ADVANCE AUTHENTICATION – The CJIN-MDN Approach

NOVEMBER 15, 2012

OVERVIEW

- History of the CJIN-MDN
- CJIS Requirements
 - Password
 - Advanced Authentication

CJIN-MDN Yesterday, Today and Tomorrow

- Proof of Concept
- eCitation
- XFILES
- FIPS 140-2 Encryption
- Radio Infrastructure End-of-Life
- Wi-Fi and Commercial Carrier Support
- Pending CJIS Requirements

CJIS CHANGES

- Password
- Advance Authentication (Two-Factor)
 - Something you know
 - Something you have

CJIN-MDN ENHANCEMENT

- Omnixx Enterprise Platform
 - Omnixx Force Client
 - Mobile Application
 - Omnixx Force Server
 - Management Console
- Combine to create a Risk-Based Advance Authentication.

RISK-BASED AUTHENTICATION

- Four step process
 - Administrative Setup
 - User Setup
 - User Login
 - Maintenance

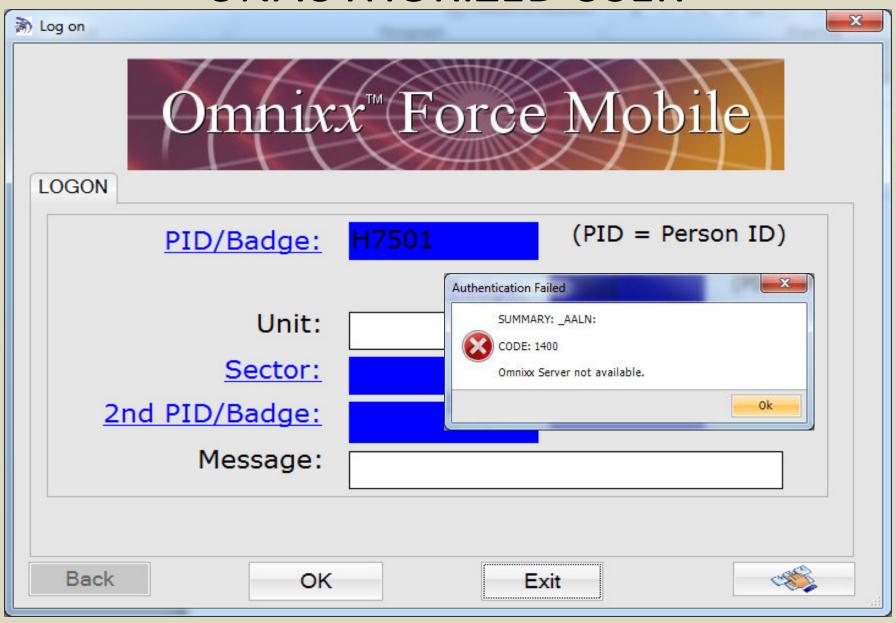
OMNIXX FORCE CONSOLE

ole - 5 - NCHPXXOFM00 - Windows Internet Explorer provided by the NC State Highway Patrol 20/private/vnc_only.php _ B × @ Omnixx 4.3.5.17 Conso 5 - NCHPXXOFM00 Ctrl Alt Shift Power Control KVM Media Tray Softkey Remote Drive Preferences Help http://207.4.83.20Video **Omnixx** Console Main Menu NCSHP Agency: Certification: SHP_CAD Omnixx Analytics & DMXLive Subagency: DMXS-Subagency Standard Authentication Select Subject RSPELL - (RODNEY SPELL) Agencies Device: Subagencies Devices **User Security Policy** Users Modify the security policy parameters and click NEXT Select User Add New User Default Security Policy (Subagency) **Modify User Change Subagency Authentication Scheme** Delete User Advanced Authentication Copy User Standard Authentication **Security Policy** Maximum Duration of Session (Minutes) VASCO Authentication Advanced Authentication Passwords Before Reuse Modify User Information 10000 Reset User Password Minimum Reuse Period (Days) Maximum Period of Inactivity (Minutes) Default Password Duration (Days) **Modify User POC Modify User Aliases** Maximum Period Between Logons (Days) **Modify User Application** Password Expiration Notice Period (Days) 14 **Modify User Certification** Maximum Logons per User **Modify User Group** Minimum Password Length Reports Allow Use on Holidays Maximum Password Length ORIS **Lockout After Failed Logons** 10 Groups **Maximum Failed Logons** Minimum number of days between password changes Transaction Groups Lockout Duration (Minutes) Certifications Password Composition Rules Allow user to reset expired password Applications Letter and Number Omnixx Switches Limited to letters and numbers, and at least one of each. Host Switches Interfaces Trainer Help Next Leading Law Enforcement Technology Datamaxx

USER SETUP

🚵 Log on	X
Omnixx [™] Force Mobile	
PID/Badge: (PID = Person ID)	
Unit:	
Sector:	
2nd PID/Badge:	
Message:	
Back OK Exit	

UNAUTHORIZED USER



USER SETUP



INITIAL LOGON



ADVANCED AUTHENTICATION



INVALID PASSWORD



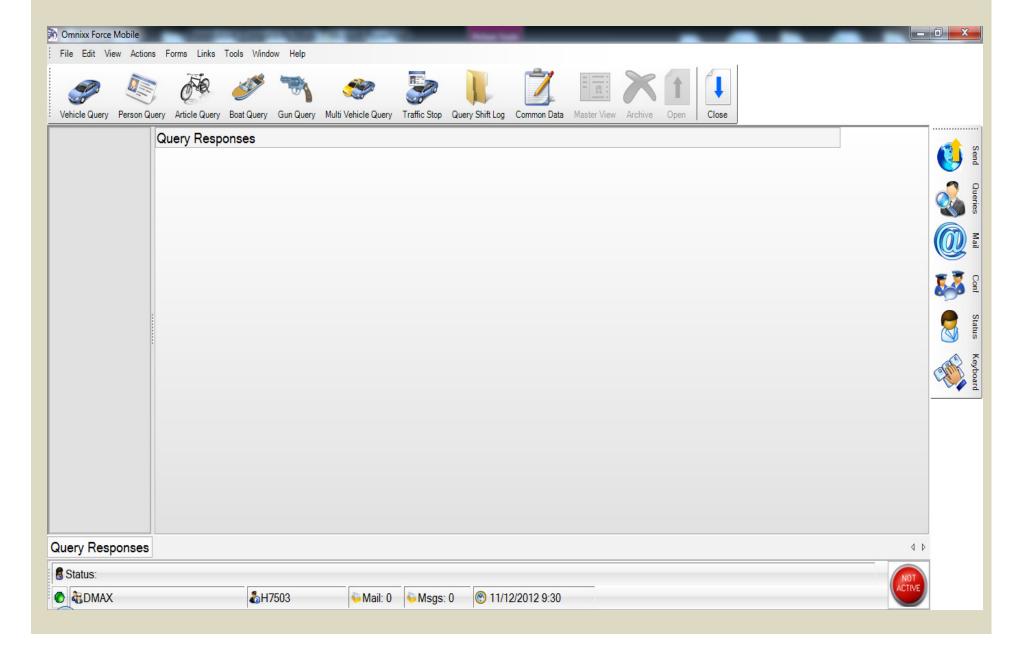
INVALID PIN



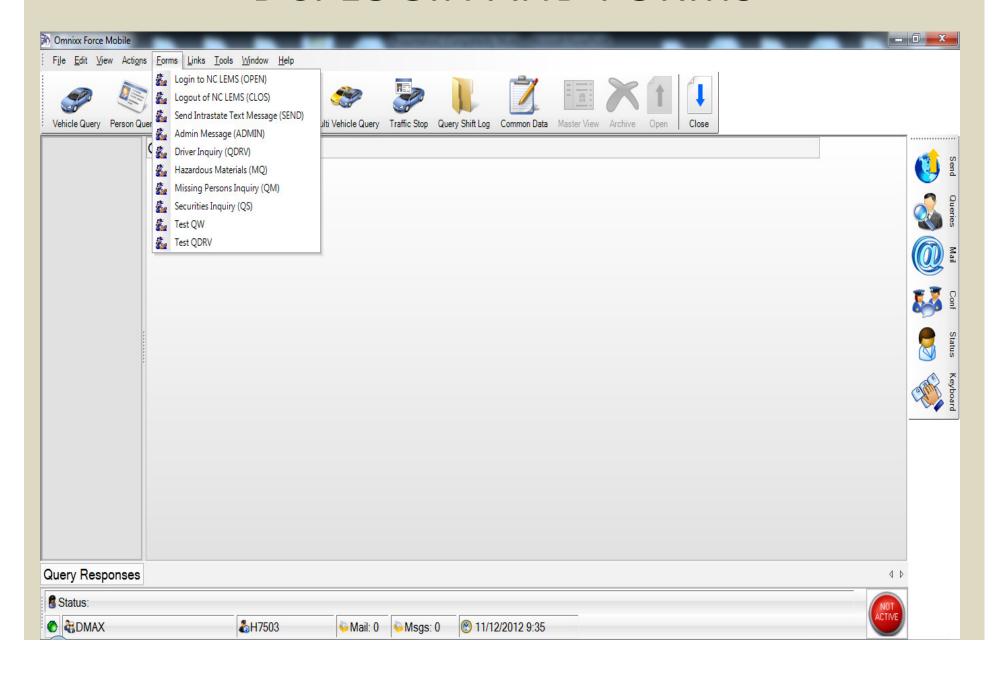
INCORRECT CHALLENGE RESPONSE



SUCCESSFUL AUTHENTICATION



DCI LOGIN AND FORMS



Maintenance

- Users can change password, PIN, and modify answers to the challenge questions.
- All other functions, including resetting forgotten passwords are handled at the Administrative level.
- Omnixx Server will enforce a password policy for field length, expiration period and use of special characters.

Questions?

Contact Information

Rodney Spell

Email: rspell@ncdps.gov

Phone: 919-662-4440