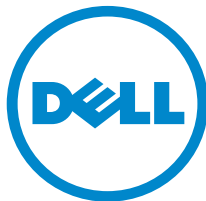


**Dell™ C7765dn  
CACStar™ Smart Card Reader  
Installation and Configuration Guide**

**Document protection for CAC/PIV enabled  
Multifunction Devices**



Information in this document is subject to change without notice.

© 2015 Dell Inc. All rights reserved.

This publication could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in later editions. Improvements or changes in the products or the programs described may be made at any time.

**Note:** For Dell technical support and downloads, visit [dell.com/support](http://dell.com/support) or contact the Dell ProSupport Help Desk for assistance by calling 1-866-516-3115, or by e-mailing [imaging\\_Solutions\\_Support\\_CAC@dell.com](mailto:imaging_Solutions_Support_CAC@dell.com).

Reproduction of these materials in any manner whatsoever without the written permission of Dell Inc. is strictly forbidden.

Trademarks used in this text: Dell and the DELL logo are trademarks of Dell Inc.; Microsoft, Windows, and Windows Server are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries; RSA and BSAFE are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries; *CACStar* is a registered trademark of Digital Imaging Technology in the United States.

Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell Inc. disclaims any proprietary interest in trademarks and trade names other than its own.

The printer software uses some of the codes defined by the Independent JPEG Group.

## **UNITED STATES GOVERNMENT RESTRICTED RIGHTS**

This software and documentation are provided with RESTRICTED RIGHTS. Use, duplication or disclosure by the Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and in applicable FAR provisions: Dell Inc., One Dell Way, Round Rock, Texas, 78682, USA.

# Table of Contents

- Introduction..... 3
- Hardware Installation..... 4
- Converting a Dell C7765dn to a CACStar Enabled Machine..... 8
- Configuring CACStar™ Security ..... 17
  - Establishing the Connection..... 17
  - Accessing the MFD/Printer Web Site..... 19
  - Admin Login..... 19
- Connectivity..... 20
  - LAN Address Configuration ..... 20
  - Local Side Configuration..... 22
- Security..... 23
  - MFD Function Enabling ..... 23
  - Email Setup ..... 24
  - Authentication Method ..... 26
  - SSL CA Certificate Checking..... 31
  - User Logging ..... 31
  - Upload Certificate..... 32
- Administrator ..... 33
  - Change Password ..... 33
  - Administrator Access..... 33
  - Firmware Update ..... 34
  - Technical Support..... 35
  - Setup Test..... 37
  - Date Time ..... 37
  - Hold Print Files..... 38
- Status..... 40
  - Card Reader..... 40
  - Network ..... 41
  - Other ..... 42
- Controlling Access to Fax and Copy ..... 43
- Appendix A..... 45
  - Setup Information Checklist..... 45

---

# Introduction

CACStar™ provides a solution to HSPD-12 requirements for CAC/PIV based protection of network data to and from printers or Multifunction Devices (MFDs). You can configure it to require an authenticated CAC/PIV card to control Copy, Print, Fax, Scan to Folder, Scan to Email, SNMP, or FTP.

Configurable authentication methods include Basic X.509 certificate on the card, PIN validation, expiration, OCSP, root certificate, LDAP, and Kerberos. CACStar will adopt the IP address of the MFD on which it is installed, so there is no host network configuration change necessary.

Configuration is easily done using secure web based access to CACStar by the network administrator. In its simplest form, the admin only needs to configure the IP address of the MFD and the IP address of the local time server. Information about many additional configuration options is described later in this guide.

Prior to starting the CACStar configuration, you must know your network infrastructure. Appendix A has a convenient list of questions and the necessary data that you will need to collect.

If you need help obtaining correct firmware or documentation, contact the Dell ProSupport Help Desk by calling 1-866-516-3115, or by sending email to [Imaging\\_Solutions\\_Support\\_CAC@dell.com](mailto:Imaging_Solutions_Support_CAC@dell.com).

This manual will guide you through installing the hardware, installing the software to convert the Dell C7765dn to be CACStar enabled, and configuration of the customer desired authentication control options.

# Hardware Installation

---

The kit contents includes:

CACStar™ I/O cover panel

Cable for connection to power USB

Cable for Ethernet connection from CACStar to MFD

Card reader with USB cable

Shelf for reader (with 2 mounting screws/lock washers)

Adhesive-backed cable tie

This User Guide

**Note:** Make sure power is off before starting this installation.

Step 1: Mount shelf to right side of scanner with 2 supplied screws.



Step 2: Mount reader to top of shelf using supplied double backed adhesive preinstalled on back of reader.



Step 3: Secure cable to rear right side of scanner with supplied cable tie.



Step 4: Connect reader to USB port on CACStar electronics.



Step 5: Connect the CACStar power cable from the microUSB port on CACStar to a USB connector on the upper back of the printer.



Step 6: Connect the CACStar Ethernet LAN port to your network on a port designated for this MFD.



Step 7: Remove the existing I/O cover from the lower right rear of the machine.



Step 8: Connect the CACStar Ethernet MFD port to the C7765dn Ethernet port.



Step 9: Install CACStar I/O cover panel in place of the existing cover.



Step 10: CACStar hardware installation is now completed. The administrator can now turn on the MFD and proceed to “Converting a Dell C7765dn to a CACStar Enabled Machine”.



# Converting a Dell C7765dn to a CACStar Enabled Machine

---

This section will cover the step-by-step instructions to convert the MFD from a “factory default” configuration to a CACStar ready configuration. The CACStar option requires Dell C7765dn Controller ROM Ver. 2.205.100 or later.

**Important Note:** Download the C7765 CACStar Setup files from [www.dell.com/support](http://www.dell.com/support) before proceeding to step 1.

To prepare for this process, please set up a dedicated PC with a direct Ethernet connection to the CACStar LAN port. On this PC, set the TCP/IP parameters as follows: IP address = 10.5.9.1; Subnet Mask = 255.255.255.0.

1. Initial TCP/IP settings:
  - a. At the printer operator panel, press the [Log In / Out] button. The display should show a button to log in to the MFD as the administrator.  
  
Note: it might be necessary to press the [Log In / Out] button more than once.
  - b. When prompted for the login name, enter “admin”
  - c. If you are prompted for a passcode, enter “1111”.
  - d. Press the “Home” hard key at the top-left corner of the panel.
  - e. Navigate using the soft keys: Tools->System Settings/Connectivity & Network Setup/Protocol Settings...
  - f. Select IPv4-IP Address Resolution and then press the [Change Settings] button.
  - g. Choose Static and then press the [Save] button.
  - h. Select IPv4-IP Address and then press the [Change Settings] button.
  - i. Set the address to 172.19.10.2 and press the [Save] button.
  - j. Select IPv4-Subnet Mask and then press the [Change Settings] button.
  - k. Set the subnet mask to 255.255.255.0 and press the [Save] button.

- l. Select IPv4-Gateway Address and then press the [Change Settings] button.
  - m. Set the Gateway address to 172.19.10.1 and press the [Save] button.
  - n. Press the [Close] button twice.
  - o. When prompted, press the [Reboot Now] button.
2. Open your Web browser, enter http://10.5.9.11 in the Address or Location field, and press the [Enter] key.

**Note:** If a certificate error screen appears, choose to ignore the error and continue.
  3. Enter the System Administrator's ID and password if prompted (default ID: "admin", default password: "1111").
  4. Display the [Properties] screen by clicking the [Properties] tab.
  5. Enable the use of plug-ins:
    - a. Navigate to Properties tab->Security->Plug-in Settings->Plug-in Settings. You may need to scroll down to find the plug-in settings.
    - b. Check the "Enabled" box.
    - c. Click the [Apply] button.
    - d. You may see a screen advising you to reboot the printer. Do not press the [Reboot Now] button.
  6. Create a self-signed certificate for the MFD:
    - a. Navigate to Properties tab->Security->Machine Digital Certificate Management.
    - b. Click the [Create New Certificate] button.
    - c. Select [Self-Signed Certificate]. Click [Continue].
    - d. Set [Digital Signature Algorithm] as necessary.
    - e. Set [Public Key Size] as necessary.
    - f. Set [Issuer] as necessary.
    - g. Set [Days of Validity] as necessary.
    - h. Click [Apply]. It may take up to 30 seconds to complete this action and there will be no progress indicators.

7. Enable SSL/TLS:
  - a. Navigate to Properties tab->Security->SSL / TLS Settings
  - b. Check the “Enabled” box for “HTTP - SSL / TLS Communication”.
  - c. Set [HTTP - SSL / TLS Communication Port Number] as necessary.
  - d. Click [Apply].
  - e. When the right frame of the web browser changes to the Machine Reboot display, click [Reboot Machine].
8. Make sure you completely close the browser and then log into the web page using HTTPS.
9. Install the CACStar authentication plug-in software:
  - a. Enter the System Administrator’s ID and password if prompted (default ID: “admin”, default password: “1111”).
  - b. Navigate to Properties tab->Security->Plug-in Settings->List of Embedded Plug-ins.
  - c. Browse and select “CACStarAuthPlugin\_A##.jar”.
  - d. Click the [Upload] button. Wait for the screen indicating successful completion of the upload.
  - e. To activate the plug-in software reboot the printer by navigating to the Status tab and clicking the [Reboot] button. Click [OK] when asked for confirmation.

10. Install the CACStar Services on the MFD:

Note: CACStar Services are the code plug-ins that provide the CACStar authentication user interface on the Dell C7765dn.

- a. On a Windows desktop, find the file called “CACStarService\_Installer\_A##.exe” and run it. This is the installer application for the CACStar services.
- b. When the installer starts, press the [Next] button to begin installation.
- c. Enter the CACStar IP address 10.5.9.11, administrator ID (default: “admin”) and administrator password (default: “1111”). Click the [Add] button.
- d. Click the [Next] button when it becomes available.

- e. On the next screen, select [Install] and click [Next].
- f. Click [Next] again when it becomes available.
- g. Click [Install]. Installation of CACStar services will commence. This process can take up to two minutes.
- h. When the installation is completed, click [Next].
- i. Click [Finish] to exit the installer.

#### 11. DHCP configuration on MFD

- a. Open your Web browser, enter <http://10.5.9.11> in the Address or Location field, and press the [Enter] key.

**Note:** If a certificate error screen appears, choose to ignore the error and continue.

- b. Enter the System Administrator's ID and the passcode if prompted (default ID: "admin", default passcode: "1111").
- c. Navigate to [Properties tab]->Connectivity->Protocols->TCP/IP
- d. Ensure that "IP Address Resolution" is set to "DHCP" under the General section.
- e. Ensure that the check box for "Release Current IP Address When the Host is Powered Off" is checked (enabled). This is near the bottom of the page.
- f. Click [Apply].
- g. If prompted to reboot, DO NOT REBOOT. Continue to step 12.

#### 12. Install the MFD Settings (Cloning File):

- a. Open your Web browser, enter <http://10.5.9.11> in the Address or Location field, and press the [Enter] key.

**Note:** If a certificate error screen appears, choose to ignore the error and continue.

- b. Enter the System Administrator's ID and the passcode if prompted (default ID: "admin", default passcode: "1111").
- c. Navigate to [Properties tab]->General Setup->Cloning.
- d. In the "Install Clone File" section, click the [Browse] button.
- e. Select the cloning file - "C7765-Cloning\_A##.dat"

- f. Click the [Install] button. A confirmation screen will be shown. Click [OK]. The clone file will be installed and the printer will automatically restart.
    - g. Wait for the printer to finish restarting.
13. Go to the MFD and log in as administrator:
  - a. At the printer operator panel, press the [Log In / Out] button. The display should show a button to log in to the MFD as the administrator.

Note: it might be necessary to press the [Log In / Out] button more than once.
  - b. When prompted for the login name, enter “admin” and press the [Enter] button.
  - c. After login is complete, the [Log In/Out] button will remain lit.
14. Change MFD administrator login to require password entry:

By default, there is no password required to log in to the MFD via operator panel. It is strongly recommended that the printer is set to require a password when logging in as administrator. The following steps are done after logging in as administrator via the operator panel:

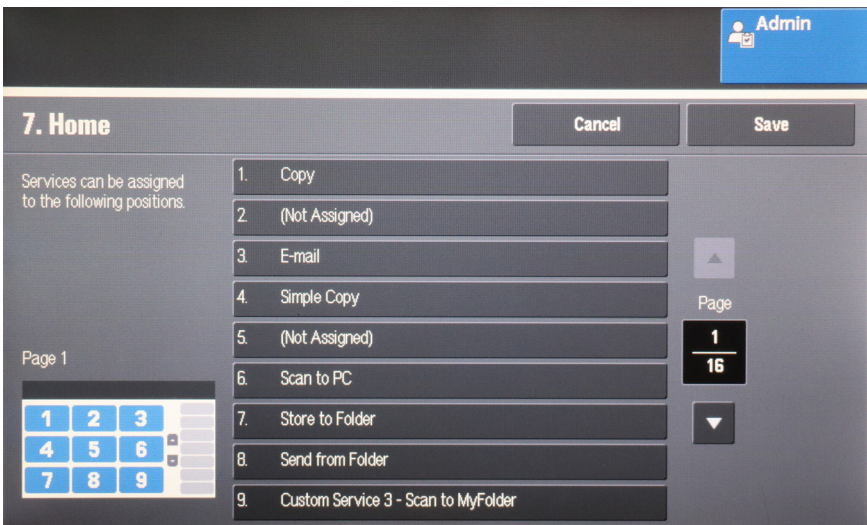
  - a. Press the “Home” hard key at the top-left corner of the panel.
  - b. Navigate using the soft keys: Tools->Authentication/Security Settings->Authentication->Passcode Policy...
  - c. Select “Passcode Entry from Front Panel” and press the [Change Settings] button.
  - d. Select [On].
  - e. Press [Save].
  - f. Press [Close].
  - g. Press [Close] again.
  - h. When the Reboot Machine prompt is shown, choose [Reboot Now].
  - i. Wait for printer to restart. For the purpose of these installation instructions, the printer has completed rebooting when the “Connecting to the security appliance...” screen appears.
  - j. Log into the MFD via the operator panel using ID = “admin”. Press [Next] and enter password = “1111”. Press [Enter].

## 15. Configure the “Home Screen” buttons:

When the CACStar services are installed above, the services are automatically assigned button positions on the Home Screen. The actual button assignments are made by the MFD, and are not necessarily the positions that a customer would prefer.

Since customer preferences are unknown in advance, this step will adjust the button positions for the CACStar services. The procedure described here can be used to change any of the Home screen buttons.

- a. Press the “Home” hard key at the top-left corner of the panel.
- b. Navigate using the soft keys: Tools->System Settings->Common Service Settings->Screen / Button Settings...
- c. In the list of settings, select [Home] and then press [Change Settings].
- d. A screen will be shown where you can change the home screen button assignments. The numbers in the image at the lower-left correspond to the numbers in the list of assignments:



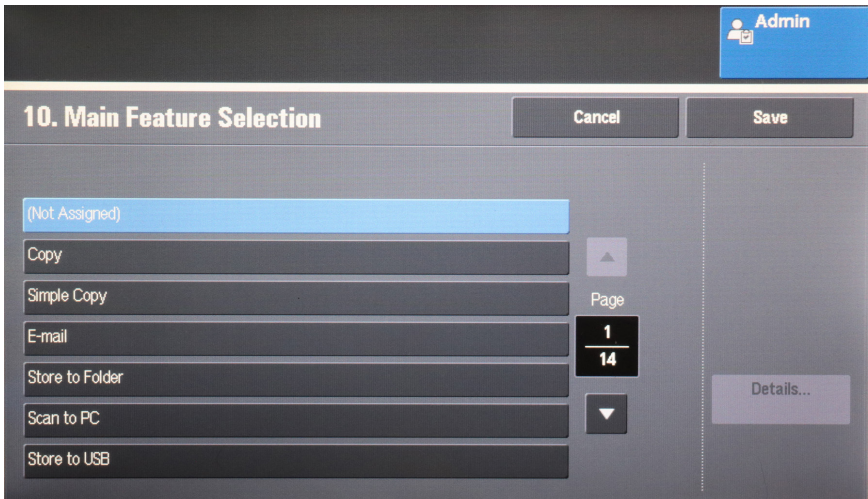
Nine settings are shown, one for each button position on a page of the Home Screen. Pressing the Down Arrow advances to the next page of the button positions.

- e. Press the Down Arrow until you see an entry named “Custom Service x – CACStar Connection UI?”. Select this entry in the list.



f. The next screen shows the list of possible assignments for the selected button position.

Press the [Up Arrow] soft key until you get to the top of the list. Choose the first entry “(Not Assigned)”.



g. Select this entry and press the [Save] button.

h. Press [Save] again to save change to the home screen buttons.

i. Press [Close] to leave the screen/button settings screen.

j. Press [Close] at the tools menu to leave the configuration screen.

k. The same assignment cannot be used more than once, with the exception of “(Not Assigned)”. To move an assignment from one button position to another, you must first go to the original button position for the service you wish to move and change its assignment to (Not Assigned). Then you can change the assignment of the desired button to the desired service. This procedure can be used to move the assignment of the “Scan to MyFolder” custom service to any desired button position.

16. Press the [Log In / Out] button to log out of the MFD.

17. Disable Sleep Mode:

**Note:** Sleep Mode must be disabled to prevent power from being turned off to the CACStar authentication controller.

You must enter “CE mode” to disable sleep mode:

a. Hold down the “0” hard key on the operator panel for 15 seconds.

b. While still holding down the “0” key, press the [Start] key.

c. At the “CE Type Passcode” prompt, use the numeric keypad to enter “6789”.

d. Press the [Confirm] soft key.

e. Press the “Home” hard key at the top-left corner of the panel.

f. Navigate using the soft keys: Tools->System Settings->Common Service Settings->Power Saver Settings...

g. Press the Down Arrow soft button until you see “Sleep Mode” in the list.

h. Select “Sleep Mode” and press [Change Settings].

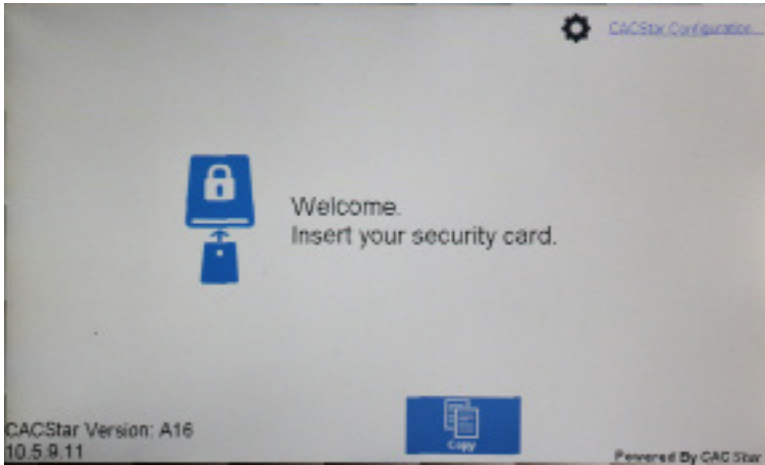
i. Select “Disabled” then press [Save].

j. Press [Close] (two times)

k. Turn the printer off, wait for the screen to go blank, then turn the printer back on.



18. Wait for the printer to go through the initialization process which will take about 75 seconds. You will then see the following screen which indicates this process has completed satisfactorily.



# Configuring CACStar™ Security

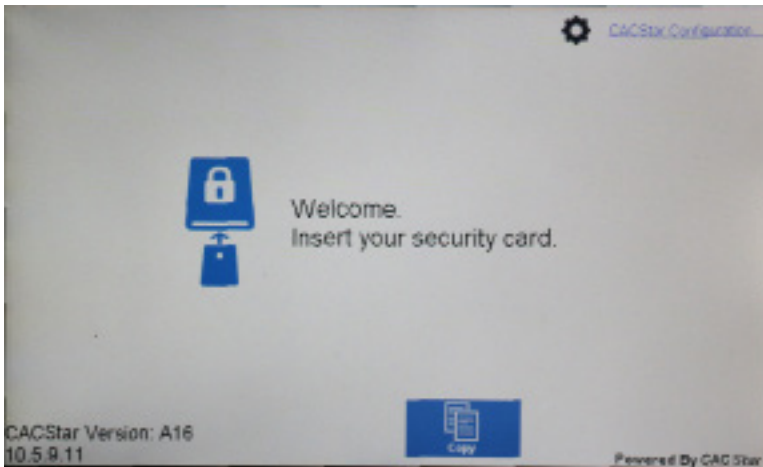
---

## Establishing the Connection

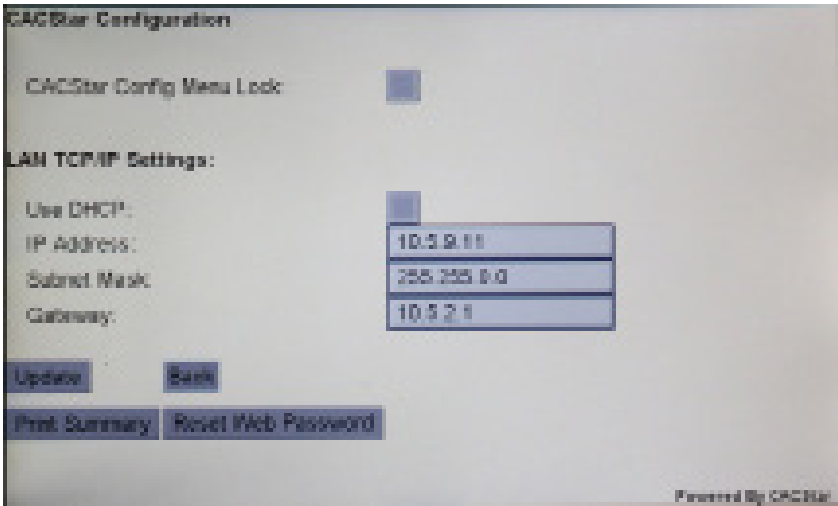
There are two choices for TCP/IP configuration:

- **DHCP:** The IP address parameters are acquired automatically from the DHCP server when the printer is turned on. Depending on the configuration of your DHCP server, it may be possible for the printer's IP address to change.
- **Manual:** You can choose a fixed IP address, subnet mask, and gateway address to ensure that the printer will always be at a known IP address.

To choose the LAN TCP/IP settings, tap the “CACStar Configuration” link on the printer's touchscreen:



Upon tapping the link, you will see a limited configuration screen where some of the CACStar parameters can be set:



- To use DHCP to acquire the IP address, make sure that the “Use DHCP” checkbox is checked, then press the [Update] button.
- To set a manual (static) IP address, clear the “Use DHCP” checkbox, and enter the appropriate values for “IP Address”, “Subnet Mask”, and “Gateway” settings, then press [Update].

**Note:** Your network administrator should supply the appropriate values.

- Additionally, if you wish to prevent future access to this menu, check the “CACStar Config Menu Lock” setting and press [Update].

## Accessing the MFD/Printer Web Site

If you wish to access the MFD/printer web site, go to the IP address assigned above. For example: <http://192.168.1.23> or <https://192.168.1.23>.

## Admin Login

Login to CACStar as the Administrator by pointing your browser to the CACStar using a secure connection on port 8443 at the IP address you assigned in the steps above.

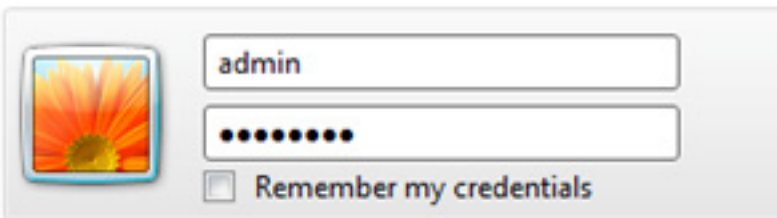
For example: <https://192.168.1.23:8443> or <https://10.5.9.11:8443>

You are likely to get an Invalid Certificate Warning from the browser. If so, override the warning and continue to the CACStar web site.

The browser will require an ID and password. The default ID is “admin”.

The default password is “1111”.

After initial login, you can change the password to one of your choice by going to the Administrator tab as shown below. Note that the CACStar admin password is separate from the password for the MFD admin. When one password is changed, the other does not change.



The image shows a login form with a square icon on the left containing a sunflower. To the right of the icon are two input fields. The top field contains the text "admin". The bottom field contains ten black dots, representing a masked password. Below the password field is a checkbox that is currently unchecked, followed by the text "Remember my credentials".

# Connectivity

---

## LAN Address Configuration

### Dell™ CAC Enabled MFD

Connectivity | Security | Administrator | Status

LAN Side Configuration | Local Side Configuration

Enter the IP Addresses and related configuration information for host network communication with the MFD

If the NTP time server box is empty, CACStar will not use time for validation.  
Enter the host network Gateway.  
Enter the DNS server IP address which is used for OCSP authentication.

Use DHCP:  ?

MFD IP Address:  ?

MFD Subnet Mask:  ?

NTP server:  ? NTP from DHCP:

Gateway:  ?

DNS Primary Server:  ? DNS from DHCP:

DNS Secondary Server:  ?

Default Domain:  ?

### Step 1 – MFD LAN IP Address

This is the same IP address that can also be configured from the operator panel as described in “Establishing the Connection” on Page 6. It does not need to be configured here if it was done using the operator panel. It is used for host computer connection to the MFD/printer, and is also used for connection to these CACStar configuration web pages using the IP address followed by “:8443”. For example: <https://192.168.1.23:8443>. If you use DHCP, this address will be set automatically. If you wish to change this address manually, it can be done using this screen.

When you press the **Update** button after changing the IP address, CACStar will switch to the new IP address which will cause your browser to be disconnected. To reconnect, redirect your browser to the new IP address you just entered.

### **Step 2 – NTP Server:**

Set this to the Network Time Protocol Server IP address or Server Name. This will allow the CACStar to validate certificates by date.

If DHCP is in use, you may check the “NTP From DHCP” box to force retrieval of the NTP Server address from the DHCP server in which case the address field is not used and may be left blank.

### **Step 3 – Configure Gateway and DNS Server**

Note: A DNS Server is required for OCSP support. It is not necessary to configure a DNS server if you are not using OCSP.

Set this to the DNS IP address to be used by the CACStar for Domain Name resolution.

Example: 10.5.1.2

If DHCP is in use, you may check the “DNS From DHCP” box to force retrieval of DNS addresses from the DHCP server - in which case the DNS address fields are not used and may be left blank.

### **Step 4 – Configure Default Domain**

This field is used for DNS Server Name resolution. Set this to the Default Domain name for the LAN.

### **Step 5 – Press Update**

# Local Side Configuration

## Dell™ CAC Enabled MFD

Connectivity | Security | Administrator | Status

LAN Side Configuration | Local Side Configuration

These are the values the CACStar uses to communicate with the MFD.

The CACStar IP Address is the IP address of the CACStar on the Local port used to communicate with the MFD. The MFD IP Address, Subnet Mask, and Gateway should be entered into the MFD using it's configuration method.

Local CACStar IP Address:  2

Local MFD IP Address:  2

Local MFD Subnet Mask:  2

Local MFD Default Gateway:  2

These settings define the IP addresses used for Local communication between CACStar and the MFD/printer. The defaults are likely to be acceptable. **Normally there is no need to enter any IP addresses on this configuration page.**

## MFD Function Enabling

### Dell™ CAC Enabled MFD

Connectivity | Security | Administrator | Status

MFD Function Enabling | Email Setup | Authentication Method | User Logging | Upload a Certificate

These are the features that can be enabled or disabled at the MFD using a CAC card.

If an item is checked, CACStar will require a user to insert their card and be authenticated before the function may be used. If an item is not checked, CACStar will always allow this function.

CAC Enable Email:	<input checked="" type="checkbox"/>	<a href="#">?</a> See Configuration Items in Email Setup
CAC Enable FTP:	<input type="checkbox"/>	<a href="#">?</a>
CAC Enable Scan to Folder:	<input checked="" type="checkbox"/>	<a href="#">?</a>
CAC Enable Printing:	<input type="checkbox"/>	<a href="#">?</a>
CAC Enable SNMP:	<input type="checkbox"/>	<a href="#">?</a>
CAC Enable LDAP:	<input type="checkbox"/>	<a href="#">?</a>
CAC SNMP Proxy:	<input type="checkbox"/>	<a href="#">?</a>
CAC Hold Print:	<input type="checkbox"/>	<a href="#">?</a>
CAC Print Server:	<input type="text"/>	<a href="#">?</a>
CAC Server Print Only:	<input type="checkbox"/>	<a href="#">?</a>

Update

Refresh

Check the boxes for Functions that require a validated CAC Card for use.

If a box is un-checked the Function will always be allowed.

For example:

If you want the MFD Scan-to-Folder Function to only be available when a validated CAC Card is installed, check the CAC Enable Scan-To-Folder box.

If you want the MFD Scan-to-Folder Function to be available all the time whether a CAC card is inserted or not, uncheck the CAC Enable Scan-To-Folder box.

Click the **Update** button after all entries are made.

### Hold Print

If enabled, Print jobs will be held in the CACStar until the user is authenticated at the printer by inserting their CAC card. After authentication, the user's jobs will be printed.



## CAC Print Server

Set this to the IP address of the Secure Print server.

## Server Print Only

If enabled, print jobs will only be allowed from the configured CAC Print Server. If not, jobs will be allowed from any IP address. For this to operate, “CAC Enable Printing” must be selected in the “Security/MFD Function Enabling” menu.

## Email Setup

### Dell™ CAC Enabled MFD

The screenshot shows a web-based configuration interface for a Dell CAC Enabled MFD. At the top, there are four tabs: Connectivity, Security, Administrator, and Status. Below these, there are five sub-tabs: MFD Function Enabling, Email Setup, Authentication Method, User Logging, and Upload a Certificate. The 'Email Setup' tab is selected. The main content area contains the following text: "These are the Email Setup options when using a CAC card to control Email from the MFD. CAC Enable Email must be selected in MFD Function Enabling before these options will be used." Below this text are several configuration fields, each with a help icon (a question mark in a blue circle):

- SMTP Address or Server Name: itekctl.us.mil
- SMTP Port Number: 587 (Default: 25)
- User Email Address From: CAC
- Force Email to Self:
- Encrypt Email: Prompt
- Email Encryption Type: 3DES
- Sign Email: Prompt
- LDAP Primary Certificate Attribute: userSMIMECertificate
- LDAP Secondary Certificate Attribute: userCertificate
- Kerberos Email Authentication:

At the bottom of the form are two buttons: "Update" and "Refresh".

If you have elected to control MFD generated email with your CAC cards, you will need to configure the item shown in the screen below.

### SMTP Address or Server Name

Set the IP address or Server Name of the SMTP server.

### SMTP Address or Server Name

Set the IP address or Server Name of the SMTP server.

## **SMTP Port Number**

Set the TCP port number for SMTP communications.

## **User Email Address From**

Select the source location for the “From” email address. Emailed scans can be from either the user’s own email address on his CAC card, or from the user’s email address on the LDAP server.

## **Force Email to Self**

Choose whether you want to force all emailed scans to the user’s own email address. If not checked, he can send to any email address.

If this option is not selected, the user can select the recipient from the printer’s internal address book or he can use the printer to enter the email address he wants to use.

## **Encrypt Email**

When sending emails of scanned documents, choose to never encrypt, always encrypt, or Prompt on each message for whether or not to encrypt.

When the MFD is operational and has been configured here to prompt for whether or not to encrypt, the display on the CAC reader will show Encrypt Email. Line 2 of the display shows No and can be toggled between Yes and No by pressing the F key. When the desired choice is selected, press the green Enter key to send the email message. You need to make this choice or press the F key within 10 seconds. If there are no key presses for 10 seconds, the system will send the message unencrypted.

## **Email Encryption Type**

Choose the encryption type from either 3DES or AES-256.

## **Sign Email**

When sending emails of scanned documents, choose to never sign, always sign, or Prompt on each message for whether or not to sign.

## **LDAP Primary Certificate Attribute**

Specify the primary LDAP attribute name which should be used to retrieve a certificate for email encryption.

## LDAP Secondary Certificate Attribute

Specify the secondary LDAP attribute name which should be used if the primary attribute fails.

## Authentication Method

### Dell™ CAC Enabled MFD

Connectivity	Security	Administrator	Status	
MFD Function Enabling	Email Setup	Authentication Method	User Logging	Upload a Certificate

If an item is checked, that method will be required for validation.  
If an item is not checked, that method will not be required.

CAC Validated Timeout:	<input type="text" value="2"/>	?
Basic:	<input checked="" type="checkbox"/>	?
OCSF:	<input type="checkbox"/>	?
OCSF Server IP:	<input type="text"/>	?
Root Certificate:	<input checked="" type="checkbox"/>	?
LDAP:	<input type="checkbox"/>	?
LDAP Server:	<input type="text" value="itekctl.us.mil"/>	?
LDAP Server Port:	<input type="text" value="389"/>	?
LDAP Query User Name:	<input type="text"/>	?
LDAP Query Password:	<input type="password"/>	?
LDAP Search Base:	<input type="text" value="dc=us,dc=mil"/>	?
LDAP Search String:	<input type="text" value="%s"/>	?
LDAP User ID Option:	<input type="text" value="upn"/>	?
Disable LDAP Referrals:	<input checked="" type="checkbox"/>	?
Kerberos:	<input checked="" type="checkbox"/>	?
KDC Server:	<input type="text" value="itekctl.us.mil"/>	?
KDC Server (alt):	<input type="text"/>	?
KDC Server (alt):	<input type="text"/>	?
KDC Server (alt):	<input type="text"/>	?
KDC Server Port:	<input type="text" value="88"/>	?
KDC Realm:	<input type="text" value="US.MIL"/>	?
KDC Principal:	<input type="text" value="SAN Principal"/>	?
PKINIT Win2k:	<input checked="" type="checkbox"/>	?
Disable Reverse DNS Lookups:	<input checked="" type="checkbox"/>	?
MFD LDAP Kerberos Proxy:	<input checked="" type="checkbox"/>	?
MFD SMB Kerberos Proxy:	<input checked="" type="checkbox"/>	?
Default SMB Server Address:	<input type="text"/>	?
Default SMB Service Name:	<input type="text"/>	?
Default SMB Username:	<input type="text"/>	?
Default SMB Password:	<input type="password"/>	?
SMB Folder Name:	<input type="text" value="%u"/>	?
SMB Folder LDAP Attribute:	<input type="text" value="homeDirectory"/>	?
SSL:	<input type="checkbox"/>	?
SSL CA Certificate Checking:	<input type="checkbox"/>	?

### Basic

This includes PIN validation, card expiration check, and X.509 card certificate validation.

If an NTP server is not configured on the LAN Side Configuration page, the expiration check is bypassed. The Basic level of authentication is always included and cannot be removed from the configuration. In some installations, this is sufficient authentication and is the only one activated.

## **OCSP**

Check this box to enable OCSP (Online Certificate Status Protocol) verification of CAC Cards. If enabled the OCSP server will be used to validate the current status of the CAC card PKI certificate.

**NOTE:** If OCSP is enabled, you must have a DNS server configured.

### **OCSP Server IP:**

This is the IP address of the OCSP server.

## **Root Certificate**

Check this box to enable Root Certificate verification of CAC Cards. If enabled, the certificate chain, including the Root CA Certificate will be used to validate the CAC card PKI certificate. The card is also checked to be certain the CAC certificate has a valid private key.

**NOTE:** If Root Certificate is enabled, all Issuer Certificates and Root CA Certificate chains for cards in use at this installation must be loaded into the CACStar. If not, Verify Failures will occur.

## **LDAP**

Check this to enable use of the Active Directory server for additional authentication

### **LDAP Server IP:**

IP address of the LDAP server.

### **LDAP Server Port:**

Port number of the LDAP server. The default is 389.

### **LDAP Query User Name:**

User Name for the LDAP service account login.

**LDAP Query Password:**

Password for the LDAP service account login.

**LDAP Search Base:**

Defines the location in the directory where a search will start.

Example: OU=Users, DC=Itek, DC=com

**LDAP Search String:**

The Search String is used by the LDAP server to find users. In conjunction with User ID options below, this field helps create the query to the LDAP server to find users by name. Any data can go in this field, but there are certain keys that will be expanded to create the query.

The keywords are:

%L – expands to become the user's last name

%F – expands to become the user's first name

%M – expands to become the user's middle name

%E – expands to the user's email address

%e – expands to the user's EDI-PI

%I – expands to the user's PIC-Identification

%s - expands to the user's SAN Principal name

**LDAP User ID options:**

Choices are cn, upn, mail, or name to be used for finding and identifying users.

**Disable LDAP Referrals:**

If this box is checked, the Referrals sent by LDAP Servers will **NOT** be followed.

**Kerberos**

If LDAP is enabled, you may choose to use Kerberos authentication for the LDAP server. If enabled, Kerberos will be used for: validating the cardholder, authentication to the LDAP server if needed, authentication to the SMTP server if so configured, and authentication to the SMB server if so configured.

**KDC Server:**

IP address or name of the Kerberos server

**KDC Server Port:**

Port number of the Kerberos server. The default is 88.

**KDC Realm:**

Kerberos Realm

**KDC Principal:**

User Name. This can be either the CN or the EDI-PI, or San Principal.

**PKINIT Win2K**

The setting affects the “Public Key Cryptography for Initial Authentication” in Kerberos. Check this box if you are using a Windows 2000 KDC Server and/or need to use the older Kerberos PKINIT command/reply set.

**Disable Reverse DNS Lookups:**

Check this box to disable Reverse DNS Lookups by Kerberos (and LDAP). This is only necessary if there is a problem using Reverse DNS Lookups. If this box is checked, host names must be used for “KDC Server” and “LDAP Server” input fields.

**MFD LDAP Kerberos Proxy**

If enabled and Kerberos is enabled, LDAP searches from the MFD will be modified to use Kerberos Authentication. The LDAP Server and Port settings must be correct.

**MFD SMB Kerberos Proxy**

If enabled and Kerberos is enabled, network scan (SMB) operations from the MFD will be modified to use Kerberos authentication.

## **Default SMB Server Address**

The IP address or server name for the default SMB server. This address will be used if the SMB server address cannot be obtained from the printer.

## **Default SMB Service Name**

The Service Name for the default SMB server, e.g. myshare\$. This name will be used as the principal for Kerberos authentication if the Service Name cannot be obtained from the printer.

## **Default SMB User Name**

The User name for the default SMB server. This is only needed if “MFD SMB Kerberos Proxy” is NOT checked - AND the “SMB Folder Name” IS configured.

## **Default SMB Password**

The Password for the default SMB server. This is only needed if “MFD SMB Kerberos Proxy” is NOT checked - AND the “SMB Folder Name” is configured.

## **SMB Folder Name**

If a Folder Name is configured, any folder name that is used by the printer will be replaced with this Folder Name. Keywords can be used in this definition so the folder name is “customized” based on the validated user.

These keywords are:

%L - expands to the user’s last name

%F - expands to the user’s first name

%M - expands to the user’s middle name

%E - expands to the user’s Email

%e - expands to the user’s EDI-PI

%I - expands to the user’s PIC-Identification

%u - expands to LDAP Attribute value

## SMB Folder LDAP Attribute

If a Folder Name is configured using %u, the LDAP Attribute defined here will be used to retrieve the path value for the %u field. Care should be taken when using “\” characters before or after the %u - based on whether the LDAP Attribute value includes “\” character(s) at the beginning or end.

## SSL CA Certificate Checking

If enabled, the host SSL certificate will be verified against the CA certificate. Therefore, the applicable CA certificate must be loaded into the CACStar.

## User Logging

### Dell™ CAC Enabled MFD

The screenshot shows a web interface for configuring user logging. At the top, there are four tabs: Connectivity, Security, Administrator, and Status. Below these, there are five sub-tabs: MFD Function Enabling, Email Setup, Authentication Method, User Logging, and Upload a Certificate. The 'User Logging' sub-tab is selected. The main content area contains the text: 'Allow a User Log File to be Created, Deleted or Uploaded.' Below this, there is a label 'Enable User Logging:' followed by a checked checkbox and a question mark icon. Underneath are four buttons: 'Update', 'View User Log File', 'Delete User Log File', and 'Refresh'.

User Logging provides a means to create, view or delete a user log file to track user activity. If this is enabled, it will log the date, user name, and other information. The log can be downloaded in a csv file format for viewing.



# Upload Certificate

## Dell™ CAC Enabled MFD

The screenshot shows a web interface with a top navigation bar containing tabs for 'Connectivity', 'Security', 'Administrator', and 'Status'. Below this is a sub-navigation bar with tabs for 'MFD Function Enabling', 'Email Setup', 'Authentication Method', 'User Logging', and 'Upload a Certificate'. The 'Upload a Certificate' tab is active. The main content area contains the following text and controls:

Upload a new Certificate File.  
Browse to the selected file and click Upload Certificate

Choose a Certificate file to upload:  
Choose File | No file chosen ?

Upload Certificate

Create Certificates Summary *This make take several seconds to complete*

View Certificates Summary

Delete Certificates

Use this page to load Issuer and Root Certificate Authority Certificates into CACStar.

PKCS7, X509, PEM and DER formats are supported.

Use the Browse button to select the Certificate file on your PC; then click the Upload Certificate button.

If your certificates are in a .txt file format, please send them to us, and we will convert them to a supported format. If desired, we can preload them into new units.

The Create Certificates Summary will create a text file listing all certificates stored in the CACStar. This is a text file that can be viewed or downloaded by selecting the View Certificates Summary button.

### Delete Certificates

Click this button to get a new page showing all installed certificates. You can check the “Delete” box for certificates to be deleted. Then click on “Delete Certificates” at the bottom of the page.

# Administrator

## Dell™ CAC Enabled MFD

Connectivity Security Administrator Status

Change Password Administrator Access Firmware Update Technical Support Setup Test Date Time Hold Print Files

Enter the new password.

Admin Password:  ?

Change Password

## Change Password

Use this feature to change the password for the administrator. When the Change Password button is clicked, the next internal web page access will require this new password.

## Administrator Access

### Dell™ CAC Enabled MFD

Connectivity Security Administrator Status

Change Password Administrator Access Firmware Update Technical Support Setup Test Date Time Hold Print Files

If desired, two LAN Side Administrator IP addresses may be defined for additional security when accessing CACStar configurations. The port is 8443 when using secure https, or it is 8080 when using non-secure http.

Allow All IPs:  ?

Administrator #1 IP Address:  ?

Administrator #2 IP Address:  ?

MFD IP Address Reference:  ?

MFD Subnet Mask Reference:  ?

Allow Telnet Access (Port 23):  ?

Use Non-Secure HTTP (Port 8080):  ?

Disable Front Panel Configuration  ?

Update

Refresh

These settings allow the admin to provide additional security by limiting CACStar admin access to specified IP addresses. If the Allow all IPs box is checked, an admin can access the CACStar configuration items from

a PC at any IP address if he knows the ID and password. If it is not checked, the admin must access the CACStar configuration pages from the IP addresses specified for Administrator #1 or #2. These addresses must be on the same subnet as the CACStar.

### Allow Telnet

If this is enabled CACStar will allow a Telnet session to occur. The Telnet session will happen over Port 23. Telnet use with CACStar is intended for diagnostics by the developers.

### Allow Non-Secure Port 8080

If this is enabled, CACStar will use Port 8080 and HTTP for HTML. Otherwise, Port 8443 and HTTPS will be used for HTML. Changing this setting requires a reboot of CACStar.

### Disable Front Panel Configuration

If this is checked, CACStar will disable the Front Panel keyboard from changing the IP address, subnet mask, and gateway. Viewing of these settings on the front panel LCD will still be allowed.

## Firmware Update

### Dell™ CAC Enabled MFD

Connectivity | Security | Administrator | Status

Change Password | Administrator Access | Firmware Update | Technical Support | Setup Test | Date Time | Hold Print Files

Update the Firmware or the Configuration settings in the CACStar.  
Browse to the selected update file and click Upload File

Choose a Firmware or Configuration file to upload:  
 No file chosen  2

Create and Export the Current Configuration.  
  2

Create and Export the currently loaded Certificates.  
  2

The new Firmware will be installed and executed at the next Boot.

Firmware Version: 6.1  
Boot Version: 1.7

Firmware is stored in flash memory and can be updated as necessary for addition of new features. The CACStar.cfg file may also be uploaded. It

is a text file that contains the CACStar configuration items.

For more details about how to update the firmware, please see the separate document “Firmware Update Procedure”.

## Create and Export Current Configuration

Create Config File will create a configuration file containing all current settings except LAN IP Address, LAN Mask, and LAN Gateway. Thus, the Config file can be used to configure other CACStars. The passwords are encrypted so they may not be edited. The first line of the file must not be edited. The MAC address and Serial Number are displayed for information purposes only and will not be used as a configuration item.

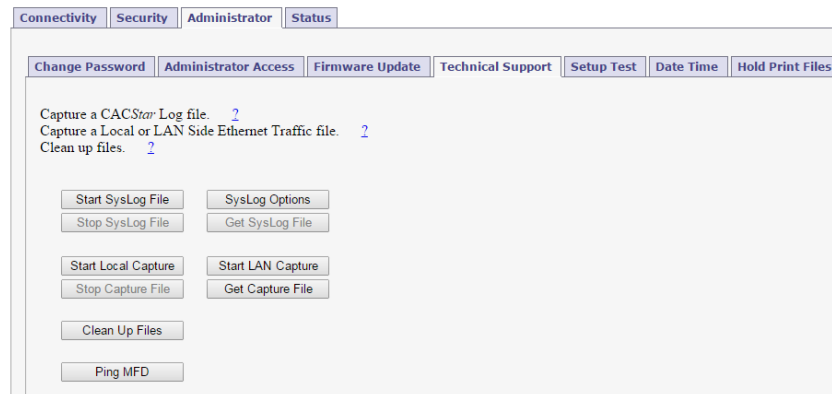
Export Config File will allow this file to be saved outside CACStar. This file should be saved as a text file. It may be edited with a text editor. It may also be uploaded to CACStar at a later date.

## Create and Export Current Certificates

Create Certificates File will create a file called “CACStarCerts.tar.gz” which will contain all currently loaded certificates. Export Certificates File will allow this file to be saved outside CACStar. This file may be loaded to any CACStar.

# Technical Support

## Dell™ CAC Enabled MFD



For help obtaining the correct firmware or documentation, contact the Dell ProSupport Help Desk by calling 1-866-516-3115, or by sending email to [Imaging\\_Solutions\\_Support\\_CAC@dell.com](mailto:Imaging_Solutions_Support_CAC@dell.com)

This page is used to obtain Log Files and Capture Files to help diagnose network and configuration concerns. Use of these features is normally in conjunction with technical support from your vendor.

### **Create SysLog File**

A log file can be created for use by CACStar Engineering to help resolve problems that may occur.

### **Ethernet Capture**

An Ethernet Capture file can be created containing information from either the Local port or the LAN port for use by CACStar Engineering in customer support activities.

### **Clean Up Files**

Removes all temporary files from CACStar. This includes log files, capture files, and upgrade files.

### **Ping MFD**

CACStar pings the MFD over its internal local link to verify communication between CACStar and the MFD.

# Setup Test

## Dell™ CAC Enabled MFD

Connectivity Security Administrator **Status**

Change Password Administrator Access Firmware Update Technical Support **Setup Test** Date Time Hold Print Files

Test the addresses entered into the CACStar for communications.  
This Test will generate a report of the success of the various addresses.

Note: This test may take a few moments to run

## Date Time

This is used to set the system date and time in CACStar if necessary. The time zone should be set to your local time zone.

## Dell™ CAC Enabled MFD

Connectivity Security Administrator **Status**

Change Password Administrator Access Firmware Update Technical Support **Setup Test** Date Time Hold Print Files

Change the Date and Time in the System Clock.  
The System Clock is used for Date and Time at Boot until a valid NTP server is found.

Current Date and Time: Mon Mar 23 13:42:46 EDT 2015

Year: 2015 2  
Month: 03  
Day: 23  
Hour: 13  
Minute: 42  
Second: 45

Local Time Zone: Eastern 2

# Hold Print Files

## Dell™ CAC Enabled MFD

Connectivity | Security | Administrator | Status

Change Password | Administrator Access | Firmware Update | Technical Support | Setup Test | Date Time | Hold Print Files

Files sent to the printer can be held until released with a CAC card and it's authentication. If both **CAC Enable Printing** and **CAC Hold Print** are selected and a Server is not, the print files will be encrypted and held inside the CACStar. Usernames are used when the information on the CAC card does not match the information that is contained in the print job file.

Expiration in Number of Days.

List all existing Hold Print Files.

Delete all existing Hold Print Files.

List all existing Hold Print Usernames.

Add a new Hold Print Username.

Export Hold Print Usernames.

Name Matching Format:  %S

Total Storage: 3773 MB  
Remaining Storage: 3726 MB

Hold Print files will be stored encrypted in CACStar and can be printed with CAC authentication at the printer.

Hold Print files expire after the set number of days. When the expiration date is reached, the file will be deleted without being printed.

Remaining storage and total storage are displayed so the user will know if held print files are reaching the maximum storage capacity. When storage is nearly full, a warning message will be displayed on the CAC reader LCD - MEMORY NEAR FULL.

### Hold Print Expiration

This sets the default expiration in number of days for all received Hold Print files. When the expiration date is reached for a Hold Print file, it will be deleted without printing.

### Hold File Name Matching Format

This field defines the format that will be used to associate the user-name in the Hold Print files with Card-Validated users. Any data can go into this field and keywords will be expanded.

These keywords are:

%F - the user's first name

%f - the first character of the user's first name

%M - the user's middle name

%m - the first character of the user's middle name

%L - the user's last name

%l - the first character of the user's last name

%e - the user's EDI-PI

%I - the user's PIC-Identification

%S - the user's SAM Account Name (from LDAP)

A number may be used between the '%' and the keyword to specify a maximum number of characters.

For example: '%5L' would indicate a maximum of 5 characters of the user's last name.

## Add Hold Print Usernames

If jobs must have user names from the host system that cannot be identified using the Name Matching information from the CAC card, a host Username can be entered into CACStar using the "Add a new Hold Print Username" command. The Username can be associated with identifying data from the CAC card as follows:

First:	<input type="text"/>
Last:	<input type="text"/>
EDI-PI:	<input type="text"/>
San Principal:	<input type="text"/>
Username:	<input type="text"/>
<input type="button" value="Submit Username"/>	

## Export Hold Print Usernames

If you want to copy the usernames from one CACStar to another, you can Export the usernames. You will get a \*\*\*.db file which you can then send to another CACStar to load them into the other CACStar.



# Status

---

The Status pages offer three views of information about the current operations of CACStar. Number of successful card validations, number of unsuccessful card validations, network operations, date/time, and firmware version are all displayed.

## Card Reader

### Dell™ CAC Enabled MFD

Connectivity	Security	Administrator	Status
--------------	----------	---------------	--------

Card Reader	Network	Other
-------------	---------	-------

Card Inserted:	Yes
Card Validated:	No
Card User Name:	
Total Validate OK:	268
Total Validate Fails:	30
<input type="button" value="Reset Counters"/>	
<input type="button" value="Refresh"/>	

## Network

# Dell™ CAC Enabled MFD

Connectivity

Security

Administrator

Status

Card Reader

Network

Other

### Lan Side

MAC Address:	00:50:27:06:93:B6
MFD IP Address:	10.5.1.39
MFD Subnet Mask:	255.255.0.0
NTP Server:	10.5.1.23
Gateway:	10.5.2.1
DNS Server:	10.5.1.23
Domain Name:	us.mil

### Local Side

Local MAC Address:	00:50:27:06:93:B7
Local CAC <i>Star</i> IP Address:	172.19.10.1
Local MFD IP Address:	172.19.10.2
Local MFD Subnet Mask:	255.255.255.0
Local MFD Gateway:	172.19.10.1
Local MFD Model:	Dell C5765dn Color MFP

## Other

# Dell™ CAC Enabled MFD

Connectivity

Security

Administrator

Status

Card Reader

Network

Other

Date/Time: Mon Mar 23 13:42:46 EDT 2015

Firmware Version: 6.1

Boot Version: 1.7

Serial Number:

Product Revision: A15

Refresh

Copyright 2014 Digital Imaging Technology

CAC*Star* is a registered trademark of Digital Imaging Technology

Patent Pending

Dell and the Dell logo are trademarks of Dell Inc.

# Controlling Access to Fax and Copy

The MFD has configuration settings to indicate whether authentication is required to access fax and copy. The CACStar user interface reads this configuration to determine whether to make fax and copy functions available from the login screen.

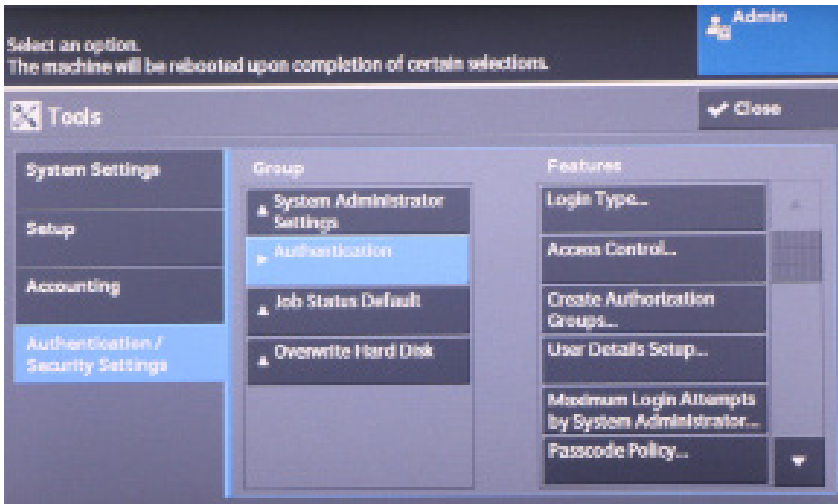
To configure access:

Step 1 Login to the MFD as administrator via the operator panel.

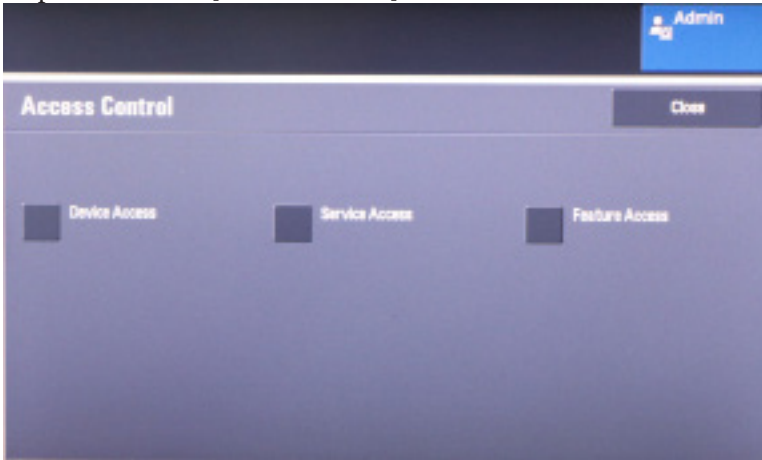
Step 2 Press the Home key.

Step 3 Press the [Tools] button.

Step 4 Navigate to Authentication/Security Settings->Authentication->Access Control...



Step 5 Press the [Service Access] button.



Step 6 Choose Fax or Copy and press the [Change Settings] button.



Step 7 Choose [Unlocked] for no authentication required; or [Locked(Show Icon)] to require authentication.

Step 8 Press the [Save] button.

Step 9 Press [Close] two times.

Step 10 Press the [Reboot Now] button when prompted.

# Appendix A

## Setup Information Checklist

- Should the MFD use DHCP to acquire an IP Address (Yes or No) ?  
If No, specify the following for the MFD:
  - IP Address
  - Subnet Mask
  - Gateway
- What is the IP address for an available NTP (Network Time Protocol) Server (or N/A if none available)?
- What are the IP Addresses for the primary and secondary DNS (Domain Name System) Servers?

### Functions

- Do you wish to use CAC/PIV control for the Scan-to-Email function (Yes or No)?
  - Is Kerberos Authentication required for accessing the Email Server and sending Email (Yes or No)?
- Do you wish to use CAC/PIV control for printing (Yes or No)?
  - If Yes, multiple secure printing modes are available.
- Do you wish to use CAC/PIV control for other network protocols (Yes or No)?
  - Other protocols include SMB, SNMP, LDAP.

### Email

If you are using CAC/PIV controlled Scan-to-Email or Kerberos authentication, please complete this section - otherwise go to the next section for LDAP.

- What is the Server Name or IP Address for the SMTP (Simple Mail Transfer Protocol) Server?
- Do you wish to retrieve the “From” address for all emails from the CAC/PIV card, or from an LDAP lookup of the CAC/PIV user (Card or LDAP) ?
-

- Do you wish to force all emails to go to the CAC/PIV Card's email address (Yes or No)?

If No, selection can be made from the Front Panel by typing in the address, or using the Network Address Book (LDAP) feature.

- Should emails be encrypted (Yes or No or Prompt)?

If Yes or Prompt, what encryption should be used (3DES or AES-256)?

## **LDAP**

- Do you wish to use the Network Address Book (LDAP) feature to lookup email addresses (Yes or No)?

If Yes, please complete this section - otherwise go to the Kerberos Section.

- What is the Server Name or IP Address for the LDAP (Lightweight Directory ) Server?

- Is Kerberos required for accessing the LDAP Server (Yes or No)?

This is usually Yes.

- What is the proper Search Base (ex: "dc=somename,dc=gov")?

## **Kerberos**

- What is the Server Name or IP Address for the Kerberos Server (if more than 1 available, please list)?

- What is the Realm Name (ex: "somename.gov")?

- Is SSL required for Kerberos Sessions (Yes or No)?