Essential Eight

Step-up your Essential 8 Maturity Level with Okta

What is the Essential Eight?

The Essential Eight is a set of foundational security controls recommended by the Australian Signals Directorate (ASD) as top priorities for preventing and responding to the compromise of networked Microsoft Windows devices.

While the eight recommended controls were borne of ASD's experience responding to compromise of Microsoft Active Directory networks, seven of the eight are broadly applicable to any operating system. Over time, the Essential Eight has been elevated to a yardstick for strong cyber hygiene.

The Essential Eight mitigation strategies are

1. Patch applications

2. Patch operating systems

3. Apply Multi-factor authentication

4. Restrict administrative privileges

5. Implement application control

6. Restrict Microsoft Office macros

7. Harden user applications

8. Backup your data

The Essential Eight is a set of foundational security controls recommended by the Australian Signals Directorate (ASD).

For more detail on how Okta's product portfolio supports Level 3 maturity, read the full document here.

Who needs the Essential Eight?

The Protective Security Policy Framework (PSPF) published by the Australian Government Department of Home Affairs has mandated that all Australian Government entities must be able to demonstrate compliance with **Maturity Level 2** for each of the eight essential mitigation strategies.

The Essential Eight are just as useful to non-Government entities ASD recommends that all Australian organisations - from small to medium sized businesses through to large enterprises - implement the Essential Eight strategies to mitigate cyber threats.

What is the Essential Eight Maturity Model?

ASD developed the Essential Eight Maturity Model (E8MM) to allow organisations to target a specific level of control maturity during an uplift project before investing in the capabilities required to progress to the next level. This was made under the assumption that achieving a modest level of maturity across all eight controls provides a better security outcome than investing scarce resources in only a few of them.

This document maps the Okta technologies applicable to implementing the Essential Eight to the highest level of maturity, **Maturity Level 3**. In our view, the current threat environment necessitates stronger, phishing resistant multifactor authentication for all users, in order to limit exposure to:

- Post-authentication attacks, in which adversaries steal and replay session tokens from the browsers of legitimate users after they sign-in to an online service,
- Adversary-in-the-Middle (AiTM) phishing attacks capable of accessing session tokens from legitimate users,
- Voice-based social engineering campaigns using phishing kits that extract and make use of user passwords and the OTP codes used for multifactor authentication within their period of validity, or that encourage users to approve push notifications.

Given the current rate of identity-based attacks, we also contend that all organisations need to invest in reducing the blast radius from any given account or device compromise. This environment necessitates least privilege access for standard user accounts and a transition to zero standing privileges for accounts with administrative permissions.

Maturity Level 3 of the Essential Eight provides a path toward these goals.

Why Okta

Highest level of assurance

Okta has been assessed against IRAP PROTECTED criteria.

Okta is the world's largest independent, platform-neutral identity provider. Our mission is to safely connect users to any technology.

We view Identity as a fundamental pillar of security. Okta is well positioned to help customers meet all their multifactor authentication requirements, and to help customers take a modern approach to governance and privileged access.

This document also maps out where Okta's approach to identity can support our customers implementation of other Essential Eight strategies.

As an organisation, Okta has been assessed against IRAP PROTECTED criteria to provide customers with the highest level of assurance about our own security.

Apply Multi-factor Authentication

Multifactor Authentication (MFA) is a vitally important tool for protecting user access to resources.

Okta products make it simple to apply MFA to workforce, customer and partner use cases. Users can be challenged at the point of authentication and as a "step-up" challenge to verify transactions or protect access to specific resources.

Collectively, Okta platforms offer the most configurable and extensible MFA use cases than any other platform.

Administrators using the Okta Platform can design authentication flows that apply MFA to an Okta single sign-on (SSO) session, as a "step-up" for access to specific applications, and in response to specific actions and risky behaviors.

Using the Auth0 Platform, web developers can design authentication flows that apply MFA to application access, or that trigger MFA for just about any event of their choosing - such as at the point of verifying a transaction.

Okta also offers the broadest available choice of MFA factors, from traditional methods like SMS and email to advanced options such as biometric authentication. These sign-in methods are available either built into the service or as simple third-party integrations.

Restrict Administrative Privileges

Okta Workforce Identity provides customers a unified approach to access, governance and privilege management with the ultimate aim of enforcing least privilege access to all resources.

- Okta Identity Security Posture Management (ISPM) allows for the discovery of highly privileged and poorly protected accounts in cloud services and SaaS applications.
- Okta Identity Governance (OIG) provides the ability to gate requests for access to privileged resources behind customisable approval flows, as well as the ability to centralise entitlement management in downstream applications and perform rapid user access reviews (certification campaigns).
- Okta Privileged Access (OPA) provides customers the ability to lock down access to servers, secrets, service accounts and other administrative resources.
- Okta Workflows allows administrators to automate the remediation of identified issues.

These tightly integrated applications provide a single administration, management and audit point for all aspects of workforce identity.

Patch applications

Okta Workforce Identity can play a supporting role in ensuring workforce applications, such as browsers, are kept up-to-date.

Okta Device Assurance features methods of constraining user access from Chrome browsers that have not been assessed to meet a minimum security posture. This evaluation relies on the device context gathered from the end-user device by a trusted agent.

Patch operating systems

Okta Workforce Identity can play a supporting role in ensuring workforce operating systems are kept up-to-date.

Okta Device Assurance features methods of constraining user access to resources from end-user device operating systems that meet a minimum version requirement, as well as other trust signals such as disk encryption and device authentication.

This evaluation relies on the device context gathered from the end-user device by a trusted agent. Okta customers can use signals on managed devices via endpoint security integrations with Crowdstrike, Jamf and Chrome Device Trust, or on unmanaged devices using Okta Verify.

These trust signals are propagated to Okta during authentication and other user interactions, and serve as metadata for evaluation of Authentication Policies. In doing so, Okta provides the control required to deny access or to enforce phishing-resistant MFA if the evaluated device posture of the device does not meet their requirements.

Restrict Microsoft Office macros

The Essential Eight Maturity Level 3 requires that all untrusted Microsoft Office macros must be disabled for all users. An exception permitting the use of trusted macros be made for an identified set of business users on a need to use basis.

These requirements are not met directly by Okta products or capabilities and hence are not in scope for this document.

Okta provides the flexibility for organisations to choose the workforce productivity tools that best meet their business and security requirements.

Backup your data

The Essential Eight Maturity Level 3 requires regular backups of data and configurations, with a retention period enforced on the basis of business criticality and BCP (business continuity planning). Backups must be secured from unauthorised viewership and their integrity must be protected.

Under the shared responsibility model, Okta is accountable for service availability and has consistently met its 99.99% uptime goal for the Workforce Identity, Customer Identity Solution and for Auth0.

Customers are responsible for backing up their data and configurations. Okta offers customers API coverage for most configuration options, and a range of third party partner solutions are available for using this API access to backup Okta configurations.

User application hardening

The Essential Eight Maturity Level 3 requires that user tools and applications like web browsers, productivity tools like Microsoft Office and developer tools like Powershell are hardened and or certain features disabled where necessary.

These requirements are not met directly by Okta products and are best met with partner solutions.

Implement Application control

The Essential Eight Maturity Level 3 requires that application controls are implemented on workstations, servers, web browsers, email clients and system folders so as to prevent malicious code from executing in a manner that puts an organisation's data at risk of exposure or damage. These requirements are not met directly using Okta products and are best met with partner solutions.

Okta plays a supporting role in ensuring end users can safely access the resources (applications) entitled to them.

The Okta Workforce Identity provides administrators with control over *who* can access *what* resources using group-based or attribute-based application assignments.

Group memberships can be seamlessly managed based on certain attribute based rules or via integration with established sources of trust, such as HRIS systems, enabling administrators to automate joiner, mover and leaver scenarios.

Okta provides reports on user app access, group membership and current assignments to give administrators a concise view of what users can access what applications, when they were granted access, and when they last accessed these applications.

Okta Identity Governance can be used to conduct periodic access certification campaigns to revalidate all application access at regular intervals.

Get Started Today

Start a Free Trial

Contact Us

Given the current threat environment, Okta is the ideal choice for organisations seeking to meet Maturity Levels 2 and 3 for MFA requirements, and those organisations seeking a streamlined approach to meeting Privileged Access requirements.

We urge all organisations to embrace phishing-resistant authentication, which dramatically reduces exposure to most common identity-based attacks, and to invest in posture management solutions that identify gaps in MFA enforcement in downstream SaaS applications and cloud services.

We also believe it's time to accelerate the journey toward zero standing privileges for administrative roles and permissions.

Okta is ready to partner with Australian organisations to help them meet these goals.

For more detail on how Okta's product portfolio supports Level 3 maturity, read the full document here.

Essential Eight

Step-up your Essential 8 Maturity Level 3 with Okta

okta

Okta Inc.
80 Pacific Hwy, Level 13
North Sydney, NSW 2060,
Australia
info_apac@okta.com
+61-2-8310-4484