neurealm

Passwordless Authentication

Executive Summary

Challenge

- Passwords lead to credential theft, a major cause of data breaches
- Healthcare faces pressure to comply with regulations like HIPAA and HITRUST
- Password resets create a high volume of helpdesk calls, increasing IT costs

Passwordless Solution

- Our solution enables seamless, secure access to healthcare systems using Entra ID
- It integrates various passwordless methods like biometrics and smart cards
- The solution offers context-aware authentication based on user roles and devices

Key Benefits

- Reduces credential theft and phishing risks
- Lowers helpdesk calls related to password resets
- Improves login experience and saves users time

Solution Overview

About the Solution

Our AI-driven passwordless authentication solution uniquely enables seamless Entra ID integration **for all enterprise and healthcare systems**—ensuring secure, compliant, and frictionless access across all healthcare environments.

Healthcare's Identity & Security Challenges

- Password/Credential theft - **30% of Data breaches**
- **$4.8 M** avg cost per incident due to credentials(2024)
- Healthcare - top target for cybercriminals
- Password Reset - **20% - 50% of Helpdesk calls**
- Challenge in connecting to Entra ID directly
- Regulatory Pressure: HIPAA, HITRUST, GDPR, and Zero Trust.

Seamless, Secure Access to EHRs & Critical Systems with Entra ID

- Bridges Non-Native Devices with Entra ID
- Biometric & Smart Card based SSO integrated into Entra ID
- Works with Microsoft 365, Epic, Cerner, Meditech, and other healthcare apps.
- Context-aware authentication based on user role, device, and location.

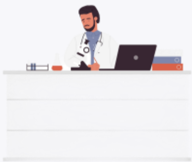
Better Security , Frictionless User Experience

- Passwordless access for all devices
- Eliminates phishing & credential theft risks.
- Reduced Helpdesk **calls by 33%**
- Save IT Cost - **$150k per 1000 users**
- Faster Login Experience - **save 24 hours per user annually**
- Regulatory Compliance: Meets NIST, GDPR, and Zero Trust principles.

User Personas

	Dr. Adam, Senior Physician	Bruce, IT Security Manager (CISO's Team)	Carla, Healthcare IT Helpdesk Lead
Challenge	● Entering passwords multiple times per shift. ● Struggles to remember complex passwords across multiple hospital systems	● Phishing attacks and credential breaches targeting hospital staff. ● Managing access for thousands of users is complex and costly. ● HIPAA, HITRUST, and NIST compliance is challenging	● 40-50% of IT support tickets are password reset requests ● Multiple authentication methods- time-consuming and costly.
Passwordless Authentication	● Fast, seamless access with biometrics/FIDO keys ● Auto-login to hospital systems, reducing login time per shift by 30%.	● Eliminates phishing risks with FIDO 2 compliant authentication ● Meets HIPAA & Zero Trust compliance with risk-based authentication and MFA.	● Reduces password reset calls by 60%, freeing up IT resources. ● Simplifies login process for doctors & nurses using hospital-approved devices.

Use Case/ Persona Journey



	Log in to Workstation		Open EHR		Accesses medical imaging,email,schedule		End of Shift/Day
Before	Enter username & password manually	✗	• Re-enter credentials • If MFA enabled , then OTP	✗	Each system requires another login	✗	Automated Logout, forgot password need reset again
After	Biometric/PIN/Security Keys	✓	SSO auto-login, no re-authentication needed	✓	Passwordless authentication → No extra logins required	✓	Auto logout ensures security → Next login is seamless

Forgot Password - IT Help Desk resets passwords

✓ No Password needed

✗ Forgot Password

Conceptual Architecture

Users	Members and Patients	Physicians and Nurses	Administrators	Operations Teams	Clinical Researchers
Channels	Mobile	Computers	Kiosks	Medical Devices	
Analytics	Security Logs & Audit Trails	Anomaly Detection & Threat Intelligence	Compliance Monitoring (SOC 2, ISO 27001, HIPAA, etc.)		
Product	Entra Verified ID				
Capability	FIDO2 Authentication (Biometric / Security Key-based authentication)	Device-Based Authentication (Windows Hello, Passkeys, Mobile MFA)	Certificate-Based Authentication (CBA)	Magic Links / One-Time Codes (Fallback Options)	
Integration	Identity Providers (IdP) (Microsoft Entra ID, Okta, Ping Identity)	Authentication Standards (OAuth 2.0, OpenID Connect, SAML, FIDO2, WebAuthn)	SSO & Federation Services (AD FS, Entra ID, Okta Federation)		
Data	User Credentials	MFA Data	Device Trust Data	Biometric Authentication Data	Access Logs & Security Events
Platform	Microsoft Entra	Microsoft Authenticator	On-Prem / Hybrid Identity Services	Microsoft Intune / MDM	

Reference Architecture

1. User logs in to a Managed Windows System

2. User authenticates using passwordless methods such as biometrics, FIDO 2 keys,Microsoft Authenticator and request got forwarded to EntraID

3. EntraID after doing basic Identity verification send the request to conditional access

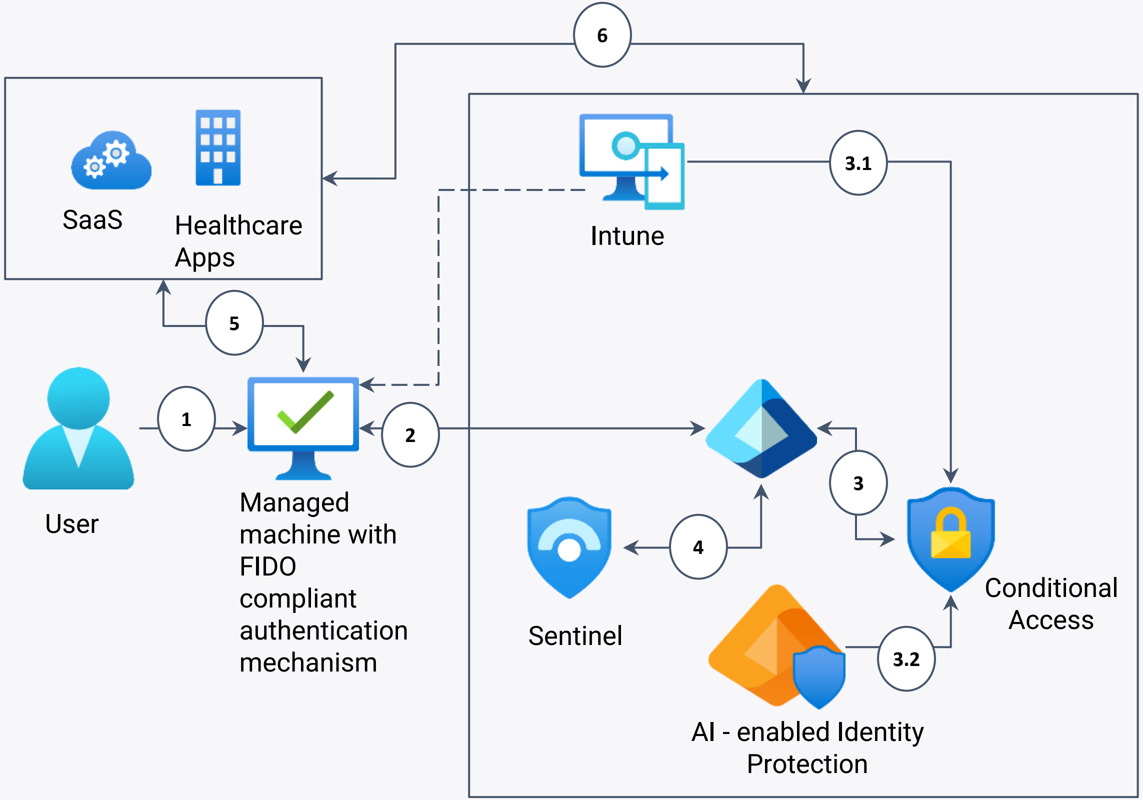
    1. Conditional access policy engine check for secured device status

    2. Checks for Identity risk

4. EntraID logs are integrated with Sentinel for further auditing and monitoring

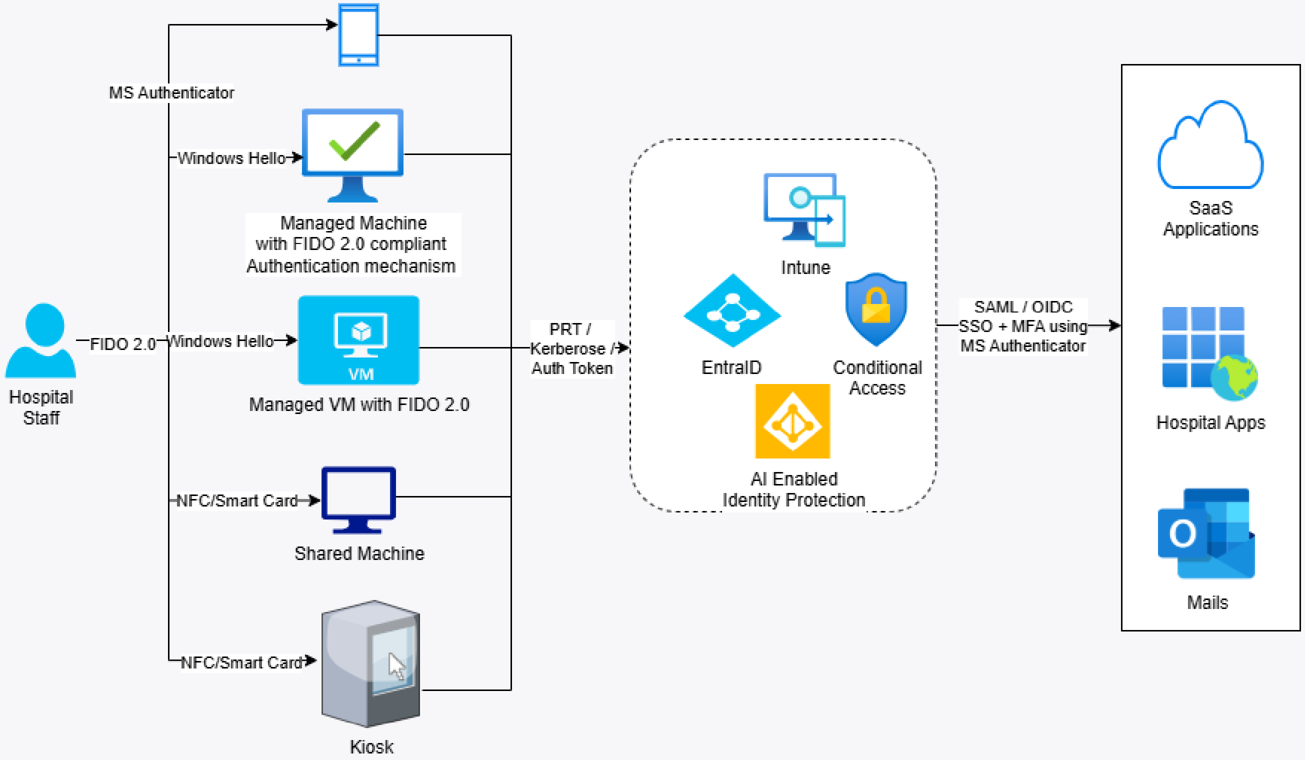
5. User access any SAML/OIDC compliant application integrated with EntraID, using browser.

6. Browser will send PRT token to EntraID for authentication and will do a Passwordless SSO to EntraID by doing same checks with conditional access and will create the application session.


6
SaaS
Healthcare Apps
Intune
3.1
5
User
1
2
Managed machine with FIDO compliant authentication mechanism
3
4
Sentinel
Conditional Access
3.2
AI - enabled Identity Protection

Integrated Architecture/Flow - Implementing Passwordless

- User logs in either using Windows Hello or NFC/Smart Card.
- EntraID is configured as IdP with devices as well as with Applications to enforce Conditional access on the basis of Roles and user attributes.
- EntraID's applies conditional access policies to validate predefined rules like passwordless, user role, device compliance, location etc.
- Access is given after successful authentication on end application using SAML/OIDC based SSO.
- Automated session lock with tap out can be implemented for shared systems and kiosk.



Key Differentiators of our Solution

Healthcare - Centric

Optimized for Healthcare environments - EHR & Clinical Workflows

Seamless integration with Shared Devices/Kiosks

Integrates Entra ID

Extends Microsoft Entra ID to work with all compliant hospital systems

Entra ID meets Healthcare compliance requirements

Support multiple passwordless methods - FIDO 2.0 compliant authentication

Enhances Security

Eliminates Credential Theft Risk

Built for Hybrid
(On Prem , Cloud)

Zero Trust Ready

Thank You

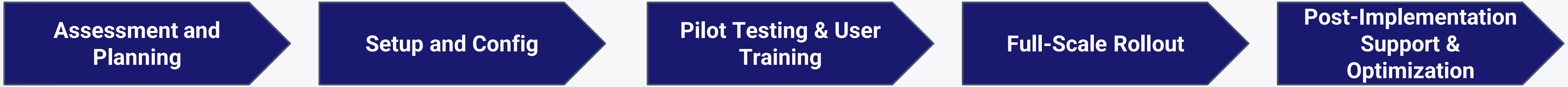
For more information, write to us at inquiry@neurealm.com

www.neurealm.com

Demo

Video link - Passwordless SignIn Demo Video_V2b.mp4

Integration/Implementation Process



Assessment and Planning

- Understand requirement
- Security & Compliance check
- Technical Readiness assessment

Setup and Config

- Enable Passwordless Authentication in Microsoft Entra ID - config FIDO keys, Windows Hello and Msft Authenticator
- Device Enrollment & Trust validation
- Application and Infra integration

Pilot Testing & User Training

- Pilot Deployment (Limited Test User group)
- User Training and Onboarding

Full-Scale Rollout

- Expand Deployment to all users
- Implement automated fallback authentication
- Monitor user adoption and feedback

Post-Implementation Support & Optimization

- User Support & Helpdesk Integration
- Performance Tuning & Optimization