Overview

This document contains an overview of the efforts undertaken by the North Carolina CJIS v5.1 Working Group. The CJIS working group was convened by the UNC School of Government and the North Carolina Local Government Information Systems Association (NCLGISA) in early August to develop proposed scenarios and identify clarification questions in order to facilitate local NC law enforcement agencies' compliance with the FBI's CJIS v5.1 requirements (released July 13, 2012). These scenarios and questions have been submitted on behalf of the working group to the SBI and FBI for comment. The next section outlines the scenarios submitted and their approval or rejection status.

The CJIS working group's primary focus was to identify FBI-approved strategies for complying with CJIS v5.1 requirement 5.6.2.2, Advanced Authentication, as the FBI will consider police vehicles to be unsecure locations after 30 Sept 2014 (extension granted in February 2013), thereby requiring Advanced Authentication mechanisms to be used on all MDTs. **Please note, the extension for the Advanced Authentication requirement does not apply if any of the following criteria apply to your agency:**

1. If your agency has purchased/implemented a new CAD/RMS since 2005 (including changing from one vendor to another), then AA is required now for all mobile devices.
2. If your agency has significantly upgraded (defined as costing 25% of the initial software contract price) its CAD/RMS since 2005, then AA is required now for all mobile devices.
3. If your LEOs remove their MDTs from the police car and engage in any activities involving CJI while the MDT is outside of the vehicle (i.e. report writing or DCI queries with the laptop sitting on the trunk of the car), then AA is required for those mobile devices.

The scenarios submitted to the SBI and FBI were specifically addressing the Advanced Authentication requirement in environments where the department's Mobile CAD/RMS solution is not CJIS-compliant (i.e., does not utilize Advanced Authentication). Currently, some of the mobile CAD/RMS vendors have already integrated Advanced Authentication into their offerings, or plan to do so before the deadline, so the agencies using those solutions will not need the measures documented in Scenario A or C (noted below).

As individual agencies develop their own solutions, outside of the model noted below, they can submit their proposed solution to the SBI directly or work with Shannon Tufts at the UNC School of Government to provide initial review and facilitation of the process[1]. For those agencies seeking to submit proposals, this is the suggested format and it is also useful to provide a flow diagram of the actual step-by-step process.

[1] Dr. Shannon Tufts, UNC School of Government, 919.962.5438, tufts@sog.unc.edu

Scenario A: FBI Approved CJIS v5.1 Compliant Solution

- FBI Approval: "We agree that as described in the vendor specific flow description (using RSA tokens or USB devices) the process would be compliant with the CSP requirement for Advanced Authentication (AA). As you correctly point out there will be variations, and each one of those would have to be given the same level of scrutiny to determine the compliance of that implementation." Email received on 19 Sept 2012 from CJIS ISO Program Analyst, FBI

- Please note that this description is vendor-specific in order to provide a high level of detail to the FBI/SBI in order to alleviate specified concerns about the vendor-agnostic/general description. The FBI could not approve the generic description noted below the vendor-specific scenario because they require specific details that can only be indicated when the hardware and software is properly identified.

Vendor Specific Flow Description (NetMotion VPN, RSA Token)

Step 1: Officer logs into MDT with user name and password.

Step 2: Officer launches NetMotion VPN Client.

a. NetMotion, a FIPS 140-2 certified VPN termination point, is configured by the local agency to require the use of AA (meeting the requirements of CJIS v5.1 Section 5.6.2.2) for the "CJIS Users" group that need to execute CJI queries from the Mobile CAD/RMS application.
b. In this example, the NetMotion server is configured to use RSA tokens for its AA requirement. The local agency determines which users are assigned to which group ("CJIS Users" or "Generic Users") based on credentials assigned by the State Bureau of Investigation to access DCI.

Step 3: At the NetMotion login prompt, the Officer is asked to enter his/her username and a unique four to eight (4-8) digit PIN that is assigned to each individual officer by the local agency, plus a six (6) digit passcode that is supplied by the RSA token. The passcode is digitally reset/refreshed every 60 seconds.

a. The system could also use a RSA USB Key that automatically provides the changing passcode, thereby only requiring the officer to know his/her username and 4 digit PIN.
b. "Generic Users", or non-CJIS users, of the NetMotion VPN are housed on a separate NetMotion server and are only required to enter a username and password to access NetMotion.

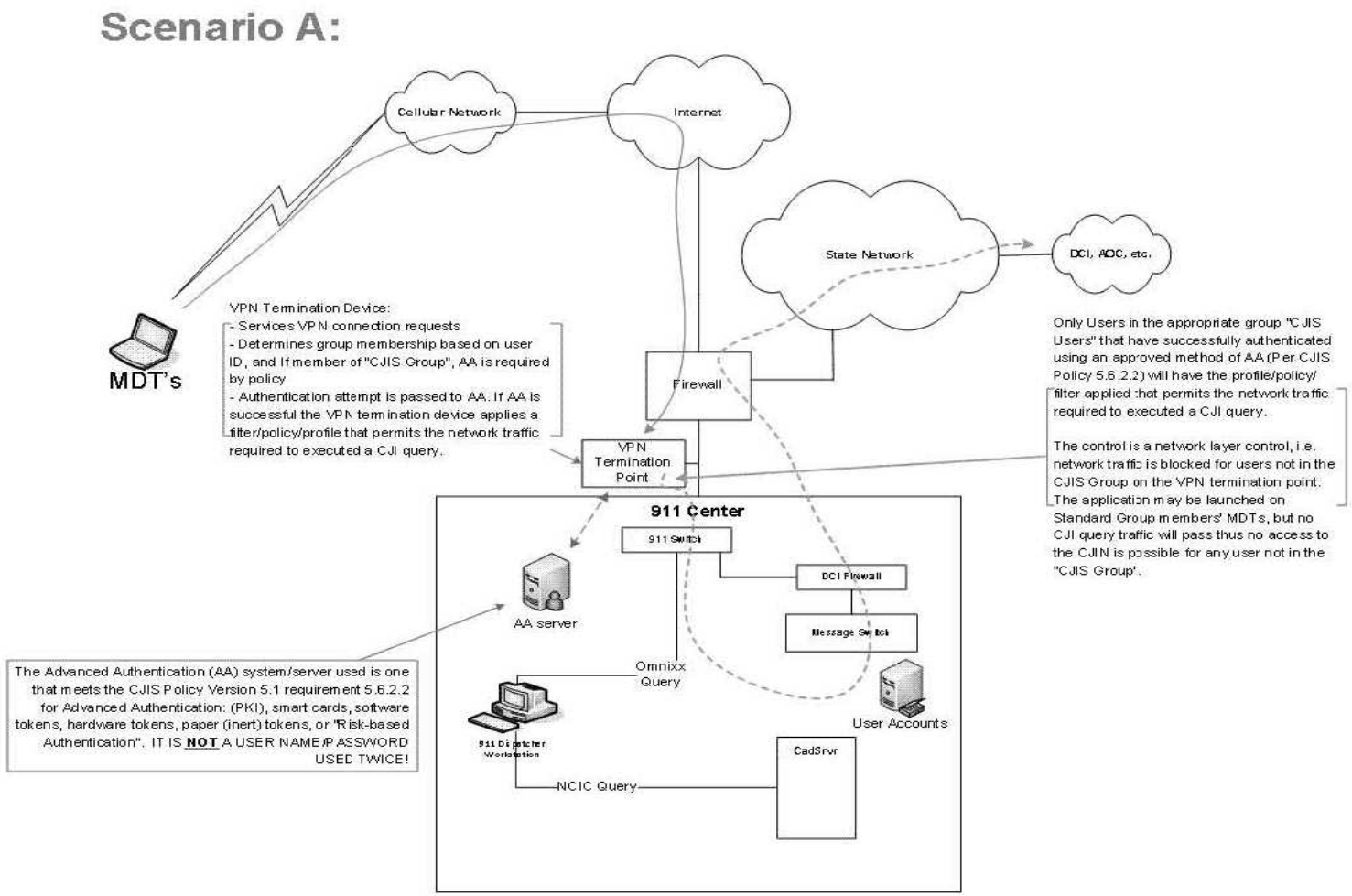
Step 4: The flow for the NetMotion VPN termination point is:

a. Receives VPN connection request from Officer in Step 1.
b. Identifies that the Officer is in the "CJIS Users" group and therefore required to use AA as specified in Step 2.
c. Passes authentication required to AA system and receives authorization.

d. Applies the "CJIS Users" policy/profile/access control filter that permits the network traffic required to execute a CJI query.

Note: The AA server is not connected to nor asserting credentials to the CJI application (i.e. OSSI MCT) but only used to validate the establishment of VPN for this particular group.

Net result: Only AA authenticated users in the appropriate group (CJIS Group) with the appropriate profile/policy/access controls applied at the VPN termination point (i.e. Cisco, Microsoft, NetMotion servers) are technically able to execute CJI queries. The control is a network layer control, i.e. network traffic is blocked for users not in the CJIS Group on the VPN termination point. The application may be launched on Generic Group members' MDTs, but no CJI query traffic will pass thus no access to the CJIN is possible for any user not in the "CJIS Group".


Scenario A:
Cellular Network
Internet
State Network
DCI, AOC, etc.
MDT's
VPN Termination Device:
- Services VPN connection requests
- Determines group membership based on user ID, and If member of "CJIS Group", AA is required by policy
- Authentication attempt is passed to AA. If AA is successful the VPN termination device applies a filter/policy/profile that permits the network traffic required to executed a CJI query.
Firewall
VPN Termination Point
Only Users in the appropriate group "CJIS Users" that have successfully authenticated using an approved method of AA (Per CJIS Policy 5.6.2.2) will have the profile/policy/ filter applied that permits the network traffic required to executed a CJI query.
The control is a network layer control, i.e. network traffic is blocked for users not in the CJIS Group on the VPN termination point. The application may be launched on Standard Group members' MDTs, but no CJI query traffic will pass thus no access to the CJIN is possible for any user not in the "CJIS Group".
911 Center
911 Switch
DCI Firewall
Message Switch
AA server
Omnixx Query
User Accounts
911 Dispatcher Workstation
CadSrvr
NCIC Query
The Advanced Authentication (AA) system/server used is one that meets the CJIS Policy Version 5.1 requirement 5.6.2.2 for Advanced Authentication: (PKI), smart cards, software tokens, hardware tokens, paper (inert) tokens, or "Risk-based Authentication". IT IS NOT A USER NAME/PASSWORD USED TWICE!

Generic Description/Vendor Agnostic Scenario A: This scenario is not approved or commented on by FBI due to limited detail, but it is offered to guide local agencies as they seek to implement a solution.

Description of the Environment:

An officer is in the police car with MDT. The MDT is running Mobile CAD/RMS application & FIPS 140-2 certified VPN capability/agent/software. There is a Local Agency Network VPN termination point, with two groups configured on VPN termination point (one group is the CJIS users group, called "CJIS Users", the other group is all non-CJIS users, called "generic group"). Those two groups have two separate policies/profiles/access control filters applied to them:

1. The VPN Termination Point leverages a username or some other identifier (varies by type of AA) to determine what "pre-defined" group a user object is a member of (i.e. rights driven access). E.g., on the VPN Termination Point/Device there exists a group, that group's name is "CJIS Users". The "CJIS Users" group has user objects associated with it, such as "JSmith". If JSmith's user name, "JSmith", is received by the VPN Termination Point/System, the VPN Termination Point/System enforces its pre-configured policy/profile. CJIS Group must use AA for VPN access and applies a policy/profile/access control filter permits the network traffic required to execute CJI queries from the Mobile CAD/RMS application.

2. In this example, all members of the "CJIS Users" group (including "JSmith") are required to use the AA server for authentication. This is accomplished by passing all received authentication data to the pre-configured AA system. The pre-configured AA system validates the authentication and acknowledges this to the VPN Termination Point/System. The VPN Termination Point/System then applies the profile/policy/filter that has been pre-configured for the "CJIS Users" group. The applied profile/policy/filter permits the network traffic required to execute a CJI query.

3. All other Groups/Users, called "Generic Users", do not have the same profile/policy/filter applied as they are not in the "CJIS Users" group and therefore are not able to successfully execute a CJI query. "Generic Users" Group uses username/password and applies a policy/profile/access control filter that explicitly prohibits the network traffic required to execute CJI queries.

4. Any AA used will meet the CJIS Policy Version 5.1 requirement 5.6.2.2 for Advanced Authentication: (PKI), smart cards, software tokens, hardware tokens, paper (inert) tokens, or "Risk-based Authentication".

5. The AA system is tied into VPN termination point (server/appliance/system) but the AA system/server not connected to the CAD/RMS application and therefore unable to assert the credentials to the CAD/RMS application.

Please note that this scenario has been REJECTED.
It is offered as a sample of what will not be allowed by the SBI/FBI.

Scenario B: FBI Rejected CJIS v5.1 Solution

- This scenario has been rejected by the FBI per the following statement:
  "Scenario B, as written, would not be in compliance with the CSP, because the access control is determined upon login of the MDT. **This would be considered local device authentication and not permissible as a proper advanced authentication (AA) solution which requires each individual's identity be authenticated at either the local agency, CSA, SIB or Channeler level**."
  Received from CJIS ISO Program Analyst, FBI, on 10 Sept 2012.

- Please note that **CJIS v5.1 does not permit local device authentication** as being compliant with the Advanced Authentication requirements.

Description of the Environment:
An officer is in the police car with MDT. The MDT is running a Mobile CAD/RMS application from a specific folder on the MDT. This folder is restricted to only those individuals that are in the appropriate group/role-based access control ("CJIS Users") , and have the "CJIS Users" profile/policy applied.

Flow Description:

Step 1: Officer logs into MDT with AA as his user object is a member of the "CJIS Users" group/role-based access control. AA systems/services are tied into an AA solution on the local agency network but functioning in an encrypted offline/cached mode until the MDT establishes a VPN connection w/ the local agency network.

Step 2: Officer launches VPN and establishes a FIPS 140-2 compliant encryption connection to local agency network.

Step 3: Officer executes Mobile CAD/RMS application. Application runs only because the Officer's user account/object/profile is a member of the "CJIS Users" group and the appropriate profile/policy/permissions are applied that provide access to the application/folder/executable.

Net result: Only AA authenticated users in the appropriate group (CJIS Group) with the appropriate profile/policy/access controls applied at folder/application are able to run the Mobile CAD/RMS application and execute CJI queries. The control is at the folder/application executable level, and only those users in the appropriate group have the ability to run the application.

Scenario C: FBI Approved Vendor Specific Scenario

- FBI Approval: "With one exception, the proposed advanced authentication solution to scenario #3 is compliant with the CJIS Security Policy. Policy needs to be instituted requiring the officer's personally owned cell phone have a PIN, or another unique form of identification, to access their phone. This ensures it's the officer responding to the PhoneFactor service (integrity of second factor) and not simply someone who happens to be in possession of the phone at the time…and has the officer's user name and password. This AA scenario narrative was presented very well and the accompanying diagram was helpful, too." Email received on November, 5, 2012 from CJIS ISO Program Analyst, FBI

- ***Please note that I have inserted the required PIN/passcode language into the Scenario description below.***

Vendor Specific Flow Description (Sonicwall VPN, Phone Factor)

Step 1: Officer logs into MDT with user name and password.

Step 2: Officer launches Sonicwall VPN Client.

a. Sonicwall NSA 4500, a FIPS 140-2 certified VPN termination point, is configured by the local agency to require the use of AA (meeting the requirements of CJIS v5.1 Section 5.6.2.2) for the "CJIS Users" group that need to execute CJI queries from the Mobile CAD/RMS application.
b. In this example, the Sonicwall server is configured to use Phone Factor for its AA requirement. The local agency determines which users are assigned to which group ("CJIS Users" or "Generic Users") based on credentials assigned by the State Bureau of Investigation to access DCI.

Step 3: At the Sonicwall login prompt, the Officer is asked to enter his/her username and password.

a. a. "Generic Users", or non-CJIS users, of the Sonicwall VPN are housed on a separate Sonicwall server and are only required to enter a username and password to access Sonicwall.
b. Upon receiving the credentials the Sonicwall VPN passes the credentials to the Phone Factor server which is setup as a RADIUS server. The PhoneFactor service places a call to the officer's personally owned cell phone and the officer must press the # key. Note: The officer's personally owned cell phone must utilize a passcode or PIN for the officer to initially access the phone to verify his/her identity).
c. If the call was successful and the officer pressed the # key, the PhoneFactor service responds to the Sonicwall VPN that the user is valid.

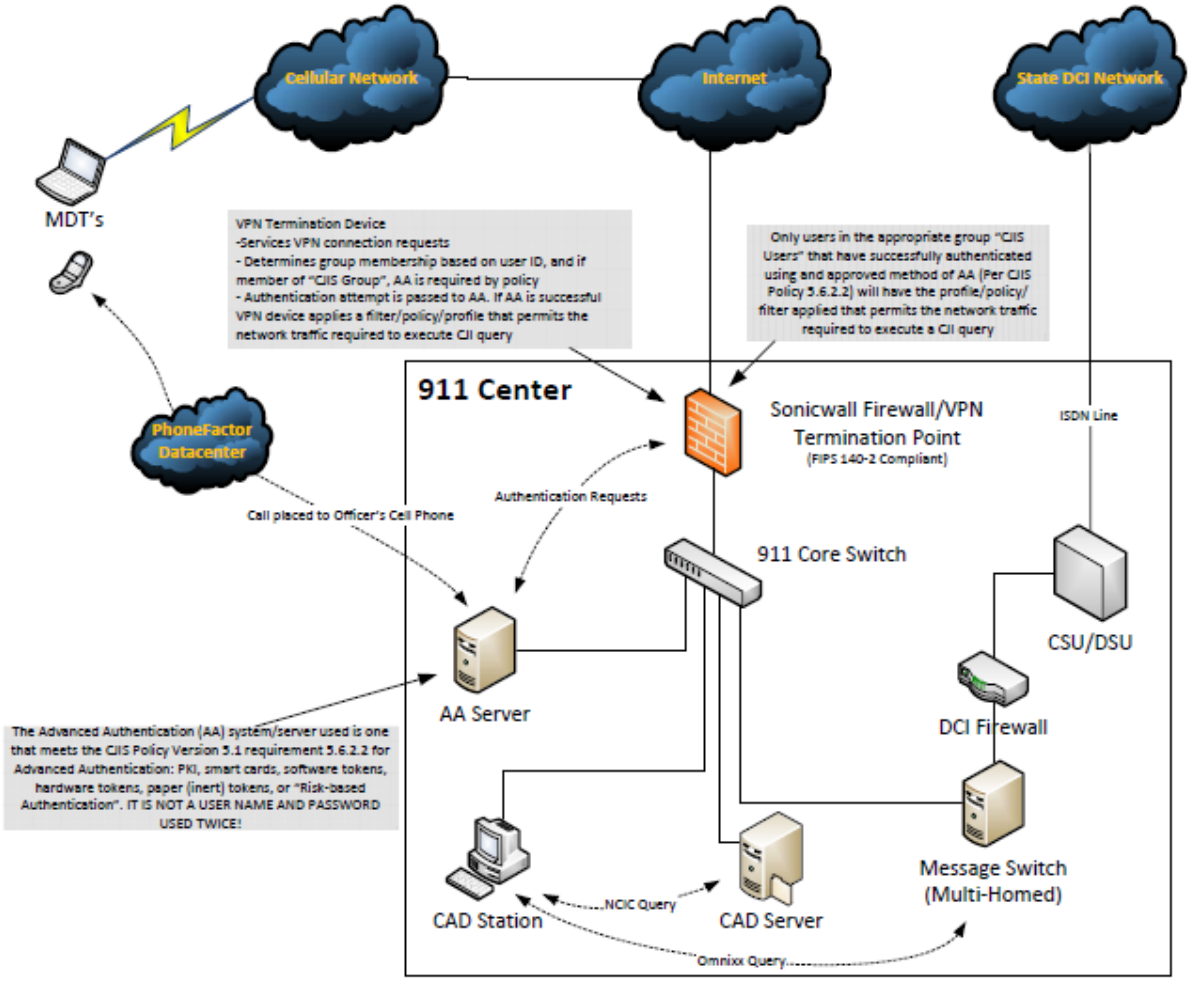
Step 4: The flow for the Sonicwall VPN termination point is:

a. Receives VPN connection request from Officer in Step 1.
b. Identifies that the Officer is in the "CJIS Users" group and therefore required to use AA as specified in Step 2 with Phone Factor integration.
c. Passes authentication required to AA system and receives authorization.
d. Applies the "CJIS Users" policy/profile/access control filter that permits the network traffic required to execute a CJI query.

Note: The AA server is not connected to nor asserting credentials to the CJI application (i.e. OSSI MCT) but only used to validate the establishment of VPN for this particular group.

Net result: Only AA authenticated users in the appropriate group (CJIS Group) with the appropriate profile/policy/access controls applied at the VPN termination point (i.e. Cisco, Microsoft, Sonicwall servers) are technically able to execute CJI queries. The control is a network layer control, i.e. network traffic is blocked for users not in the CJIS Group on the VPN termination point. The application may be launched on Generic Group members' MDTs, but no CJI query traffic will pass thus no access to the CJIN is possible for any user not in the "CJIS Group".

Scenario C Flow Diagram



Additional Approved Scenarios

The following jurisdiction-specific scenarios have all been approved by the FBI and/or NC DOJ/SBI.

Davidson County CJIS Advanced Authentication

Step 1: Officer logs into MDT with user name and password.

Step 2: Officer launches NetMotion VPN Client.

a) NetMotion, a FIPS 140-2 certified VPN termination point, is configured by the local agency to require the use of AA (meeting the requirements of CJIS v5.1 Section 5.6.2.2) for the "CJIS Users" group that need to execute CJI queries from the Mobile CAD/RMS application.
b) The NetMotion server is configured to use RSA tokens for its AA requirement. The NetMotion server is dedicated to Law Enforcement only.

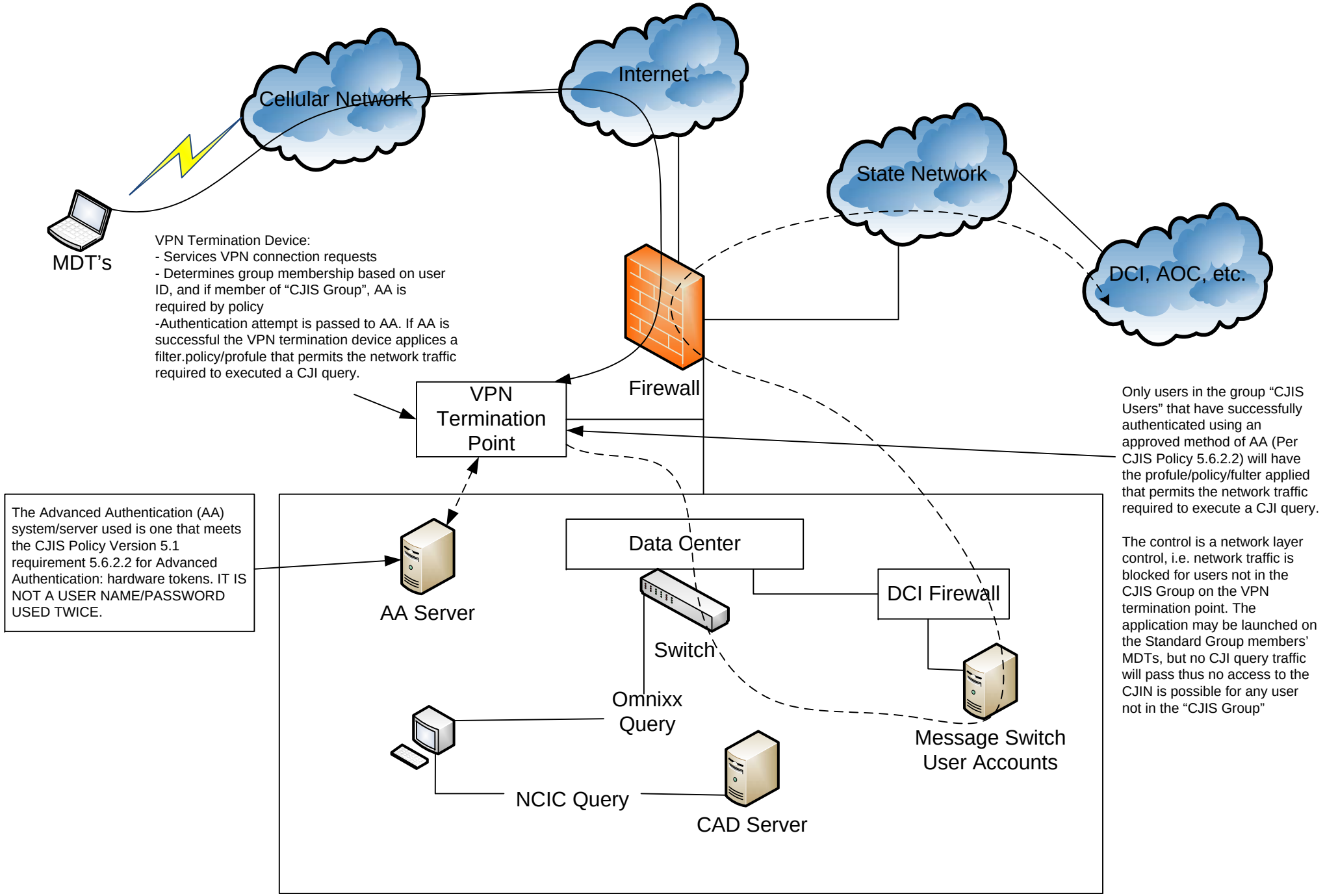
Step 3: At the NetMotion login prompt, the Officer is asked to enter his/her username and a unique four to eight (4-8) digit PIN that is assigned to each individual officer by the local agency, plus a six (6) digit passcode that is supplied by the RSA token. The passcode is digitally reset/refreshed every 60 seconds.

a) The system could also use a RSA USB Key that automatically provides the changing passcode, thereby only requiring the officer to know his/her username and 4 digit PIN.

Step 4: The flow for the NetMotion VPN termination point is:

a) Receives VPN connection request from Officer in Step 1.
b) Identifies that the Officer is in the "CJIS Users" group and therefore required to use AA as specified in Step 2.
c) Passes authentication required to AA system and receives authorization.
d) Applies the "CJIS Users" policy/profile/access control filter that permits the network traffic required to execute a CJI query.

Note: The AA server is not connected to nor asserting credentials to the CJI application (i.e. OSSI MCT) but only used to validate the establishment of VPN for this particular group.
Net result: Only AA authenticated users in the appropriate group (CJIS Group) with the appropriate profile/policy/access controls applied at the VPN termination point (i.e. Cisco, Microsoft, NetMotion servers) are technically able to execute CJI queries. The control is a network layer control, i.e. network traffic is blocked for users not in the CJIS Group on the VPN termination point.


Cellular Network
Internet
State Network
DCI, AOC, etc.
MDT's
VPN Termination Device:
- Services VPN connection requests
- Determines group membership based on user ID, and if member of "CJIS Group", AA is required by policy
-Authentication attempt is passed to AA. If AA is successful the VPN termination device applices a filter.policy/profule that permits the network traffic required to executed a CJI query.
Firewall
VPN Termination Point
Only users in the group "CJIS Users" that have successfully authenticated using an approved method of AA (Per CJIS Policy 5.6.2.2) will have the profule/policy/fulter applied that permits the network traffic required to execute a CJI query.
The control is a network layer control, i.e. network traffic is blocked for users not in the CJIS Group on the VPN termination point. The application may be launched on the Standard Group members' MDTs, but no CJI query traffic will pass thus no access to the CJIN is possible for any user not in the "CJIS Group"
The Advanced Authentication (AA) system/server used is one that meets the CJIS Policy Version 5.1 requirement 5.6.2.2 for Advanced Authentication: hardware tokens. IT IS NOT A USER NAME/PASSWORD USED TWICE.
AA Server
Data Center
DCI Firewall
Switch
Omnixx Query
Message Switch User Accounts
NCIC Query
CAD Server

Approved Scenario for Law Enforcement Agencies that are Participants in the Gaston County Consolidated Public Safety System that Includes the City of Gastonia Police Department, Gaston County Police Department, and Gaston County Sheriff's Department.

This is a Vendor Specific Flow Description for a NetMotion VPN, Entrust Tokens, and New World Systems solution.

Step 1: User logs into MDT with user name and password.

Step 2: The NetMotion VPN client launches.

a. NetMotion, a FIPS 140-2 certified VPN termination point, is configured by the local agency to require the use of AA (meeting the requirements of CJIS v5.1 Section 5.6.2.2) for all users of the Gaston County Consolidated Public Safety System Mobile CAD/RMS application.

b. In this example, the NetMotion server is configured to use Entrust tokens for its AA requirement.

c. Only those users that have been successfully logged on, with the appropriate software installed on the mobile device, and with the appropriate configuration through the New World Systems message switch can execute CJIS queries.

Step 3: At the NetMotion login prompt, the User is asked to enter his/her username and a unique four (4) digit PIN that has been assigned to each individual user by the local agency, plus an eight (8) digit passcode that is supplied by the Entrust IndentityGuard Mini Token OE. The passcode is digitally reset/refreshed every 60 seconds.

a. The system could also use an Entrust IndentityGuard Mobile OTP Softkey supplied on a Smartphone that automatically provides the changing passcode.

Step 4: The flow for the NetMotion VPN termination point is:

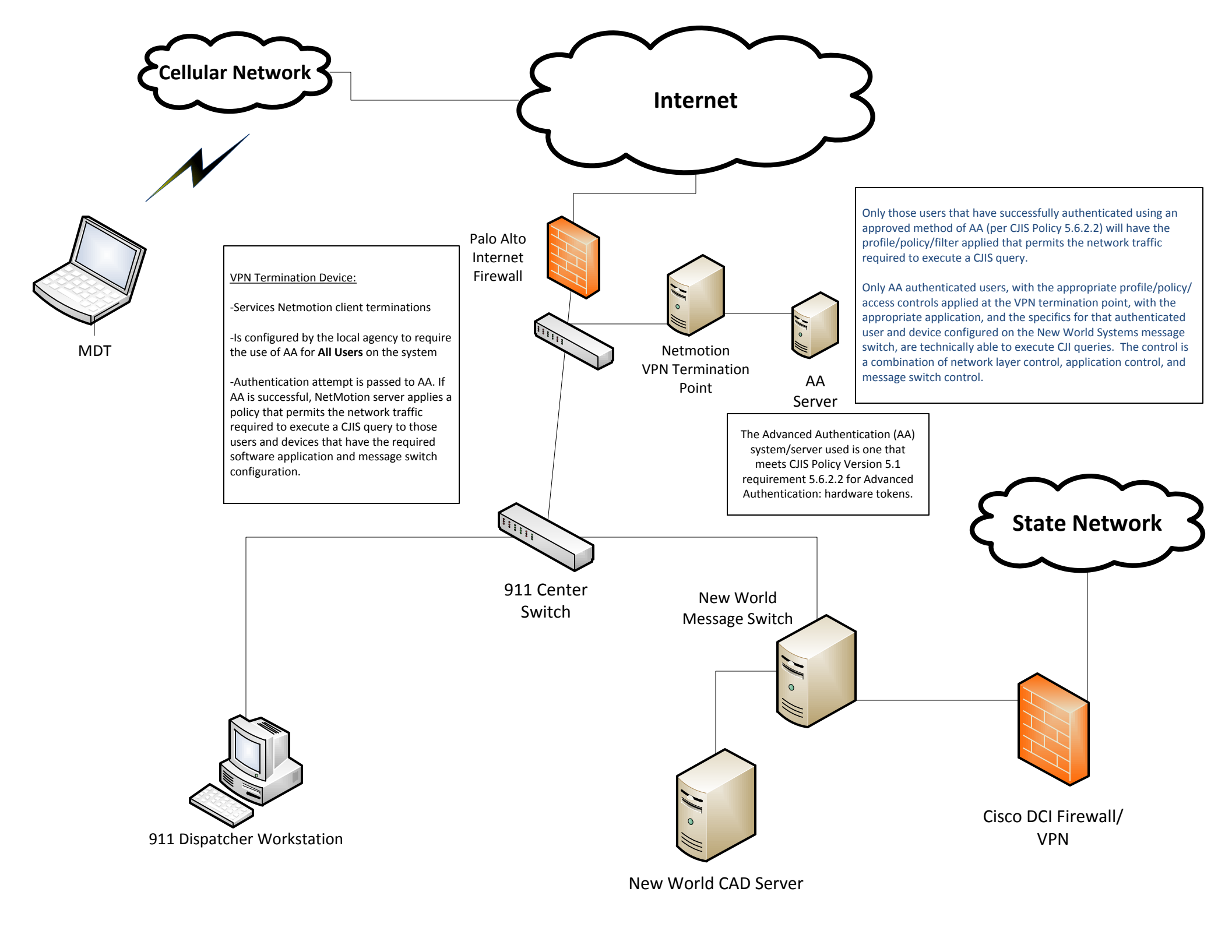
a. Receives VPN connection request from User in Step 1.

c. Passes authentication required to AA system and receives authorization.

d. Applies the policy/profile/access control filter that permits the network traffic required to execute a CJI query if and only if the appropriate application resides on the mobile device and the specifics for that user and device have been previously configured on the New World Systems message switch.

Note: The AA server is not connected to nor asserting credentials to the CJIS application (i.e. NWS Mobile Management Server or Message Switch) but only used to validate the establishment of VPN for the authenticated users.

Net result: Only AA authenticated users, with the appropriate profile/policy/access controls applied at the VPN termination point (i.e. Avaya, Microsoft, NetMotion servers), with the appropriate application, and the specifics for that authenticated user and device configured on the New World Systems message switch, are technically able to execute CJI queries. The control is a combination of network layer control, application control, and message switch control.


Cellular Network
Internet
MDT
Palo Alto
Internet
Firewall
Netmotion
VPN Termination
Point
AA
Server
VPN Termination Device:
-Services Netmotion client terminations
-Is configured by the local agency to require the use of AA for **All Users** on the system
-Authentication attempt is passed to AA. If AA is successful, NetMotion server applies a policy that permits the network traffic required to execute a CJIS query to those users and devices that have the required software application and message switch configuration.
Only those users that have successfully authenticated using an approved method of AA (per CJIS Policy 5.6.2.2) will have the profile/policy/filter applied that permits the network traffic required to execute a CJIS query.
Only AA authenticated users, with the appropriate profile/policy/ access controls applied at the VPN termination point, with the appropriate application, and the specifics for that authenticated user and device configured on the New World Systems message switch, are technically able to execute CJI queries. The control is a combination of network layer control, application control, and message switch control.
The Advanced Authentication (AA) system/server used is one that meets CJIS Policy Version 5.1 requirement 5.6.2.2 for Advanced Authentication: hardware tokens.
911 Center
Switch
State Network
New World
Message Switch
911 Dispatcher Workstation
New World CAD Server
Cisco DCI Firewall/
VPN

Kernersville Police Department – DCI Access From Mobile Computers

Specifications

Computer Model: Portege M750
Operating System: Windows XP (SP3) All Security Updates Patched on Weekly Basis
DCI Access Provided By Sungard Public Sector MCT (EXE Version: 7/16/2012; Data/Config Version: 300)

Overview of Process

- Officer Enters Windows Login
  - Windows Logon (Active Directory)
- Private Network Aircard Connectivity Through Verizon VZAccess Manager (No Login Prompt)
  - Private Network Connected to Corporate Network via IP-SEC/GRE (AES 256) FIPS 140-2 Compliant Cisco routers
  - All Traffic Forced Through Tunnel
- Officer Starts MCT Application
  - Presented with AA(2FAONE) (PIN + Proximity Card)
  - Presented with MCT Login
  - Presented with CJIS/DCI Logon

Detailed Explanation of Process

Step 1) Officer logs into Windows/MCT via Active Directory Credentials.

Step 2) Officer is automatically displayed the front end computer software that manages the aircards, VZ Access Manager (v 7.3), provided by Verizon Wireless. Inside the VZ Access Manager software, the officer clicks on the connect button to activate the connectivity on the aircard.

2a) The aircard is associated with a private network provided by Verizon Wireless and the laptop is given a private IP address. The private network is connected to the Town of Kernersville's corporate network by a redundant IP-SEC/GRE (AES 256) tunnel from one of two FIPS 140-2 Compliant Cisco routers. All internet traffic from and to the officer's laptops is routed through a corporate firewall and is subject to all firewall rules as if it were located physically on the trusted corporate LAN. At this point the officer is connected to the internal corporate network.

Step 3) Officer launches OSSI MCT Program provided by Sungard Public Sector.

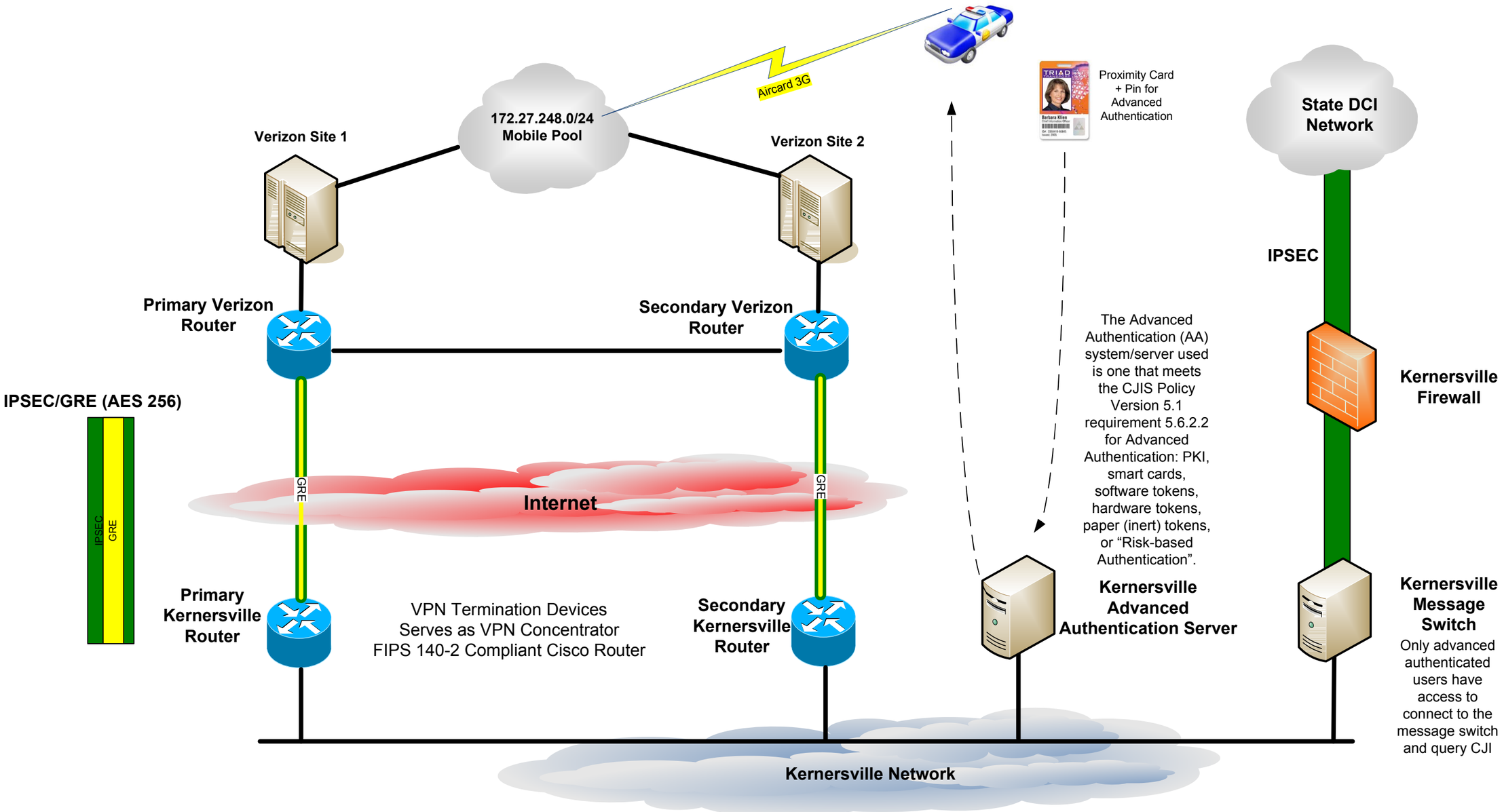
3a) Officer is presented with AA (2FAONE) dialog requesting 4-digit PIN and proximity card reading. Officer enters PIN and swipes a proximity card to authenticate to the AA server. Credentials are then passed to the Advanced Authentication Server which authorizes or denies access based on correct PIN, correct proximity card, and correct group membership of "CJIS Users" group.

3b) After successful Advanced Authentication the officer is presented with a logon screen for MCT access. This login and password combination grants the officer access to

Computer Aided Silent Dispatch, Mapping, and Mobile Field Reporting. As well as an internal message system used to communicate between the telecommunications dispatch office as well as other officers currently logged in the MCT program.

3c) After MCT authentication the officer is presented with an additional logon screen for CJIS/DCI access. This login and password combination are sent through an internal server (message switch) provided by Sungard Public Sector and sent through an IP-SEC tunnel established with the State of North Carolina. The CJIS/DCI login and password combination are then authenticated at the State level. After successful authentication the user is displayed a message notifying whether logon was successful or unsuccessful. If successful, the officer now has the capability to query CJI.

Summary: For access to the MCT/DCI program users must use advanced authentication as well as be a member of the "CJIS Users" group. All advanced authentications are done in real time by a back end advanced authentication server. If a user does not pass advanced authentication, separate from Windows credentials, they have no access to the MCT program and cannot query CJI.


Aircard 3G
172.27.248.0/24
Mobile Pool
Verizon Site 1
Verizon Site 2
Primary Verizon
Router
Secondary Verizon
Router
IPSEC/GRE (AES 256)
IPSEC
GRE
GRE
GRE
Internet
Primary
Kernersville
Router
VPN Termination Devices
Serves as VPN Concentrator
FIPS 140-2 Compliant Cisco Router
Secondary
Kernersville
Router
Proximity Card
+ Pin for
Advanced
Authentication
The Advanced Authentication (AA) system/server used is one that meets the CJIS Policy Version 5.1 requirement 5.6.2.2 for Advanced Authentication: PKI, smart cards, software tokens, hardware tokens, paper (inert) tokens, or “Risk-based Authentication”.
Kernersville
Advanced
Authentication Server
State DCI
Network
IPSEC
Kernersville
Firewall
Kernersville
Message
Switch
Only advanced authenticated users have access to connect to the message switch and query CJI
Kernersville Network

Approved Scenario for New Hanover County CJIS Advanced Authentication

Step 1: Officer logs into MDT with user name and password.

Step 2: Officer launches Cisco AnyConnect VPN Client.

a) AnyConnect, a FIPS 140-2 certified VPN termination point, is configured by the local agency to require the use of AA (meeting the requirements of CJIS v5.1 Section 5.6.2.2) for the "CJIS Users" group that need to execute CJI queries from the Mobile CAD/RMS application.
b) The Cisco AnyConnect VPN Termination Point (ASA Firewall) is configured to integrate RSA tokens for its AA requirement. The AnyConnect VPN Client Policy application is configured to require local law enforcement agencies to Advanced Authentication via RSA hardware authenticators (tokens).

Step 3: At the AnyConnect login prompt, the Officer is asked to enter his/her username and a unique password. The user will then be prompted to enter a six (6) digit passcode that is supplied by the RSA token and then a unique four to eight (4-8) digit PIN that is assigned to each individual officer by the local agency. The passcode is digitally reset/refreshed every 60 seconds.

a) The system could also use a RSA USB Key that automatically provides the changing passcode, thereby only requiring the officer to know his/her username and 4–8 digit PIN.

Step 4: The flow for the AnyConnect VPN termination point is:
a) Receives VPN connection request from Officer in Step 1.
b) Identifies that the Officer is in the "CJIS Users" group and therefore required to use AA as specified in Step 2.
c) Passes authentication required to AA system and receives authorization.
d) Applies the "CJIS Users" policy/profile/access control filter that permits the network traffic required to execute a CJI query.

Note: The AA server is not connected to nor asserting credentials to the CJI application (i.e. OSSI MCT) but only used to validate the establishment of VPN for this particular group.

Net result: Only AA authenticated users in the appropriate group (CJIS Group) with the appropriate profile/policy/access controls applied at the VPN termination point (i.e. Cisco, Microsoft, NetMotion servers) are technically able to execute CJI queries. The control is a network layer control, i.e. network traffic is blocked for users not in the CJIS Group on the VPN termination point.

Chapel Hill Police Department, North Carolina

VENDOR SPECIFIC FLOW DESCRIPTION FOR ADVANCED AUTHENTICATION

(NetMotion, 2FA, SunGard OSSI MCT)

Operating Environment:

1) User assigned Active Directory user name and password logon to Windows XP and Windows 7 operating systems,
2) NetMotion connectivity authenticated with assigned user name and password,
3) Verizon Air Card wireless connectivity established following successful authentication to NetMotion,
4) 2FA ONE Client installed locally on all MDTs on which OSSI MCT is installed,
5) 2FA ONE client connected to 2FA ONE Server,
6) 2FA ONE logon experience set to “Contactless” only – all other logon methods are disabled on MDTs – users cannot logon with user name and password in any case.
7) 2FA ONE Secured Applications “Enforce Authentication” template provisioned to all users that access SunGard OSSI applications,
8) Agency issued and managed officer identification badges containing HID Global PROX (RFID) technology.
9) RFID reader locally connected to all MDTs.

Scenario C – Assigned Active Directory User Name and Password System Logon with Enforce Authentication Set on NetMotion

Step 1: Officer comes on shift and powers on the MDT.

Step 2: Officer is presented with “Contactless Logon – Please present card”, logon tile.

(Figure 2-1)

Step 3: An officer, who has been previously authorized and enrolled in the 2FA ONE system, presents their agency issued officer identification badge that contains HID PROX (RFID) technology to a locally connected RFID reader. The HID PROX number is read by reader and passed to the 2FA ONE Client application.

Step 4: Upon validation of the officer's credentials, the "Contactless Logon" screen identifies the officer's name and requests the officer enter their associated PIN. The officer enters their PIN that they previously selected and is known by the 2FA ONE software and clicks the right facing arrow or presses Enter.

(Figure 4-1)

Step 5: The 2FA ONE client logs the officer's access (user name, date, time, and authentication type) to the MDT in the local event log. The officer's assigned desktop appears.

(Figure 5-1)

Step 6: The officer opens NetMotion Mobility XE, the application launches, and 2FA ONE Secured Application's Enforce Authentication template is triggered. If the officer clicks Cancel or clicks away from the Authentication window OSSI MCT is closed by 2FA ONE. The officer must represent their badge and enter their PIN as they initially did when logging on to Windows.

(Figure 6-1)

Step 7: 2FA ONE validates the officer's credentials, logs the fact that advanced authentication occurred at the application level in the application event log (username, domain, authentication method, login template specific to MCT) and provides the officer access to NetMotion. The officer must enter their User name and Password.

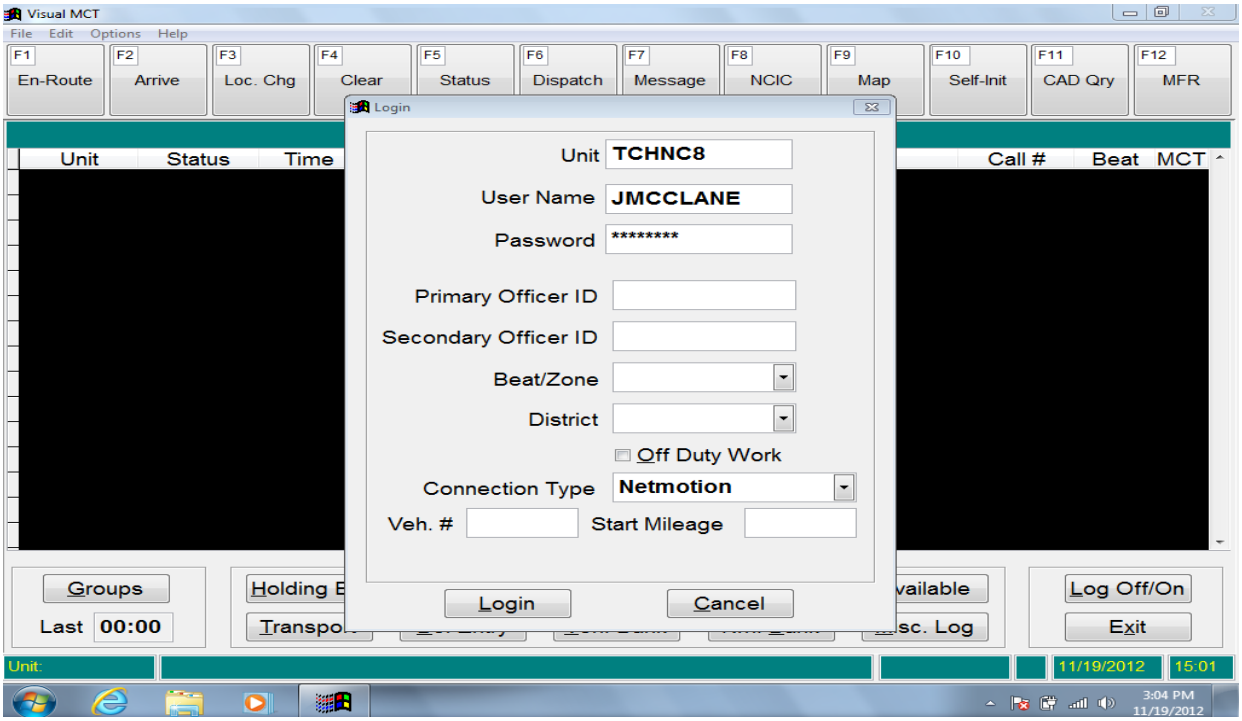
Note: A configurable option, 2FA ONE is capable of providing the officer's assigned User name and Password to OSSI MCT, also known as SSO.

Step 8: The officer enters in the required information and clicks "OK". The officer's credentials are validated against NetMotion, a FIPS 140-2 certified VPN termination point, the VPN security is configured by the local agency. The officer's credentials include the officer's user name and a strong password per the CJIS Policy 5.1. Mobility client validates the credentials provided by 2FA ONE against NetMotion's server-side software. The NetMotion server-side software passes the logon request to

Microsoft Active Directory. Active Directory is configured with a Password Policy and is applied to an OU. Users in a non-secured environment are organized into these OU, thereby meeting the password policy. Connectivity is established upon successful validation of the officer's credentials. (Negative Use Case: Credentials are not accepted and Mobility XE informs user of failed logon.) Upon establishing a valid connection, 2FA ONE Client synchronizes with the 2FA ONE Server to obtain any updates to the officer's credentials or policy profile.

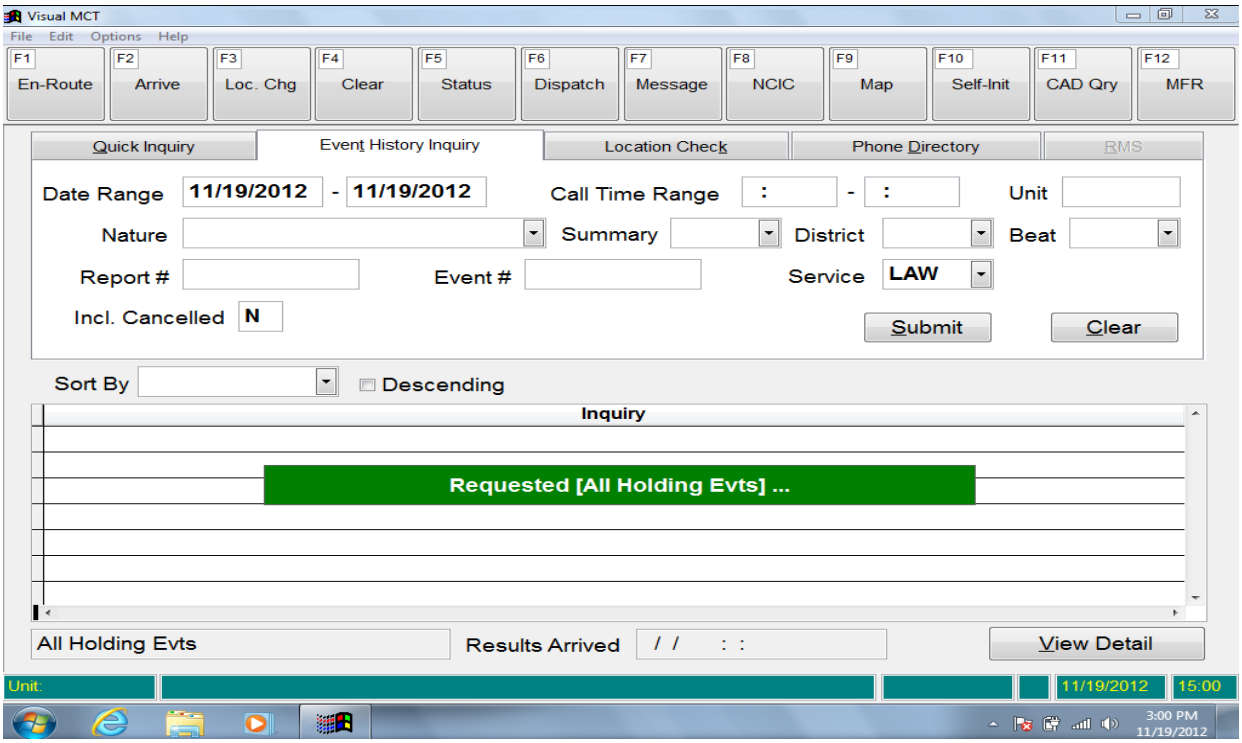
Step 9: The officer opens OSSI MCT, the application launches. The officer must enter their User name and Password.

Note: A configurable option, 2FA ONE is capable of providing the officer's assigned User name and Password to OSSI MCT, also known as SSO.



(Figure 9-1)

Step 10: The officer enters in the required information and clicks "Login". The officer's credentials are validated against OSSI and upon validation the officer is granted access to MCT.



(Figure 10-1)

Step 11: During the shift the officer touches or clicks on the lock MDT icon located in the taskbar.

(Figure 11 -1)

Once locked the officer must represent their badge and enter their PIN as they did in **Step #2** prior to regaining access to the desktop and the running OSSI MCT.

Step 12: At the end of their shift the officer logs off OSSI MCT and Windows. The officer is presented with the “Contactless Logon – Please present card.”

(Figure 12-1)

The Verizon and NetMotion connection are both disconnected.

Chapel Hill Police Department, North Carolina

VENDOR SPECIFIC FLOW DESCRIPTION FOR ADVANCED AUTHENTICATION

(NetMotion, 2FA, SunGard OSSI MCT)

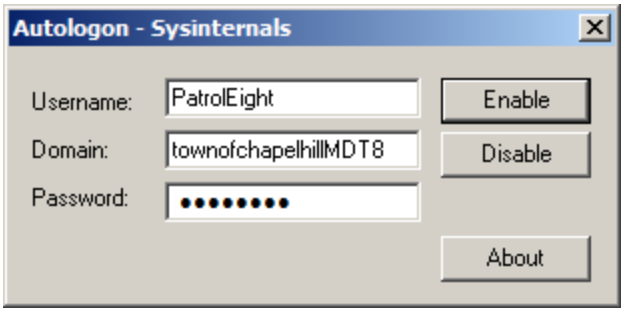
Operating Environment:

1) Generic username and password logon to Windows XP and Windows 7 operating systems,
2) Microsoft Certificate Services with machine-based X.509 certificates issued to each MDT,
3) NetMotion connectivity authenticated through machine-based certificate,
4) Verizon Air Card wireless connectivity established following successful authentication to NetMotion,
5) 2FA ONE Client installed locally on all MDTs on which OSSI MCT is installed,
6) 2FA ONE client connected to 2FA ONE Server,
7) 2FA Shared Workstation enabled on all MDTs,
8) 2FA ONE Secured Applications "Enforce Authentication" template provisioned to all users that access SunGard OSSI applications,
9) Agency issued and managed officer identification badges containing HID Global PROX (RFID) technology.
10) RFID reader locally connected to all MDTs.

Scenario A – Generic Operating System Logon

Step 1: Officer comes on shift and powers on the MDT.

Step 2: Windows is configured to auto-logon with a generic, local user name and password.



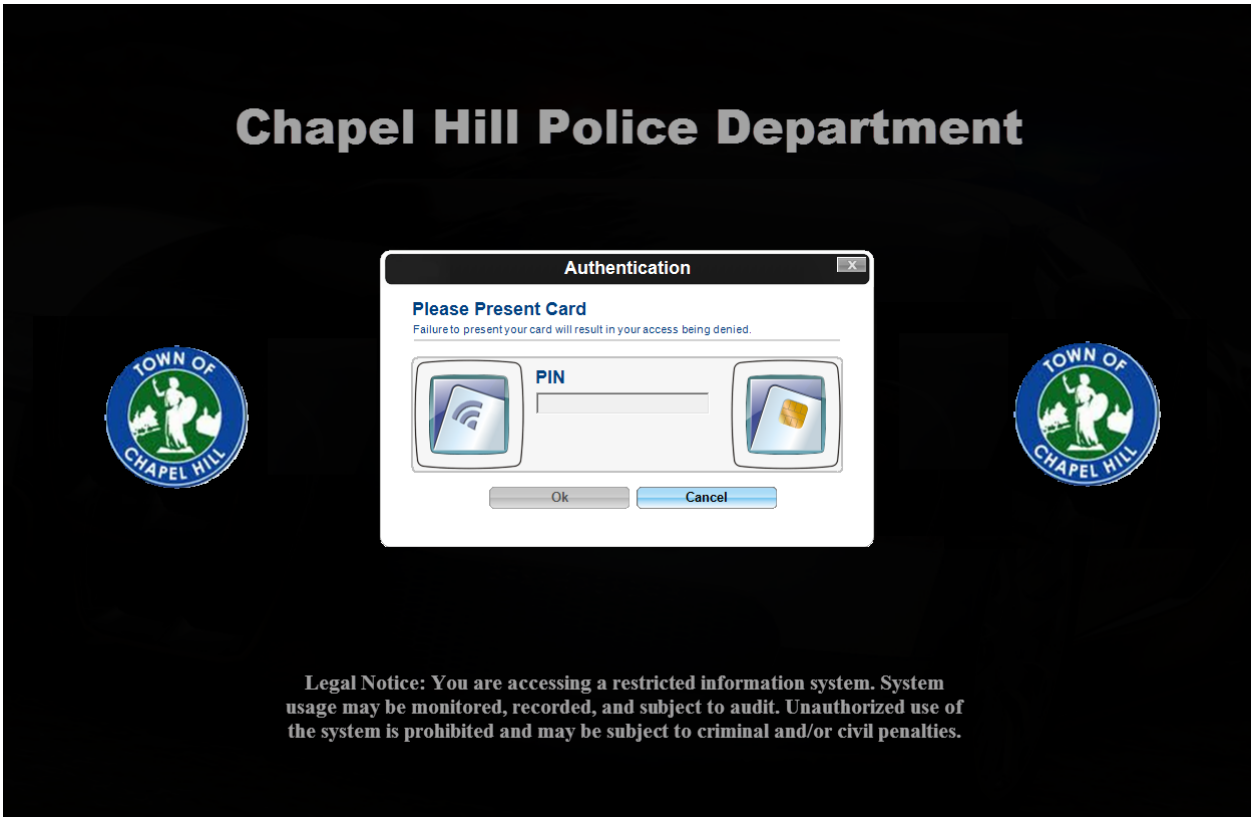
(Figure 2-1)

During the Windows logon process the officer is not prompted to logon to the local machine.

Note: Autologon is Microsoft Corporation published application provided to customers by NetMotion for optimal use with NetMotion for customers who utilize the auto-logon process. The screen in Figure 2-1 is not displayed or accessible to the officer, rather it is pre-configured by an administrator.

Step 3: During Windows logon the Verizon Air Card is activated to facilitate a X.509 certificate exchange between the locally installed NetMotion Mobility XE client, a FIPS 140-2 certified VPN termination point, and the NetMotion Server. The VPN security is configured by the local agency. X.509 certificates are issued to each MDT by a local administrator assigned the role of Local Registration authority (LRA). NetMotion validates that the machine certificate is valid, has not been revoked, and the machine account exists within the Active Directory. Upon validation the Verizon Air Card connection is fully established and an audit log to the local Windows operating system occurs.

Step 4: Immediately following local logon to Windows, the 2FA ONE client secures the MDT with Shared Workstation.



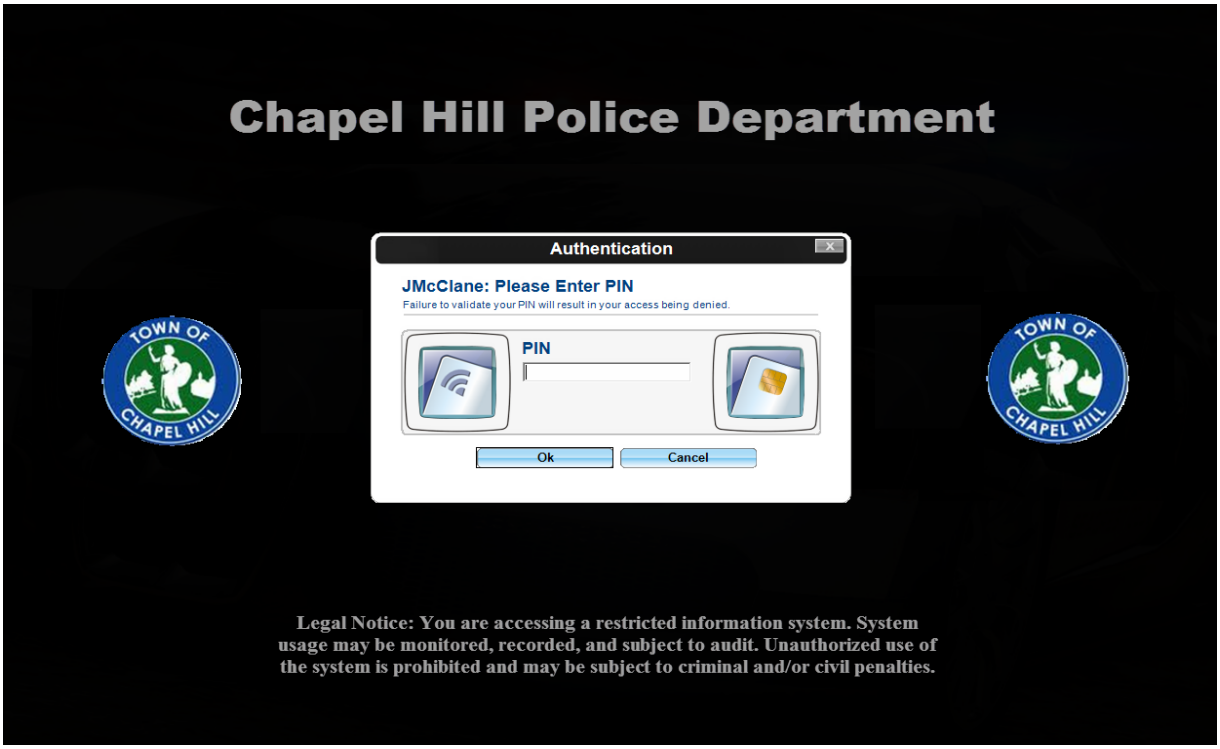
(Figure 4-1)

2FA ONE Shared Workstation is a secure shell around the Windows operating system, similar to a secure screen-saver, configured by local administrators that cannot be bypassed by administrators or local users without two-factor authentication.

Step 5: An officer, who has been previously authorized and enrolled in the 2FA ONE system, presents their agency issued officer identification badge that contains HID PROX (RFID) technology to a locally connected RFID reader. The HID PROX number is read by reader and passed to the 2FA ONE Client application. The 2FA ONE client application sends a web-services call to the 2FA ONE Server to ensure the officers credentials are authorized and have not been revoked. Upon validation that the credentials

are authorized, the officer's 2FA ONE profile information is sent from the 2FA ONE Server to the 2FA ONE client for PIN validation.

Step 6: Upon validation of the officer's credentials, the "Authentication" screen identifies the officer's name and requests the officer enter their associated PIN. The officer enters their PIN that they previously selected and is known by the 2FA ONE software and clicks "Ok".

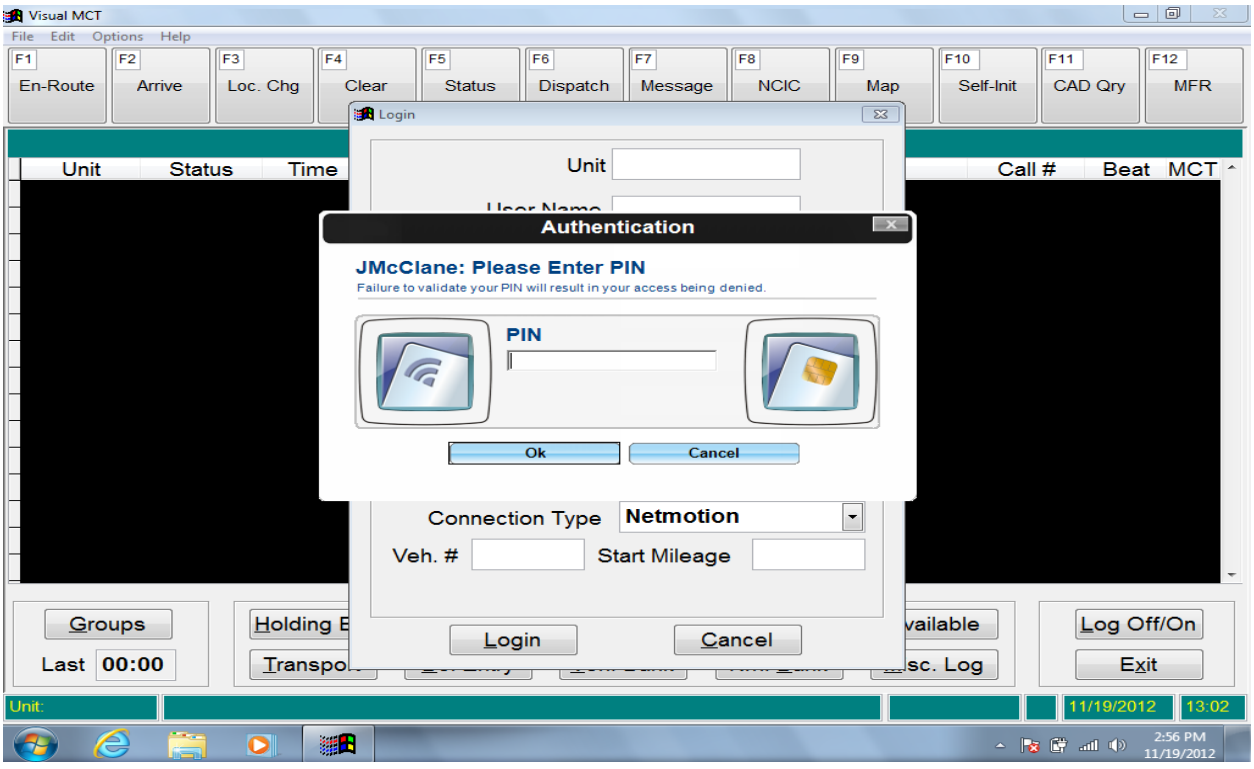


(Figure 6-1)

Step 7: The 2FA ONE client logs the officer's access (user name, date, time, and authentication type) to the MDT in the local event log, the Shared Workstation screen disappears and the desktop of the generically logged on user is made accessible to the officer.

(Figure 7-1)

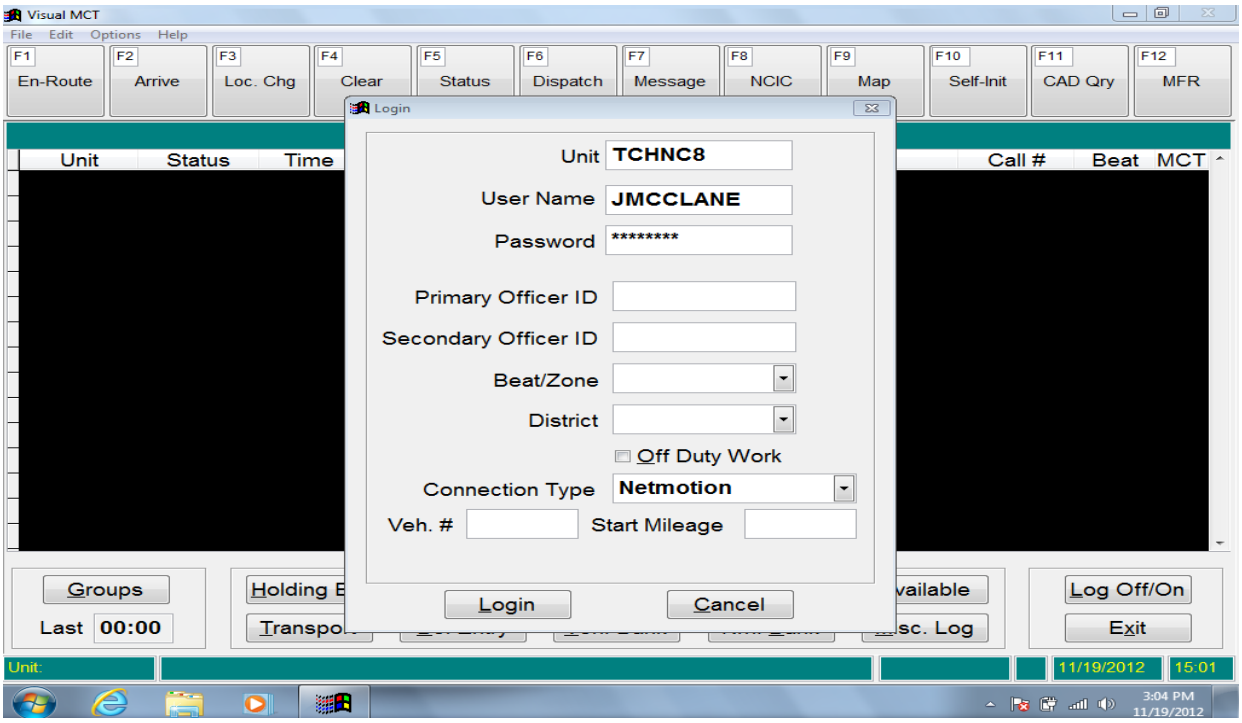
Step 8: The officer opens OSSI MCT, the application launches, and 2FA ONE Secured Application's Enforce Authentication template is triggered. If the officer clicks Cancel or clicks away from the Authentication window OSSI MCT is closed by 2FA ONE. The officer must represent their badge and enter their PIN as they initially did when authenticating to Shared Workstation.



(Figure 8-1)

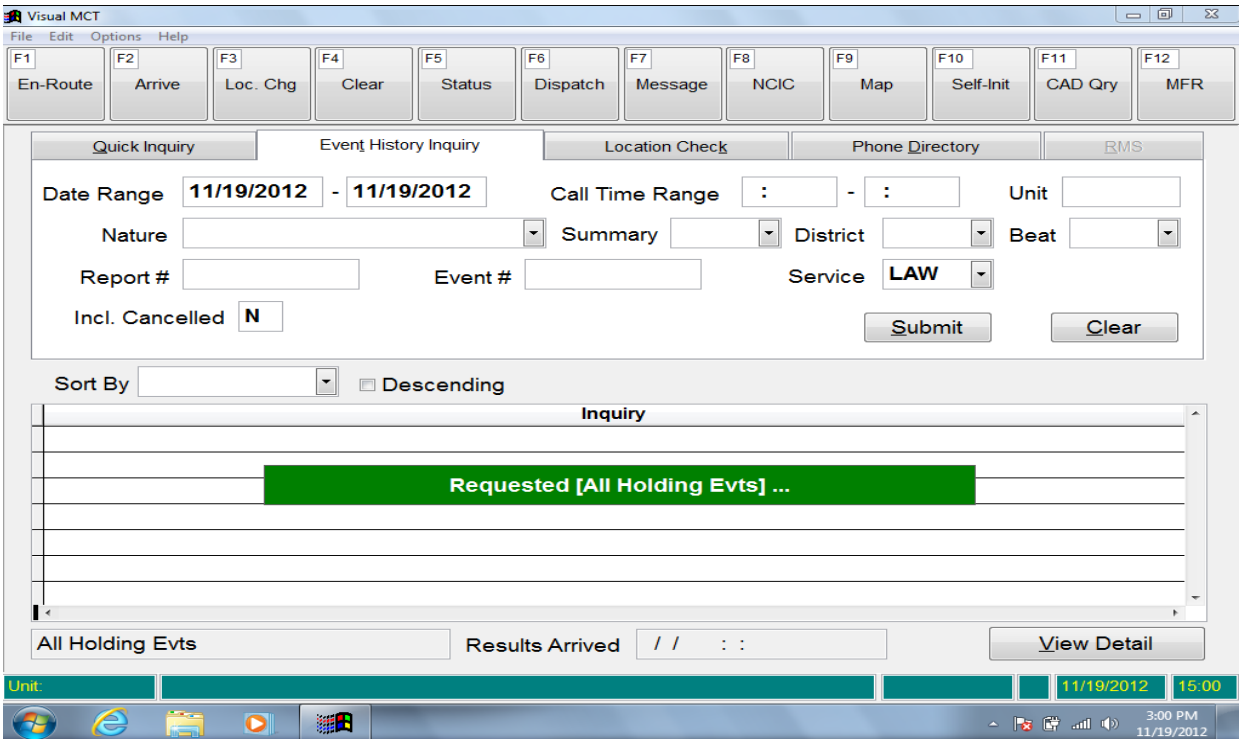
Step 9: 2FA ONE validates the officer's credentials, logs the fact that advanced authentication occurred at the application level in the application event log (username, domain, authentication method, login template specific to MCT) and provides the officer access to OSSI MCT. The officer must enter their User name and Password.

Note: A configurable option, 2FA ONE is capable of providing the officer's assigned User name and Password to OSSI MCT, also known as SSO.



(Figure 9-1)

Step 10: The officer enters in the required information and clicks "Login". The officer's credentials are validated against OSSI and upon validation the officer is granted access to MCT.



(Figure 10-1)

Note: A configurable option, 2FA ONE is capable of providing the officer's assigned User name and Password to OSSI MCT, also known as SSO.

Step 11: During the shift the officer touches or clicks on the lock MDT icon located in the taskbar.

(Figure 11 -1)

Once locked the officer must represent their badge and enter their PIN as they did in **Step #4** prior to regaining access to the desktop and the running OSSI MCT.

Step 12: At the end of their shift the officer may either logoff OSSI MCT or tap their agency-issued identification badge on the RFID reader, and 2FA ONE will logoff the officer from MCT and lock the workstation, again presenting the officer with the secured Shared Workstation screen.

Note: A configurable option, 2FA ONE is capable of automatically locking the MDT and presenting the officer with the secured Shared Workstation screen after a configurable time of inactivity.

(Figure 12-1)

The Verizon and NetMotion connection will remain active unless disconnected manually by the officer.

Chapel Hill Police Department, North Carolina

VENDOR SPECIFIC FLOW DESCRIPTION FOR ADVANCED AUTHENTICATION

(Net Motion, Imprivata, SunGard OSSI MCT)

Scenario A - Imprivata OneSign in Single User mode, Net Motion VPN in Unattended Mode

Single User mode means that the end user is logging into their Windows MDT that is joined to the Active Directory domain using their domain account (versus a local PC account or a generic domain account for the MDT). Using Windows 7 Enterprise, this is what they will see with the OneSign agent installed in this configuration. Advanced Authentication (2-factor) will occur at the Windows logon.

This setup will require the Net Motion VPN to be configured in "Unattended Mode" which uses a PKI certificate assigned to the MDT that allows the device itself to authenticate to Net Motion once it is powered on thus creating an encrypted VPN tunnel prior to the Windows logon event. This means that when the user logs into Windows, they are not using cached domain credentials (i.e. offline Windows authentication) and the MDT will be able to communicate with a domain controller. This will be true even when using Imprivata OneSign for Advanced Authentication as the agent and the authentication modality being used are part of the Windows logon process. PKI certificates will be provided by Microsoft Certificate Services.

For OneSign, our agent uses SSL to communicate to an OneSign appliance (or virtual machine) in order to authenticate the user. With the VPN tunnel established via Unattended Mode, the agent will be able to authenticate the user with whatever modality they are assigned in OneSign policy. Here are the steps a user would go through in this configuration:

Step 1 – Officer boots up MDT (network connection is available via Verizon air card or MiFi LTE Wi-Fi signal. This allows the Net Motion encrypted VPN connection to be established via Unattended Mode).

Step 2 – Officer authenticates with Advanced Authentication 2-factor method (Proximity Card + Domain Password (or PIN)

Step 3 – Upon successful authentication, the Officer is granted access to the Windows desktop from which they can access the OSSI application.

Step 4 – OPTIONAL: with Imprivata OneSign **Single Sign-On**, we can also manage the passwords for accessing CJIS data so that a strong password is used and/or the user isn't required to know their password because SSO is logging them in.

If a user account needs their access to be revoked, the IT Administrators can simply disable their domain account and OneSign will also disable their access to the MDT and their applications.

Net Result: With Net Motion Unattended Mode and Imprivata OneSign, you can configure specific MDT's to use this configuration so that any CJIS user who requires Advanced Authentication can authenticate with the modality they choose (i.e. Fingerprint, Proximity card, ID Token, etc.). OneSign policy can control access to the Windows desktop by enforcing the use of Advanced Authentication when authenticating. Although not required, Single Sign-On provides additional benefits for both user convenience and security around access and password management for the CJIS application(s).

Scenario B - Imprivata OneSign in Shared Workstation mode, Net Motion VPN in Unattended Mode

Shared workstation mode means that the MDT is either auto logged-in or manually logged in to the Windows desktop with a common generic domain account (versus a named user domain account). This might typically be the case if a CJIS user is not issued a MDT and has to share a MDT that may be assigned to a specific police vehicle. If the MDT is joined to the domain, then Net Motion Unattended Mode could still be used to help establish the VPN connection when the MDT is powered on as explained in Scenario 1. Once the MDT is logged in, the OneSign Agent in Shared Workstation mode will automatically lock the screen and require the user to use Advanced Authentication to access the desktop. The screen below is what the user will see. OneSign policy can be configured to not allow access until a successful Advanced Authentication has occurred.

For IT administrators, OneSign policy can be configured to allow them to login with an account that has local admin rights if needed. In this scenario, Advanced Authentication (2-factor) will occur at the Windows logon level via the OneSign Shared Workstation agent which uses Windows API's in order to determine if a user can even log into this MDT. For example, domain based computers can have a policy that restricts which users or groups can even log in. The OneSign agent in Shared Workstation mode will honor that policy setting even though the Windows logged in user is a generic domain account as previously described.

Here are the steps a user would go through in this configuration:

Step 1 – Officer boots up MDT (network connection is available via Verizon air card or MiFi LTE Wi-Fi signal. This allows the Net Motion encrypted VPN connection to be established via Unattended Mode).

NOTE: Officer can log into Windows with a generic domain account OR you can have the MDT auto login with a generic domain account.

Step 2 – After logging into the desktop, the OneSign Agent in Shared Workstation mode will lock the MDT. (VPN tunnel is already established)

Step 3 - Officer authenticates to the OneSign Agent with Advanced Authentication 2-factor method (Proximity Card + Domain Password (or PIN). Upon successful authentication, the Officer is granted access to the Windows desktop from which they can access the OSSI application.

Step 4 – OPTIONAL: with Imprivata OneSign **Single Sign-On**, we can also manage the passwords for accessing CJIS data so that a strong password is used and/or the user isn't required to know their password because SSO is logging them in. If a user account needs their access to be revoked, the IT Administrators can simply disable their domain account and OneSign will also disable their access to the MDT and their applications.

Net Result: With Net Motion Unattended Mode and Imprivata OneSign, you can configure specific MDT to use this configuration so that any CJIS user who requires Advanced Authentication can authenticate with the modality they choose (i.e. Fingerprint, Proximity card, ID Token, etc.). OneSign policy can control access to the Windows desktop by enforcing the use of Advanced Authentication when authenticating. Although not required, Single Sign-On provides additional benefits for both user convenience and security around access and password management for the CJIS application(s).

Scenario C - Imprivata OneSign and ProveID for Advanced Authentication at the CJIS Application Level

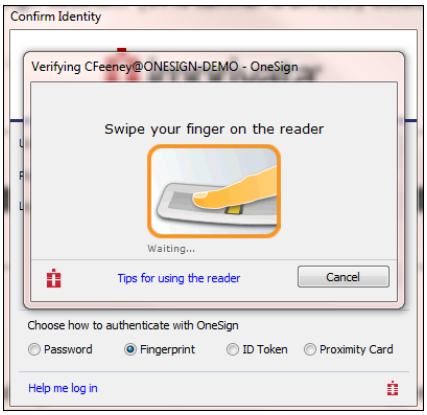
Imprivata OneSign ProveID can be used to enable strong authentication within an application workflow (ex: logging into the application). For the CJIS Advanced Authentication requirement, ProveID could be used to require two-factor authentication before the user is allowed to login to the OSSI application. In this configuration, applications can take advantage of existing authentication methodologies including fingerprint biometrics, proximity cards, smart cards, one-time passwords, USB tokens and phone-based authentication.

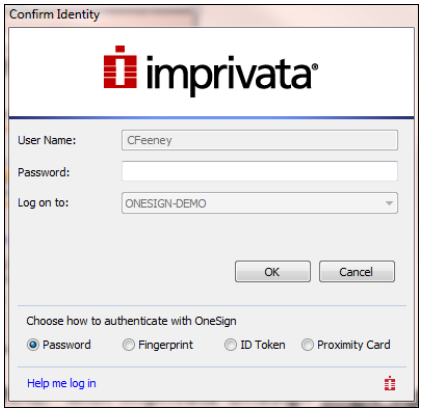
Here are the steps a user would go through in this configuration:

Step 1 – Officer boots up MDT (network connection is available via Verizon air card or MiFi LTE Wi-Fi signal. This allows the Net Motion encrypted VPN connection to be established via Unattended Mode).

Step 2 – After logging into the desktop, the OneSign Agent is either already running (i.e. Scenario 1 – which in this case, the user could just log in with their AD user name and password) or in Shared Workstation mode, the OneSign Agent will lock the computer and the user could log in with their AD user name and password in order to establish a OneSign session (VPN tunnel is already established).

Step 3 – Depending on Scenario, once the user is logged in, they can now access the CJIS application. However, with ProveID enabled, when they open the application, they will see an OneSign dialog similar to either of these screens. The screen on the left is shown if a fingerprint feader is used for Advanced Authentication. If fingerprint biometrics is not used, then the user will see the screen on the right.





Step 4 – The user must authenticate correctly and if they do, Imprivata OneSign **Single Sign-On**, can also be used to log the user into the application. We could also allow the user to then login to the application. Most customers would prefer that OneSign logs them in after they've successfully authenticated.

NOTE: If the user tries to cancel or bypass the ProveID authentication screen, OneSign can close the CJIS application. OneSign SSO can also be used to manage the passwords for accessing CJIS data so that a strong password is used and/or the user isn't required to know their password because SSO is logging them in. If a user account needs their access to be revoked, the IT Administrators can simply disable their domain account and OneSign will also disable their access to the MDT and their applications.

Net Result: With Imprivata OneSign ProveID, you can configure a specific MDT to use this configuration so that any CJIS user who requires Advanced Authentication can authenticate with the modality they choose (i.e. Fingerprint, Proximity card, ID Token, etc.) when accessing their CJIS application. OneSign policy can control access to the application by enforcing the use of Advanced Authentication when authenticating. Although not required, Single Sign-On provides additional benefits for both user convenience and security around access and password management for the CJIS application(s).

Chapel Hill Police Department, North Carolina

VENDOR SPECIFIC FLOW DESCRIPTION FOR ADVANCED AUTHENTICATION

(NetMotion, 2FA, SunGard OSSI MCT)

Operating Environment:

1) User assigned Active Directory user name and password logon to Windows XP and Windows 7 operating systems,
2) Microsoft Certificate Services with machine-based X.509 certificates issued to each MDT,
3) NetMotion connectivity authenticated through machine-based certificate,
4) Verizon Air Card wireless connectivity established following successful authentication to NetMotion,
5) 2FA ONE Client installed locally on all MDTs on which OSSI MCT is installed,
6) 2FA ONE client connected to 2FA ONE Server,
7) 2FA ONE logon experience set to "Contactless" only – all other logon methods are disabled on MDTs – users cannot logon with user name and password in any case.
8) 2FA ONE Secured Applications "Enforce Authentication" template provisioned to all users that access SunGard OSSI applications,
9) Agency issued and managed officer identification badges containing HID Global PROX (RFID) technology.
10) RFID reader locally connected to all MDTs.

Scenario B – Assigned Active Directory User name and Password System Logon

Step 1: Officer comes on shift and powers on the MDT.

Step 2: During the Windows boot process the Verizon Air Card is activated to facilitate a X.509 certificate exchange between the locally installed NetMotion Mobility XE client, a FIPS 140-2 certified VPN termination point, and the NetMotion Server. The VPN security is configured by the local agency. X.509 certificates are issued to each MDT by a local administrator assigned the role of Local Registration authority (LRA). NetMotion validates that the machine certificate is valid, has not been revoked, and the machine account exists within the Active Directory. Upon validation the Verizon Air Card connection is fully established and an audit log to the local Windows operating system occurs.

Step 3: Officer is presented with "Contactless Logon – Please present card", logon tile.

(Figure 3-1)

Step 4: An officer, who has been previously authorized and enrolled in the 2FA ONE system, presents their agency issued officer identification badge that contains HID PROX (RFID) technology to a locally connected RFID reader. The HID PROX number is read by reader and passed to the 2FA ONE Client application. The 2FA ONE client application sends a web-services call to the 2FA ONE Server to ensure the officers credentials are authorized and have not been revoked. Upon validation that the credentials are authorized, the officer's 2FA ONE profile information is sent from the 2FA ONE Server to the 2FA ONE client for PIN validation.

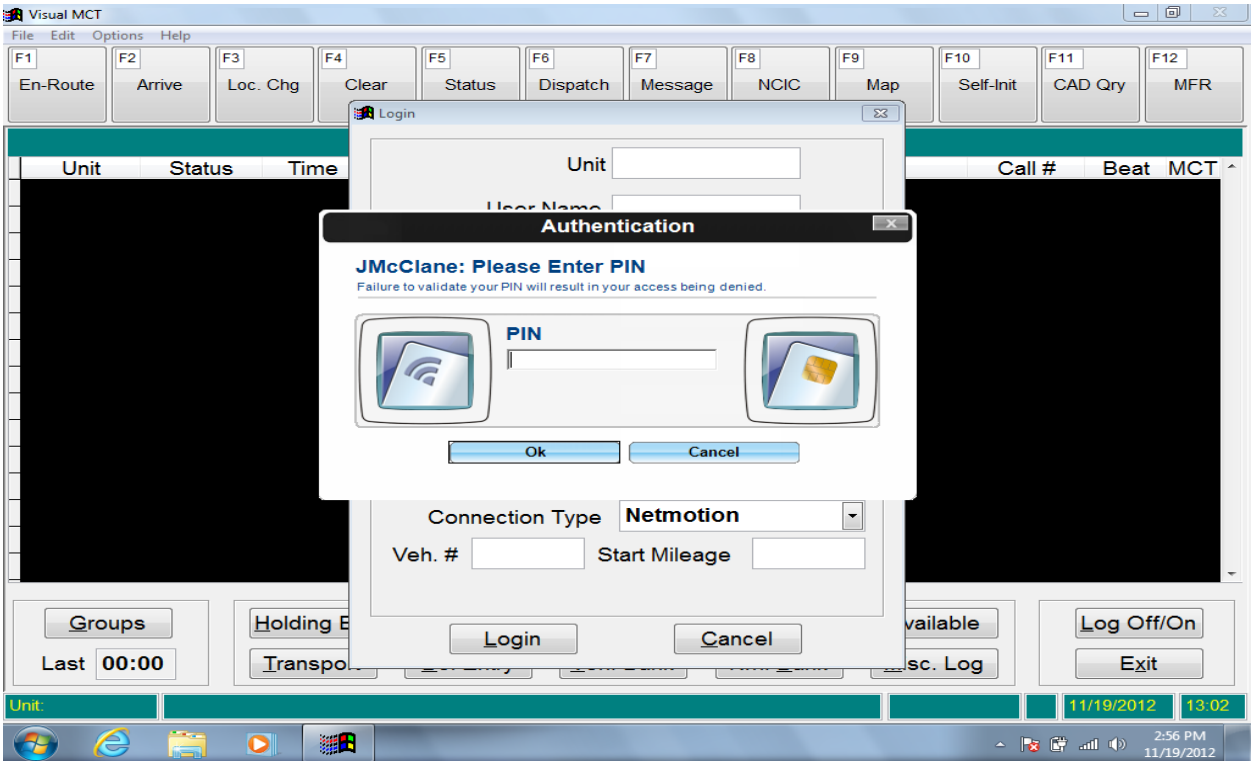
Step 5: Upon validation of the officer's credentials, the "Contactless Logon" screen identifies the officer's name and requests the officer enter their associated PIN. The officer enters their PIN that they previously selected and is known by the 2FA ONE software and clicks the right facing arrow or presses Enter.

(Figure 5-1)

Step 6: The 2FA ONE client logs the officer's access (user name, date, time, and authentication type) to the MDT in the local event log. The officer's assigned desktop appears.

(Figure 6-1)

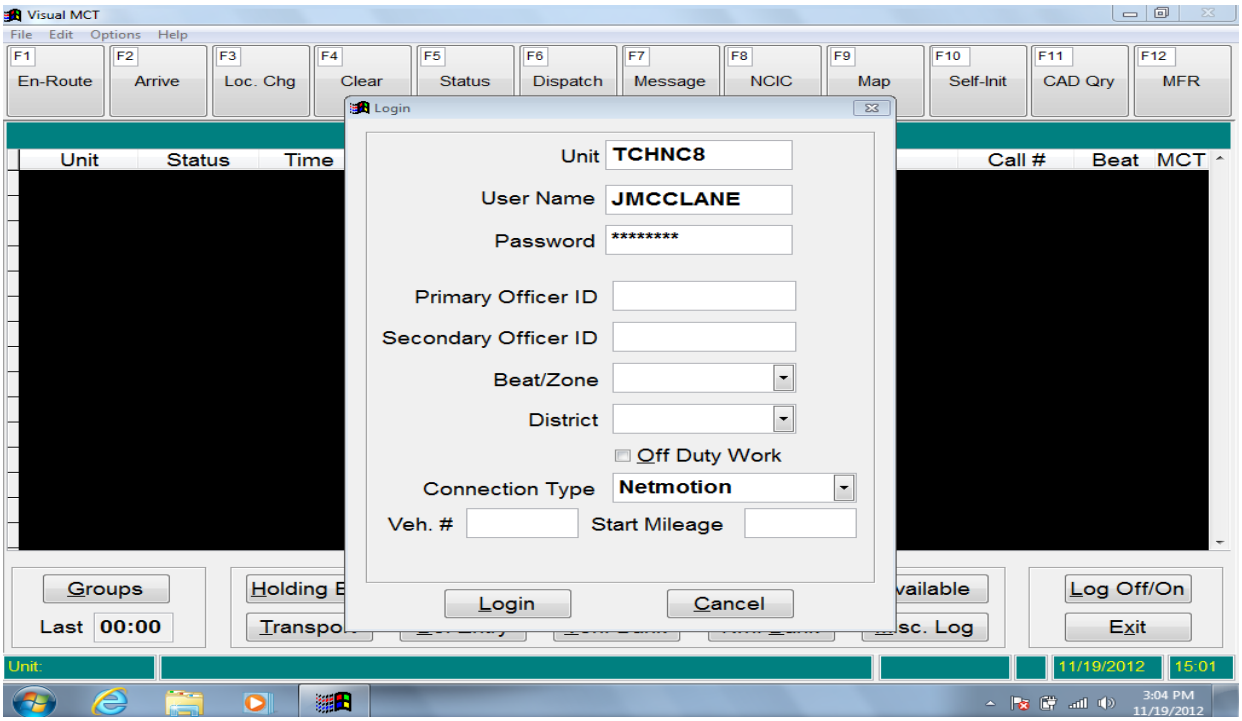
Step 7: The officer opens OSSI MCT, the application launches, and 2FA ONE Secured Application's Enforce Authentication template is triggered. If the officer clicks Cancel or clicks away from the Authentication window OSSI MCT is closed by 2FA ONE. The officer must represent their badge and enter their PIN as they initially did when logging on to Windows.



(Figure 7-1)

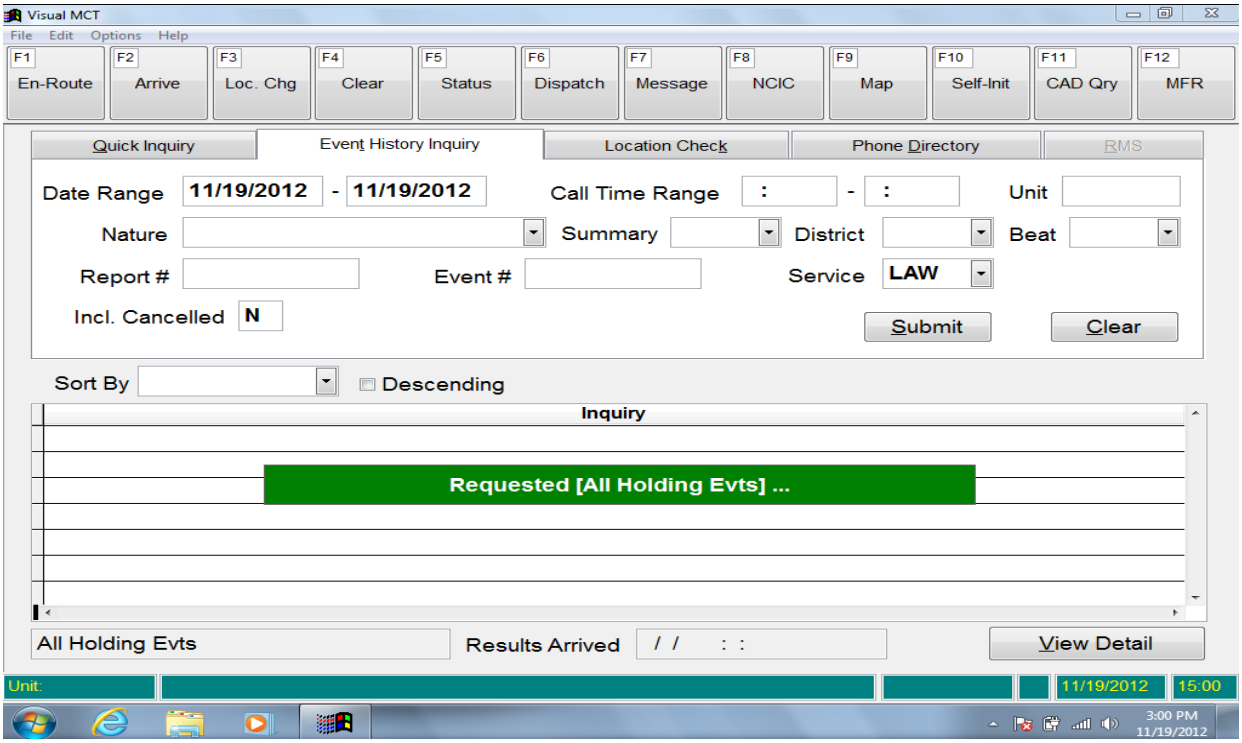
Step 8: 2FA ONE validates the officer's credentials, logs the fact that advanced authentication occurred at the application level in the application event log (username, domain, authentication method, login template specific to MCT) and provides the officer access to OSSI MCT. The officer must enter their User name and Password.

Note: A configurable option, 2FA ONE is capable of providing the officer's assigned User name and Password to OSSI MCT, also known as SSO.



(Figure 8-1)

Step 9: The officer enters in the required information and clicks “Login”. The officer’s credentials are validated against OSSI and upon validation the officer is granted access to MCT.



(Figure 9-1)

Step 10: During the shift the officer touches or clicks on the lock MDT icon located in the taskbar.

(Figure 10 -1)

Once locked the officer must represent their badge and enter their PIN as they did in **Step #3** prior to regaining access to the desktop and the running OSSI MCT.

Step 11: At the end of their shift the officer logs off OSSI MCT and Windows. The officer is presented with the "Contactless Logon – Please present card."

(Figure 11-1)

The Verizon and NetMotion connection will remain active unless disconnected manually by the officer.