CORE
TECHNOLOGY®
at the center of connectivity

Technical Security Information

To assist you in answering technical security questions about Core Technology Corporation's software, we have compiled a list of the most frequently asked about subjects. The exact technical descriptions will depend on the Core Technology products you have in your configuration. Please read all sections that apply to the Core Technology products you use.

Contents

How are criminal justice information (CJI) users authenticated?

When more than one Core Technology product or configuration applies, combinations of the following authentication descriptions may apply. Please read all sections that apply to the Core Technology products you use.

Talon via Local Area Network (LAN)

- Each end user requires a valid “Talon” username and password to access the Talon system. The username is unique for the system. Please see the **Talon Password Policies** section for more information
- The username and unique device ID can be linked in the server software configuration, so the end user’s credentials must not only be in the system independently, they must also be used together in order to be granted access. This limits users to only the device(s) they have been authorized to use, and it provides an easy method to revoke that right
- The system also enforces that only one user can connect from an authorized username account at a time. This guarantees exclusive use of the device for an authorized user when they need it, but allows an expensive device to be shared when appropriate
- The system includes server administration software to allow access control of users, passwords, and device IDs. A user can be disabled to prevent unauthorized access. The device ID can be disabled separately to prevent unauthorized access

Talon via Internet

In addition to the **Talon via LAN** authentication description above, the following also applies:

- Whether a VPN is used or not, the method used for remote Talon MDC or Desktop clients to communicate back to the server is a secure, encrypted, VPN-like connection. The Talon MDC or Desktop client connects on a single, encrypted port back to the server. The server software will reject any client connection on this single port if the client is not communicating with the correct protocol. In addition, the client connection will be rejected if the client is not an authorized user, if the connection is not originating from an authorized device, or if the device is not associated with the user. Communication is encrypted end-to-end. This method of secure communication limits remote access to only one specific application instead of general access to a network and/or server for even more security than a VPN.
- Data is encrypted on the entire path to and from the device and server using AES 256-bit encryption provided by BC-FJA (Bouncy Castle FIPS Java API). Please see the **Software Encryption Certificates** section for more information. The NIST certificate number is 3152
- Usage of VPN software is independent of Core Technology's Talon solution

Talon React App

The previous **Talon via LAN** authentication description applies to the Talon React App. Additionally, the App enforces advanced authentication using the Talon Authentication Matrix. See the **Talon Authentication Matrix (TAM)** section below for an explanation of the user authentication method using TAM.

It is recommended by Core Technology and mandated by state requirements that Mobile Device Manager Software (e.g., Meraki Systems, MaaS360, etc.) be used with the Talon React App.

Advanced Authentication Products

Talon Authentication Matrix (TAM)

In addition to the Talon descriptions above (**Talon via LAN**, **Talon via Internet**), the following also applies when TAM is used in conjunction with Talon (Desktop/MDC). Additionally, the Talon React App requires this second-factor authentication method:

- This TAM second-factor authentication application requires the user to authenticate initially using the first-factor Talon authentication methods described above, which requires a valid "Talon" username and password and proof of possession of the valid hardware device.
- Through a secure communication protocol, an electronic GRID of alphanumeric characters is used to provide a disguised one-time passcode to the user. The user will be required to analyze the GRID and identify the alphanumeric characters found in his or her predefined pattern. Each logon will utilize a different GRID resulting in a unique passcode. This one-time passcode, generated by token software on the device, will be used in addition to the username/password and unique device ID to grant access.
- The one-time passcode is generated based on a combination of the device ID, information about the user and a time stamp nonce.
- The passcode will be valid for 60 seconds. In the unlikely event that a hacker has broken the 256-bit encryption used for messages, this feature adds a time sensitive code to avoid previously captured information from being reused in replay attacks.
- No key is stored on the hardware device. The information used to generate the key is gathered in real-time and submitted to a secure server, over an encrypted connection. Since nothing is stored on the device, nothing can be taken or copied from the device and moved to another device. In addition, because the information is only stored at the server, it is not susceptible to offline passive attacks.
- The entire authentication transaction is encrypted, using FIPS 140-2 compliant 256-bit AES encryption. This prevents eavesdropper attacks. Please see the **Software Encryption Certificates** section for more information. The NIST certificate number is **2473**.

Core Authentication Matrix (CAM)

Core Authentication Matrix may be used independent of any Talon products to secure a device with multi-level authentication. CAM provides additional security to the typical user authentication of a login username and password, which may be defined in the enterprise directory (Microsoft Active Directory – NTLM or Radius).

- The CAM second-factor authentication application requires the user to authenticate initially using the first-factor enterprise authentication method for the device by providing a valid "enterprise" username and password.
- Through a secure communication protocol, an electronic GRID of alphanumeric characters is used to provide a disguised one-time passcode to the user. The user will be required to analyze the GRID and identify the alphanumeric characters found in his or her predefined pattern. Each logon will utilize a different GRID resulting in a unique passcode. This one-time passcode, generated by token software on the device, will be used in addition to the username/password and unique device ID to grant access.
- The one-time passcode is generated based on a combination of the device ID, information about the user and a time stamp nonce.
- The passcode will be valid for 60 seconds. In the unlikely event that a hacker has broken the 256-bit encryption used for messages, this feature adds a time sensitive code to avoid previously captured information from being reused in replay attacks.
- No key is stored on the hardware device. The information used to generate the key is gathered in real-time and submitted to a secure server, over an encrypted connection. Since nothing is stored on the device, nothing can be taken or copied from the device and moved to another device. In addition, because the information is only stored at the server, it is not susceptible to offline passive attacks.
- The entire authentication transaction is encrypted, using FIPS 140-2 compliant 256-bit AES encryption. This prevents eavesdropper attacks. Please see the **Software Encryption Certificates** section for more information. The NIST certificate number is **2437**.

Talon Password Policies

- User accounts may be administratively locked
- User accounts are automatically locked after five (5) failed login attempts
- Passwords are encrypted when transmitted
- Passwords are not displayed when entered
- Passwords may not be the same as the username
- Passwords may not be a dictionary word or proper name
- Passwords must contain a minimum of eight (8) characters
- Passwords must be changed at least every ninety (90) days
- Passwords may not be the same as the last ten (10) passwords

Talon Event/Activity Logging

The following events/activities are logged. The lines marked with an asterisk (*) will be logged in an upcoming software version release:

- Successful/Unsuccessful system log on attempts
- Successful/Unsuccessful attempts to access, create, write, delete, or change permission on user account

  NOTE: If your agency is self-hosted and has its own MultiBridge (meaning you are not hosted on the Core Service Bureau), then we do not have control over user access to file directories.
- Successful/Unsuccessful attempts to change passwords
- Successful/Unsuccessful actions by privileged accounts
- Successful/Unsuccessful attempts for users to access/modify/destroy audit log file.

  NOTE: If your agency is self-hosted and has its own MultiBridge (meaning you are not hosted on the Core Service Bureau), then we do not have control over user access to file directories.
- Date and time of event
- Component of information system (i.e., software/hardware component)
- Type of event
- User/subject identity
- Outcome (success/failure of event)

Logs are retained until the agency manually removes the logs.

Data Encryption

Talon (Desktop and MDC)

Data Transactions

The user authentication transaction and all CJI data being sent and received from the Talon MDC or Desktop client software uses AES 256-bit encryption provided by BC-FJA (Bouncy Castle FIPS Java API), This encryption is present independent of the network used (e.g., LAN, WAN, internet, fiber, etc.). Please see the **Software Encryption Certificates** section for more information. The NIST certificate number is 3152.

Data at Rest

CJI data at rest on the device is also encrypted using AES 256-bit encryption provided by BC-FJA (Bouncy Castle FIPS Java API). Please see the **Software Encryption Certificates** section for more information. The NIST certificate number is 3152.

Advance Authentication Products

Data Transactions

Core Technology's Advanced Authentication products (Talon Authentication Matrix and Core Authentication Matrix) encrypt the entire user authentication transaction using FIPS 140-2 compliant 256-bit AES encryption. Please see the **Software Encryptions Certificates** section for more information. The NIST certificate number is **2473**.

Data at Rest

There is no CJI data at rest on the device.

Talon React App

Data Transactions

The user authentication transaction and all CJI data being sent and received from the Talon React App uses FIPS 140-2 compliant 256-bit AES encryption. Please see the **Software Encryption Certificates** section for more information. The NIST certificate number is **2473**.

Data at Rest

There is no CJI data at rest on the device. The Talon React App does not cache any data on the device and clears the browser cache when the application is closed.

Software Encryption Certificates

NIST Certificate Number 3152

Core Technology software provides encryption according to the Federal Information Processing Standards (FIPS) approved encryption algorithms. All data being sent and received from the software uses AES 256-bit encryption provided by BC-FJA (Bouncy Castle FIPS Java API). BC-FJA (Bouncy Castle FIPS Java API) cryptographic algorithms are FIPS 140-2 validated. Data is encrypted on the entire path to and from the device and server.

NIST Certificate Number 2473

Additionally, Core Technology's software encrypts communication with application servers using encryption provided by OpenSSL FIPS. OpenSSL FIPS cryptographic algorithms are also FIPS 140-2 validated.

CSB Hosted Users - Core Technology Internal Security

For those agencies that are hosted at the Core Service Bureau (CSB), Core Technology Corporation adheres to the CJIS Security Policy. Core Technology will submit, as needed, the following for each employee with a potential need to support the agency. Please contact Core Technology for these or other records.

- Fingerprints
- Signed security addendums
- Security-awareness training logs