Framework Mapping: Cisco Duo + Essential Eight

Achieving Maturity Level 2 with modern identity security

Contents

Executive Summary

As cyber threats increasingly target identities, credentials, and endpoint access, organisations must adopt stronger, more adaptive controls to protect critical systems.

The Australian Cyber Security Centre (ACSC) Essential Eight provides a prioritised framework to mitigate these cyber risks, with Maturity Level 2 (ML2) emerging as the baseline for effective defence—particularly across government and regulated industries. Its emphasis on phishing-resistant multi-factor authentication (MFA) at ML2 reflects a broader shift toward identity as a critical security control, establishing stronger identity assurance as a practical safeguard against capable and sophisticated adversaries.

Cisco Duo enables organisations to accelerate their journey to Essential Eight compliance by delivering phishing-resistant MFA device trust, and adaptive access controls across users, devices, and applications.

By combining Zero Trust principles with practical deployment flexibility, Duo helps organisations not only meet Essential Eight requirements but also improve resilience against modern identity-driven attacks.

Overview of Essential Eight

The Essential Eight is a set of eight mitigation strategies developed by the Australian Cyber Security Centre (ACSC) to reduce the likelihood and impact of common cyber threats, including phishing, credential theft, and exploitation of vulnerabilities. It provides a practical, prioritised approach to improving cyber resilience by focusing on the most effective baseline controls organisations can implement.

These controls span application security, patch management, user behaviour, privileged access, and data protection. While each control delivers value individually, they are most effective when implemented together as part of a layered approach to defence.

Maturity Levels

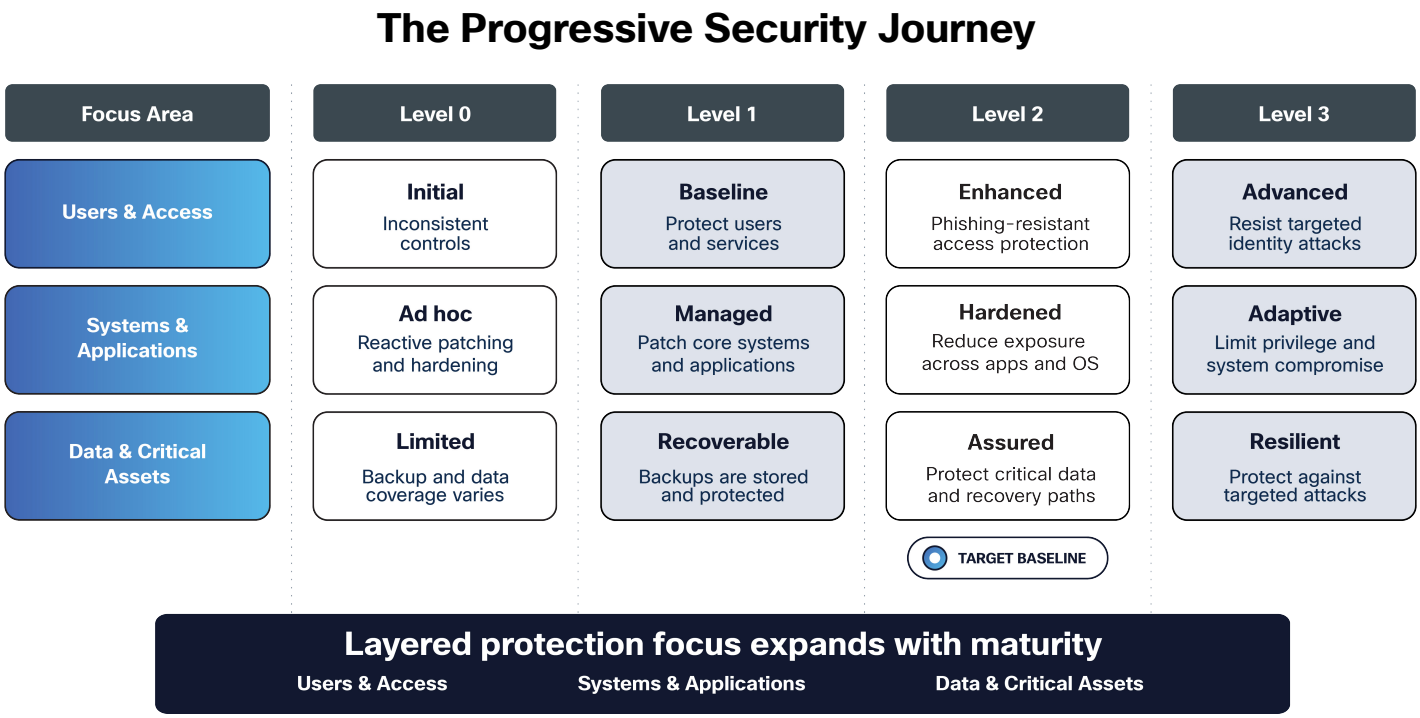
To support progressive adoption, the ACSC defines a maturity model that enables organisations to strengthen their security posture over time, aligning controls to the sophistication of potential adversaries.

Each level builds on the previous one:

- **Maturity Level 0** highlights gaps in implementation, leaving systems more exposed
- **Maturity Level 1** establishes foundational protections against opportunistic threats
- **Maturity Level 2** introduces stronger controls to address credential theft and phishing
- **Maturity Level 3** targets advanced, sophisticated attacks

A key requirement at Maturity Level 2 is phishing-resistant MFA, reflecting the growing role of identity as a primary attack vector.

As organisations progress through these levels, they move from basic protections to stronger identity verification, device trust, and continuous access control, providing a foundation for broader Zero Trust and modern defensible architecture strategies.



Cisco Duo: Identity Security for Essential Eight Alignment

Cisco Duo is a cloud-based platform that supports organisations in achieving Essential Eight Maturity Level 2 by enforcing phishing-resistant MFA, device trust, and adaptive access for users, devices, and applications.

Duo directly satisfies the MFA control — including a hardware-free option via Proximity Verification. By enforcing strong authentication, validating device posture, and applying contextual access policies, and complements, other native Essential Eight controls, serving as an identity and device enforcement layer to apply access policies based on user, device, and risk context.

As organisations progress toward higher maturity levels within the Essential Eight, identity becomes a central control point. At Maturity Level 2, protecting against credential theft, phishing, and unauthorised access requires stronger assurance of who is accessing systems and from what device.

The table summarises how Cisco Duo addresses the Essential Eight mitigation strategies, highlighting multi-factor authentication as the main control with added features supporting the other pillars.

Table 1. Cisco Duo alignment to the Essential Eight (At-a-Glance)

Essential Eight Control	ACSC Intent (ML2-Aligned)	How Cisco Duo Helps	Key Capabilities
Application Control	Prevent execution and access of unapproved applications	Helps enforce application access policies by restricting access based on device posture, including operating system and browser version compliance	OS and browser version enforcement, device posture checks, policy engine
Patch Applications	Mitigate known application vulnerabilities through timely patching	Helps enforce application patch compliance by restricting access from devices running unsupported or outdated application versions	Application version checks (e.g., browsers), device health, conditional access policies
Office Macro Settings	Prevent execution of unapproved applications	Helps reduce macro-related risk by restricting access to sensitive resources from high-risk or non-compliant endpoints	Contextual access policies, adaptive authentication, device posture evaluation
User Application Hardening	Reduce application attack surface (e.g., hardened browsers and plugins)	Supports application hardening by enforcing access from approved, up-to-date browsers and client environments	Browser version validation, plugin checks, device posture enforcement
Restrict Admin Privileges	Secure and tightly control privileged account usage	Helps secure privileged access through phishing-resistant MFA and adaptive access controls	Phishing-resistant MFA, adaptive policies, step-up authentication
Patch Operating Systems	Ensure OS vulnerabilities are remediated within required timeframes	Helps enforce operating system compliance by restricting access from unpatched or unsupported devices	OS version checks, device compliance policies, access controls
Multi-Factor Authentication PRIMARY CONTROL	Enforce MFA for users, privileged accounts, and internet-facing systems (phishing-resistant at ML2)	Provides phishing-resistant multi-factor authentication as a primary control to help protect access to users, systems, and internet-facing services in line with ML2 requirements	FIDO2/WebAuthn, passkeys, Verified Push, adaptive MFA
Regular Backups	Ensure backups are protected, accessible, and resilient to compromise	Helps protect access to backup systems and administrative interfaces by enforcing strong authentication and access controls	MFA for administrators, access control policies, identity verification

Application Control

Essential Eight goal:
Prevent execution and access of unapproved applications.

Duo helps enforce:
Cisco Duo contribution is adjacent: helping to ensure that even when applications are reachable, only trusted users on trusted devices can authenticate to them. Cisco Duo helps enforce application access by restricting entry based on device operating system and browser version compliance.

Key capabilities:
- Application-level access enforcement via SSO and policy engine
- Device Trust validation before application access
- Granular access policies by user, group, and application
- Integration with Zero Trust architectures

Technical insight:
Cisco Duo evaluates user identity and device posture at login, including operating system and browser version checks, helping restrict access to applications from devices that do not meet defined security requirements.

ML2 Focus:
At Maturity Level 2, organisations must move beyond basic controls to enforce strong identity verification and trusted endpoints. Cisco Duo supports this by gating application access based on user identity and device posture, reducing the risk of unmanaged or compromised devices in attacks.

Audit Signal:
Verification that only authorised users and trusted devices can access approved applications.

Audit Evidence:
Application Policy settings and Device Trust reports showing OS and browser compliance.

Patch Applications

Essential Eight goal:
Ensure applications are updated to mitigate vulnerabilities.

Cisco Duo helps enforce:
Cisco Duo helps enforce application patch compliance by restricting access from devices running unsupported or outdated application versions. While Cisco Duo does not patch software – it make patch compliance a precondition for access.

Key capabilities:
- Device Health checks for application versions
- Policy-based version enforcement
- Conditional access to block non-compliant devices
- Visibility into endpoint application posture

Technical insight:
While Cisco Duo does not perform application patching, it acts as an access enforcement layer, evaluating application versions (such as browsers) and restricting access until required updates are applied.

ML2 Focus:
ML2 requires protection against adversaries exploiting known vulnerabilities. Cisco Duo helps reduce this exposure by ensuring that only devices with up-to-date applications can access critical systems, effectively enforcing patch compliance at the point of access.

Audit Signal:
Evidence that access is restricted for devices running unsupported or outdated application versions.

Audit Evidence:
Device Health and Endpoint Visibility showing browser/version compliance and policy enforcement.

Configure Microsoft Office Macro Settings

Essential Eight goal:
Block or restrict macros from untrusted sources.

Cisco Duo helps enforce :
Cisco Duo reduces macro-related risk by limiting access to sensitive systems based on user trust and device security posture. Cisco Duo's role is to limit the blast radius if a macro-based phishing attack succeeds by denying the compromised endpoint access to sensitive systems.

Key capabilities:
- Contextual access policies
- Endpoint compliance enforcement
- Adaptive authentication for risky sessions

Technical insight:
Duo minimizes the blast radius of macro-based attacks by preventing compromised or high-risk endpoints from accessing sensitive systems.

ML2 Focus:
At ML2, organisations must assume successful phishing attempts. Duo helps contain these threats by ensuring that even if a macro-based attack lands, compromised endpoints cannot be used to access critical resources without meeting strict identity and device requirements.

Audit Signal:
Controls demonstrating that high-risk or non-compliant endpoints cannot access sensitive resources.

Audit Evidence:
Policy logs and authentication events filtered by device posture and risk conditions.

User Application Hardening

Essential Eight goal:
Reduce attack surface in commonly used applications.

Cisco Duo helps enforce:
Cisco Duo supports application hardening by enforcing access from approved, up-to-date browsers and client environments. While Cisco Duo does not patch or harden applications–it make patch compliance a precondition for access.

Key capabilities:
- Browser version enforcement
- Plugin and extension checks
- Blocking unsupported or vulnerable clients
- Enforcement of secure configurations

Technical insight:
Cisco Duo helps ensure authentication occurs only from approved and appropriately configured application environments, reducing the risk of exploitation via vulnerable software.

ML2 Focus:
ML2 requires stronger protections against exploit-based attacks. Cisco Duo supports this by helping ensure user access is restricted to hardened application environments, reducing the available attack surface.

Audit Signal:
Enforcement of approved browser configurations and restriction of vulnerable client applications.

Audit Evidence:
Device Health reports showing browser versions and policy enforcement decisions.

Restrict Administrative Privileges

Essential Eight goal:
Limit and secure use of privileged accounts.

How Cisco Duo helps enforce:
Cisco Duo protects administrative access with strong MFA and adaptive policies, ensuring elevated privileges are tightly controlled.

Key capabilities:
- Phishing-resistant MFA for privileged users
- Adaptive authentication and step-up controls
- Integration with directory and access workflows
- Coverage across cloud, VPN, and servers

Technical insight:
Cisco Duo reduces the risk of credential theft and privilege escalation by requiring strong authentications for all administrative actions.

ML2 Focus:
At ML2, adversaries are assumed to target privileged accounts. Cisco Duo mitigates this by enforcing phishing-resistant MFA and adaptive controls for administrative access, significantly reducing the likelihood of privilege compromise.

Audit Signal:
Strong authentication and policy enforcement applied consistently to privileged accounts.

Audit Evidence:
Admin activity logs and MFA authentication logs for privileged access events.

Patch Operating Systems

Essential Eight goal:
Ensure operating systems are securely patched.

How Cisco Duo helps enforce:
Cisco Duo helps enforce operating system compliance by restricting access from devices running unpatched or unsupported operating systems.

Key capabilities:
- OS version checks across major platforms
- Policy enforcement for minimum OS versions
- Access blocking or remediation workflows
- Integration with device management systems

Technical insight:
Cisco Duo acts as a policy enforcement point, helping ensure only devices meeting defined operating system requirements can access corporate environments.

ML2 Focus:
ML2 emphasizes defending against exploitation of known OS vulnerabilities. Cisco Duo supports this by enforcing strict OS compliance at authentication, preventing high-risk endpoints from accessing sensitive systems.

Audit Signal:
Access controls preventing devices with unsupported or unpatched operating systems.

Audit Evidence:
Device Insight and Device Health showing OS version compliance and access decisions.

Multi-Factor Authentication (MFA)

PRIMARY CONTROL

Essential Eight goal:
Require strong authentication for sensitive access.

How Cisco Duo helps:
Multi-Factor Authentication (MFA) stands as the core capability of Cisco Duo, serving as the primary control in the Essential Eight framework. By providing strong, modern authentication methods that are resistant to phishing, Cisco Duo directly supports compliance with Essential Eight Maturity Level 2 (ML2).

Key capabilities:
- Proximity-based verification
- FIDO2/WebAuthn and passkeys
- Duo Verified Push (anti-fatigue protection)
- Biometrics, hardware tokens, passwordless
- Adaptive MFA policies based on risk

Technical insight:
Cisco Duo helps enable verifier impersonation-resistant authentication, helping protect access to users, systems, and internet-facing services.

ML2 Focus:
ML2 mandates phishing-resistant MFA for internet-facing services and users. Cisco Duo directly addresses this requirement with FIDO2, passkeys, and verified authentication flows, making it a **foundational control** for achieving ML2 compliance.

Audit Signal:
Deployment of phishing-resistant MFA with coverage across users, admins, and internet-facing services.

Audit Evidence:
Authentication Logs and Policy Settings, demonstrating phishing-resistant MFA enforcement (e.g., FIDO2/WebAuthn), user enrolment status, and access activity across users, systems, and internet-facing services.

11

Regular Backups

Essential Eight goal:
Maintain secure, reliable data backups.

How Cisco Duo helps enforce:
Cisco Duo helps protect access to backup environments by enforcing strong authentication and access controls for administrative users. Cisco Duo protects the administrative path to backup infrastructure rather than the backup data itself.

Key capabilities:
- Strong authentication for backup administrators
- Access control for backup consoles and infrastructure
- Protection of cloud and on-premises environments

Technical insight:
While Cisco Duo does not provide backup capabilities directly, it helps protect the systems and administrative access used to manage backups, reducing the risk of unauthorised access or disruption to backup environments.

ML2 Focus:
ML2 assumes adversaries will attempt to disrupt recovery capabilities (e.g., ransomware). Cisco Duo mitigates this risk by ensuring backup systems are protected with strong authentication and access controls, preserving organisational resilience.

Audit Signal:
Strong access controls and authentication protecting backup systems from unauthorized access.

Audit Evidence:
Authentication logs and access policies applied to backup administrators and critical systems.

Strengthening Identity Security to Support Essential Eight Alignment

As organisations move from defining Essential Eight controls to applying them in practice, identity becomes a critical enforcement point across users, devices, and applications. Cisco Duo supports this shift by helping organisations strengthen identity verification, validate device trust, and apply adaptive access policies based on risk and context, contributing to improved security outcomes and alignment with Essential Eight Maturity Level 2.

Key Benefits

- **Mitigate credential-based attacks:** Prevent phishing and account takeover with strong, phishing-resistant authentication.
- **Enable Zero Trust access:** Continuously verify user identity and device posture before granting access.
- **Enhance visibility and control:** Gain centralised logging and real-time insight into authentication and access activity.
- **Improve user experience:** Reduce friction with passwordless and biometric authentication options.
- **Accelerate alignment:** Support rapid alignment with Essential Eight requirements across hybrid environments.

Cisco Duo helps organisations defend against credential misuse and phishing—key drivers of modern cyber incidents.

Technical Capabilities

Cisco Duo helps enable Essential Eight alignment through a comprehensive set of identity and device security capabilities. Together, these capabilities allow organisations to verify users, validate devices, and enforce access policies based on risk and context, ensuring that every access request is continuously evaluated before access is granted.

Phishing-Resistant Authentication

- FIDO2/WebAuthn and passkeys
- Biometrics (Face ID, fingerprint, Windows Hello)
- Duo Verified Push (protection against MFA fatigue attacks)

Device Trust and Posture Assessment

- OS version and patch compliance enforcement
- Browser and plugin version control
- Security posture checks (encryption, antivirus, firewall)

Adaptive Policy Engine

- Context-aware access decisions (user, device, location, risk)
- Step-up authentication for privileged or high-risk scenarios

Visibility and Monitoring

- Centralized authentication logs
- SIEM integration for compliance and incident response
- Behavioural analytics to detect anomalies

Secure Access Enablement

- VPN and VPN-less access (Duo Network Gateway)
- Integration with identity providers and SSO platforms

As organisations look to apply Essential Eight controls more effectively, the focus shifts from defining protections to operationalising them in practice—particularly through identity, device trust, and access control.

Getting Started with Cisco Duo

As organisations work to strengthen their cybersecurity posture and align with the Australian Essential Eight, identity has become a critical control point. Achieving Maturity Level 2 requires strong authentication, device trust, and continuous access verification—not just traditional perimeter defences.

Cisco Duo provides a practical and scalable way to implement these controls, starting with phishing-resistant multi-factor authentication and extending across users, devices, and applications. With flexible deployment options and broad integration support, organisations can quickly protect internet-facing systems, secure privileged access, and expand coverage across their environment over time.

By applying identity and device-based access policies consistently, Duo helps organisations not only meet Essential Eight requirements, but also strengthen resilience against modern, identity-driven threats and support broader Zero Trust and modern architecture initiatives.

Start with a free Identity Security Assessment to gain a clear, data-driven view of your identity security posture. The assessment helps you uncover visibility gaps, identify misconfigurations, evaluate MFA effectiveness, and prioritise actions to reduce identity-based risk—aligned to frameworks like Essential Eight and Zero Trust.

Then, start your 30-day free trial and see how Cisco Duo can help you implement phishing-resistant MFA, improve visibility and control, and accelerate your journey toward Essential Eight maturity.

Resources

Explore these resources to see how Cisco Duo can help you accelerate Essential Eight compliance and strengthen your security posture.

MFA Buyer's Evaluation Guide
A practical guide to help you understand what to look for in a modern MFA solution and how different approaches compare.

Guide to building End-to-End Phishing Resistance
A closer look at how phishing-resistant authentication and device trust can significantly reduce credential-based attacks.

Understanding the Business Impact of Cisco Duo
A look at the business value organizations are seeing with Cisco Duo, based on a Forrester Total Economic Impact™ study showing a 198% ROI and $4.4M NPV.

Why Customers Choose Cisco Duo for User Authentication
Insights from customer reviews and feedback highlighted in Gartner Peer Insights™.