

1	Introduction	1
2	Getting Started.....	2
2.1	Connecting to the LAN and Acquiring an IP Address	2
2.2	Gathering Information	3
3	First Configuration Steps.....	5
3.1	Downloading the S3845cdn Setup File For CACStar	5
3.2	Setting the MFD and CACStar Administrator Password	6
3.2.1	Changing Password on the MFD	6
3.2.2	Changing Password on CACStar	10
3.3	Configuring the LDAP Search Base on the MFD	11
3.4	Configuring CACStar for Authentication	13
3.5	Loading Certificates for Root Chain Validation	15
4	Next Steps: Configuring Additional Apps	16
4.1	Configuring Access for Apps.....	17
4.2	Configuring Scan to Email	17
4.3	Scan to Network Folder.....	21
4.3.1	The CACStar “SMB Address Book”	22
5	Print Release	24
6	Replicating the Configuration to Other Machines	25
6.1	Saving the Printer Configuration	25
6.2	Loading the Printer Configuration Into Another Printer	27
6.3	Saving the CACStar Configuration	29
6.4	Loading the CACStar Configuration into Another Machine	30
7	troubleshooting	32
7.1	Error Messages.....	32
7.1.1	Problems Occurring After Power-on.....	32
7.1.2	Problems Occurring During Authentication.....	32
8	Gathering Error Logs	35

Thank you for choosing a Dell Color Smart Multifunction Printer S3845cdn with the CACStar CAC security option. The CACStar security option enables authenticated access to your printer via CAC or PIV smart cards. CACStar and our printer together offer flexible solution that will support your needs.

This guide is designed to assist you in setting up your S3845cdn for use in your environment, compliant with MFD STIG Version 2 Release 10 (28 July 2017).

2 GETTING STARTED

The guide assumes no previous experience with CACStar or the S3845cdn MFD. It also assumes that the CACStar security option has already been installed on the S3845cdn.

If you have received your CACStar option separately from the printer, it must be physically installed. Refer to the CACStar Option Installation Guide for the installation procedure before proceeding further

With the CACStar option installed to the printer, we can proceed with installation. This section covers the following topics:

- Connecting to the LAN
- Gathering information required to configure the authentication

2.1 CONNECTING TO THE LAN AND ACQUIRING AN IP ADDRESS

Connecting your device to the LAN usually requires registration of the device's Ethernet (MAC) address with the network switch to which the device will be connected. For this purpose, the MAC address of the CACStar option must be used. You can find this address in two ways:

- The label affixed to the CACStar option enclosure (figure 1 below)
- Printer on the CACStar summary printout

Figure 1: Location of MAC Address Label



By default, the CACStar option acquires its IP address via DHCP, so after the MAC address is registered with the switch, you can connect the LAN cable to the port on the CACStar option, and turn the printer on.

As soon as CACStar acquires an IP address, a CACStar summary page will automatically print (later, during configuration, this automatic printout can be disabled.) On this summary page, the acquired IP address will be shown on the third line of the summary page, under “LAN MFD IP Address”. **This is the address that will always be used to connect to the MFD and CACStar administration web pages.**

2.2 GATHERING INFORMATION

The basic information that is required to successfully authenticate includes:

- Domain controller name
- Domain Name
- Kerberos Realm
- IP Address for NTP server (usually the domain controller’s IP address)
- Search Base for LDAP queries
- SMTP server address

Most of this information can be acquired using a command, included in Windows, called GPRresult. To use the command, open a command prompt or PowerShell. Change the current directory to a folder for which you have “write” permissions. Then enter the following command:

```
gprresult /r > gprresult.txt
```

open the file in notepad. The GPRResult command generates quite a bit of information. However, the information that is needed can be found by searching for the string “USER SETTINGS” (without quotes). It should look something like this:

USER SETTINGS

```
-----
CN=John Q. Public,OU=Users,OU=testlab,DC=mydomain,DC=com
Last time Group Policy was applied: 12/06/2017 at 2:54:49 PM
Group Policy was applied from:      dc001.mydomain.com
```

In the first line, copy all of the text after the first field, as in the highlighted portion in the example above, beginning with “OU=Users”, and extending to the end of line. **This is your “search base” value.**

In the line starting with “Group Policy was applied from”, the entire value after the colon is the FQDN of the domain controller (“dc001.mydomain.com” in this example). The domain is the portion of the FQDN following the first period (“mydomain.com” in this example.). The Kerberos realm is the uppercased version of the domain name.

From your command prompt, ping the domain controller to get its IP address. For this example, you would use the command:

```
ping dc001.mydomain.com
```

For purposes of this example, let’s say that the IP address shown by the ping command is 192.168.100.1. We will use this for the NTP server address.

At this point we have all the information we need except for the SMTP server address. To get this information, you can either get the value from the configuration of another digital sender device on your network. If another device is not available, then you will need to ask the System Administrator for the appropriate SMTP server address. **You should also provide the IP and/or MAC address of the printer to the SA, in case it needs to be registered with the SMTP server for authentication.** *For purposes of our example, let’s say that the SMTP server IP address is 192.168.100.2.*

To recap, for this example, we have gathered the following information, which can be used to configure your device on the network:

Domain controller name	dc001.mydomain.com
Domain name	mydomain.com
Kerberos realm	MYDOMAIN.COM
NTP Server IP address	192.168.100.1
Search Base	OU=Users,OU=testlab,DC=mydomain,DC=com
SMTP server address	192.168.100.2

3 FIRST CONFIGURATION STEPS

Configuration of your device is accomplished primarily via the CACStar administrative web site (<https://<device-ip-address>:8443>)

Note: When the CACStar option is installed on the printer, the CACStar Setup file used during the installation takes care of most of the STIG compliance requirements. The printer settings that are included in the initial setup file are listed in Appendix A. Appendix A also includes information on how to manually set the various settings.

3.1 DOWNLOADING THE S3845CDN SETUP FILE FOR CACSTAR

On the Dell support website (<http://support.dell.com>), you can navigate to the support page for the S3845cdn printer, and select “Drivers and Downloads”. Select the file called “Dell Color MFP S3845cdn CACStar Setup Files” to download it.

The screenshot shows the Dell Support website interface. The main heading is "Support for Dell Color Smart Multifunction Printer S3845cdn". On the left, there is a sidebar with navigation options: "Support topics & articles", "Drivers & downloads", "Manuals & documents", "Warranty", "System configuration", and "Parts & accessories". The "Drivers & downloads" section is active, displaying a search bar and filters for "Keyword", "Operating system" (set to "Windows 7, 64-bit"), "Category" (set to "All"), and "Format" (set to "All"). Below the filters is a table of drivers:

Name	Category	Last Updated	Download
Dell Color Smart Multifunction Printer S3845cdn Software Suite and Driver	Application	10 Nov 2017	Download
Dell Color MFP S3845cdn CACStar Setup Files	Application	09 Nov 2017	Download
Dell Color Smart Multifunction Printer S3845cdn PCL Driver	Drivers for OS Deployment	10 Nov 2017	Download

The downloaded file needs to be unzipped to a folder of your choosing. One of the unpacked files is called “CACStar_S3845cdn_Install.zip”. This is a file can be uploaded directly to the S3845 under the “Cloning” section of the printer’s administrative website.

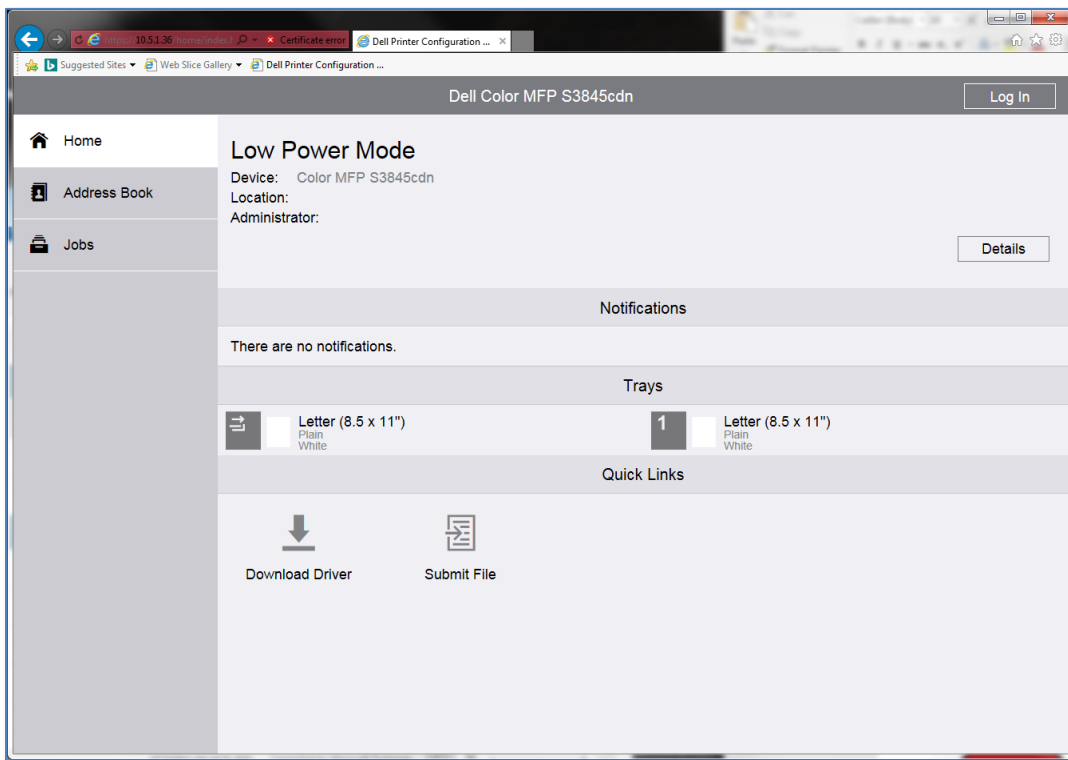
3.2 SETTING THE MFD AND CACSTAR ADMINISTRATOR PASSWORD

By default, the administrator password for the printer and CACStar web sites is “admin”. This should be changed as soon as possible.

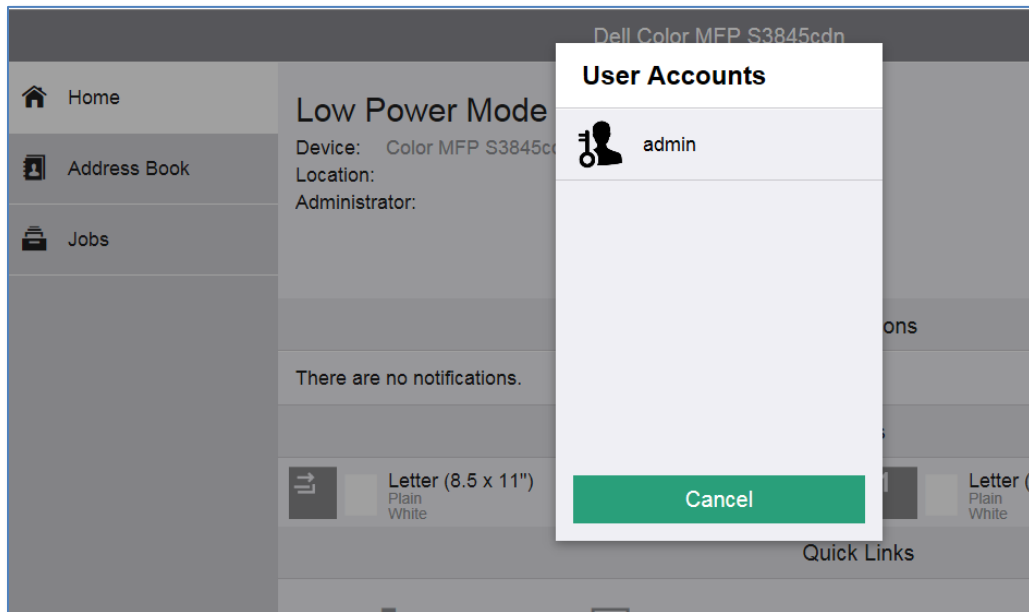
3.2.1 CHANGING PASSWORD ON THE MFD

To change the password in the MFD:

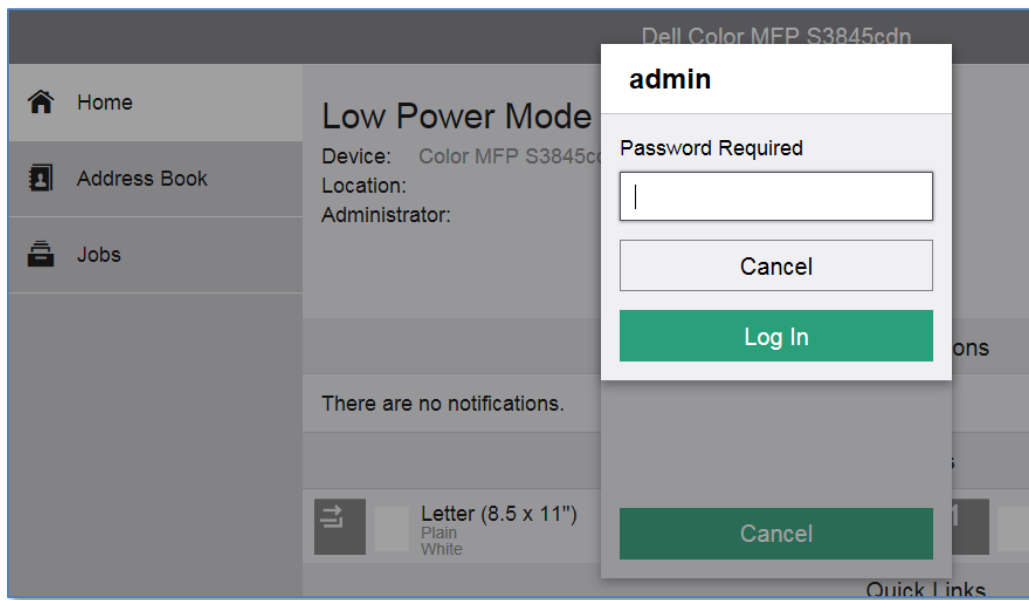
1. Open a web browser to the printer’s website:



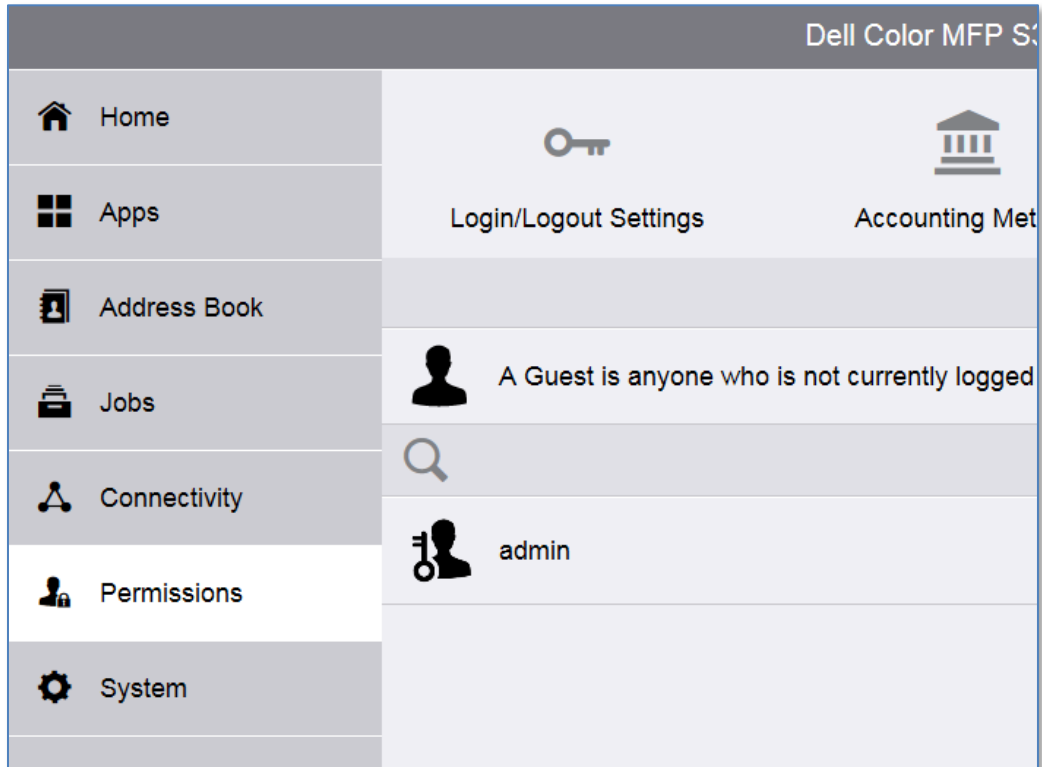
2. Click the [Log In] button, then select "admin".



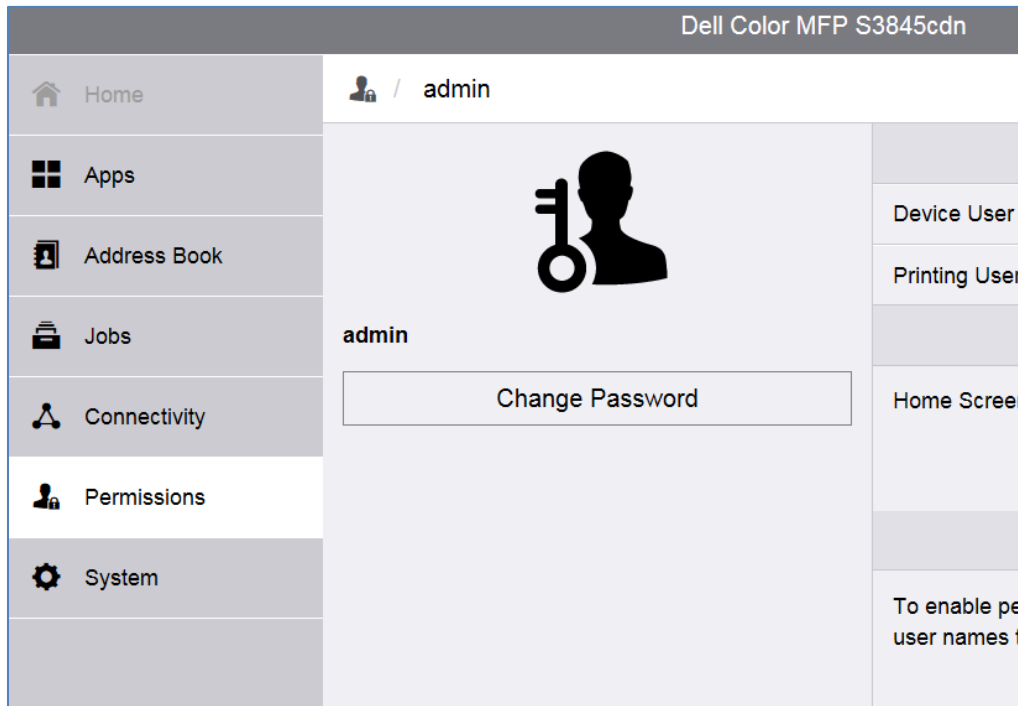
3. Enter the current password (default="admin")



- Click the [Permissions] link on the left-hand side of the page. In the “User Accounts” section, click the entry for “Admin”.



5. Click the [Change Password] button.

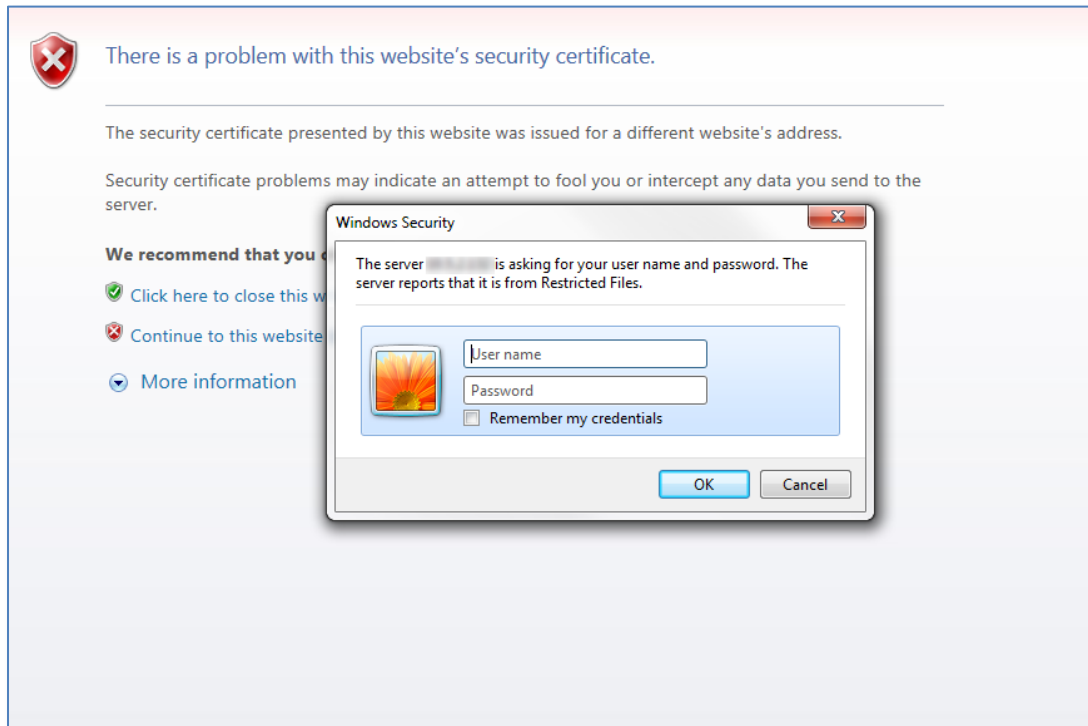



6. Enter the current password into the "Old Password" field, and the new password into the other two fields. Click OK.

3.2.2 CHANGING PASSWORD ON CACSTAR

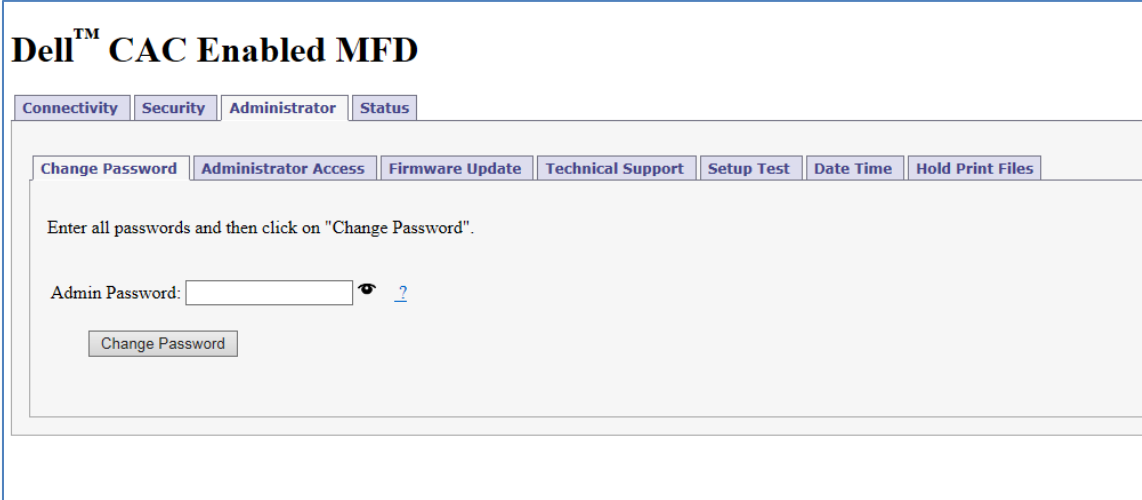
To change the admin password on CACStar:

1. Open a web browser to the CACStar web site (<https://<ip-address>:8443>). Enter the username "admin" and the current password (default="admin") when prompted:



2. Set the administrator password in the [Administrator tab]->[Change Password sub-tab]. Hovering your mouse over the  icon will reveal what has been entered, so that you can verify your password before

setting it. Click the [Change Password] button to activate the new password.



The screenshot shows the Dell™ CAC Enabled MFD web interface. At the top, there are navigation tabs: Connectivity, Security, Administrator, and Status. Below these, there are sub-tabs: Change Password, Administrator Access, Firmware Update, Technical Support, Setup Test, Date Time, and Hold Print Files. The main content area contains the text: "Enter all passwords and then click on 'Change Password'." Below this text is a label "Admin Password:" followed by a text input field, a toggle icon (an eye with a slash), and a help icon (a question mark). At the bottom of the form is a "Change Password" button.

3.3 CONFIGURING THE LDAP SEARCH BASE ON THE MFD

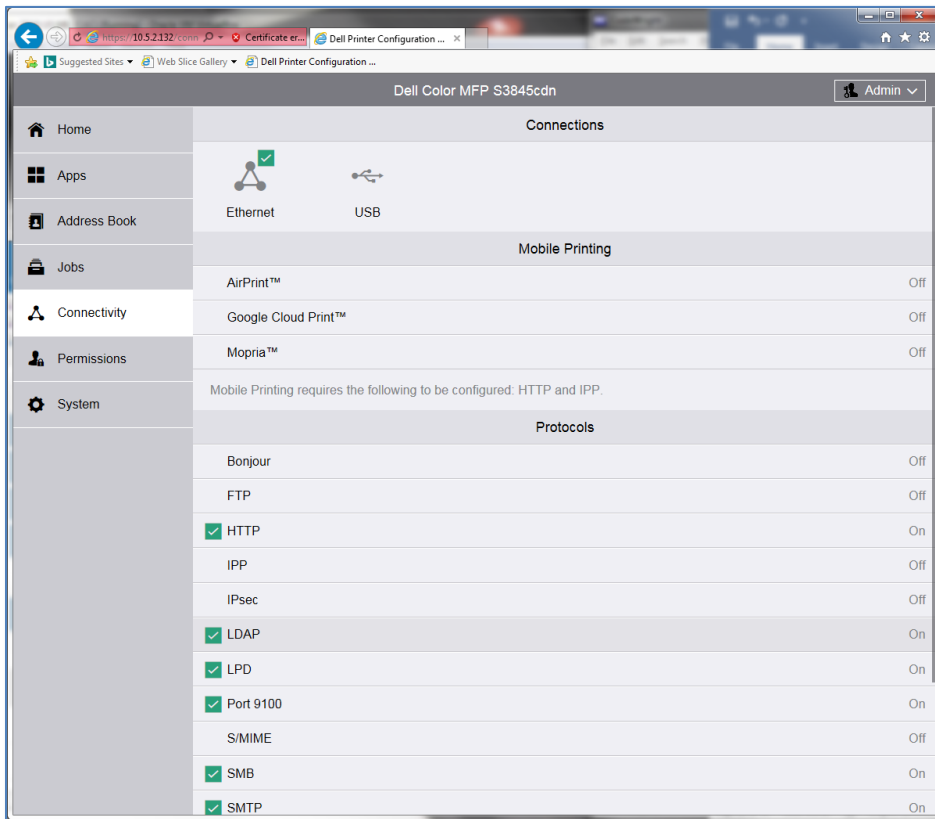
If you want to use either of the following functions:

- Lookup email recipients in the Active Directory address book
- Scan to Active Directory "Home Folder"

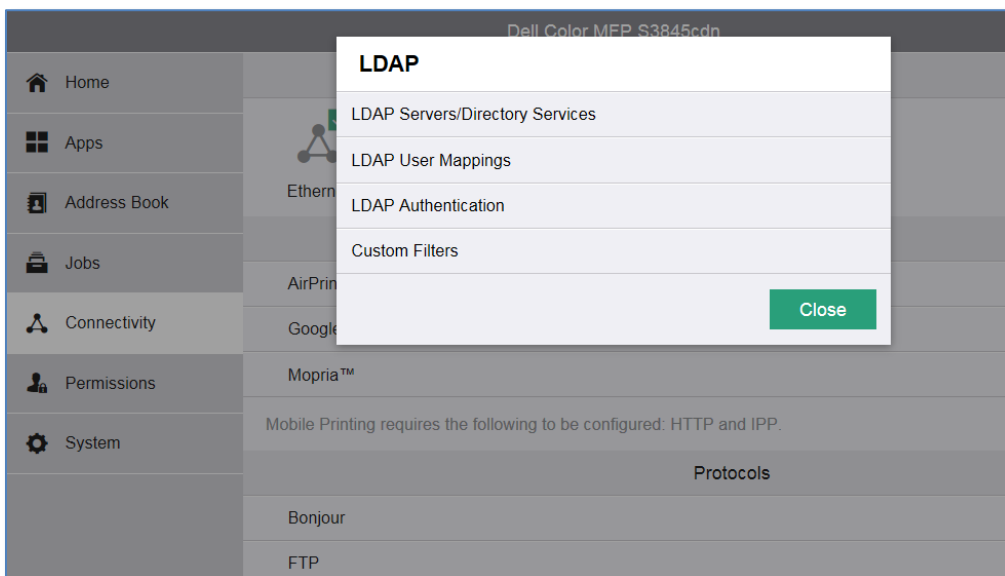
Then you will need to enter the "Search Base" (gathered earlier) into the MFD's LDAP configuration. Follow this procedure:

1. Log into the MFD web site(<https://<ip-address>>) as "admin".

- Click the “Connectivity” link on the left side of the page.



- Click LDAP, then “LDAP Servers/Directory Services”:



4. Enter the gathered Search Base string into the "Search Directory Root" field. Leave all of the other settings as shown in the figure. Click OK

The screenshot displays the configuration window for CACStar. On the left is a sidebar menu with options: Home, Apps, Address Book, Jobs, Connectivity, Permissions, and System. The main area is divided into two sections: 'Server Information' and 'Advanced Settings'.
Server Information:
 - IP Address/Host Name : Port*: 172.19.10.1 : 389
 - Backup IP Address/Host Name : Port: [] : 389
 - LDAP Server: Other
Advanced Settings:
 - Search Directory Root: **OU=Users,OU=testlab,DC=mydomain,DC=com** (highlighted)
 - Login Credentials for Database Search: Predefined
 - Login Name: []
 - Password: []
 - Retype Password: []
 - Maximum Number of Search Results: 5-100, 50
 - Search Timeout: Specify Timeout
 - Timeout: 5-120 Seconds, 30
 - LDAP Referrals: [] (disabled)
Perform Search On:
 - Perform Search On: Surname & Given Name Fields
 - * Required
 At the bottom right are 'Cancel' and 'OK' buttons.

3.4 CONFIGURING CACSTAR FOR AUTHENTICATION

To configure your device to authenticate via an Active Directory server using Kerberos, we will use all the information gathered in section 2.2. Use the following procedure:

1. Open a web browser to the CACStar administrative web site (<https://<ip-address>:8443>)
2. Navigate to the [Connectivity tab]->[LAN Side Configuration sub-tab]. Enter the value gathered for the NTP server address in the "NTP Server IP Address" field. Click [Update].

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: ?

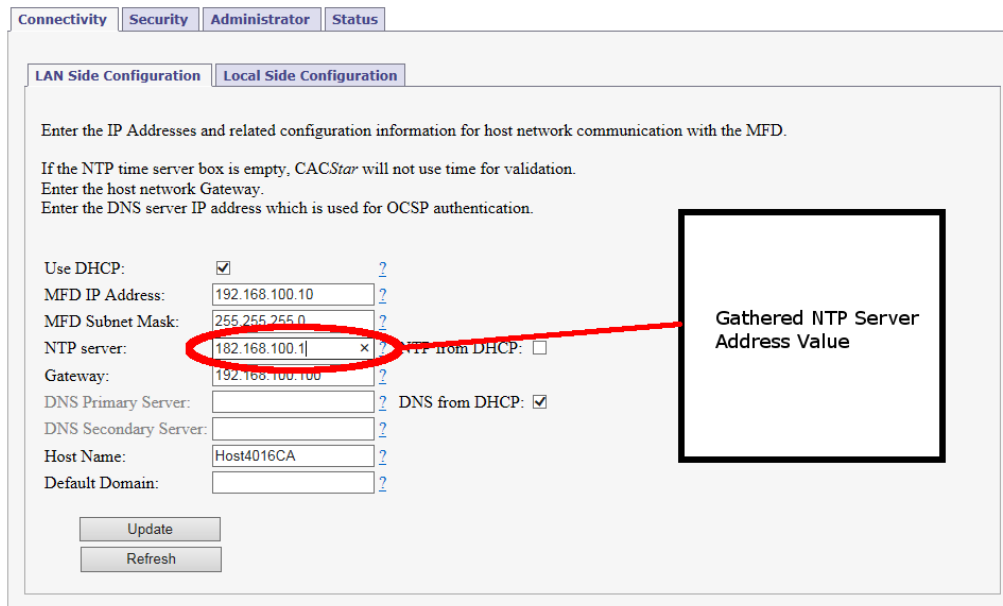
Host Name: ?

Default Domain: ?

Update

Refresh

Gathered NTP Server Address Value



- Navigate to the [Security Tab]->[Authentication Method sub-tab]. Enter the gathered information into the form as indicated in the diagram below. Click [Update].

Dell™ CAC Enabled MFD

Connectivity | Security | Administrator | Status

MFD Function Enabling | Email Setup | Authentication Method | SMB Address Book | User Login

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

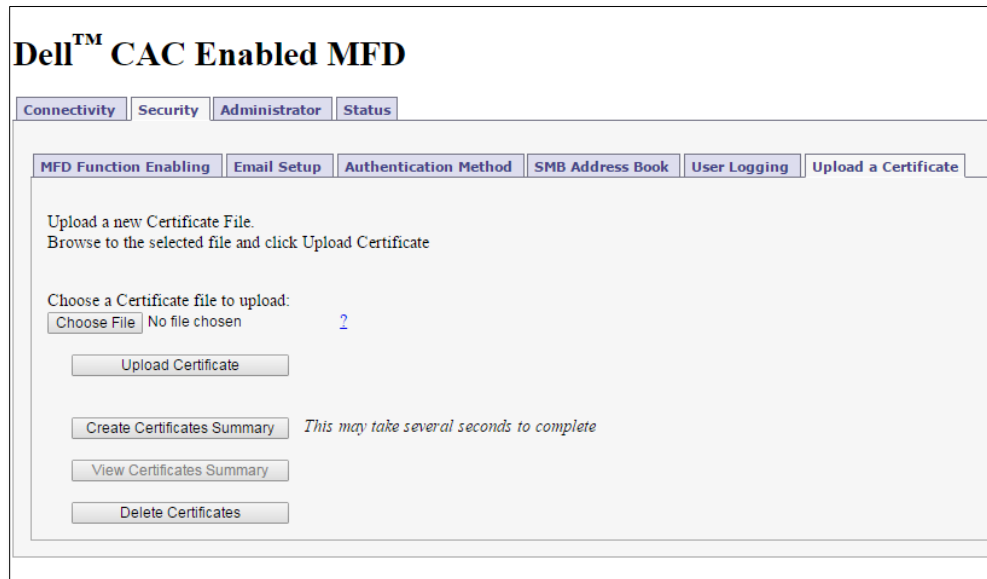
CAC Validated Timeout:	<input type="text" value="60"/>	?	
Basic:	<input checked="" type="checkbox"/>	?	Enable: Root Certificate LDAP Kerberos
OCSP:	<input type="checkbox"/>	?	
OCSP Server IP:	<input type="text"/>	?	
Root Certificate:	<input checked="" type="checkbox"/>	?	Enter name of Domain Controller in: - LDAP Server - KDC Server
LDAP:	<input checked="" type="checkbox"/>	?	
LDAP Server:	<input type="text" value="dc001.mydomain.com"/>	?	
LDAP Server Port:	<input type="text" value="636"/>	?	
LDAP Query User Name:	<input type="text"/>	?	
LDAP Query Password:	<input type="password"/>	?	
LDAP Search Base:	<input type="text" value="OU=Users,OU=testlab"/>	?	
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="dc001.mydomain.com"/>	?	Additional Realms Configuration Kerberos Realm
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="MYDOMAIN.COM"/>	?	Disable Reverse DNS Lookups
KDC Realm Domains:	<input type="text"/>	?	
KDC Principal:	<input type="text" value="SAN Principal"/>	?	Enable the Kerberos Proxies for LDAP and SMB
PKINIT Win2k:	<input checked="" type="checkbox"/>	?	
Disable Reverse DNS Lookups:	<input checked="" type="checkbox"/>	?	
MFD LDAP Kerberos Proxy:	<input checked="" type="checkbox"/>	?	Set LDAP port to 636 and enable SSL
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"/>	?	
SMB Folder LDAP Attribute:	<input type="text"/>	?	
SSL:	<input checked="" type="checkbox"/>	?	
SSL CA Certificate Checking:	<input type="checkbox"/>	?	

Update

Refresh

3.5 LOADING CERTIFICATES FOR ROOT CHAIN VALIDATION

When CACStar is configured to “root chain validation” of certificates, the appropriate CA certificates must be loaded into the CACStar appliance. As shipped from the factory, CACStar has most DOD CA certificates preinstalled, but as new CA’s are put into service, it is necessary to load updated certificates. The [Security]->[Upload a Certificate] page on the CACStar EWS is used to upload certificates:



Certificates can be uploaded in the following formats:

- DER (binary encoding)
- PEM (Base64 encoding) – **Note: Multiple PEM-format certificates can be concatenated into larger file for “batch” uploads.**
- PKCS#7

To upload a certificate:

1. Click the [Choose File] button, select the certificate file to upload
2. Click the [Upload Certificate] button after the file is selected.

4 NEXT STEPS: CONFIGURING ADDITIONAL APPS

Your S3845cdn comes with several applications built in. This guide will only discuss a limited set of these applications; these applications are the basic set that you are likely to use:

Applications that can be CAC-enabled, or may be left unlocked for all users:

- Copy (simple copy functionality)
- Fax (sending of scanned documents over an analog phone line using Fax communications commands)

Applications that are always CAC-enabled:

- Scan to Email (usually send-to-self only, but can also allow for Global Address Book via LDAP)
- Scan to Network Folder (Active Directory “Home Folder” or another network folder)
- Print Release (the printer holds your document until you authenticate at the printer and release it.)

You will likely use one or more of these applications, but you might not use them all. Consult with your System Administrators to determine which of these applications will be used.

4.1 CONFIGURING ACCESS FOR APPS

When the CACStar option is installed using version “A01” of the CACStar setup file (see section 3.1), the printer will already be set so that Copy Apps (Copy, ID Card Copy) are available to all users without authentication, while all other apps require authentication for access.

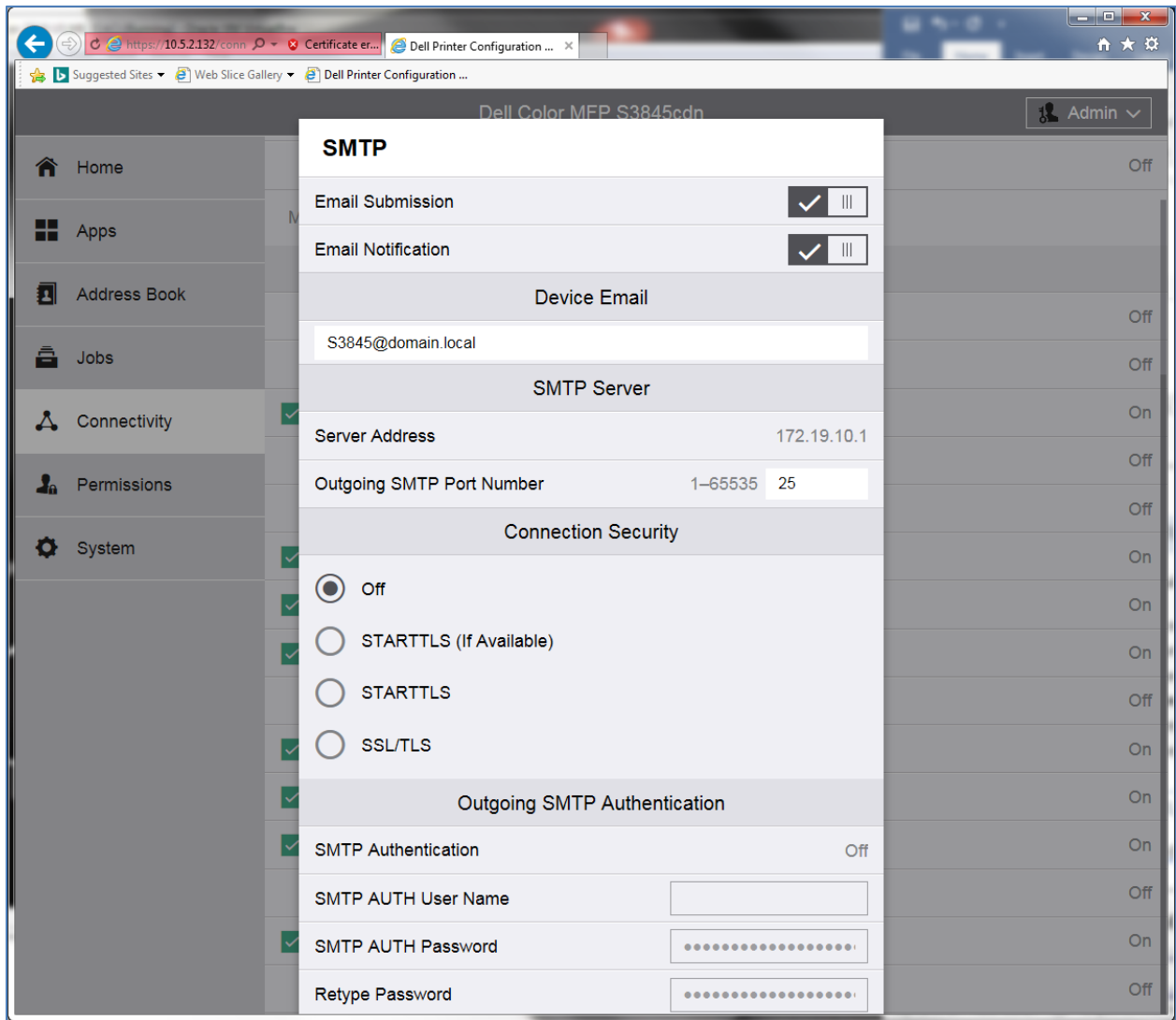
To change the configuration for which apps are available to guest (unauthenticated) users, refer to the S3845cdn Users Guide (“Dell Printer Configuration Web Tool”->“Permissions”).

4.2 CONFIGURING SCAN TO EMAIL

Upon installation of the CACStar option, the MFD will be configured for “email to self only” (i.e. email can only be sent to the authenticated user’s email, and no additional recipients can be selected. This is the typical configuration for DOD environments.)

To verify proper configuration of the MFD itself, log into the S3845 admin web site as “admin”, and go to the “Connectivity” section of the website, and select “SMTP” to view the MFD settings for connectivity. **Important!**

The settings need to be set as shown here. If they differ, make the necessary changes to make them match.



To allow emails to be sent via your network, use the SMTP server address information gathered earlier to configure the CACStar email settings. The [Security]->[Email Setup] page on the CACStar EWS is where the above information is configured:

Dell™ CAC Enabled MFD

Connectivity | Security | Administrator | Status

MFD Function Enabling | Email Setup | Authentication Method | SMB Address Book | 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: 2

SMTP Port Number: 2 *Default: 25*

User Email Address From: 2

Force Email to Self: 2

Encrypt Email: 2

Email Encryption Type: 2

Sign Email: 2

LDAP Primary Certificate Attribute: 2

LDAP Secondary Certificate Attribute: 2

Kerberos Email Authentication: 2

Setting	Description
SMTP Address or Server Name	The FQDN or IP address of the SMTP server. Use the SMTP server address information that you gathered here.
SMTP Port Number	The TCP port used for communication with the SMTP server. The default value of 25 is appropriate in most cases.
User Email Address From	<p>The “from” address for sent emails will be automatically filled in by CACStar to reflect the user who generated the email. This “from” address can be acquired from the user’s card (the “CAC” setting) or from the directory server (“LDAP”).</p> <p>The default setting is “CAC”, which is appropriate for most cases.</p>
Force Email to Self	No change is required to this setting, because the printer is properly configured to enforce “email to self” operation.

Setting	Description
Encrypt Email	<p>Chooses whether to encrypt outgoing emails.</p> <p>To use this feature when not “forcing email to self”, then directory access (LDAP) <i>must</i> be configured, and encryption certificates for recipients in the directory must be published in the directory.</p> <p>Choices for this setting are:</p> <ul style="list-style-type: none"> • “Yes”: Always encrypt outgoing messages • “No”: Never encrypt outgoing messages • “Prompt”: ask the user via the operator panel each time a message is sent whether or not the message should be encrypted. <p>The default setting is “No”.</p>
Email Encryption Type	<p>Chooses the encryption method to use when encrypting.</p> <p>Choices for this setting are:</p> <ul style="list-style-type: none"> • 3DES • AES-256 <p>The default setting is “AES-256”.</p>
Sign Email	<p>Chooses whether or not to digitally sign outgoing emails.</p> <p>Choices for this setting are:</p> <ul style="list-style-type: none"> • “Yes”: Always sign outgoing messages • “No”: Never sign outgoing messages • “Prompt”: ask the user via the operator panel each time a message is sent whether or not the message should be signed. <p>Change this setting to “Yes” (the default is “no”)</p>
LDAP Primary Certificate Attribute LDAP Secondary Certificate Attribute	<p>Indicates which LDAP attribute to query to acquire a recipient’s encryption certificate. If you are not encrypting emails, then these settings are not used.</p> <p>The default Primary attribute is “userSMIMECertificate” The default Secondary attribute is “userCertificate”</p>

Setting	Description
Kerberos Email Authentication	<p>When “checked”, GSSAPI authentication is used when connecting to the SMTP server. Note: CACStar’s Kerberos authentication feature must be enabled before enabling this setting.</p> <p>Leave this setting unchecked (disabled) unless your System Administrator tells you that authentication is required for the SMTP server. For digital senders, it is unusual to require authentication to SMTP servers.</p> <p>The default setting is Disabled (“unchecked”).</p>

4.3 SCAN TO NETWORK FOLDER

Scan to Network Folder is starting to see increased use in DOD environments. You will want to one of these locations:

- The users Active Directory “Home Folder”
- A fixed network folder, which multiple users might use for scanned file storage
- A ‘dynamic’ folder location, based information about the user. This is similar to, but not the same as, the Active Directory “home folder”.

When the S3845 has been configured with the LDAP Search Base (see section 3.3 for more information), and the MFD SMB Kerberos Proxy has been enabled (as indicated in section 3.4) your printer is already configured to support scanning to the Active Directory “Home Folder”.

When scanning to network folders, it is important to make sure that the “MFD SMB Kerberos Proxy” is enabled in the CACStar admin web site (the location of this setting is shown in step 3 of section 3.4. This will ensure that the cardholder’s credentials are used when storing the scanned file.

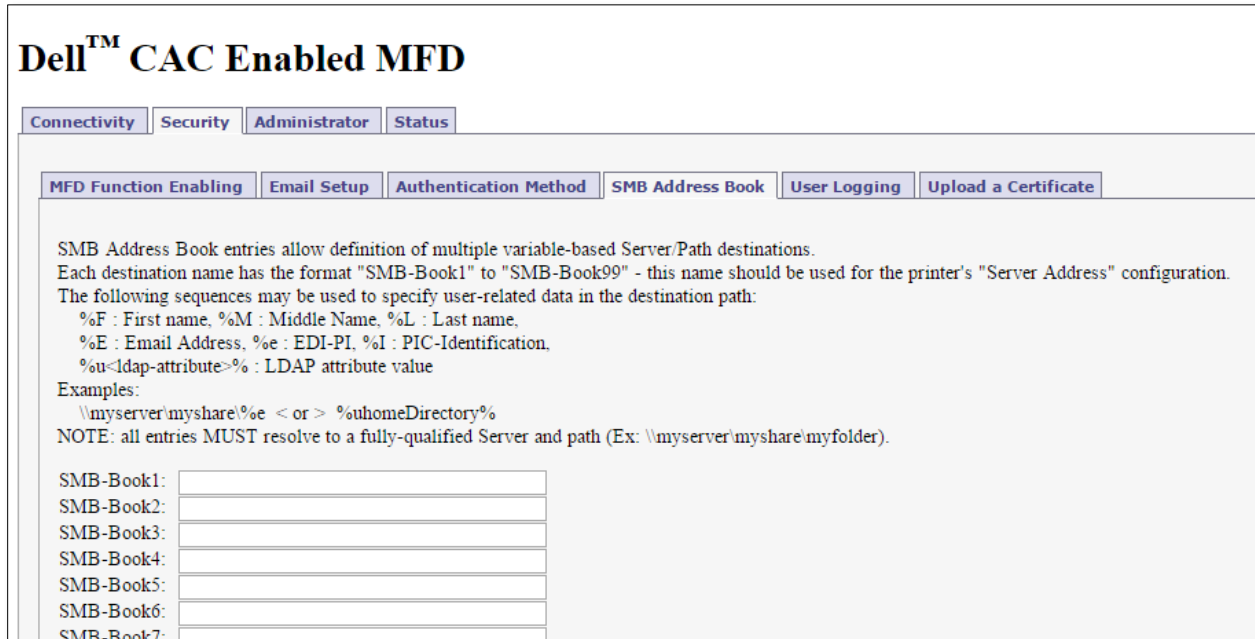
Additional scanning destinations may be configured via the admin web site on the MFD (see the S3845 User Guide for more information.

“Dynamic” network folder paths are accessible by using the CACStar “SMB Address Book”. The SMB Address Book provides “virtual servers” that can be referenced by MFD address book entries to provide access to dynamic network folder paths. Discussion of the SMB Address Book is found in section 4.3.1.

Note: When creating additional scanning destinations, you will need to enter a username and password for the address book entry, but they will not be used for the actual transfer itself.

4.3.1 THE CACSTAR “SMB ADDRESS BOOK”

The [Security]->[SMB Address Book] page of the CACStar EWS allows the administrator to define dynamic address book entries that the MFD can use by referencing specially-define server names in the MFD’s address book.



As shown in the figure above, each entry in the CACStar SMB Address Book is identified by name: “SMB-Book<n>”, where the <n> is replaced with a number 1-99. There can be up to 99 entries in the SMB Address Book.

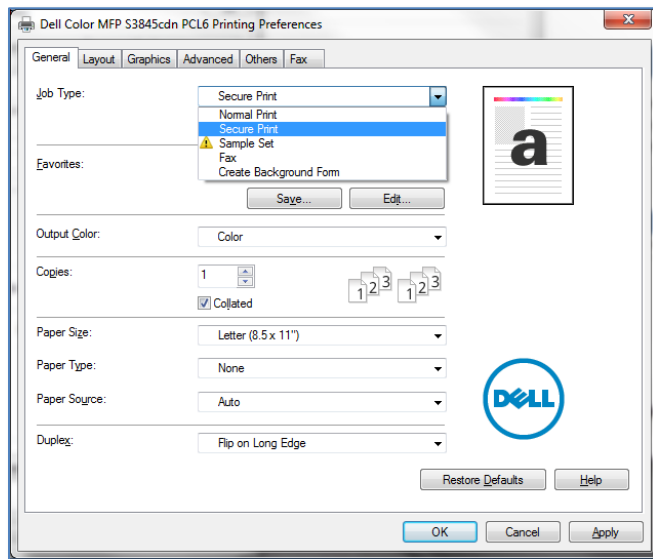
To configure an entry, you can use a combination of fixed characters and “variable fields” that are prefixed with a percent sign (%). The character following the percent sign indicates which variable data is substituted in place of the variable field. The following table shows the possible variable fields that be used:

Variable	Substitution Made
%F	The authenticated user’s “first name”
%M	The authenticated user’s “middle name”
%L	The authenticated user’s “last name”
%E	The authenticated user’s email address
%e	The authenticated user’s EDI/PI (personnel identifier)
	– Available for CAC users only

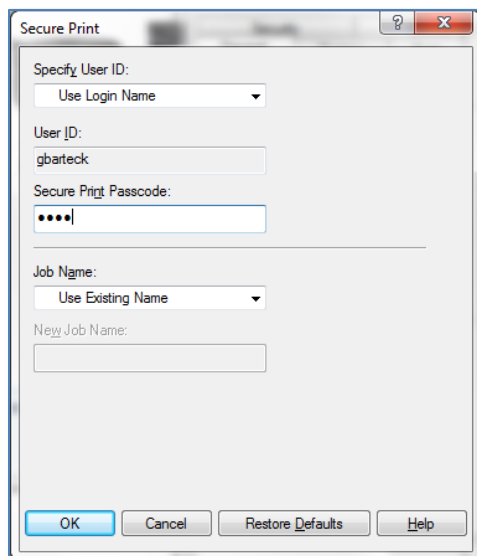
%l	Identification from the PIC field of the user's CAC card. – Available for CAC users only
%u<attribute>%	An LDAP attribute query is made, where the attribute name is enclosed between the leading "%u" and the trailing "%". Important: LDAP must be configured to utilize the %u expansion macro.

5 PRINT RELEASE

The S3845 can hold submitted print jobs inside the printer until the job submitter releases them at the printer's local User Interface. This type of job is called a "Secure Print" job. A user specifies the printing of "Secure Print" jobs in the driver settings:



After Secure print is selected as the job type, click the [Setting...] button to configure secure print parameters:



Ensure that the “Specify User ID” setting is set to “Use Login Name”, and enter a PIN code to associate with stored jobs. When authenticated at the printer with your smart card, you should not require the PIN to release your jobs, but if you want to release your jobs without authenticating, the PIN will be required, so you should remember the PIN, just in case.

With secure print selected as the job type, the will be stored by the printer until the user uses his smart card to authenticate at the printer. Then The “Jobs” tile can be selected at the printer operator panel, where the job(s) held for that user can be released.

Important:

In the CACStar configuration (*Administrator tab->Hold Print Files sub-tab*), the Setting for “**Name Matching Format**” must be set to its default value of “%S” to ensure proper matching of the user to his held print jobs. If this setting is not correct, change it to the proper value of “%S” and click the **[Update Format]** button.

6 REPLICATING THE CONFIGURATION TO OTHER MACHINES

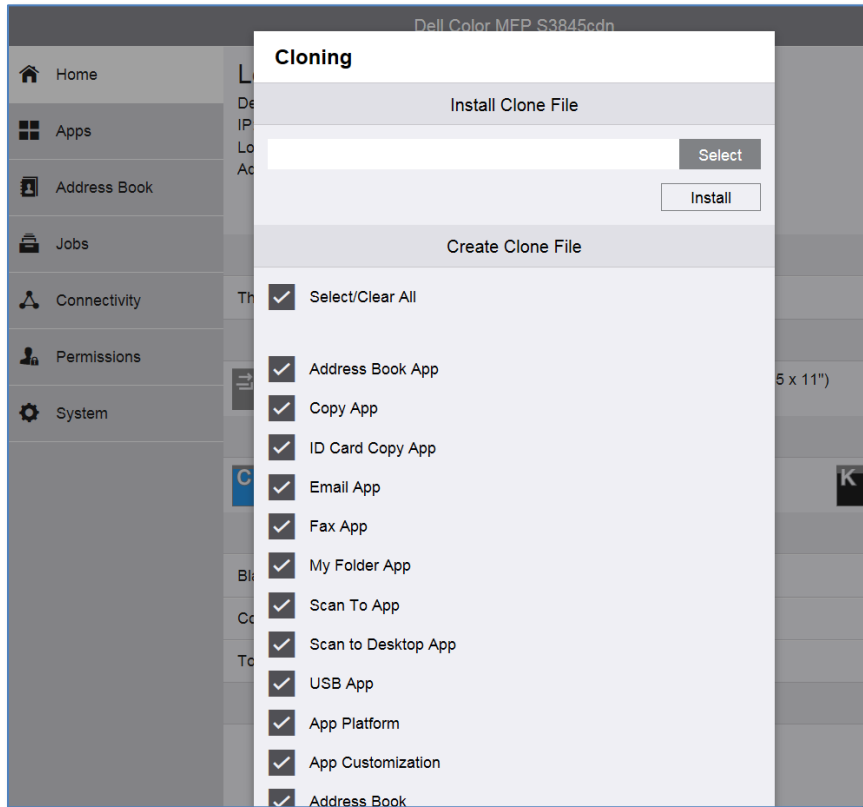
After the configuration is complete, you will want to save the configuration of both the printer and the CACStar option. This way the configuration can be copied to additional machines with a minimum of effort.

6.1 SAVING THE PRINTER CONFIGURATION

The printer’s configuration is saved by using the following procedure:

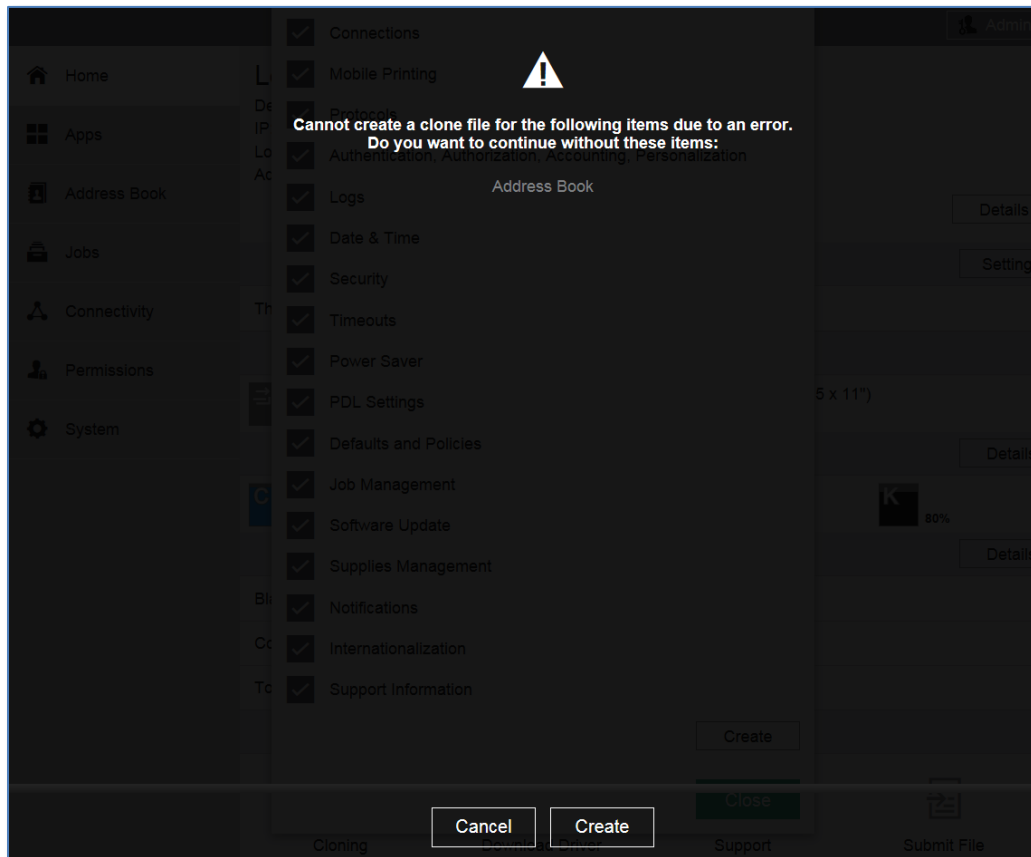
1. Log into the printer’s admin website as “admin”
2. Click the “Home” link on the left-hand-side of the page

3. Scroll down to the bottom of the page, and click the "Cloning" icon. You will see a lengthy list of items that can be saved. You want all settings to be selected:



4. Scroll down to the bottom, and click the [Create] button.
5. If you get an error screen indicating that the clone file cannot be created because of an error in the Address Book, this is usually because there are no Address Book Entries to save. This is normal. Click the

[Create] button to continue.



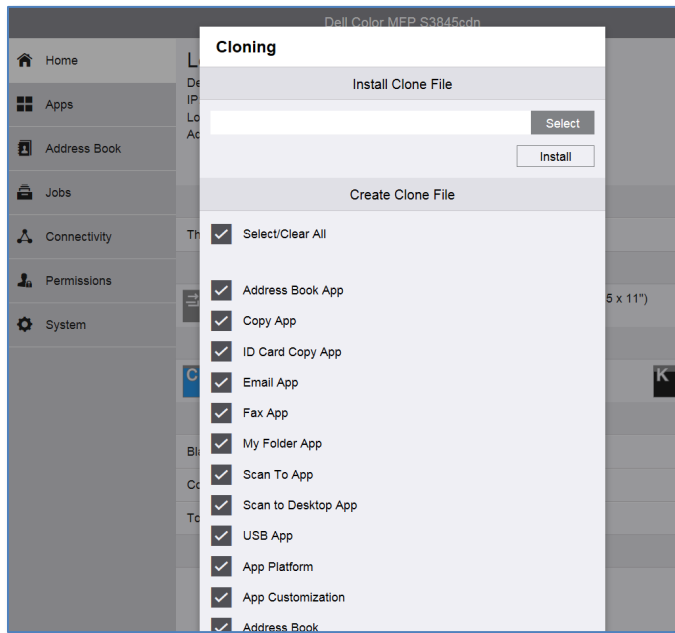
6. A file called “cloning.zip” will be downloaded. Save this to a folder of your choosing. You may rename this file if you wish, but do not change the “.zip” extension.

6.2 LOADING THE PRINTER CONFIGURATION INTO ANOTHER PRINTER

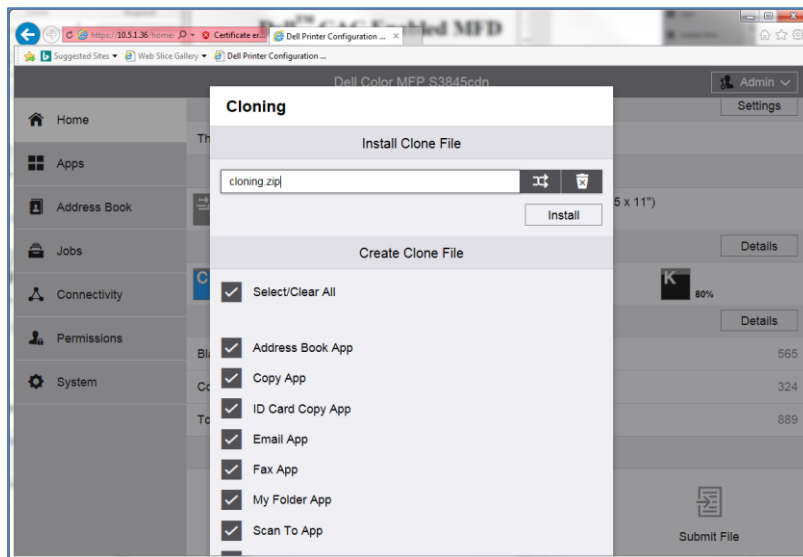
To load a saved printer configuration (cloning.zip) into another printer, follow this procedure:

1. Log into the printer’s web site as “admin”.
2. Click the “Home” link on the left-hand-side of the page.

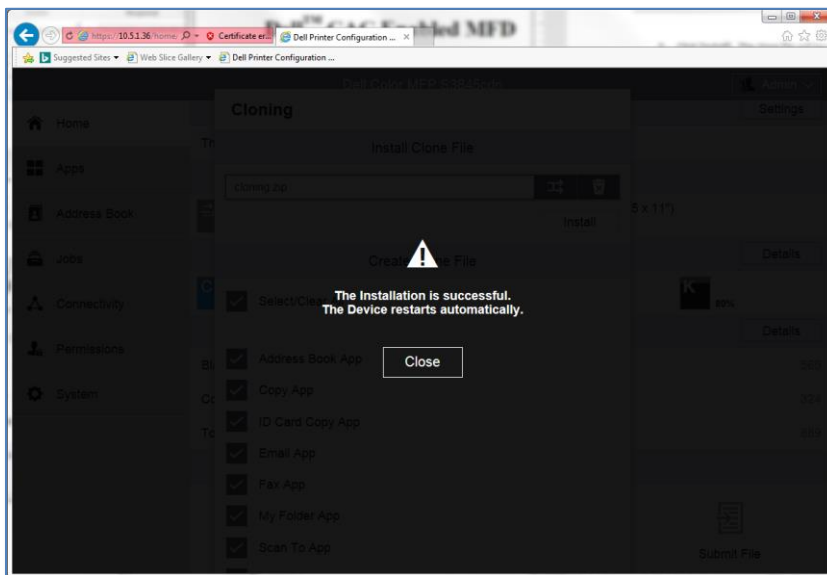
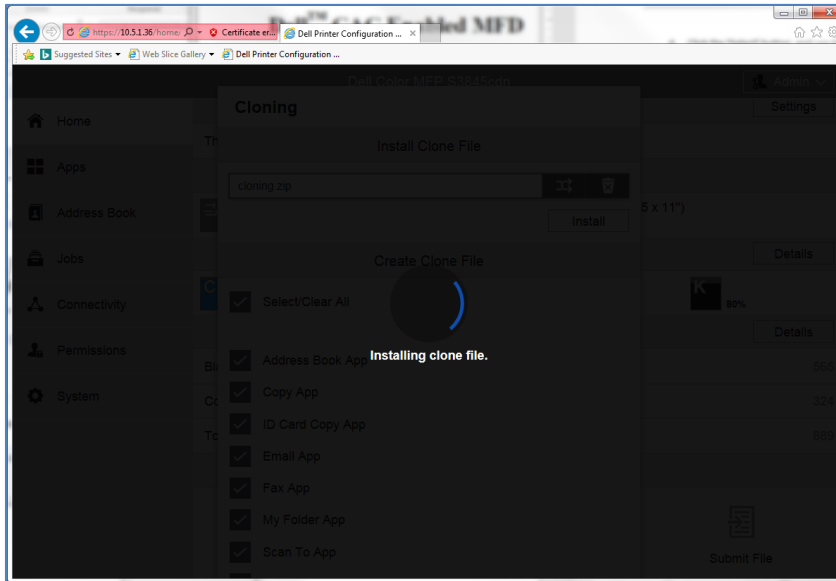
3. Scroll down to the bottom of the page and click the “Cloning” icon:



4. Click the [Select] button, and use the file selection dialog to select the previously saved cloning.zip file:



5. Click [Install]. The clone file will be installed, and the printer will reboot:



6.3 SAVING THE CACSTAR CONFIGURATION

To save the CACStar configuration settings, follow this following procedure:

1. Log into the CACStar web site as “admin”

2. Navigate to the [Administrator tab]->[Firmware Update sub-tab]:

The screenshot shows the Dell™ CAC Enabled MFD Administrator interface. At the top, there are tabs for Connectivity, Security, Administrator, and Status. Under the Administrator tab, there are sub-tabs: Change Password, Administrator Access, Firmware Update (selected), Technical Support, Setup Test, Date Time, and Hold Print Files. The main content area contains the following text and controls:

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: 8.5
Boot Version: 1.9

3. Click the [Create Config File] button.
4. When the screen refreshes, click the [Export Config File] button. A file called "cacstar.cfg" will be downloaded. Save this file in the same folder where you stored the printer's cloning.zip file.

6.4 LOADING THE CACSTAR CONFIGURATION INTO ANOTHER MACHINE

To load a saved CACStar configuration into another device, follow this procedure:

1. Log into the CACStar web site as "admin"

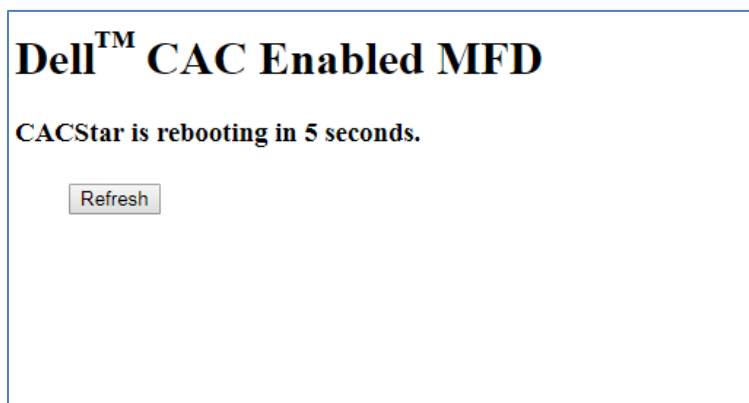
2. Navigate to the [Administrator tab]->[Firmware Update sub-tab]:

The screenshot shows the 'Dell™ CAC Enabled MFD' interface with the 'Administrator' tab selected. Underneath, the 'Firmware Update' sub-tab is active. The page contains instructions to update firmware or configuration settings, a file upload section with a 'Choose File' button and an 'Upload File' button, and options to create and export configuration files and certificates. A 'Reboot CACStar' button is also present. At the bottom, the current firmware and boot versions are displayed as 8.5 and 1.9 respectively.

3. Click the [Choose File] button, and select your previously saved “cacstar.cfg” file.
4. Click [Upload File] to install the saved configuration. You will see a screen acknowledging the configuration update. Click [Refresh]:

The screenshot shows the 'Dell CAC Enabled MFD' interface with the 'CACStar Configuration Import' sub-tab. A message states 'The Configuration Import File Status: Completed successfully.' Below the message is a 'Refresh' button.

5. Click the [Reboot CACStar] button. The CACStar option will restart. This will take about 30 seconds.



7 TROUBLESHOOTING

This section describes the most common problems you might come across.

7.1 ERROR MESSAGES

7.1.1 PROBLEMS OCCURRING AFTER POWER-ON

Error Message Text	What happened?	What to do about it
Unable to communicate with NTP Server. Contact the Network Administrator – Please press ‘Yes’	An NTP server address is configured, but CACStar is unable to establish communications with it.	Check to ensure that the network cable is attached correctly Verify the configured NTP server address. Refer to the procedure in 2.2 Gathering Information for information on how to get the IP address of the NTP server.

7.1.2 PROBLEMS OCCURRING DURING AUTHENTICATION

Error Message Text	What happened?	What to do about it
--------------------	----------------	---------------------

Error Message Text	What happened?	What to do about it
Authentication Failed: LDAP Bind Error	<p>CACStar was unable to acquire a Kerberos ticket for the LDAP service on the LDAP server.</p> <p>This is usually caused by one of two things:</p> <ol style="list-style-type: none">1. LDAP Server address setting contains an IP address, rather than a host name, and the "Disable reverse DNS lookups" setting is 'checked'.2. The DNS server's reverse lookup database may be returning an incorrect name. This may happen as servers are taken out of service, or are replaced with a different hostname at the same IP address.	<p>The best course of action is to ensure that the correct FQDN of the domain controller is entered for the "LDAP Server Address" setting on the CACStar configuration, and to set "Disable reverse DNS lookups" to enabled (checked).</p> <p>Also, print a CACStar configuration summary, and verify that the DNS server information (at the end of the summary) is correct.</p>
Authentication Failed: Kerberos error (connection)	<p>CACStar was unable contact the Kerberos server.</p>	<p>Check the "KDC Server" address setting in the CACStar configuration. This should be the FQDN of the domain controller. Check with your System Administrator for the correct value.</p>

Error Message Text	What happened?	What to do about it
Authentication Failed: Kerberos error (PKINIT)	<p>An error occurred while communicating with the Kerberos server. Obtaining a “syslog” with the “PKCS” syslog option enabled can provide more detailed information on the failure. However, common causes are listed below:</p> <ul style="list-style-type: none">- With “Root Certificate” checking enabled, the CA certificates required to validate certificates may be missing.- The user’s card credentials are not recognized.- The current date/time for CACStar is out-of-sync with the date/time on the Kerberos server.-	

8 GATHERING ERROR LOGS

Sometimes, when trying to diagnose a problem, a debugging log must be captured. The CACStar debug logging (syslog) feature is found in the [Administrator tab]->[Technical Support sub-tab]:



Clicking the [Syslog Options] button allows selection of the items captured in the log:

Dell CAC Enabled MFD

SysLogging Options

If an item is checked, that option will be logged.
If an item is not checked, that option will not be logged.

Reader Connection:

Card Communication:

Card Container:

Container Parse:

Card Expiration:

PKCS:

OCSF:

PIN:

Challenge:

LDAP:

SMB:

HTTP:

SMTP:

RP Send/Receive:

The following table describes the various logging options:

Option Name	Purpose
Reader Connection	Include information about detection and use of the card reader hardware. This setting is seldom used, and only if it is suspected that the card reader is broken
Card Communication Card Container Container Parse Card Expiration	Include information about low-level communications with a smart card. This setting is seldom used.

Option Name	Purpose
PKCS	<p>Include information related to Kerberos Authentication</p> <p>This setting is useful to debug Kerberos Errors.</p>
OCSP	<p>Include information regarding OCSP verification of certificates.</p> <p>When using Kerberos Authentication, OCSP is normally not used, as the cardholder certificate will be validated by the Kerberos Server.</p>
PIN	<p>Include card communications related to PIN processing.</p> <p>This setting is seldom used.</p>
Challenge	<p>Include information related to the “challenge” portion of card authentication.</p> <p>This setting is seldom used.</p>
LDAP	<p>Include information related to communications with the LDAP server.</p> <p>This is useful for diagnosing LDAP related problems.</p>
SMB	<p>Include information related to Server Message Block (SMB) communications.</p> <p>This setting is useful when diagnosing problems with scan-to-network-folder.</p>
HTTP	<p>Include information related to CACStar’s embedded web server communications.</p> <p>This setting is seldom used.</p>
SMTP	<p>Include information related to SMTP server communications.</p> <p>This setting is useful for diagnosing problems with scan-to-email operations.</p>

When the appropriate Syslog options have been chosen, click the [Update] button to save the settings, then click the [Home] button to return to the Administrator->Technical Support page.

The basic procedure for generating and collecting a log is:

1. Click [Start Syslog File]
2. Perform the operation that is being diagnosed
3. Click [Stop Syslog File]
4. Click [Get Syslog File]. A file called "cacstar.log" will be downloaded. This file can be viewed in wordpad, or any text editor that understands Unix-style line endings (line-feeds only at the end of a line). **Note: notepad is not a suitable program for looking at log files.**

Capturing debugging logs should only be done at the direction of Dell technical support. The content of the log file will not be useful to an end-user. Call Dell technical support at (800) 822-8965 for assistance.