more requirements, please reach out to our Sales team or write to us at sales-info@arraynetworks.com

Array

Array Networks India Private Ltd TAC
& RMA Center,
IndiQube Sigma Ground floor, Wing
B, No.3B,7th C Main, Koramangala
3rd Block, Bangalore - 560 034,
Karnataka, India

www.array-networks.co.in

☎ +1-800-572-7729