Practical tips to improve security right now

David Guest

Architect and Technology Evangelist

Kocho
BECOME GREATER

Why Identity Security Matters

- Rising Credential Breaches
  - Over 60% of security breaches involve compromised credentials, highlighting identity as a critical vulnerability.
- Expanded Attack Surface
  - Hybrid and remote work increase attack surfaces, making traditional security models less effective.
- Identity as Security Perimeter
  - Identity now acts as the new perimeter, requiring strong authentication and access controls.
- Protecting Digital Assets
  - Prioritising identity protection prevents unauthorised access, breaches, and ensures compliance.

General Rules

- Alignment with Zero Trust
  - Use Zero Trust principles to ensure robust access control and continuous verification.

- Use the Actionable Insights and Best Practices
  - The section provides practical guidance, quick wins, and best practices.

Core security features of Entra ID

Risk Analysis (P2)

Identification of risk at sign-in for individual user.

Privileged Identity Management

PIM provides just-in-time access with approval workflows and audit logs to manage elevated privileges securely.

Identity Protection

Risk-based Conditional Access and real-time detection mitigate identity threats effectively.

Access Reviews

Automated periodic validation of user access ensures only authorized users retain access rights.

Quick wins for rapid security improvement

Risk-Based Conditional Access
Conditional Access dynamically adapts to risky sign-ins, enhancing threat protection.

VIP Users
If nobody else gets risk marking, then at least the important accounts (Exec, Admins)

Multi-Factor Authentication
Enabling MFA blocks 99.9% of automated cyberattacks, significantly improving security posture.

Privileged Identity Management
Activating PIM removes standing admin privileges, reducing the attack surface effectively.

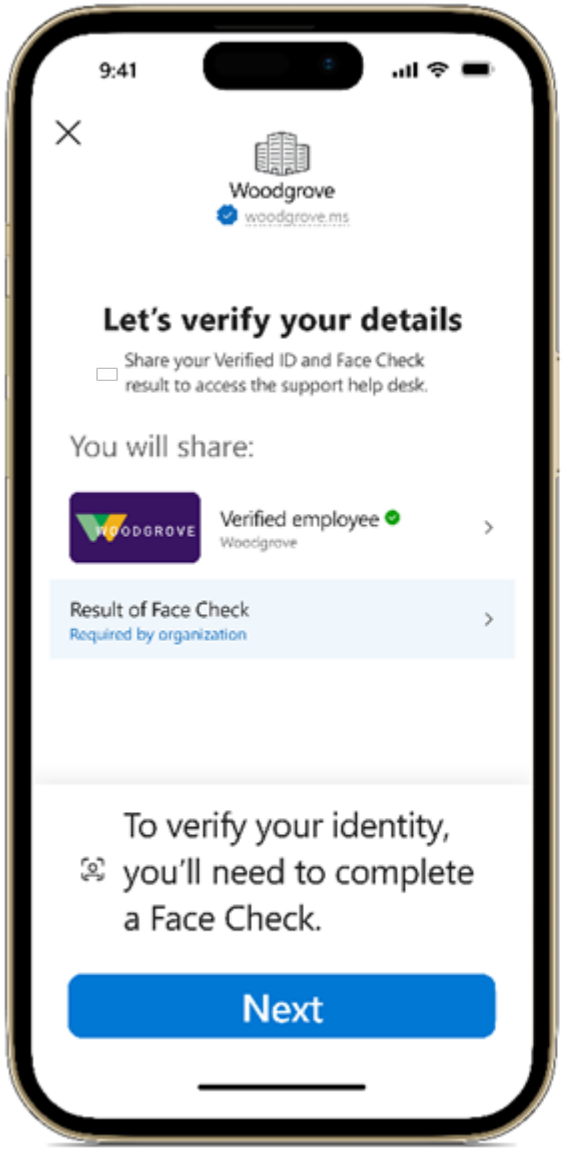
Passwordless Authentication
Deploying passwordless methods like Windows Hello, passkeys and security keys (FIDO) reduces password risks.

Recent Issues

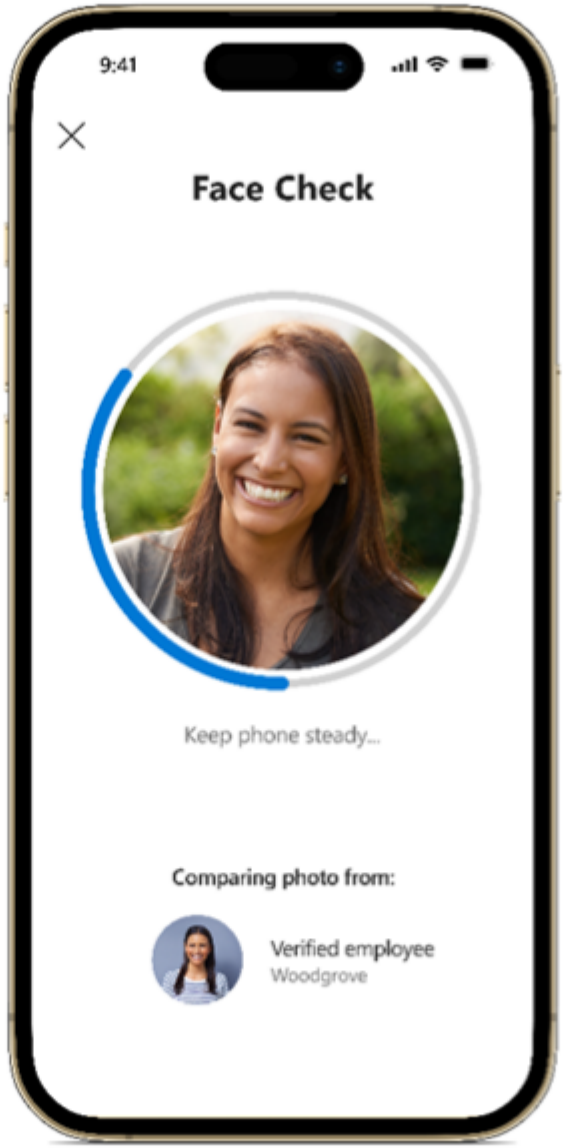
Who is calling???

Who is calling

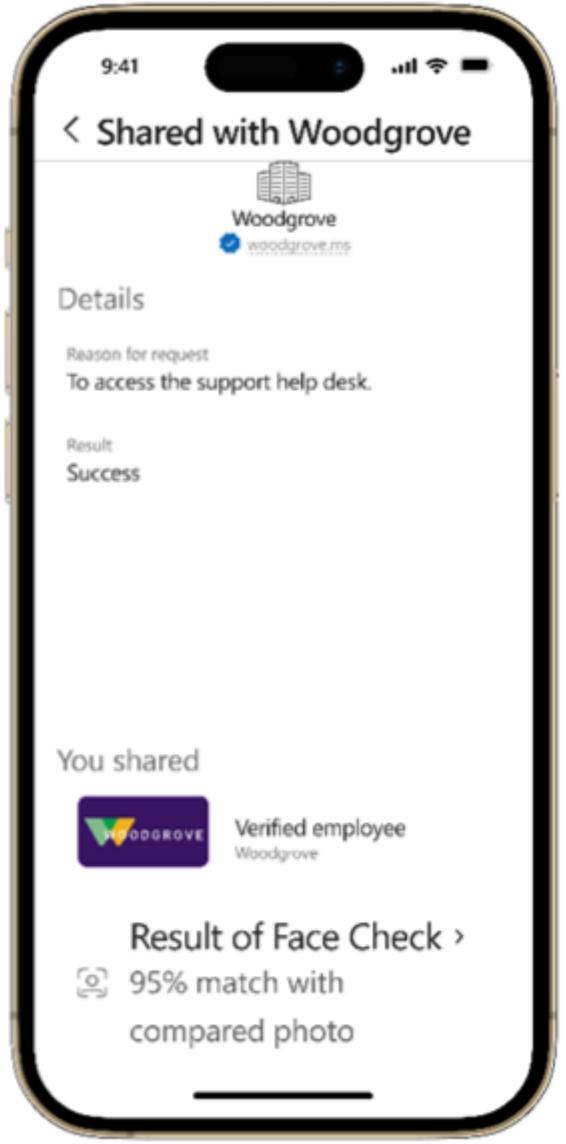
- → Allc
- → Rea
- →
- → AI-I
- →
- → Hig
- →
- → Priv
- →



Verify



Confirm



Review

ntial.

roviding

ards

Thank you

David Guest

Solution Architect & Technology Evangelist

david.guest@kocho.co.uk

Why Identity Security Matters

- Rising Credential Breaches
  - Over 60% of security breaches involve compromised credentials, highlighting identity as a critical vulnerability.
- Expanded Attack Surface
  - Hybrid and remote work increase attack surfaces, making traditional security models less effective.
- Identity as Security Perimeter
  - Identity now acts as the new perimeter, requiring strong authentication and access controls.
- Protecting Digital Assets
  - Prioritising identity protection prevents unauthorised access, breaches, and ensures compliance.

General Rules

- Alignment with Zero Trust
  - Use Zero Trust principles to ensure robust access control and continuous verification.

- Use the Actionable Insights and Best Practices
  - The session provides practical guidance, quick wins, and best practices.

Core security features of Entra ID

Risk Analysis (P2)

Identification of risk at sign-in for individual user.

Privileged Identity Management

PIM provides just-in-time access with approval workflows and audit logs to manage elevated privileges securely.

Identity Protection

Risk-based Conditional Access and real-time detection mitigate identity threats effectively.

Access Reviews

Automated periodic validation of user access ensures only authorized users retain access rights.

Quick wins for rapid security improvement

Risk-Based Conditional Access
Conditional Access dynamically adapts to risky sign-ins, enhancing threat protection.

VIP Users
If nobody else gets risk marking, then at least the important accounts (Exec, Admins)

Multi-Factor Authentication
Enabling MFA blocks 99.9% of automated cyberattacks, significantly improving security posture.

Privileged Identity Management
Activating PIM removes standing admin privileges, reducing the attack surface effectively.

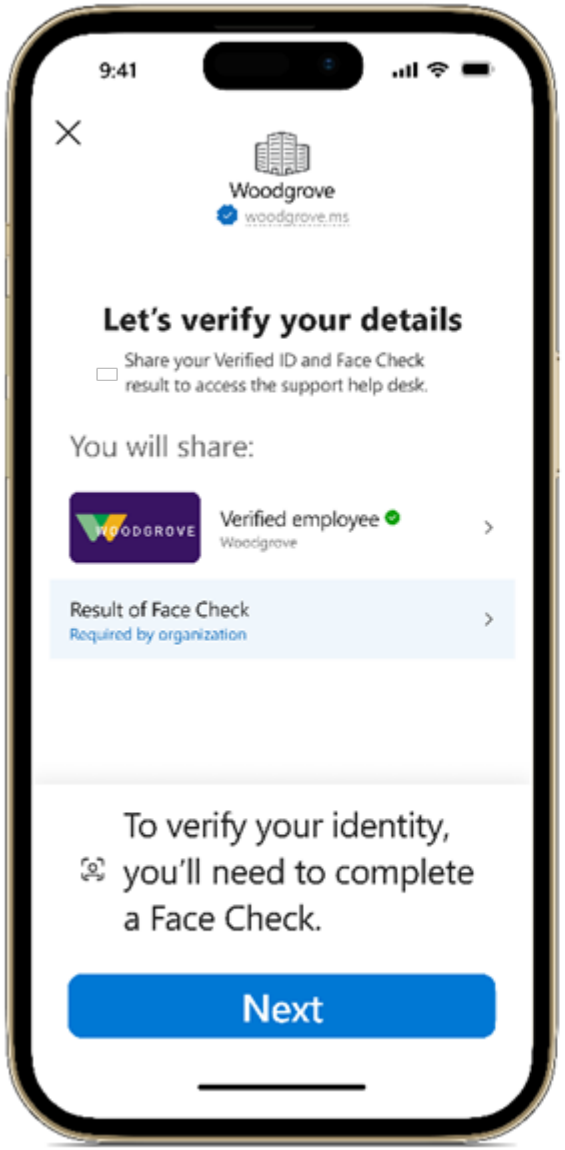
Passwordless Authentication
Deploying passwordless methods like Windows Hello, passkeys and security keys (FIDO) reduces password risks.

Recent Issues

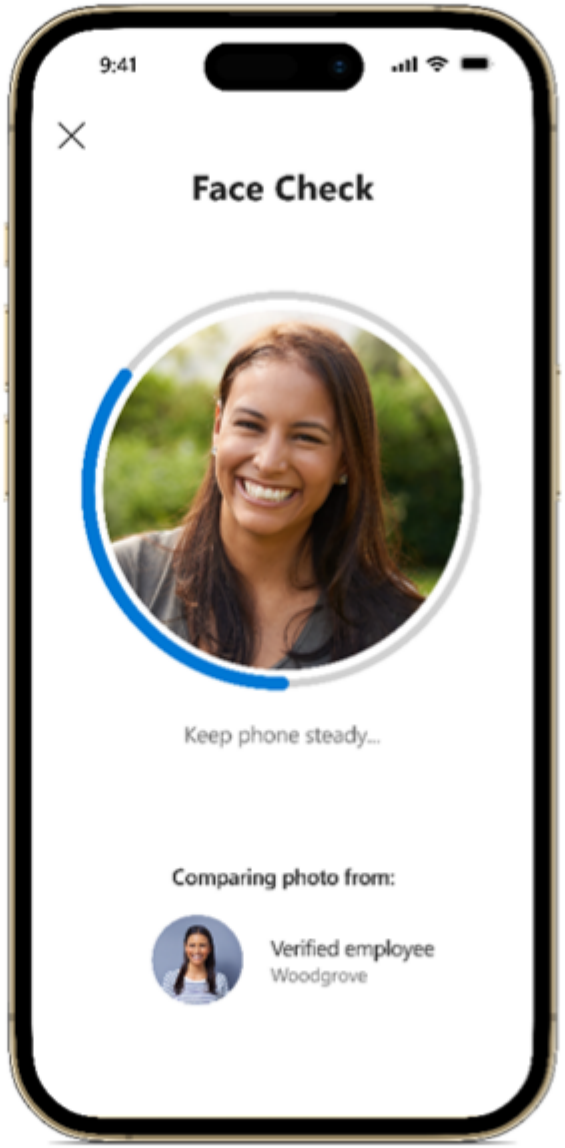
Who is calling ???

Who is calling

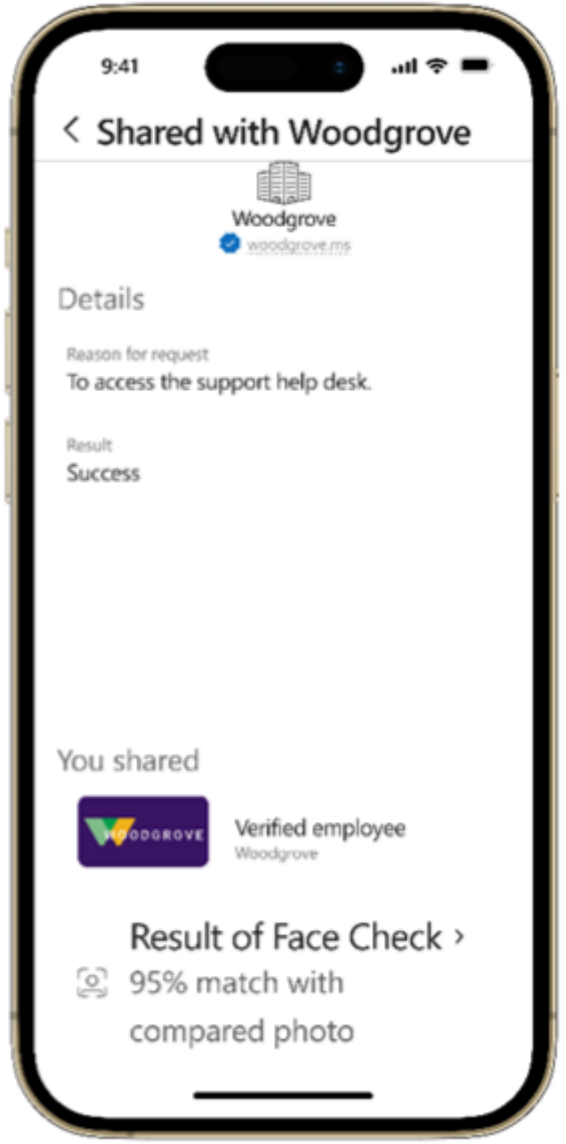
- → Allc
- → Rea
- →
- → AI-I
- →
- → Hig
- →
- → Priv
- →



Verify



Confirm



Review

ntial.

roviding

ards

Thank you

David Guest

Solution Architect & Technology Evangelist

david.guest@kocho.co.uk