

Dell™ S2815dn CACStar™ Smart Card Reader Installation and Configuration Guide

Document protection for CAC/PIV enabled
Multifunction Devices



Table of Contents

Introduction.....	5
Initial Setup.....	6
Accessing the MFD/Printer Web Site	9
Admin Login.....	9
Connectivity.....	10
LAN Side Configuration.....	10
Local Side Configuration.....	12
Security.....	13
MFD Function Enabling	13
Email Setup.....	15
Authentication Method.....	17
User Logging	24
Upload Certificate.....	24
Administrator	26
Change Password	26
Administrator Access.....	26
Firmware Update.....	28
Technical Support.....	30
Setup Test.....	31
Date Time	32
Hold Print Files.....	33
Hold File Name Matching Format	34
Status.....	36
Card Reader	36
Network.....	37
Other.....	38

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.

This manual will guide you through installing the hardware, installing the software to convert the Dell S2815dn to be CACStar enabled, and configuration of the customer desired authentication control options.

Initial Setup

1. The printer must be configured to use DHCP which is the default configuration.
2. Turn the power on. After initialization is complete, the Card Reader display will say **Waiting For Card**. This will take about 1 ½ minutes.

Manual LAN IP Address Configuration:

3. Using the card reader keypad, enter the IP address to be used to access both the CACStar and the MFD/printer. See Figure 1 below.
 - a. Press the F key; the display will say **Information**.
 - b. Press the F key again; the display will say **Configuration**.
 - c. Press the Enter key; the display will show **DHCP** and the current setting. The default is OFF.
 - d. Press the F key again; the display will show **LAN IP Address** and the current setting.
 - e. Press the Enter key; the display will show **Enter New Value**.
 - f. Enter the desired IP Address and press Enter. Use the IP address you want to use for the host connection to the MFD/printer.
 - i. Example: 192.168.1.23 Enter.
 - g. The display will say **Setting Value** for about 5 seconds.
 - h. Press the F key; the display will say **LAN Subnet Mask** and the current setting.
 - i. Press the Enter key; the display will show **Enter New Value**.
 - j. Enter the desired subnet mask like you did the IP Address.

- k. If you wish to enter the gateway, press the F key again and enter it as you did the IP Address.
- l. Press the EXit key twice to return to **Waiting for Card**.
- m. To confirm this operation was successful, you can ping the CACStar at its new IP address from your PC.

Automatic (DHCP) LAN IP Address Configuration:

4. Using the card reader keypad, enable DHCP using the following steps. See Figure 1 below.
 - a. Press the F key; the display will say **Information**.
 - b. Press the F key again; the display will say **Configuration**.
 - c. Press the Enter key; the display will show **DHCP** and the current setting. The default is OFF.
 - d. Press the Enter key; the display will show **F = Change X = Exit**.
 - e. Press the F key to change the setting from OFF to ON.
 - f. Press the Enter key. After about 3 seconds, CACStar will reboot.
 - g. After reboot and initialization, press the F key; the display will say **Information**.
 - h. Press the F key again; the display will say **Configuration**.
 - i. Press the Enter key; the display will show **DHCP** and the current setting.
 - j. Press the F key again; the display will show **LAN IP Address** and the current setting.

- k. To confirm this operation was successful, you can ping the CACStar at its new IP address from your PC.

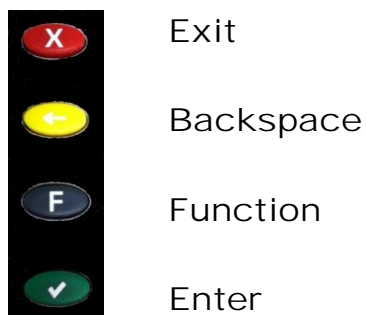


Figure 1 – Keypad Function Buttons

Accessing the MFD/Printer Web Site

If you wish to access the MFD/printer web site, go to the same URL but do not use port 8443. For example: <http://192.168.1.23> or <https://192.168.1.23>

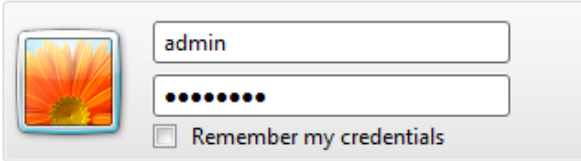
Admin Login

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 “password”.

A screenshot of a web login form. On the left is a square icon with a sunburst pattern. To its right are two input fields: the top one contains the text 'admin', and the bottom one contains ten black dots representing a password. Below these fields is a checkbox with the text 'Remember my credentials'.

After initial login, you can change the password to one of your choice by going to the Administrator tab.

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

Connectivity

LAN Side 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: ?

Update

Refresh

Step 1 – MFD IP Address

This is the IP address that is used for access to these administrator web pages. It is also used for host computer connection to the MFD/printer. This IP address was already set in the initial setup process using the card reader keypad.

If you wish to change this address, it can be done using this screen or from the card reader keypad.

Note: When you press the **Update** button, the CACStar will switch to the new IP address which will cause your browser to be disconnected from the CACStar. 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

The screenshot shows a web interface for configuring a Dell CAC Enabled MFD. At the top, there are four tabs: "Connectivity", "Security", "Administrator", and "Status". The "Administrator" tab is selected. Below this, there are two sub-tabs: "LAN Side Configuration" and "Local Side Configuration". The "Local Side Configuration" tab is active. The page contains the following text and form fields:

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 its configuration method.

Local CACStar IP Address: ?

Local MFD IP Address: ?

Local MFD Subnet Mask: ?

Local MFD Default Gateway: ?

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

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

Make sure these values were entered into the MFD using the MFD/printer operator panel.

Security

MFD Function Enabling

Dell™ CAC Enabled MFD

Connectivity | Security | Administrator | Status

MFD Function Enabling | Email Setup | Authentication Method | SMB Address Book | User Logging | Upload a Certificate | Device Certificate Management

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 type="checkbox"/>	? See Configuration Items in Email Setup
CAC Enable FTP:	<input type="checkbox"/>	? 2
CAC Enable Scan to Folder:	<input type="checkbox"/>	? 2
CAC Enable Printing:	<input type="checkbox"/>	? 2
CAC Enable Copy:	<input checked="" type="checkbox"/>	? 2
CAC Enable SNMP:	<input type="checkbox"/>	? 2
CAC Enable LDAP:	<input type="checkbox"/>	? 2
CAC SNMP Proxy:	<input type="checkbox"/>	? 2
CAC Hold Print:	<input type="checkbox"/>	? 2
CAC Print Server:	<input type="text"/>	? 2
CAC Server Print Only:	<input type="checkbox"/>	? 2

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

Connectivity Security Administrator Status

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

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.

SMTP Address or Server Name:	<input type="text" value="itekctl.us.mil"/>	?
SMTP Port Number:	<input type="text" value="587"/>	? <i>Default: 25</i>
User Email Address From:	<input type="text" value="CAC"/>	?
Force Email to Self:	<input type="checkbox"/>	?
Encrypt Email:	<input type="text" value="Prompt"/>	?
Email Encryption Type:	<input type="text" value="AES-256"/>	?
Sign Email:	<input type="text" value="Prompt"/>	?
LDAP Primary Certificate Attribute:	<input type="text" value="userSMIMECertificate"/>	?
LDAP Secondary Certificate Attribute:	<input type="text" value="userCertificate"/>	?
Kerberos Email Authentication:	<input checked="" type="checkbox"/>	?

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 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.

Kerberos Email Authentication

Check this box if you want to use Kerberos for Email Login Authentication.

If this box is checked, the "Kerberos" section of "Authentication Method" web page must be completed properly.

Authentication Method

Dell™ CAC Enabled MFD

Connectivity | Security | Administrator | Status

MFD Function Enabling | Email Setup | Authentication Method | SMB Address Book | User Logging | Upload a Certificate | Device Certificate Management

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:	60	?
Basic:	<input checked="" type="checkbox"/>	?
OCSP:	<input type="checkbox"/>	?
OCSP Server IP:		?
Root Certificate:	<input checked="" type="checkbox"/>	?
LDAP:	<input type="checkbox"/>	?
LDAP Server:		?
LDAP Server Port:	389	Default: 389
LDAP Query User Name:		?
LDAP Query Password:		?
LDAP Search Base:		?
LDAP Search String:	%s	Name: %F %M %L Email %E EDI-PI %e PIC-Idem %I SAN Principal %u
LDAP User ID Option:	upn	?
Disable LDAP Referrals:	<input checked="" type="checkbox"/>	?
Kerberos:	<input type="checkbox"/>	?
KDC Server:		?
KDC Server (alt):		?
KDC Server (alt):		?
KDC Server (alt):		?
KDC Server Port:	88	Default: 88
KDC Realm:		?
KDC Realm Domains:		?
KDC Principal:	SAN Principal	?
PKINIT Win2k:	<input checked="" type="checkbox"/>	?
Disable Reverse DNS Lookups:	<input type="checkbox"/>	?
MFD LDAP Kerberos Proxy:	<input type="checkbox"/>	?
MFD SMB Kerberos Proxy:	<input type="checkbox"/>	?
Default SMB Server Address:		?
Default SMB Service Name:		?
Default SMB Username:		?
Default SMB Password:		?
SMB Folder Name:		Name: %F %M %L Email %E EDI-PI %e PIC-Idem %I LDAP %u
SMB Folder LDAP Attribute:		?
SSL:	<input type="checkbox"/>	?
SSL CA Certificate Checking:	<input type="checkbox"/>	?

Additional Realms Configuration

CAC Validated Timeout

This setting is the number of minutes of inactivity before a CAC Validated session will be terminated.

If this setting is 0, the timeout is disabled.

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.

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 CAC*Star*. 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. Multiple entries are allowed.

KDC Server IP: IP address of the Kerberos server
KDC Server Port: Port number of the Kerberos server.

The default is 88.

KDC Realm: Kerberos Realm

KDC Realm Domains: This setting is used to map domains to the realm, and is usually only needed if multiple realms are defined. You can enter one or more host names or domain names prefixed by a period and separated by commas.

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 Username:

The Username 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.

SMB Address Book

Dell™ CAC Enabled MFD

Connectivity Security Administrator Status

MFD Function Enabling Email Setup Authentication Method SMB Address Book User Logging Upload a Certificate

SMB Address Book entries allow definition of multiple variable-based Server/Path destinations. Each destination name has the format "SMB-Book1" to "SMB-Book99" - this name should be used for the printer's "Server Address" configuration. The following sequences may be used to specify user-related data in the destination path:
%F : First name, %M : Middle Name, %L : Last name,
%E : Email Address, %e : EDI-PI, %I : PIC-Identification,
%u<ldap-attribute>% : LDAP attribute value

Examples:
\\myserver\myshare\%e < or > %uhomeDirectory%

NOTE: all entries MUST resolve to a fully-qualified Server and path (Ex: \\myserver\myshare\myfolder).

SMB-Book1:

SMB-Book2:

SMB-Book3:

SMB-Book4:

SMB-Book5:

SMB-Book6:

SMB-Book7:

SMB Address Book entries allow definition of multiple variable-based Server/Path destinations.

Each destination name has the format "SMB-Book1" to "SMB-Book99" - this name should be used for the printer's "Server Address" configuration.

The following sequences may be used to specify user-related data in the destination path:

- %F : First name, %M : Middle Name, %L : Last name,
- %E : Email Address, %e : EDI-PI, %I : PIC-Identification,
- %u<ldap-attribute>% : LDAP attribute value

Examples:

\\myserver\myshare\%e < or > %uhomeDirectory%

NOTE: all entries MUST resolve to a fully-qualified Server and path (Ex: \\myserver\myshare\myfolder).

User Logging

Dell™ CAC Enabled MFD

Connectivity Security Administrator Status

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

Allow a User Log File to be Created, Deleted or Uploaded.

Enable User Logging: ?

Update

View User Log File

Delete User Log File

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

Connectivity Security Administrator Status

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

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.

Device Certificate Management

Dell™ CAC Enabled MFD



Generate and upload a Certificate Signing Request (CSR). Once the request is processed by a Trusted Certificate Authority, upload the signed certificate.

Administrator


Change Password


Dell™ CAC Enabled MFD


Connectivity Security **Administrator** Status

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

Enter all passwords and then click on "Change Password".
Note: the MFD Passwords are only needed if "CAC Enable Copy" or "CAC Enable Fax" options are enabled.

Admin Password:  [?](#)

MFD Web Admin Password:  [?](#)

MFD Panel Lock 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: [?](#)

SMB Disable NBSS: [?](#)

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.

SMB Disable NBSS

If this box is checked, CACStar will suppress NBSS traffic from the printer. This setting is only required when SMB/Kerberos Proxy is enabled and the local network does not allow NBSS traffic.

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 ?

Create and Export the Current Configuration.
 ?

Create and Export the currently loaded Certificates.
 ?

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

Firmware Version: 6.7
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.

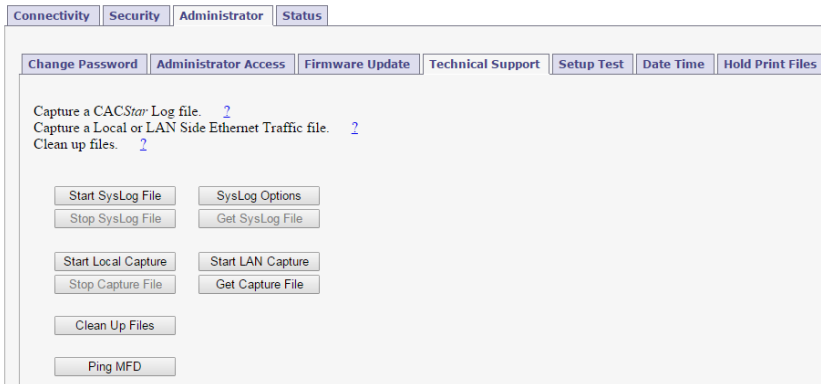
Create and Export Current Certificates

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

For help obtaining the correct firmware or documentation, contact Dell's ProSupport Help Desk by calling 1-866-516-3115, or by sending email to Imaging_Solutions_Support_CAC@dell.com

Dell™ CAC Enabled MFD



The screenshot shows a web interface with a top navigation bar containing tabs: Connectivity, Security, Administrator, and Status. Below this is a secondary navigation bar with tabs: Change Password, Administrator Access, Firmware Update, Technical Support (which is selected), Setup Test, Date Time, and Hold Print Files. The main content area displays three links: 'Capture a CACStar Log file.' with a question mark icon, 'Capture a Local or LAN Side Ethernet Traffic file.' with a question mark icon, and 'Clean up files.' with a question mark icon. Below these links are several buttons: 'Start SysLog File' and 'SysLog Options' in the first row; 'Stop SysLog File' and 'Get SysLog File' in the second row; 'Start Local Capture' and 'Start LAN Capture' in the third row; 'Stop Capture File' and 'Get Capture File' in the fourth row; 'Clean Up Files' in the fifth row; and 'Ping MFD' in the sixth row.

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.

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

Setup Check Test

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

Setup Test:
DNS Test:
Resolv.conf settings:
Resolv.conf size: 41
nameserver 10.5.1.23
nameserver 10.5.1.2

End of Resolv.conf settings.
Dhclient-script size: 6469
Configuration settings:
LDAP Server: [itekctl.us.mil], IP Address [10.5.1.23].
KDC Server: [itekctl.us.mil], IP Address [10.5.1.23].
Email Server: [itekctl.us.mil], IP Address [10.5.1.23].

NTP Test:
Mode 1 test:
Test Passed:
25 Mar 14:41:35 ntpdate[4233]: adjust time server 10.5.1.23 offset 0.002822 sec

Mode 2 test:
Test Passed:
25 Mar 14:41:43 ntpdate[4263]: adjust time server 10.5.1.23 offset 0.013250 sec

Kerberos Test:
Test Passed.
Setup Test Complete.

Date Time

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 Hardware Clock.
The Hardware Clock is used for Date and Time at Boot until a valid NTP server is found.

Current Date and Time: Tue Aug 5 15:05:19 EDT 2014

Year: 2014 [?](#)
Month: 08
Day: 05
Hour: 15
Minute: 05
Second: 19

Local Time Zone: Eastern [?](#)

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.

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:

Total Storage: 3716 MB
Remaining Storage: 3651 MB

Hold Print Files

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 username 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

The screenshot shows a web interface with a top navigation bar containing 'Connectivity', 'Security', 'Administrator', and 'Status'. The 'Status' tab is selected. Below this, there are three sub-tabs: 'Card Reader', 'Network', and 'Other'. The 'Card Reader' sub-tab is active and displays the following information:

Card Inserted:	No
Card Validated:	No
Card User Name:	
Total Validate OK:	552
Total Validate Fails:	197

At the bottom of the Card Reader section, there are two buttons: 'Reset Counters' and 'Refresh'.

Network

Dell™ CAC Enabled MFD

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

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

Lan Side	
MAC Address:	00:50:27:01:90:30
MFD IP Address:	10.5.9.10
MFD Subnet Mask:	255.255.0.0
NTP Server:	10.5.1.2
Gateway:	10.5.2.1
DNS Server:	10.5.1.23
DNS Server:	10.5.1.2
Local Side	
Local MAC Address:	00:50:27:01:90:31
Local CACStar 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 C3765dnf Color MFP

Other

Dell™ CAC Enabled MFD

Connectivity

Security

Administrator

Status

Card Reader

Network

Other

Date/Time: Thu Jan 1 01:46:31 GMT 1970

Firmware Version: 8.4

Boot Version: 1.9

Serial Number: US-014CV7-71970-123-0001

Product Revision: A27

Kbd-Disp Version: 01.04

Refresh

Copyright 2016 Digital Imaging Technology

CACStar is a registered trademark of Digital Imaging Technology

Patent Pending

Dell and the Dell logo are trademarks of Dell Inc.

