Partner Flyer

Security

Advanced Authentication for Meeting the CJIS Mandate

The Criminal Justice Information Sharing Act (CJIS) has been a mandate since 2012. The most recent version CJIS 5.6, specifies: advanced authentication provides for additional security to the typical user identification and authentication of login ID and password, such as: biometric systems, user-based (PKI), smart cards, software tokens, hardware tokens, or "Risk-based Authentication." The challenge has been to implement a solution that is affordable, adaptable and is user and IT friendly.

Advanced Authentication at a Glance:
Advanced Authentication lets you choose the method and appliance that is right for your organization which future proof's your investment as CJIS policies evolve.

Using Right Framework

NetIQ® Advanced Authentication (AA) provides an integration framework for multi-factor authentication methods and appliances as well as other strong authentication technologies, delivering an industry-leading level of choice and flexibility. Micro Focus® provides the broadest set of application coverage to ensure that all of them are secured and CJIS compliant. Your organization will appreciate AA's support for a wide range of readers for proximity cards, fingerprint scanners for biometric scans, and other types of devices. Having the freedom to choose the right multi-factor solution for your environment gives you the freedom to deploy a solution that fits your user's authentication needs while maintaining a high level of security for your information and applications. It enables users to walk up to a computer, tap their card, and have access to all their appropriate applications or information in seconds.

Single Sign-On with Advanced Authentication Muscle

NetIQ Access Manager™ and SecureLogin deliver single sign-on for the breadth of your environment. Used together with AA allows you to meet regulatory and logical obligations across your web-based and Microsoft Windows applications. SecureLogin is compatible with the industry's standard VPN client, so even for Windows forms that are limited to password authentication, it stipulates a secondary or "step-up" authentication at the startup of an application or specified transaction, thus proving identity when and where you require it.

Securing Access to Environment

As organizations of all shapes and sizes continue to fall victim to outsider breaches, it is clear that protecting access to internal information with traditional username and password is no longer sufficient. Today, not only do organizations have information in digital format, users and their devices used to access them are continuously connected and exposed to a variety of attacks. Even when users are working from inside an organization's facilities, many of the services they access no longer reside inside their firewall's perimeter, but rather out in the cloud, allowing ubiquitous access for all, both friend and foe.

Since criminals and conspirators are effective at duping people into divulging their credentials (what they know), an effective way to increase security is to leverage what they have (such as a FIDO U2F device) or what they are (such as a biometric reader). Advanced Authentication allows a central place for all authentication policies to be managed. This approach is necessary because organizations are usually forced to administer and maintain multiple infrastructures. Not only are multiple authentication infrastructures complicated to manage, but they are also less secure. What you need is a single, two factor or multi-factor authentication framework for all of your devices and methods. Having a

Contact us at:
www.microfocus.com

Like what you read? Share it.

single framework keeps costs down, security up, and Advanced Authentication scales to any size environment.

Advanced Authentication provides broad platform support for the platforms that are key to your environment, including Windows Credential Provider, OSX, iOS, Android, Windows Mobile and Linux Pluggable Authentication.

About Envoy Data Corporation

Envoy Data Corporation's security solution practice and customer service make them an excellent choice for purchasing and deploying Advanced Authentication. Envoy Data Corporation (EDC) has over 15 years' experience architecting, distributing, deploying, and supporting complete multi-factor authentication solutions, and can assist you with a solution specified for your environment. Using Advanced Authentication's open integration framework, EDC will match the authentication experience to fit your user's needs.

In recent years, government regulators have set more stringent security policies that are more specific about the requirements for securing access to protected information. As a result, your IT security managers may face an increasingly complex challenge of keeping up with their access control needs and potential solutions. EDC's trained professionals stay current on the latest government security policies and are experts at designing an authentication that matches your organization's needs.