


How Okta supports missions at the tactical edge


Tactical Identity Bridge Appliance (TIBA)


Continuous application access is critical for agencies to achieve their mission. Agencies that use a modern, cloud-native Identity and Access Management (IAM) solution need edge sites to function in Denied, Disrupted, Intermittent, and Limited Bandwidth (DDIL). They also require comprehensive solutions to ensure users can benefit from continued seamless access without friction, understanding that some services may be limited in capacity due to environmental conditions.


In a Zero Trust Architecture (ZTA), where the principle is “never trust, always verify,” Identity is a crucial and foundational component to authenticate and authorize, enforcing granular least-privileged access. The majority of cyber attacks involve credential use or misuse in the network. Identity-centric architectures must be robust enough to not be bypassed in non-optimal environments.


Obstacles


-  Maintain persistent security posture

-  Provide frictionless user experience

-  Manage unfavorable network environments

-  Synchronize with enterprise ICAM capabilities

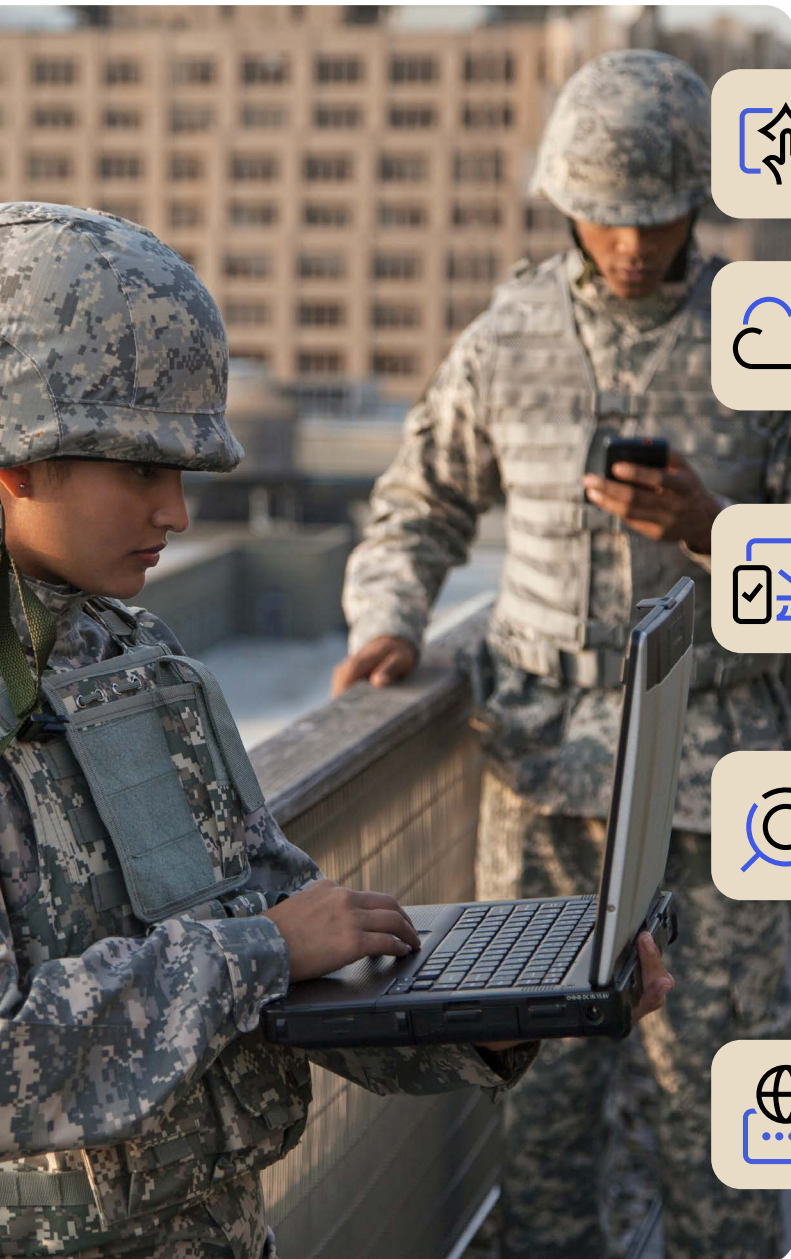
-  Interoperate with modern cloud ICAM services

-  Zero Trust management



Uninterrupted Identity services

Okta has partnered with SelecTech to field the Tactical Identity Bridge Appliance, or TIBA. Strengthening enterprise IAM, the TIBA is a robust, standards and compliance-based unified solution built on microservices technology that adheres to stringent DoD security requirements, and is tailored for secure deployment at the tactical edge. By securely implementing robust cryptographic protocols (PKI and FIDO2.1), user access control, privileged user access control, and user Identity management, the system safeguards mission resources by ensuring access is granted exclusively to authorized and active users.



Intelligent monitoring and routing

Adapt to network conditions, ensuring optimal user experiences.



Cloud-native IAM integration

Leverage Okta for US Military¹ when connected to the network.



DDIL mode high-level functionality

Authenticate and authorize users into local applications, maintain a local directory service with roles and attributes, utilize phishing-resistant multi-factor authentication (MFA), and more.



Bi-directional directory synchronization

Through system for cross-domain Identity management (SCIM) API and with optional exclusions by group or attribute.

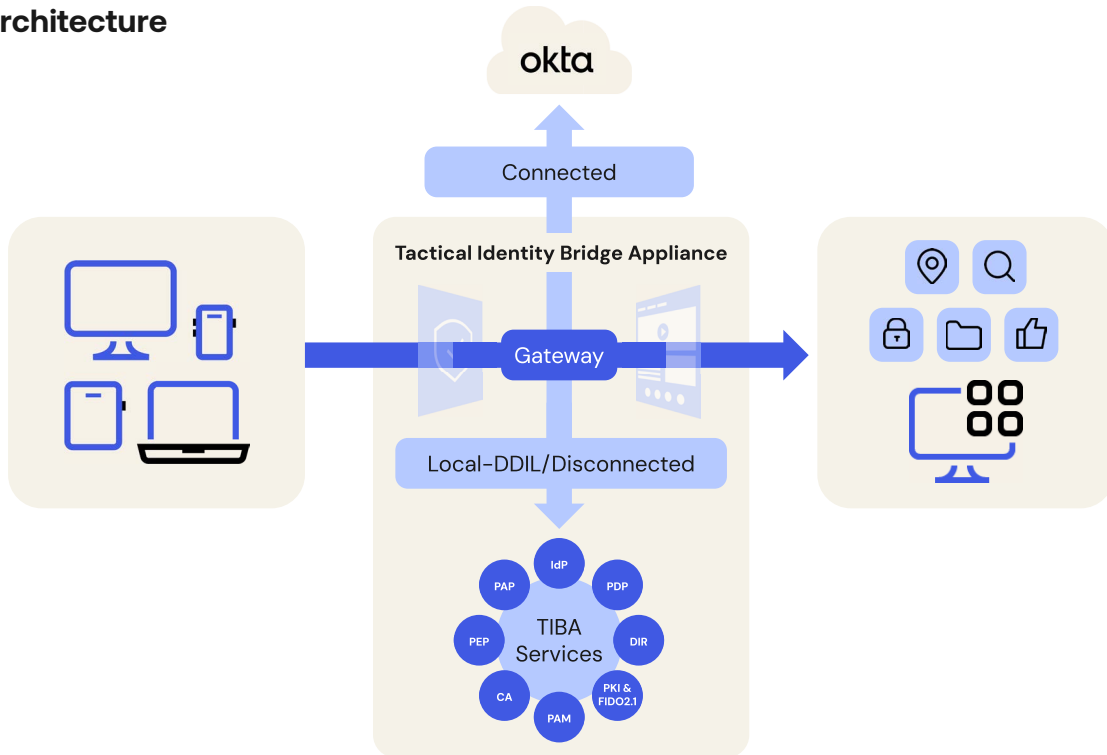


Support new users and cryptographic credentials

Strong MFA cryptographic credential issuance and lifecycle management when offline, including temporary credentials for lost badges or foreign allies.

[1] Okta for US Military is Okta's Impact Level 4 (IL4) Provisional Authorization (PA) that can service IL5 environments.

Reference architecture



Operation modes

Normal operation

Up until the network cutoff, a user is provisioned from the enterprise Identity and attributes Okta for US Military holds within Okta Universal Directory or a Component’s local user store. TIBA knows when Okta is available and will send users to Okta for verification via Okta Verify, PIV/CAC, push-notification, etc.

Offline communication

TIBA recognizes the change in network and handles all authentication and authorization. This includes replacing a lost credential, seamless access management, and the ability to create new users.

Normal/Restored Operation

TIBA recognizes the change in network and passes all authentication and authorization back to Okta as primary Identity Provider (IdP) via the Okta Tactical Edge Connector. TIBA can exclude what gets synchronized back to the enterprise system of record.

To learn more about TIBA capabilities, use cases, and operation modes, visit okta.com/dod or schedule a demo with us: federal@okta.com.

About Okta

Okta is the World’s Identity Company. We free everyone to safely use any technology—anywhere, on any device or app. Our Workforce and Customer Identity Clouds enable secure yet flexible access, authentication, and automation that transforms how people move through the digital world and puts Identity at the heart of business security and growth.