Entrust®
Securing Digital Identities & Information

@Entrust
EntrustSecurity

Deploying Advanced Authentication for CJIS Compliance

A proven, cost-effective strong authentication approach for law enforcement compliance in the United States

Get this White Paper

Entrust.com
1-888-690-2424
Entrust@Entrust.com

Entrust is a registered trademark of Entrust, Inc. in the United States and certain other countries. Entrust is a registered trademark of Entrust Limited in Canada. All other company and product names are trademarks or registered trademarks of their respective owners.

The material provided in this document is for information purposes only. It is not intended to be advice. You should not act or abstain from acting based upon such information without first consulting a professional.

ENTRUST DOES NOT WARRANT THE QUALITY, ACCURACY OR COMPLETENESS O F THE INFORMATION CONTAINED IN THIS ARTICLE. SUCH INFORMATION IS PROVIDED "AS IS" WITHOUT ANY REPRESENTATIONS AND/OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, BY USAGE OF TRADE, OR OTHERWISE, AND ENTRUST SPECIFICALLY DISCLAIMS ANY AND ALL REPRESENTATIONS, AND/OR WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, NON-INFRINGEMENT, OR FITNESS FOR A SPECIFIC PURPOSE.

Entrust®
Securing Digital Identities & Information

Table of Contents

Empowering Law Enforcement through Technology

For the law enforcement community, intelligence is a critical component of fighting crime. Whether patrolling in the community, protecting a border or access to an event, combating smuggling and piracy, or stopping child-trafficking, being able to verify identities and securely access and share intelligence, is critical to success.

In the United States, the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Division provides a central source of law enforcement-related information.

CJIS securely stores information on criminal groups and activities, biometric data, case histories, as well as other data for law enforcement, academic research, community awareness and support.

CJIS information is available to United States federal, state and local law enforcement agencies, law enforcement in Canada, Puerto Rico, U.S. Virgin Islands and Guam, as well as qualified academic, employment, licensing and community groups.

> *CJIS information is available to United States federal, state and local law enforcement agencies, law enforcement in Canada, Puerto Rico, U.S. Virgin Islands and Guam, as well as qualified academic, employment, licensing and community groups.*

Protecting Access to CJIS Data

To help protect access to this sensitive information, a strict set of security controls is defined in the FBI's CJIS Security Policy and must be adhered to by organizations that access CJIS information.

Applicable to criminal and non-criminal agencies alike, the policy provides a "minimum set of security requirements" for access to the CJIS database maintained by the FBI.

These requirements help ensure the security of sensitive information and provide guidance in the protection of critical Criminal Justice Information (CJI) — "from creation through dissemination; whether at rest or in transit."

The FBI's CJIS Security Policy (Section 5.6.2.2) requires organizations to implement advanced authentication controls to securely and properly access the CJIS database from non-secure locations.

Learn the reasons behind this policy change, understand the strategy for advanced authentication and review the options available to organizations to meet the stronger authentication requirements.

For information about the policy and/or compliance audits, please contact the FBI's CJIS division or visit **www.fbi.gov/about-us/cjis**.

What is Criminal Justice Information (CJI)?

CJI is sensitive information or data that is critical to the core missions of federal, state or local law enforcement agencies.

- Biometric Data
- Identity History Information
- Biographic Data
- Property Data
- Case/Incident History

For detailed definitions, see the CJIS Security Policy at **entrust.com/cjis**.

Evolving Environments for Law Enforcement Authentication

The growth of the Internet and mobile technology has helped law enforcement by facilitating the timely dissemination of crime-related information.

But it comes with the risk of sensitive information being accessed by unauthorized personnel. Simple username and password authentication is no longer sufficient protection against unauthorized access to computer networks.

Criminal organizations employ sophisticated techniques to illegally access computer networks for financial gain or competitive advantage.

Password Vulnerability

Password vulnerabilities take on many shapes, from simply peering over a user's shoulder to the more sophisticated techniques. The most popular techniques to illegally obtain passwords include malware, physical breach and rainbow tables.

Trojans, Keyloggers & Malware

These techniques are often passed to the system from a variety of sources, such as email, compromised websites, file-sharing or hacking. After compromising a system, many of these threats begin collecting usernames and passwords.

Physical Breach

By taking advantage of a breach in building security, a hacker can plug in a low-cost microcontroller hidden in a keyboard or mouse to capture plaintext passwords, hashed passwords and other data.

Rainbow Tables

A relatively new hacking technique — the use of rainbow tables — increases the threat even further. When a computer user sets a password on any system, the password is stored in a hashed format. A hashed format can be thought of as a numerical representation of the plaintext password.

When a user logs in, the hash of the entered password is compared to the hash of the stored password. If they match, the login is correct.

It is virtually impossible to “unhash” into the plaintext version. The possible combinations of upper and lowercase letters, numerals and special characters used in a password can number in the billions or trillions. So, it seems safe.

Today, any hacker can purchase a multi-terabyte external hard drive on the Internet that’s fully loaded with billions of plaintext passwords and their hashed equivalent (i.e., rainbow tables). Alternatively, hackers can download free software to create their own rainbow tables.

When the hacker gains possession of a hashed password (by means described earlier), it can take minutes to search the rainbow table and find the plaintext equivalent.

Since the employee has dozens of systems requiring a password outside of the enterprise, they begin to share the passwords across systems. The attacker will go after the weakest link, and reuse that same password for enterprise access.

Consequences of Unauthorized Access

Unauthorized access to the CJIS database presents a number of negative consequences for law enforcement, including:

- Modification or removal of arrest histories
- Access to information that could be used for fraud, blackmail or intimidation
- Embarrassment for law enforcement and government officials or agencies
- Compromise of ongoing investigations
- Jeopardizing safety of citizens
- Placing law enforcement officials at risk

Because of these threats, the FBI's CJIS Security Policy (Section 5.6.2.2) requires organizations to implement advanced authentication controls to securely and properly access the CJIS database from non-secure locations.

> *"The CJIS Security Policy provides Criminal Justice Agencies (CJA) and Noncriminal Justice Agencies (NCJA) with a minimum set of security requirements for the access to Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Division systems and information and to protect and safeguard Criminal Justice Information (CJI).*
>
> *This minimum standard of security requirements ensures continuity of information protection. The essential premise of the CJIS Security Policy is to provide the appropriate controls to protect CJI, from creation through dissemination; whether at rest or in transit."*
>
> — *Criminal Justice Information Service (CJIS) Security Policy*

Advanced Authentication

Advanced authentication securely verifies an individual's identity beyond a traditional username and password. It plays a key role in helping determine an individual is who they say they are.

Authentication methods can involve up to three factors:

Knowledge	Something the user knows *(password, PIN)*
Possession	Something the user has (token, smartcard, mobile smart credential)
Attribute	Something the user is (biometric, fingerprint, retinal scan)

Adding factors of authentication adds security and can help limit vulnerability to identity attacks. Properly designed and implemented strong authentication methods can offer stronger breach prevention with minimal user impact.

Traditionally, most law enforcement agencies relied on simple username and passwords, combined with established security processes, to manage risk.

Risks have significantly increased as field-based officers and agents access networks and databases from remote locations and identity attacks have become more common.

Deploying an advanced software authentication platform helps reduce the increased risk this creates while minimizing the day-to-day impact on the user.

Complying with the CJIS Policy

Per the CJIS Security Policy, “The agency shall identify information system users and processes acting on behalf of users and authenticate the identities of those users or processes as a prerequisite to allowing access to agency information systems or services.”

And while establishing identities secured via simple usernames and passwords is permissible for standard authentication from a secure location, access to the CJIS database from non-secure locations (e.g., patrol car) requires more advanced authentication.

> ***5.6.2.2 Advanced Authentication***
> “Advanced Authentication (AA) provides for additional security to the typical user identification and authentication of login ID and password, such as: biometric systems, user-based public key infrastructure (PKI), smart cards, software tokens, hardware tokens, paper (inert) tokens, or “Risk-based Authentication” that includes a software token element comprised of a number of factors, such as network information, user information, positive device identification (i.e. device forensics, user pattern analysis and user binding), user profiling, and high-risk challenge/response questions.”

While preventing and solving crime is a universal goal of law enforcement, there can be significant differences in authentication requirements between organizations and between user groups within an organization.

To accommodate these differences, the FBI CJIS Security Policy (Section 5.6.2.2) provides a number of acceptable advanced authentication options that law enforcement agencies can choose from.

While the demand for advanced authentication has extended beyond traditional users, technologies are also emerging that present law enforcement agencies and departments with new opportunities to improve security, while reducing operating costs.

The following authentication methods, which have broad acceptance across verticals, meet the CJIS Security Policy requirements for advanced authentication.

Authenticator	Description
Biometrics	Biometrics measure and analyze human physical characteristics — such as fingerprints, eye retinas and irises — and facial patterns to identify users. Because they can be expensive and difficult to manage, they are typically not very cost-effective for most large-scale enterprise or law enforcement deployments.
User-Based Public Key Infrastructure (PKI)	Powerful in-house or hosted PKI models allow organizations to establish and maintain a trustworthy environment by providing certificates that secure many off-the-shelf applications using encryption, digital signatures and strong certificate authentication. These solutions enable law enforcement to control access to resources, prevent theft of information and comply with regulations, including the CJIS Security Policy regulation regarding advanced authentication.
Smartcards	Because smartcards provide portable, two-factor protection for digital credentials, they are a versatile option for law enforcement considering convergence of physical and logical access security. The same card that is used for controlling access to a building (or locations within a building) can be used for logical access, whether it is network sign-on, remote access, etc.
Mobile Smart Credentials	Taking advantage of near-field communication (NFC) and Bluetooth standards, mobile smart credentials embed digital certificates on smartphones to create trusted identity credentials for stronger, more convenient enterprise or law enforcement authentication. This effectively transforms a mobile device into an efficient, cost-effective smartcard. Always on hand, these multipurpose credentials securely access computer workstations, network resources, data, cloud applications, physical doors or buildings, and also enable users to digitally sign transactions and encrypt data.

Authenticator	Description
Soft Tokens	One-time-passcode (OTP) tokens are generated on mobile devices or laptops, enabling organizations to leverage devices for strong authentication that are already widely deployed within an organization. This makes for a convenient, cost-effective way to roll-out strong authentication to a broader base of an organization's staff. Digital identities, such as those powered by a PKI, also provide benefits of second-factor authentication, without having to deploy a physical OTP. Digital certificates provide an advantage of extensibility to other functions, beyond authentication, such as encryption and digital signatures.
Physical Tokens	One of the original second-factor authentication options, tokens deliver strong authentication via a variety of form factors, including random-number OTP tokens, USB tokens and even credit card-sized tokens. Physical tokens traditionally have been relatively expensive to deploy, manage and maintain. New platform approaches to authentication have simplified the management complexity and reduced OTP token prices. Tokens can be used very effectively in combination with other authentication methods to provide agency-wide coverage based on user risk profiles.
Paper (Inert) Tokens (Grid Cards)	Security grid cards can provide strong second-factor protection using a grid card issued to each user. Users are asked to enter characters from the grid at login. Inexpensive to produce and deploy, and easy to use and support, these highly intuitive cards have a very high success rate in the enterprise. Grid cards can be produced and distributed in a number of ways, including a credit card-like format in thin plastic, paper and even virtually for electronic storage.

Authenticator	Description
Risk-Based Authentication	These non-invasive methods use a combination of techniques that are transparent to the user and only ask for additional authentication from the user when the defined criteria are not met. These transparent methods may include: ***Machine Authentication*** This non-invasive method of strengthening user authentication stores and validates a "fingerprint" of a registered machine. The fingerprint consists of a variety of elements gathered from the user's machine such as the operating system, screen resolution, browser type or even IP address. The stored machine fingerprint is compared with information gathered from the machine when a user attempts to log in. This method does not require any user interaction beyond initially registering the machine and can be very cost effective to deploy. ***IP-Geolocation*** Authenticated users can register locations where they frequently access the corporate network. During subsequent authentications, the server compares their current location data — including country, region, city, ISP, latitude and longitude — to those previously registered. Organizations only need to "step up" authentication when the values don't match. Organizations can create blacklists of regions, countries or IPs based on fraud histories. They can even leverage an open fraud intelligence network to receive updated lists of known fraudulent IPs based on independent professional analysis. ***Knowledge-Based Authentication (KBA)*** When using risk-based authentication, knowledge-based authentication is employed when the risk criteria are not met. This intuitive method of authentication uses challenge questions and answers to provide strong authentication. This enhances authentication without the need to deploy anything physical to the end-user.

Entrust®
Securing Digital Identities & Information

Selection Criteria for Law Enforcement Authentication

With such a broad range of authentication methods available, selecting the appropriate solution can be daunting. When comparing authentication options, a solution that provides multifactor authentication methods from a single administration and management platform provides the most flexibility and allows law enforcement agencies to match the appropriate authentication method with the user risk profile.

Assess key criteria when evaluating a strong authentication solution for law enforcement:

Cost	There are two critical components to total cost of ownership: purchase cost and operating cost. Be sure to thoroughly evaluate both the up-front purchase costs and the costs over the lifetime of the deployment, including device replacement, management and renewal costs. Lower total cost allows the deployment of strong authentication to more users for the same amount of budget dollars extending the security coverage.
Usability	Not all users are the same and not all user environments are created equal. When choosing authentication methods, consider the user's technical capabilities; ease-of-use consideration (e.g., desk vs. car) and environmental conditions (e.g., user likely to get wet, dirty, etc.). No matter what the authentication method or deployment plan, new authentication methods should not fundamentally change the way employees are accustomed to working. Choose a system that can follow existing user-interaction models and minimize the need for additional technology knowledge for employees.
Flexibility	Invest in a platform with multiple authentication options that allow companies to match the authentication method to the risk profile of the user. Investing in systems that provide only certain authentication methods ignores the inevitable need to make changes and enhancements to authentication over time. Choose a platform that addresses all needs now and can grow and change as requirements evolve.

Assess key criteria when evaluating a strong authentication solution for law enforcement:

Integration	Authentication is one part of an identity-based security model. Choose a platform that is integrated with key enterprise applications, including: • Leading VPN remote access vendors, such as NetMotion, Cisco, Check Point and Juniper • Standard Microsoft Windows client • Web services and leading applications like Microsoft Outlook Web Access or SharePoint
Security Leadership	Choose a company that is an established security leader with a trusted reputation and focused dedication to assist in determining the proper balance between security requirements, budget and usability for the company's unique situation.

Entrust Solutions for CJIS Compliance

Entrust's comprehensive suite of identity-based security solutions are designed, in part, to help law enforcement comply with requirements mandated by the Federal Bureau of Investigation's (FBI) Criminal Justice Information Services (CJIS) Division.

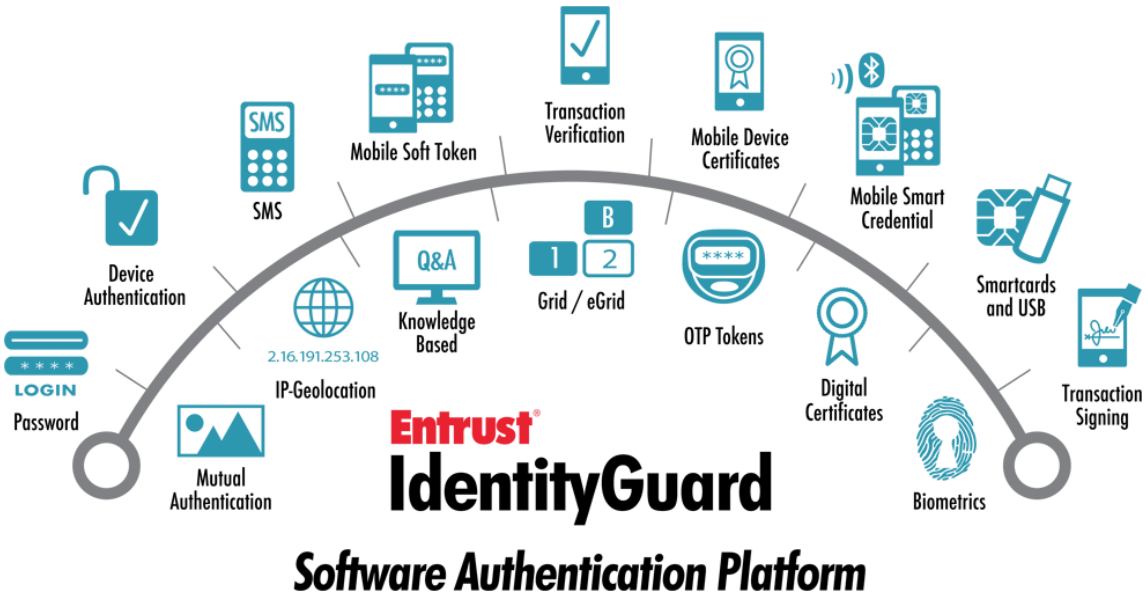
Entrust IdentityGuard

Entrust's strong authentication platform enables identity-based security to safeguard access to sensitive information and intellectual property for agents, officers, court officials and more.

While harnessing the power of existing end-user devices as authenticators for physical, logical and cloud application access provides clear value, Entrust's comprehensive authentication platform also integrates with existing IT systems and business processes for unmatched deployment versatility.

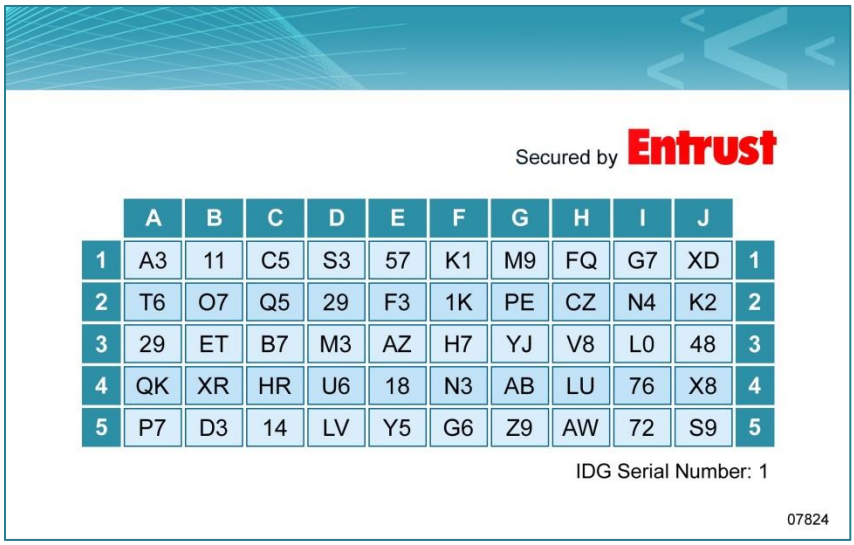
With the flexibility to be co-deployed alongside outgoing legacy systems, Entrust's comprehensive software authentication platform bridges emerging technologies for strong mobility, cloud and smart credentialing offerings.

The solution enables organizations to layer security — according to access requirements or the risk of a given transaction — across diverse users and applications.



Entrust's diverse set of authentication capabilities include user-based public key infrastructure (PKI), smartcards (plastic and mobile), software tokens, hardware tokens, grid cards and eGrids (inert tokens), risk-based authentication (e.g., machine, IP-geolocation, knowledge-based), out-of-band one-time passcode (delivered via voice, SMS or email), out-of-band transaction verification and a range of OTP tokens.

Offering the broadest range of authenticators in the market, Entrust's software authentication platform is often leveraged to solve challenges related to specific use cases, including CJIS compliance for secure access to FBI databases.



The Entrust-patented grid card is a credit card-sized authenticator consisting of numbers and characters in a row-column format. Upon login, users are presented with a coordinate challenge and must respond with the information in the corresponding cells from the unique grid card they possess.

Extending the Security Investment

In an economy where budgets and resources are constantly under pressure, organizations cannot afford to buy single-purpose solutions.

Entrust's platform approach to advanced authentication allows organizations to leverage their existing investment to increase security and productivity in other areas.

Logical Access Control

Entrust solutions authenticate individuals prior to accessing sensitive computer networks, a method commonly known as secure logical access control (LAC). Entrust supports a broad range of user authentication methods including physical (e.g., a one-time-passcode token or grid card), mobile- and smartcard-based, or online (e.g., passwords plus questions and answers).

This allows organizations to deploy authentication methods that will ensure strong authentication of the user, be convenient and simple for the individual to use, and meet the budgetary requirements of the organization.

Physical Access Control

Entrust authentication solutions integrate with physical access control (PAC) systems to ensure only authorized individuals have physical access to buildings, arms lockers and lockups (e.g., confiscated material, evidence).

Employing the latest technology, Entrust captures user information, encodes it on the latest standards-based chip technology and ensures user information remains secure and tamper-proof on the device while communicating with the PAC system.

For physical access control to permanent or virtual borders, Entrust PKI capabilities provide tamper-proof credentials for citizens based on International Civil Aviation Organization (ICAO) Basic Access Control (BAC) and Extended Access Control (EAC) international standards.

Combined Physical & Logical Access Control

Entrust solutions allow law enforcement agencies and organizations to consolidate physical and logical access control with a uniform user identity that is managed via a single comprehensive software platform.

This provides the user with the convenience of a single authenticator while consolidating management, improving the return on investment and providing a stronger security position.

Secure Collaboration

The critical exchange of sensitive intelligence — whether within a single law enforcement organization or across the globe — must be executed securely and in a timely manner to protect the integrity of both the information and investigation.

Entrust secure collaboration solutions provide the ability to share and communicate information securely between individuals and groups.

The information may be encrypted — preventing unauthorized reading of the text — either by the individual at the time of sending or automatically before it leaves the organization. This facilitates the secure, free flow of information that is critical to preventing and fighting crime.

Entrust®
Securing Digital Identities & Information

Entrust IdentityGuard provides strong authentication for applications, including:

- Remote access (secure IPSEC and SSL VPN provided from leading vendors, including NetMotion, Cisco, Check Point, Citrixl, Juniper and Avaintail)
- Native Microsoft® Windows® desktop application integration
- Leading Web applications like Microsoft® Outlook Web Access
- Smartcard management, including physical and logical access
- Mobile authentication on smartphone platforms (e.g., Google Android, RIM BlackBerry, Apple iOS, Symbian, Windows Mobile)
- Multifactor options for diverse user groups for any environment (e.g., grid cards, physical tokens, mobile devices or smartcards)

Entrust IdentityGuard Helps:

- Issue, vet and manage all digital identities within an organization or law enforcement agency — and all from a single software authentication platform
- Simplify migration from outgoing legacy systems via advanced co-deployment capabilities
- Streamline administration with central policy management that can help decrease the risk of policy inconsistency
- Integrate with existing IT systems and business processes for unmatched deployment versatility
- Enable compliance to industry regulations such as HIPAA, CJIS and SOX
- Harness the power of existing end-user mobile devices as authenticators for physical, logical and cloud application access
- Prepare for what comes next thanks to a standard-based architecture and open platform committed to adding new and innovative authentication options

Entrust IdentityGuard — Industry Accolades

- Winner in SC Magazine Awards for “Best Multifactor Product,” **SC Magazine, February 2014**
- Winner in SC Magazine Awards for “Best Multifactor Product,” **SC Magazine, February 2012**
- Finalist in SC Magazine Awards for “Best Multifactor Product,” **SC Magazine, February 2011**
- Finalist in SC Magazine Awards for “Best Managed Security Service,” **SC Magazine, February 2011**
- Winner of “Best Buy” award for top authentication platform (five-star rating), **SC Magazine, January 2011**
- Winner of “Best Buy” award for top authentication platform (five-star rating), **SC Magazine, January 2010**
- Winner of “Product Innovation Award,” **Network Products Guide, January 2009**
- Finalist of “Best Security Solution” in the **24th Annual SIIA CODiE Awards, January 2009**

Entrust & You

More than ever, Entrust understands your organization's security pain points. Whether it's the protection of information, securing online customers, regulatory compliance or large-scale government projects,

Entrust provides identity-based security solutions that are not only proven in real-world environments, but cost-effective in today's uncertain economic climate.

Now part of Datacard Group, Entrust offers software authentication platforms that strengthen security in a wide range of identity and transaction ecosystems. Government agencies, financial institutions and other enterprises rely on Entrust solutions to strengthen trust and reduce complexity for consumers, citizens and employees.

Entrust offers an expanded portfolio of solutions across more than 150 countries. Together, Datacard Group and Entrust issue more than 10 million secure identities every day, manage billions of secure transactions annually and issue a majority of the world's financial cards. For more information about Entrust products and services, call **888-690-2424**, email **entrust@entrust.com** or visit **entrust.com/cjis**.

Company Facts

Website: www.entrust.com
Employees: 359
Customers: 5,000
Offices: 10 Globally

Headquarters

Three Lincoln Centre
5430 LBJ Freeway, Suite 1250
Dallas, Texas 75240

Sales

North America: 1-888-690-2424
EMEA: +44 (0) 118 953 3000
Email: entrust@entrust.com

@Entrust
EntrustSecurity