thalescpl.com

THALES

How to become CJIS Compliant with SafeNet Trusted Access

Introduction

Cybercrime is recognized by the U.S. federal government as being a major threat to economic and national security. Indeed, numerous cyber attacks carried out in recent years have been aimed at government and state bodies. At the frontline of crime prevention, law enforcement agencies are vulnerable to network vulnerabilities, threats, and events which could undermine their professional abilities.

In order to ensure that law enforcement agents operate in a secure environment, the Criminal Justice Information Services Security Policy (CJIS-SP) defines requirements of timely availability of shared information and data confidentiality. The CJIS-SP must be adhered to by any organization that exchanges criminal records, including all local, state, and federal agencies that access and handle criminal justice information through its lifecycle—from creation through dissemination, whether at rest or in transit.

CJIS Authentication Requirements

To become compliant with CJIS-SP, law enforcement agencies need to implement advanced authentication (section 5.6.2.2) for cases where the risk of unauthorized access is high.

In order to successfully pass the triennial compliance and security audits by the FBI CJIS Division, CJIS-SP provides a list of advanced authentication methods that agencies can implement. Below are some guidelines that provide insight into how to select the advanced authentication method that is most appropriate to your agency.

Benefits

- **Fully automated**—Reducing the time and cost of provisioning, administration, and management of users and tokens.
- **Widest token choice**—Hardware, software, SMS, certificate/PKI-based and passwordless authentication solutions accommodate multiple use cases and risk levels.
- **Low TCO**—Reducing the total cost ofoperation compared to traditional strong authentication environments.
- **Scalability**—A comprehensive solution prepared for growth and evolving needs based on the rapid changes in the threat landscape.

Choosing an Advanced Access Management and Authentication Solution

Consider a solution that offers a choice of 2FA (two factor authentication methods)

An access management and authentication solution that offers a range of multi factor authentication methods, and form factors allows organizations to address different levels of assurance. It also lets law enforcement officers choose their authentication method depending on their user preferences and security needs.

Consider a solution that will allow you to meet CJIS schedules in a timely manner

Service-based solutions that do not require extensive infrastructure investments allow agencies to shorten time to deployment considerably. Moreover, service-based solutions offer scalability and flexibility from a budget and user management perspective.

Consider a solution that meets TCO expectations.

There are several factors that lower the overall implementation and running costs of an access management and authentication solution:

- Automated management workflows: Access management and authentication solutions that offer automated provisioning and automated workflows typically require lower management
- **Self-service portals:** Offering comprehensive self-service functions to end users lowers help desk costs by allowing them to manage ongoing administrative tasks themselves.
- **Service-based delivery:** Service-based solutions eliminate infrastructure investments and maintenance costs, significantly lowering the total cost of operations and ownership.

About SafeNet Access Management and Authentication Solutions for CJIS compliance

SafeNet Trusted Access enables law enforcement agencies to meet the CJIS Security Policy for advanced authentication with a fully automated strong authentication solution that can be delivered as a cloud-based service or installed in a local data center.

SafeNet Trusted Access addresses numerous use cases, assurance levels, and threat vectors with unified, centrally managed policies—managed from one authentication back end delivered in the cloud or on-premises.

SafeNet Trusted Access offers fully automated provisioning, and user and token administration, significantly reducing management overhead and investments compared to traditional authentication solutions. SafeNet Authentication Solutions support the broadest range of authentication methods and form factors—all of which meet the CJIS requirement for advanced authentication.

Supported Authentication Methods

- OTP Push
- OTP Software
- OTP Hardware
- Pattern-based Authentication
- Out-of-band via email and SMS text messages
- Password
- Kerberos
- Google Authenticator
- PKI Credentials
- Passwordless Authentication
- Biometric
- 3rd Party

Easily extend MFA to cloud apps

SafeNet Trusted Access Management AND multi factor authentication in One

With SafeNet Trusted Access, businesses get the best of both worlds—a broad range of authentication methods combined with intuitive cloud-based access management and single sign on.

SafeNet Trusted Access easily lets you apply the multi-factor authentication methods deployed for VPNs to cloud and web-based applications. By federating your cloud apps via SAML or OIDC and applying the same authentication methods to both VPNs and cloud apps, organizations are able to achieve consistent access security across their IT ecosystem.

About Thales's SafeNet Access Management and Authentication Solutions

Thales's industry-leading Access Management and Authentication solutions let enterprises centrally manage and secure access to enterprise IT, web and cloud-based applications. Utilizing policy-based SSO and universal authentication methods, enterprises can effectively prevent breaches, migrate to the cloud securely and simplify regulatory compliance.

> thalescpl.com <

Americas – Thales eSecurity Inc. 2860 Junction Ave, San Jose, CA 95134 USA • Tel:+1 888 744 4976 or +1 954 888 6200 • Fax:+1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific – Thales Transport & Security (HK) Lt, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel:+852 2815 8633 • Fax:+852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Europe, Middle East, Africa – Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel:+44 (0)1844 201800 • Fax:+44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com