How to Secure Data in Collection-Master

Presented by Luis Gomez

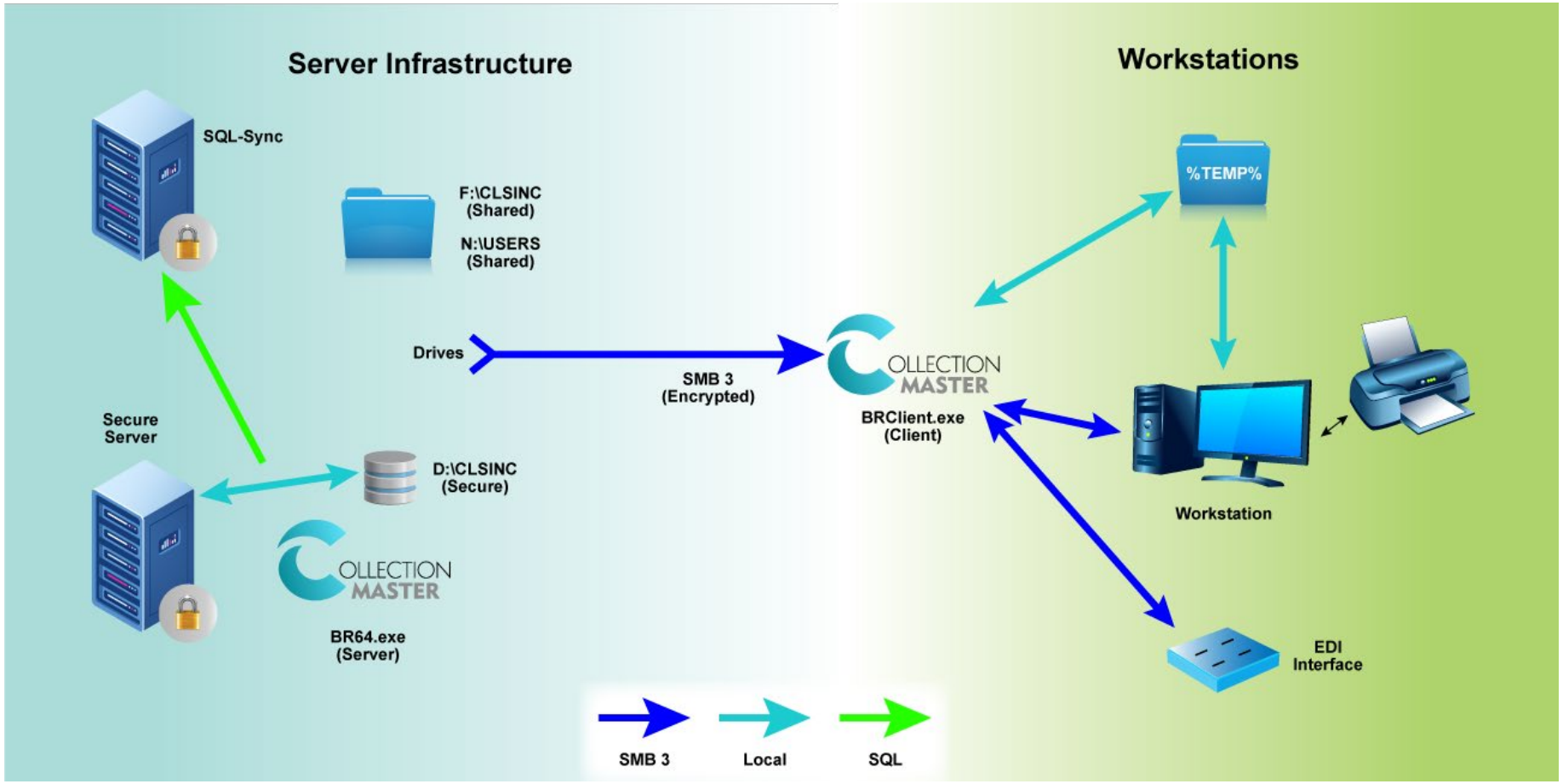
The Mastermind Series

Presented by VERTICAN TECHNOLOGIES

Resources

- PDR Documents
  - https://vertican.tech/cm/pdr/how-to-secure-data-in-collection-master/
- Mastermind Series
  - Video: Printing in Collection-Master
  - Presentation: Printing in Collection-Master

How to Secure Data in Collection-Master



Secure Data

Drive	Description	Location on Sever
F:	Primary Drive for Collection-Master	F:\CLSINC\
N:	Users Home Directory	N:\USERS\[LOGIN_NAME]

Drive	Description	Location on Sever
H:	Archive Claims (History)	D:\CLSINC\HISTORY
I:	Active Claims (Data)	D:\CLSINC\DATA
K:	Accounting (Perm)	D:\CLSINC\PERM
L:	Common Files (Common)	D:\CLSINC\COMMON
M:	Shared Files (Share)	D:\CLSINC\SHARE

Pros

- Enhanced protection against crypto & other viruses
- Direct access to critical data folders limited
- Greater security & compliance
- Critical data folders outside of F:\CLSINC
- Restricts users from running in Distributed Mode
- Prevent user tempering (Move/Delete) accidentally or maliciously
- Targeted backups
  - Critical data folders are segmented

Cons

- External access to the Secure Data folders is unavailable.
  - ODBC, a legacy solution will not work.
  - WB32 or Distributed Mode will not work.
- Vertican Custom Programs may not be compatible.
  - Additional changes may be required
- External Custom Programs may not be compatible.
  - Make sure to test these carefully before implementing Secure Data
- Troubleshooting sometimes requires access to the actual data folders.
  - In these cases, access to the actual file server may be required.

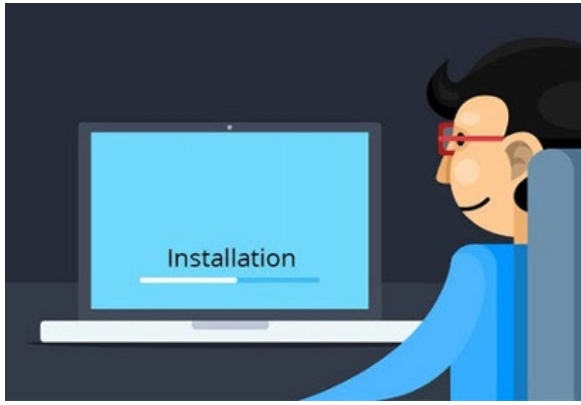
Requirements

- Collection-Master 9.1 or higher
- Client Server implemented

Installation Instructions

- Complete instructions in manual
- BACKUP BACKUP BACKUP (and then BACKUP again!)
  - Setup your Test Environment /w Secure Data First.
- All users out of Collection-Master
  - Including automation such as SQL-Sync or Export2CM
- F:\CLSINC\BATCH\Move_2_Secure_Data.cmd
  - Moves COMMON/DATA/HISTORY/PERM & Share Folders
- Edit Mapdrive._CS
- 2-S-3-F4 – Validate Bank Accounts (Update Path)

Move_2_Secure_Data.cmd



C:\Windows\system32\cmd.exe

```
This script will aid in moving Collection-Master data in order to utilize
Secure Data. Before continuing, it is imperative that the instructions
on configuring Secure Data be read.

Please ensure that you have a verified, accurate and reliable BACKUP prior
proceeding.

If you wish to continue please type CONFIRM
If you wish to cancel please type CANCEL or close the window.
>CONFIRM

Enter Secure Data path e.g. S:\CMDATA\):S:\CMDATA\

You have chosen to use S:\CMDATA\ as your Secure Data location. Is this correct?
 (Y/N)Y
```

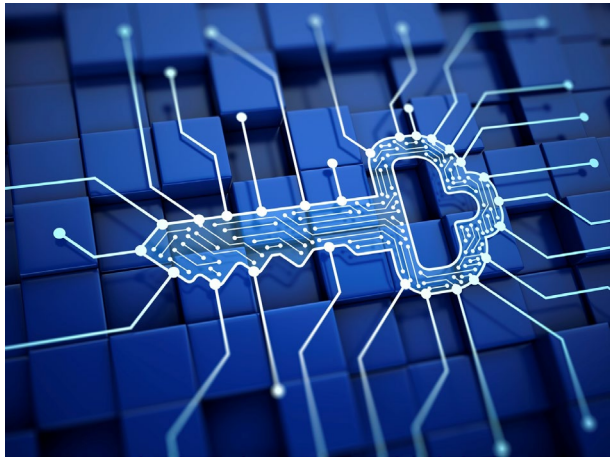
Sample Mapdrive._cs

```
Rem [---- Start of CM-SETUP ----]

Drive F,F:\,F:\,CLSINC
Drive G,F:\,F:\,CLSINC
Drive H,S:\CMDATA\,No_Drive,HISTORY
Drive I,S:\CMDATA\,No_Drive,DATA
Drive K,S:\CMDATA\,No_Drive,PERM
Drive L,S:\CMDATA\,No_Drive,COMMON
Drive M,S:\CMDATA\,No_Drive,SHARE
Drive N,N:\,N:,USERS\[LOGIN_NAME$]

Rem [---- End of CM-SETUP ----]
```

Encryption



- Windows SMB3 – Encryption in Motion
  - Workstations MAP F: & N: drives, any information transferred over this PIPE should be over SMB3 with Encryption Enabled.
  - Will protect files being imported into Collection-Master as well as other applications such as Mail Merge.
- Client Server Encryption
  - Client Server runs on the file server with the visual components being transferred to the client over a private TSL Encryption.
- Encryption at Rest
  - In Client Server, all communication with the storage device is direct to a local device on the server. Encrypting data at rest is best with a hardware solution.

Local Profile

- On your Client, some information will be stored in your Local Profile.
  - %Appdata%
  - %TEMP%
  - Make sure to enable encryption for your Local Profile
    - BitLocker or other software encryption is appropriate.
    - Laptops – encrypt the entire machine!
- Temporary Files stored on the Network
  - F:\CLSINC\TEMP\[Session]
- Files in your N:\Users\[Login_Name] folder.

Non-Public Information (NPI) – SSN #, D/L, DOB

- When exporting data outside Collection-Master, consider if NPI is required
  - If NPI is included, security concerns increase
- CMvX NPI Filter
  - “M” – Mask NPI (DOB = 01/01/CCYY)
  - “Y” – Filter NPI (Blank)
  - “N” – Include NPI

Printing

- Direct Printing
  - :\\UNC_PATH\
    - Client Server will connect over SMB3 directly from the server to the device
- Windows Printing (Including UNC Paths)
  - Controlled by the Workstation
  - Collection-Master builds a spool file on the local %TEMP% folder.
  - The spool file is fed to Windows Printing
- PDF, EXCEL-IT, HTML, E-Mail, etc.
  - Controlled by the Workstation
  - A spool file is created in CLSINC\TEMP\[SESSION] over SMB3
  - The spool file is fed to the application


Q
A

The Mastermind Series

To learn about upcoming trainings:
https://vertican.tech/mastermind/

To view past trainings:
https://vimeo.com/vertican/