A BIO-key® Solution.

Solution Brief

Password Security and CJIS Compliance

Table of Contents

Securing Access to Law Enforcement Applications

Computers and information technologies are critical tools for police work today. Officers need immediate access to law enforcement applications, whether they are working in police stations, squad cars, or otherwise mobile and operating remotely. It's essential for officers to easily login to the department's computer system, regardless of where they are located, and connect to the applications they need to do their jobs.

An IT service provider and/or the internal computer support staff in a police department have other concerns. IT staffers must manage the security of the department's system as well as the connections to state and Federal resources available over the Internet. A department's system must verify the personal identities of officers, managers, and administrative personnel, and protect against access by unauthorized people and processes as defined by the Criminal Justice Information Services (CJIS) Security Policy.[1]

With the increased reliance on computer technologies in the field, it is especially important to ensure that the department's system complies with the CJIS policy for identification and authentication when officers are accessing applications from outside physically secure locations. It's also important to track and audit all access to the system, another CJIS policy. Finally, there's a management context to consider. IT staffers need to deploy a solution for password security that is easy to install, maintain, and affordable for their department.

Of course, an effective solution for password security must strike the right balance among officers' needs for easy authentication to law enforcement applications, cost-effective system management for IT staffers, and CJIS compliance requirements. A well–designed solution optimizes both usability and password security.

The PortalGuard Solution

Supporting Seamless Authentication For Police Work

This is where PortalGuard makes a difference. It provides seamless authentication to law enforcement applications running within a police department as well as easy system management.

PortalGuard complies with CJIS security policies for Auditing and Accountability (Policy Area 4), Access Control (Policy Area 5), and Identification and Authentication (Policy Area 6). PortalGuard capabilities for specific policy areas and topics are summarized in Appendix A.

Policy Area 6 Compliance: Identification and Authentication

PortalGuard excels with its support of Policy Area 6 requirements, a topic of great concern to many local police departments. PortalGuard delivers a comprehensive password security solution for identification and authentication.

PortalGuard replaces the out-of-the-box Windows Workstation authentication services with a set of enhanced security capabilities. As a result, PortalGuard ensures complete password management, both when officers are working within a physically secure location, such as a police station, as well as when they are working remotely, in a squad car or connecting from a remote location.

PortalGuard delivers flexible and easily managed Password Rules to support consistent authentication regardless of location. PortalGuard also supports Two Factor Authentication (2FA), required to meet the Advanced Authentication mandate for password access outside a physically secure location.

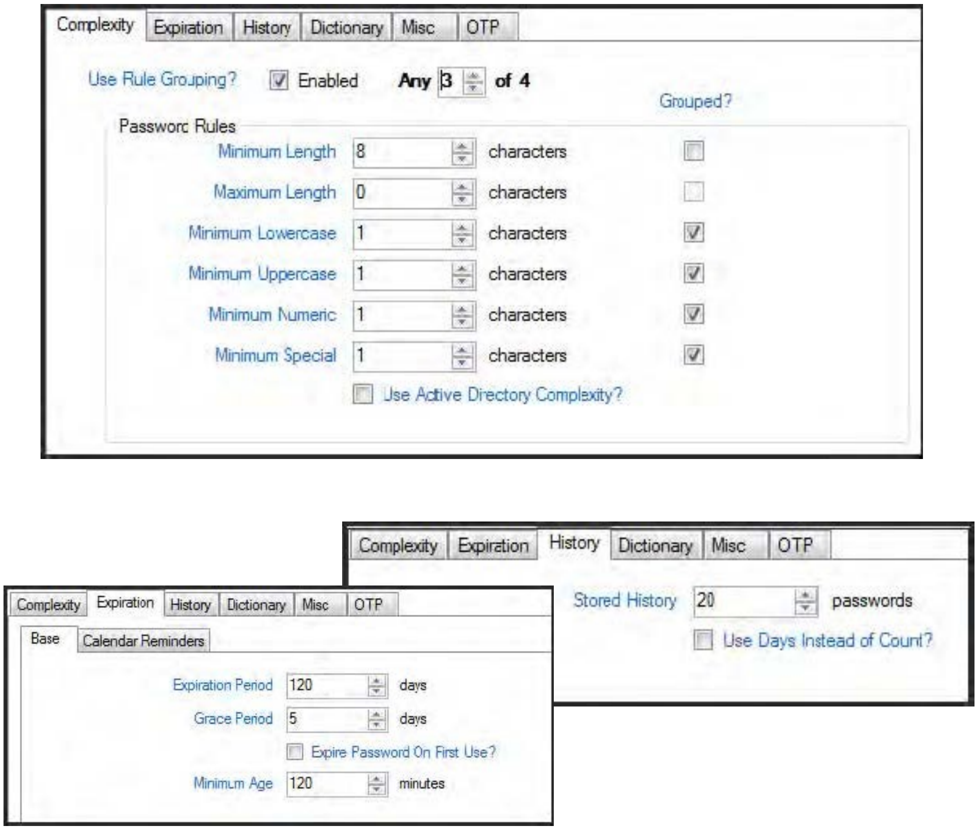
Maintaining Password Rules

IT staffers must ensure that officers have appropriately defined passwords when accessing a police department’s system. To conform to the Policy Area 6 mandate, the passwords must:

- Be a minimum length of eight (8) characters
- Not be a dictionary word or proper name
- Not be the same as the User ID
- Expire within ninety (90) days
- Not be identical to the previous ten (10) passwords
- Not be transmitted in the clear outside the secure location
- Not be displayed when entered

An IT staffer sets up the officers' accounts and issues unique user IDs when the officers join the department and first log into the system. When accessing the system, officers must enter passwords that conform to the password rules and change passwords when prompted to do so. Behind the scenes and transparent to the officers, IT staffers must enforce the password rules for the department's system

With PortalGuard, IT staffers define the password rules once and then maintain them consistently across the department's system. IT staffers set password complexity (including minimum password length), expiration, history, and dictionary terms from an easy-to-use management environment, as shown in Illustration 1.



Use Rule Grouping? ☑ Enabled **Any** 3 **of 4**

Password Rules

			Grouped?
Minimum Length	8	characters	□
Maximum Length	0	characters	□
Minimum Lowercase	1	characters	☑
Minimum Uppercase	1	characters	☑
Minimum Numeric	1	characters	☑
Minimum Special	1	characters	☑

□ Use Active Directory Complexity?

Expiration Period 120 days

Grace Period 5 days

□ Expire Password On First Use?

Minimum Age 120 minutes

Stored History 20 passwords

□ Use Days Instead of Count?

Illustration 1. PortalGuard features multiple tabs for managing password policies.

All password communications are transmitted as HTTPS/SSL requests and thus are never transmitted in the clear, even within a secure location. As a result, a police department can rely on PortalGuard to meet, or exceed, and then manage the password rules mandated by Policy Area 6.

Two Factor Authentication When Outside a Physically Secure Location

Many officers spend most of their work shifts outside their police stations: patrolling in squad cars, investigating incidents, and otherwise doing their jobs from remote locations. They use laptops mounted in squad cars and other kinds of department-issued mobile devices to connect over wireless networks to the law enforcement applications their department maintains.

When accessing these applications remotely, CJIS compliance requires Advanced Authentication with the "intent of meeting the standards of Two-Factor authentication."[2] Two-Factor Authentication combines two factors for authentication – something you know (a password) and something you have (a hardware or software token). This second factor is a One-Time Password (OTP) retrieved from a hardware key fob, smartcard, proximity badge, department issued mobile device, telephone voice message, or printed list available from the dispatcher at headquarters.

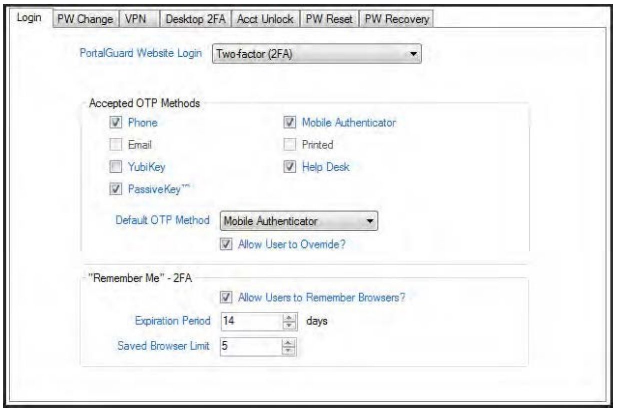
While enhancing password security, Two-Factor Authentication can impede usability. There are various situations to consider. For instance, officers may need to file incidence reports from the laptops in their squad cars. They may need to run a local application and then log into the department system. They may need to check on a situation alert from a department-issued mobile device. Adding this second factor to each username/password challenge can make repeated (and frequent) logins a time-consuming and difficult-to-use effort. Officers need a solution that affirms their identities and also expedites authentication.

PortalGuard can be configured to accommodate numerous hardware- or software-generated OTP. When securing laptops, PortalGuard includes PassiveKey, a unique capability that is installed as a web browser plug-in. PassiveKey supports Internet Explorer, Firefox, and Chrome on Windows work-stations. PassiveKey provides a transparent method for eliminating browser -based OTP prompts. PortalGuard can secure laptops disconnected from the network and allow Two-Factor Authentication with YubiKey, a hardware-based token.

PortalGuard also delivers PassiveKey Mobile to support Two-Factor Authentication through any browser on any operating system. PassiveKey Mobile is essential for securing smartphones, tablets, and access through desktop virtualization environments provided by Citrix and VMWare. Once officers authenticate manually with the second factor through a browser, PassiveKey Mobile remembers the second factor for a predefined period of time.

PortalGuard thus makes Two-Factor Authentication seamless by optionally storing the second factor for a period of time defined by the police department's operating policies. (Illustration 2 shows the management options.) This verifies that the officer requesting access to the law enforcement applications outside the police station is in fact using a predefined laptop or mobile device.

[2] See Criminal Justice Information Services (CJIS) Security Policy Section 5.6.2.2, (http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view)



PortalGuard Website Login: Two-factor (2FA)

Accepted OTP Methods

- ☑ Phone
- □ Email
- □ YubiKey
- ☑ PassiveKey™
- ☑ Mobile Authenticator
- □ Printed
- ☑ Help Desk

Default OTP Method: Mobile Authenticator

☑ Allow User to Override?

"Remember Me" - 2FA

☑ Allow Users to Remember Browsers?

Expiration Period: 14 days

Saved Browser Limit: 5

Illustration 2. IT staffers can determine the expiration period for suppressing the One Time Password prompt for Two Factor Authentication based on the security policy of their police department.

Policy Area 4: Auditing and Accountability

As part of Policy Area 4, IT staffers need to track and time stamp all events related to accessing the department's system. These events include successful logins, unsuccessful logins, and password resets. (See Appendix A for a summary of policy requirements and PortalGuard capabilities.)

PortalGuard maintains a continuous log of all authentication activities it handles – both the successful and unsuccessful login events. IT staffers can rely on PortalGuard to track all login-related events occurring on the system. PortalGuard includes several out-of-the-box reports for auditing.

In addition, IT staffers can also use their own analysis applications to develop customized reports. The logging produces SQL-formatted data, which can then be easily exported and transferred to an auditing and reporting tool such a Crystal Reports.

Simple to Administer

While needing a solution for CJIS compliance, police department executives and local government managers are also concerned about costs and predictable budgeting. Ensuring compliance should not become a financial drain on local resources.

The license fee for PortalGuard is based on a flat, server-pricing model and is designed for predictable budgeting. There is no head count or device count to consider. A single PortalGuard server can control access to multiple systems and services without additional cost. PortalGuard accommodates officers using multiple systems and devices during their shifts, a trend that is likely to only accelerate in the years ahead with the introduction of innovative digital devices into police work.

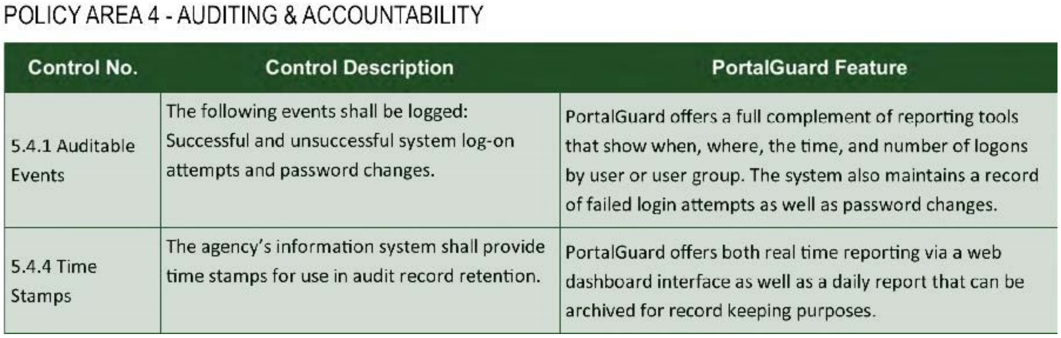
Optimizing Password Management for CJIS Compliance

An IT service provider and/or the internal computer support staff in a police department must now ensure password security for CJIS compliance, both when officers are working within a physically secure environment and when they are mobile, outside the police station. As part of the CJIS mandate, IT staffers need to consider a password management solution for Advanced Authentication involving Two-Factor Authentication.

PortalGuard delivers a CJIS-compliant solution for password security that also seeks to enhance usability. Officers can securely login to the department system and maintain their passwords. IT staffers can easily manage and track passwords across the department. They can ensure that only authorized officers, managers, and administrative staffers are gaining access, and they can log all events to verify security. With a CJIS-compliant solution in place, IT staffers can refocus their attention to supporting officers and maintaining the various law enforcement applications needed within the department.

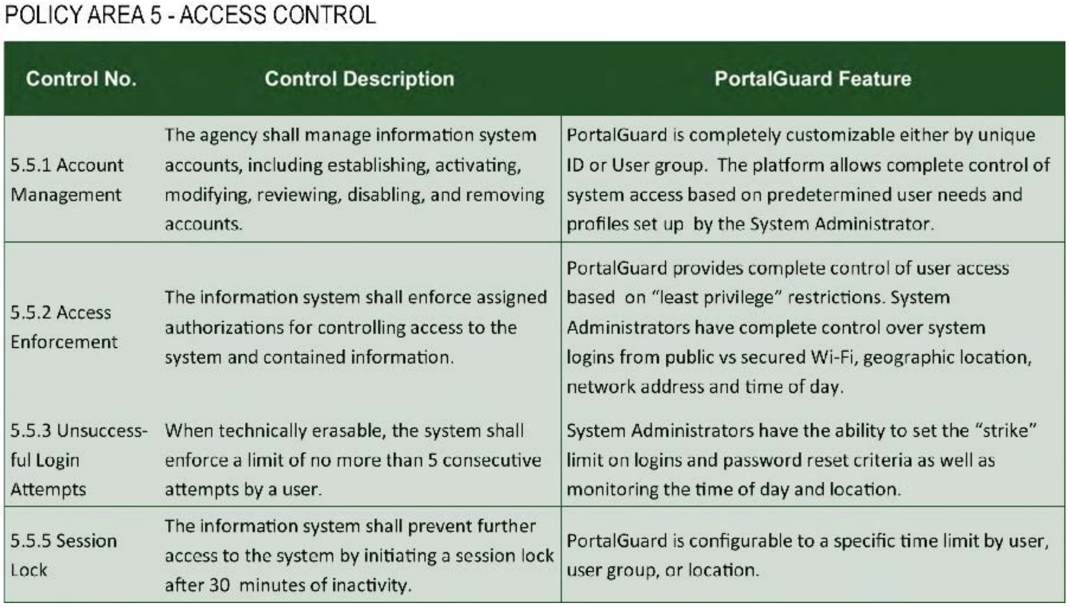
Appendix A

CJIS Guidelines and PortalGuard Features



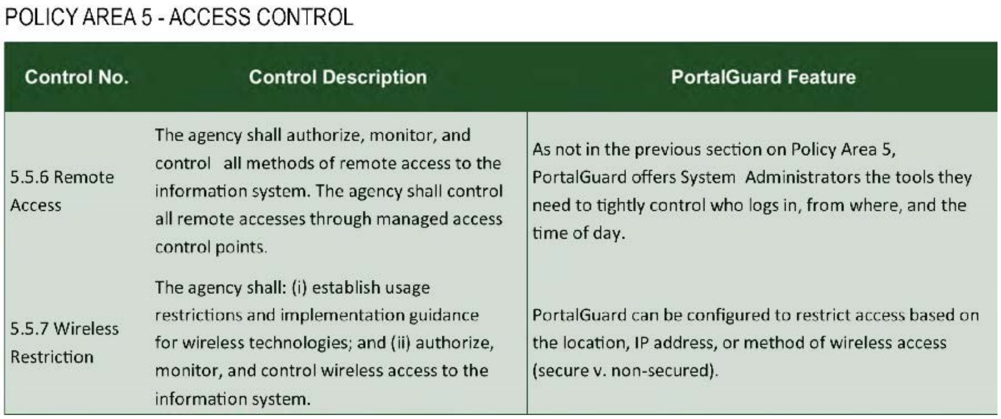
POLICY AREA 4 - AUDITING & ACCOUNTABILITY

Control No.	Control Description	PortalGuard Feature
5.4.1 Auditable Events	The following events shall be logged: Successful and unsuccessful system log-on attempts and password changes.	PortalGuard offers a full complement of reporting tools that show when, where, the time, and number of logons by user or user group. The system also maintains a record of failed login attempts as well as password changes.
5.4.4 Time Stamps	The agency's information system shall provide time stamps for use in audit record retention.	PortalGuard offers both real time reporting via a web dashboard interface as well as a daily report that can be archived for record keeping purposes.



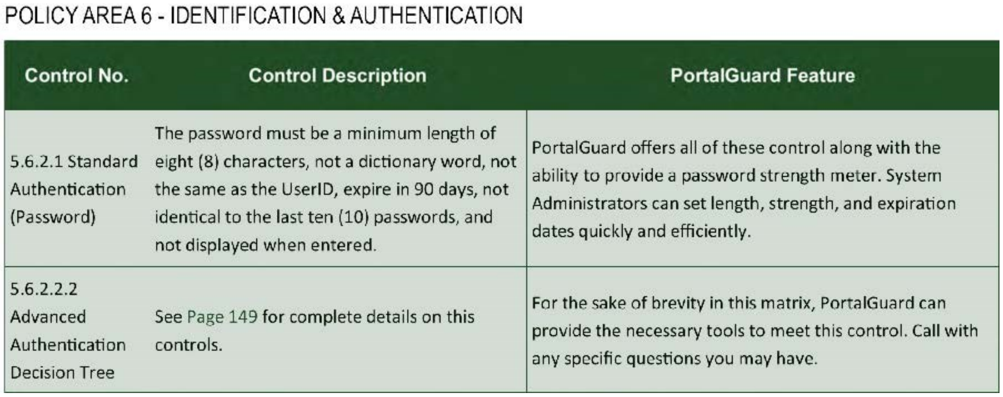
POLICY AREA 5 - ACCESS CONTROL

Control No.	Control Description	PortalGuard Feature
5.5.1 Account Management	The agency shall manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts.	PortalGuard is completely customizable either by unique ID or User group. The platform allows complete control of system access based on predetermined user needs and profiles set up by the System Administrator.
5.5.2 Access Enforcement	The information system shall enforce assigned authorizations for controlling access to the system and contained information.	PortalGuard provides complete control of user access based on "least privilege" restrictions. System Administrators have complete control over system logins from public vs secured Wi-Fi, geographic location, network address and time of day.
5.5.3 Unsuccessful Login Attempts	When technically erasable, the system shall enforce a limit of no more than 5 consecutive attempts by a user.	System Administrators have the ability to set the "strike" limit on logins and password reset criteria as well as monitoring the time of day and location.
5.5.5 Session Lock	The information system shall prevent further access to the system by initiating a session lock after 30 minutes of inactivity.	PortalGuard is configurable to a specific time limit by user, user group, or location.



POLICY AREA 5 - ACCESS CONTROL

Control No.	Control Description	PortalGuard Feature
5.5.6 Remote Access	The agency shall authorize, monitor, and control all methods of remote access to the information system. The agency shall control all remote accesses through managed access control points.	As not in the previous section on Policy Area 5, PortalGuard offers System Administrators the tools they need to tightly control who logs in, from where, and the time of day.
5.5.7 Wireless Restriction	The agency shall: (i) establish usage restrictions and implementation guidance for wireless technologies; and (ii) authorize, monitor, and control wireless access to the information system.	PortalGuard can be configured to restrict access based on the location, IP address, or method of wireless access (secure v. non-secured).



POLICY AREA 6 - IDENTIFICATION & AUTHENTICATION

Control No.	Control Description	PortalGuard Feature
5.6.2.1 Standard Authentication (Password)	The password must be a minimum length of eight (8) characters, not a dictionary word, not the same as the UserID, expire in 90 days, not identical to the last ten (10) passwords, and not displayed when entered.	PortalGuard offers all of these control along with the ability to provide a password strength meter. System Administrators can set length, strength, and expiration dates quickly and efficiently.
5.6.2.2.2 Advanced Authentication Decision Tree	See Page 149 for complete details on this controls.	For the sake of brevity in this matrix, PortalGuard can provide the necessary tools to meet this control. Call with any specific questions you may have.