

Attention Disbursing Officers and Supply Officers

**NAVY CASH[®]
SOP CHANGE NOTICE
NAVSUP PUB 727**

**Navy Cash Fleet Support Groups
NAVSUP Fleet Logistics Centers
Norfolk
San Diego
Yokosuka**

Navy Cash SOP Change Notice 2013-010

5 November 2013

Subject: **NAVY CASH SYSTEM ADMINISTRATION PASSWORD CHANGES**

Attention: Disbursing Officers/Supply Officers

1. Background. A Communications Tasking Order (CTO) issued by Navy Cyber Forces (CTO 13-15) has directed that all passwords for local administrator accounts be changed and that these passwords then be changed every 60 days thereafter. This task and others outlined by the CTO are in direct response to current threats to DoD systems and are not specific to Navy Cash.

To comply with this emergent requirement, the JPMorgan Chase (JPMC) Navy Cash Technical Support group (NCTS) will equip the Navy Cash servers on all ships with a password rotation tool that Disbursing Officers (DOs) can use to change all Navy Cash administrative passwords automatically. After successful completion of pilot testing, the new password rotation tool will be provided to all Navy Cash ships remotely and applied automatically using Windows Server Update Services (WSUS) (for software release 1.4.6 build 3 and 3a) and BMC Patch Manager (for software release 1.4.7 build 0 and 1). NCTS will also update the Navy Cash Disbursing Web Site (www.navycashcenter.com) to support this new functionality.

2. Disbursing Officer Action. Once the new password rotation tool is installed on the Navy Cash server on the ship, the DO must take the necessary steps to ensure that all Navy Cash operating system and database system administration (sys admin) passwords are changed immediately and that these passwords are then changed every 60 days thereafter.

The CTO issued by Navy Cyber Forces also reiterates the prohibition on the use of flash media, the requirement to disable the command prompt for all non-administrator accounts, and the critical importance of anti-virus definitions. These provisions are already in place for the Navy Cash system, but DOs must take the necessary steps to remind all Navy Cash system users periodically that they must conduct only official, authorized business on the Navy Cash system. They must access only that data, control information, software, hardware, and firmware for which they are authorized access, and assume only those roles and privileges for which they are authorized. And, they must not introduce or use any unauthorized software, firmware, electronic files, or hardware, including any flash media.

Finally, DOs must check the main Symantec Antivirus (or Endpoint Protection) window daily to confirm that the virus definitions file date is not more than one day older than the present date or that the "Protection definitions are current" link is displayed. The LiveUpdate tool on Navy Cash servers, workstations, and laptops is configured to run each day at 1000 GMT, when it contacts a Symantec Internet site to determine if a newer virus definitions file is available. Updates will generally occur automatically. If the automated update function does not appear to be running, the updates can be applied manually by

Page 1 of 4

Please route immediately to the Supply Officer and Disbursing Officer

clicking on the "LiveUpdate" button or link. If the date is older than seven days, contact the Navy Cash Central Support Unit (CSU) at 1-866-662-8922 or navycashcenter@ezpaymt.com and request assistance. DOs should review Navy Cash SOP Change Notice 2013-008, Maintaining Laptop Security Patches and Updates, which includes detailed procedures for ensuring virus definitions are kept up to date, specifically for Navy Cash laptops kept in storage and generally for all Navy Cash servers, workstations, and laptops.

3. Official Change to Navy Cash SOP. This Navy Cash SOP Change Notice represents an official change to the Navy Cash SOP (NAVSUP PUB 727). Each DO shall retain a copy of this Navy Cash SOP Change Notice on file for inspection with the current version of the SOP.

4. List of Effective Navy Cash SOP Change Notices.

- ~~2012-001~~ ~~Automatic EOD Now Mandatory~~ *CANCELED*
- ~~2012-002~~ ~~Required Navy Cash Documentation in Financial Returns~~ *CANCELED*
- 2012-003 Residual Funds on Visitor Cards
- 2012-004 Transfer Member Profile and Unsuspend Account Using Disbursing Web Site
- 2012-005 Automated Transfer of Dormant Profiles
- 2012-006 Navy Cash Depot Shipping Address Change
- 2012-007 Navy Cash, Marine Cash, and Navy Cash Visitor Card Cardholder Agreement
- 2012-008 Staff, Air Wing, Squadron, and Generic Private Merchants Settle Only to Merchant Strip Account
- 2012-009 Bank/Credit Union Account Information on Cardholder Web Site
- 2012-010 Automated EOM Spreadsheet Alternative
- 2012-011 Court Orders and Levies and Subpoenas on Navy Cash Accounts
- ~~2013-001~~ ~~Enrollment Forms Missing in Document Storage System Ashore~~ *CANCELED*
- 2013-002 Updating Generic Private, Staff, Air Wing, and Squadron Merchant Linked Accounts at Turnover
- 2013-003 Use of Official Mail Manager Merchant Card Now Mandatory
- 2013-004 Update to Navy Cash Cardholder Web Site
- 2013-005 Enrollment Forms Missing in Document Storage System Ashore—Revised
- 2013-006 Distribution of Ship's Store Profits to MWR and Other Miscellaneous Payments — Revised Procedures
- 2013-007 DASR and Revision to the Navy Cash Documentation Required in Financial Returns
- 2013-008 Maintaining Laptop Security Patches and Updates
- 2013-009 Before Cardholders Leave the Ship for a Pending Transfer or Discharge
- 2013-010 Navy Cash System Administration Password Changes

5. Points of Contact. If you have any questions, please contact:

Karl Larson at NAVSUP Headquarters
Navy Cash Information Assurance Officer
karl.larson1@navy.mil
(717) 605-3506 DSN: 430-3506

Hugh Chin at NAVSUP FLC Norfolk
hugh.chin@navy.mil
(757) 443-1189 DSN: 646-1189

Please route immediately to the Supply Officer and Disbursing Officer

Andy Yager at NAVSUP FLC San Diego
andrew.yager@navy.mil
(619) 556-6493 DSN: 526-6493

§§§§§

8.4.34 Navy Cash System Administration Password Control
(in version 1.14 of the Navy Cash SOP associated with release v1.4.7)

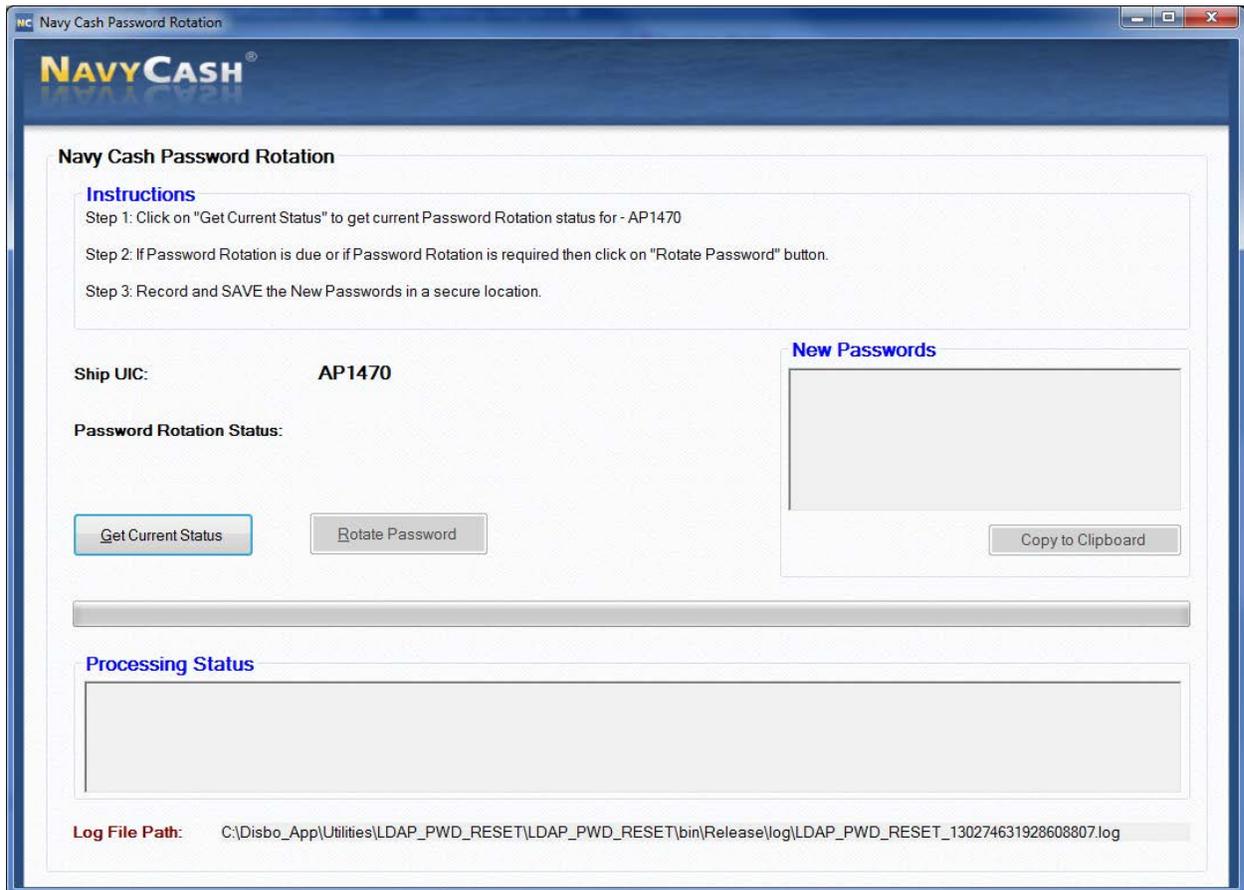
8.4.38 Navy Cash System Administration Password Control
(in version 1.13 of the Navy Cash SOP associated with release v1.4.6)

a. To comply with Navy Information Assurance (IA) requirements for local administrator accounts, Navy Cash operating system and database administration passwords must be changed every 60 days.

b. Navy Cash is equipped with a password rotation tool that shows the due date for the next password change and provides a single button that can be used to change all administrative passwords automatically.

c. Password Rotation Process

(1) The Disbursing Officer or ship's IT logs in to the Navy Cash server on the ship as an administrator (NC_ADMIN) and then starts the Navy Cash Password Rotation tool. The tool must be run on the active server node. If run incorrectly, it will alert the user with an error message.



Please route immediately to the Supply Officer and Disbursing Officer

(2) The Disbursing Officer or ship's IT clicks on the "Get Current Status" button.

(a) The password rotation tool tries to communicate via HTTPS with navycashcenter.com. If successful, navycashcenter.com responds with a list of the current passwords, the rotation status (due date for the next password change), and the "Rotate Password" button is enabled.

(b) If the tool cannot reach navycashcenter.com, the Disbursing Officer or ship's IT should attempt to reach the Navy Cash Disbursing Web Site (www.navycashcenter.com) using a browser and start troubleshooting.

(3) If the due day for the change in operating system and database administration passwords is approaching or the change in passwords is required for other reasons, the Disbursing Officer or ship's IT clicks on the "Rotate Password" button.

(a) The password rotation tool again communicates with navycashcenter.com. If successful, navycashcenter.com generates and responds with the new passwords. The password rotation tool changes the Navy Cash operating system and database administration passwords for all scheduled tasks automatically, notifies navycashcenter.com to confirm the password changes were successful, displays the new passwords in the "New Passwords" box, and enables the "Copy to Clipboard" button.

(b) The new set of passwords are stored on the Navy Cash backend ashore, and navycashcenter.com tracks the ship's confirmation of the change in passwords.

(4) Prior to logging out of or closing the password protection tool, the Disbursing Officer or ship's IT must record the new passwords.

(a) Write down the passwords for each operating system and database user profile, or click the "Copy to Clipboard" button and paste the list of passwords and operating system and database user profiles into a Word document.

(b) The list can then be printed out, but the electronic file for the document must be deleted and must not be stored electronically on any hard drive or other storage media. The list of passwords and operating system and database user profiles, whether handwritten or printed Word document, must be stored in a safe at all times.

(c) When the Disbursing Officer or ship's IT logs out of or closes the password protection tool, the "new" passwords are deleted from memory.

(5) The "Processing Status" box displays the high-level success or failure at every level and will indicate to the Disbursing Officer or ship's IT that the password changes were successful.

(6) The "Log File Path" shows the file location where the Navy Cash Password Location tool saves its log files, which provide a detailed record of any status or error messages during the password rotation process, if additional details are required.