Meeting CJIS Compliance with WDL

BEYOND IDENTITY

Secure Workstation Authentication with Beyond Identity Windows Desktop Login and YubiKeys

Introduction

Law enforcement agencies operate under strict security mandates to protect sensitive Criminal Justice Information (CJI). The FBI's Criminal Justice Information Services (CJIS) Security Policy sets rigorous standards, particularly for user authentication when accessing systems containing CJI. Beyond Identity understands these critical requirements and offers robust solutions designed to help agencies meet and exceed CJIS compliance obligations.

This document outlines how Beyond Identity's Windows Desktop Login (WDL) solution, when implemented using YubiKeys configured for PIV (Personal Identity Verification), directly addresses the authentication requirements of the CJIS Security Policy, providing a secure, compliant, and user-friendly login experience for workstations.

Understanding Key CJIS Authentication Requirements

The CJIS Security Policy mandates several specific controls relevant to desktop and workstation login security:

1. **Advanced Authentication (Multi-Factor Authentication - MFA)**
   Requires the use of at least two distinct authentication factors (Something You Know, Something You Have, Something You Are) for accessing CJI, especially outside physically secure locations.

2. **Unique User Identification**
   Prohibits shared accounts, requiring every user to have a unique identifier tied to their authentication credentials for accountability.

3. **Audit Logging**
   Mandates comprehensive logging of authentication events (successful and failed attempts) with retention for audit purposes (typically at least one year).

4. **FIPS 140-2/3 Validated Cryptography**
   Requires the use of federally validated cryptographic modules for protecting authentication secrets and ensuring the integrity of security functions.

5. **Session Management**
   Stipulates controls like session timeouts and automatic workstation locking to prevent unauthorized access after periods of inactivity.

Beyond Identity's WDL enhances standard Windows login by replacing or augmenting password-based authentication with strong, phishing-resistant methods. When deployed with YubiKeys, the solution leverages hardware-based credentials for desktop access.

Beyond Identity's Solution: Windows Desktop Login (WDL) with YubiKey PIV

Beyond Identity's WDL enhances standard Windows login by replacing or augmenting password-based authentication with strong, phishing-resistant methods. When deployed with YubiKeys, the solution leverages hardware-based credentials for desktop access.

How Beyond Identity WDL with YubiKeys Addresses CJIS Requirements

Our WDL solution using YubiKey PIV is specifically designed to meet the stringent demands of CJIS compliance:

Fulfills Advanced Authentication (MFA) Mandate:

- The physical YubiKey hardware token serves as the **"Something You Have"** factor.
- The requirement for the user to enter a secret PIN to unlock the PIV credential on the YubiKey during login satisfies the **"Something You Know"** factor.
- This combination provides strong, two-factor authentication that aligns precisely with the CJIS definition of Advanced Authentication.

Ensures Unique User Identification:

- During the secure enrollment process, a unique digital certificate is issued by Beyond Identity's Certificate Authority and provisioned directly onto the user's specific YubiKey (in the PIV slot).
- This certificate is cryptographically bound to the individual user's identity within the agency's directory (e.g., Active Directory or Entra ID User Principal Name).
- Every login attempt verifies this unique, user-specific certificate, guaranteeing individual accountability and preventing credential sharing.

Provides Comprehensive Audit Logging:

- The Beyond Identity platform centrally captures and stores detailed audit logs for all significant authentication and credential lifecycle events.
- Key events relevant for CJIS audits include:
  - **Certificate Issued/Certificate Revoked**: Tracks the lifecycle of the certificate on the YubiKey.
  - **Desktop login setup enrollment**: Records when a YubiKey is enrolled for WDL for a user.
  - **Desktop login attempts**: Logs every desktop login attempt (both success and failure), including user identity and timestamp, providing a clear audit trail for access monitoring.
- These logs are readily available for review and reporting to satisfy CJIS audit requirements.

Utilizes FIPS 140-2/3 Validated Cryptography:

- We recommend using YubiKey 5 FIPS Series tokens, which are themselves FIPS 140-2 Level 3 validated, ensuring the hardware component meets stringent federal cryptographic standards.
- Our backend systems and cloud services, including the Certificate Authority responsible for issuing PIV certificates, utilize cryptographic modules validated against the FIPS 140-3 standard. This ensures that critical operations like key generation, certificate issuance, and overall platform security adhere to the latest federal security standards for cryptography.

Strong Phishing Resistance:

- Authentication relies on the hardware YubiKey and its private key, which never leaves the device. There are no passwords to be phished or static secrets transmitted that could be intercepted. This cryptographic-based approach provides a high degree of resistance against common phishing and credential theft attacks.

Supports Session Management Policies:

- Beyond Identity secures the critical authentication event. Standard Windows operating system features (configured via Group Policy or Mobile Device Management) handle session timeout and workstation locking policies, complementing our secure login process.

Key Benefits for Law Enforcement Agencies

Beyond meeting compliance checkboxes, implementing WDL with YubiKeys offers tangible benefits:

Enhanced Security: Significantly reduces the risk of unauthorized access via stolen or weak passwords.

Robust Compliance: Provides a clear, auditable path to meeting CJIS MFA and identification requirements.

Offline Authentication: Enables users (e.g., officers in patrol vehicles) to log into their workstations even without network connectivity, using the YubiKey and PIN locally.

Suitable for Diverse Environments: Works effectively in settings where mobile phones are restricted or undesirable as authenticators (e.g., secure facilities and jail systems, roaming and shared workstations).

Streamlined User Experience: Once enrolled, login is often faster and simpler than typing complex passwords, especially using the PIN associated with the YubiKey.

Hardware (YubiKey) vs. Virtual Authentication for CJIS

While CJIS allows various MFA methods, YubiKeys offer distinct advantages in the law enforcement context compared to purely software-based ("virtual") methods like mobile authenticator apps:

Physical Security: A dedicated hardware token is generally more resistant to remote malware or OS compromise than software on a multi-purpose device like a smartphone.

Offline Capability: Hardware keys excel in enabling secure offline login, a critical need for field operations.

Environmental Suitability: Ideal for situations where personal devices are prohibited or unreliable.

Both hardware tokens and compliant virtual authenticators can meet CJIS technical requirements for MFA. However, the robustness, offline capabilities, and physical nature of YubiKeys often make them a preferred and highly reliable choice for the restricted and demanding operational environment of law enforcement.

Conclusion

Beyond Identity is committed to providing law enforcement agencies with authentication solutions that meet the highest standards of security and compliance. Our Windows Desktop Login solution, utilizing FIPS-validated YubiKeys in PIV mode, offers a direct and effective way to satisfy CJIS Advanced Authentication requirements. It enhances security posture, supports operational needs like offline access, and provides the necessary auditability for compliance verification.
We are confident that this solution offers a secure, compliant, and reliable path forward for agencies modernizing their workstation authentication infrastructure.

Disclaimer: This document provides general information regarding the alignment of Beyond Identity's solutions with the CJIS Security Policy. The specific implementation within an agency's unique environment is subject to their own risk assessment and final compliance validation by relevant auditing bodies. Beyond Identity is available to provide further technical details and support documentation to assist with compliance efforts.