

Okta for US Military

The DoW's mission-ready identity partner

As the largest government agency with core national security responsibilities, the US Department of War (DoW) faces unique challenges in balancing speed, quality, user experience, and stringent security requirements. Okta for US Military provides a mission-focused Identity platform to address these demands, enabling:

- Efficient risk management across applications and compliance frameworks.
- Agile operations for cloud-based and tactical edge deployments.
- Identity-driven breakthroughs in operational efficiency.

Okta for US Military is a purpose-built identity solution offered exclusively to the DoW and its mission partners. Authorized at Impact Level 5 (IL5), this cloud-native offering delivers a next-generation security architecture that centralizes access to mission-relevant resources, Controlled Unclassified Information, and National Security Systems for approved users.

Architectural flexibility and interoperability.

The Okta Platform, built on Zero Trust principles, provides core identity management for the modern agency. This architecture delivers centralized, risk-based, and automated security controls and access policies essential for the Total Force: primary workforce, extended workforce (contractors), allies, Veterans, and beneficiaries. Okta also ensures interoperability with existing defense ICAM, data, and attribute services and supports both Common Access Card (CAC) and non-CAC communities.

Future-proof integration capabilities.

To enable evolving agency needs, Okta facilitates secure integration with diverse systems, including on-premises and cloud deployments. Okta also supports flexible, policy-driven routing to appropriate identity proofing based on NIST Identity Assurance Levels (IALs) required for each application or transaction. These capabilities, combined with trusted partnerships, provide a proactive defense for mission app owners against identity attacks.



Modern security features ¹

Okta incorporates modern security features for stringent government requirements. These include AWS GovCloud and secure Okta.mil web domain hosting and DISA-approved network traffic handling. These security measures deliver a robust and compliant environment for sensitive government data and operations.



Secure access management

Single Sign-On: Unify access and enforce strong authentication across apps and devices without hindering legitimate access.

Adaptive MFA: Strengthen access security with a risk-aware policy framework and a range of modern phishing-resistant authentication methods. Okta's Adaptive MFA capability works with all industry leading third-party authenticators.

Secure Partner Access: Facilitate secure and efficient interactions with supply chain and distribution partners by enabling secure import of external identities and automated app assignment.

Device Access: Secure device access from the initial login, regardless of whether devices are managed or unmanaged.

API Access Management: Onboard, integrate, and secure user-friendly API access to improve interoperability between agency networks and systems.

Okta FastPass: Okta FastPass: Deliver a secure, passwordless sign-in experience across operating systems, browsers, and applications. When properly configured on support devices, FastPass supports Authentication Assurance Level (AAL) 2 and AAL3. FastPass is Okta's first-party authenticator.



Identity management

Universal Directory: Centralize user, group, and device management in a single control plane for holistic governance and simplified workforce management at scale.

Identity Governance: Enable confident and secure access decisions at scale for mission compliance and governance.



Orchestration & integration

Workflows: Automate identity processes with no-code orchestration to customize user lifecycle management, streamline audits and reporting, and strengthen your agency's security posture.

Lifecycle Management: Automate user lifecycle transactions (joiner/mover/leaver) based on imports and triggers from Active Directory, LDAP, and modern HR systems to support day-one access and optimize software license utilization and recovery.



Identity security & threat protection

Identity Threat Protection with Okta AI: Proactively safeguard your ecosystem with identity intelligence, risk signals, and Universal Logout to detect and respond to threats in real time.

About Okta

Okta is The World's Identity Company™. We secure Identity, so everyone is free to safely use any technology. Our customer and workforce solutions empower businesses and developers to use the power of Identity to drive security, efficiencies, and success — all while protecting their users, employees, and partners. Learn why the world's leading brands trust Okta for authentication, authorization, and more at okta.com/dod or contact our sales team at okta.com/contact-sales.

¹ Reference the [Okta US Public Sector resource page](#) to stay current with Okta products and feature availability within our FedRAMP and US DoD's Defense Information Systems Agency (DISA) authorized environments.