ControlCase^{TM} Data Discovery

Version 10.4.5 Updated Sep 2021	CDD Endpoint Quick Start Guide

ControlCase Data Discovery (CDD) helps you find credit and debit card information (and other sensitive data) that could be stored in your systems in violation of the Payment Card Industry Data Security Standard (PCI DSS) or other regulations

Table of Contents

1. PREREQUISITES

Please ensure the following:

1. The CDD Installation machine (scanner machine) needs to be a "brand new install" of 64 Bit
   a. **Windows 2019 Server,**
   b. **Windows 2016 Server,**
   c. **Windows Server 2012 R2 Service Pack 1,**
   d. **Windows 8.1 or**
   e. **Windows 10 Enterprise.**

   We do not support any other operating systems, even if CDD may install on them.

2. Windows Operating system should be in the **English** language (other languages are not supported at this time).

3. The machine should be a 1 or 2 core 2.4GHz CPU or better with at least 200GB disk space free and 8 GB RAM. If Windows can run well on the hardware, so can CDD.

4. CDD installs on both **physical** and **virtual machines**.

5. We need **administrator credentials** on this machine to install the software and this administrator account must have ALL access rights to the machine including but not limited to "Run as Service", "Install scheduled tasks", "Access the network", "RDP inbound".

6. 32-bit Visual C++ Redistributable for Visual Studio 2015, 2017 and 2019 from Microsoft https://aka.ms/vs/16/release/vc_redist.x86.exe (even if the OS is 64 bit)
   Alternate URL: https://support.microsoft.com/en-in/help/2977003/the-latest-supported-visual-c-downloads

7. Open the firewall rule to access the ControlCase API. See the section "Firewall Rule" for more information.
   a. Non- EU environment : https://cs-api.controlcase.com
   b. Europe (EU) environment : https://cs-api-eu.controlcase.com

8. The file system targets that need to be scanned should allow standard Windows Networking (Port 445), Administrative shares (ADMIN$ etc) and RPC ports. Windows File sharing needs to be enabled on both scanner and target machines.

   More information on permissions, firewall ports, protocols etc. required by CDD can be found at https://help.controlcase.com/kb/cddsettings/

CONTROLCASE   12015 Lee Jackson Memorial Hwy ● Suite 520 ● Fairfax, Virginia 22033 USA
Phone: +1.703.483.6383 (Support/Sales)   www.controlcase.com

P a g e | 3

2. DOWNLOAD AND INSTALL

Please see the below links to download the CDD Endpoint installer.

1. Non-EU environments:
   https://home.controlcase.com/downloads/CDD_Endpoint_10.4.5.0.exe

2. Europe (EU) environment:
   https://home.controlcase.com/downloads/CDD_Endpoint_10.4.5.0_EU.exe

You will need the **Activation key** to install the CDD Endpoint. Please see the steps below on how to generate the activation key from SkyCAM portal.
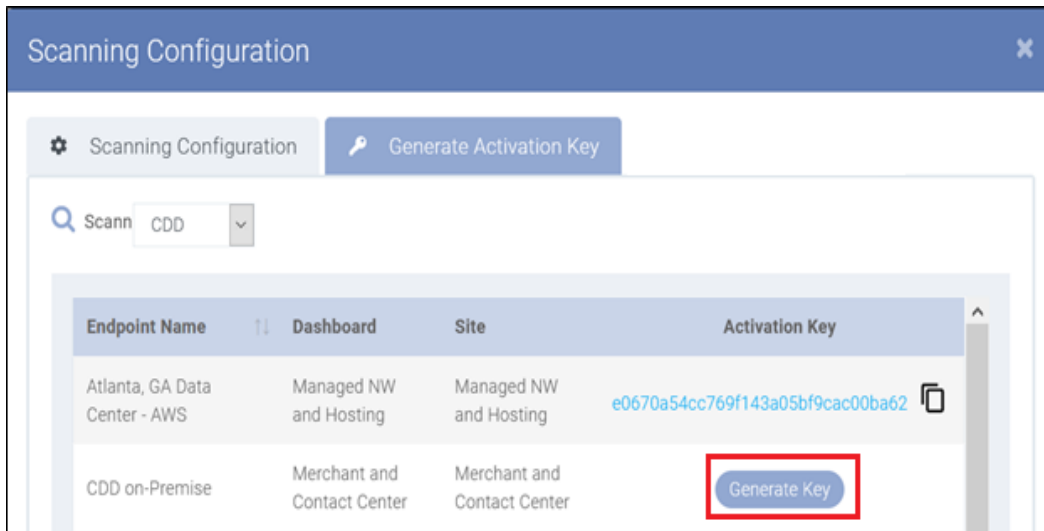
1. Log into the **ControlCase SkyCAM** portal.

2. Select the **Compliance Scanner** from the drop-down menu.
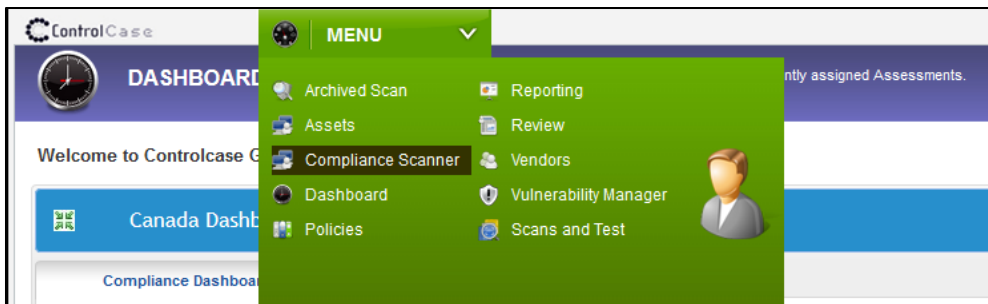
3. Select the **Generate Activation Key** tab.
4. Select the **CDD** option from drop-down.
5. Click on **Generate key** to generate the activation key.

CONTROLCASE   12015 Lee Jackson Memorial Hwy ● Suite 520 ● Fairfax, Virginia 22033 USA
Phone: +1.703.483.6383 (Support/Sales)   www.controlcase.com

P a g e | **4**

6. Copy the Activation and keep it handy. You will be asked to provide the Activation key at the time of CDD Endpoint installation.

Please see the ControlCase Knowledgebase link https://help.controlcase.com/kb/endpoints/ for step-by-step guide on how to install the CDD Endpoints.

POST installation

1. Access the CDD Endpoint software (http://localhost:745/cdd/).
2. Once the endpoint is activated, you can change the credentials for the default user by logging into the CDD Endpoint. The default credentials to login as below.
   Default Username: cdduser
   Default Password: cddpassword
   You will need the login credentials to enter the credentials in the password vault for scanning if you do not wish to enter the credentials in SkyCAM portal.

CONTROLCASE   12015 Lee Jackson Memorial Hwy ● Suite 520 ● Fairfax, Virginia 22033 USA
Phone: +1.703.483.6383 (Support/Sales)   www.controlcase.com
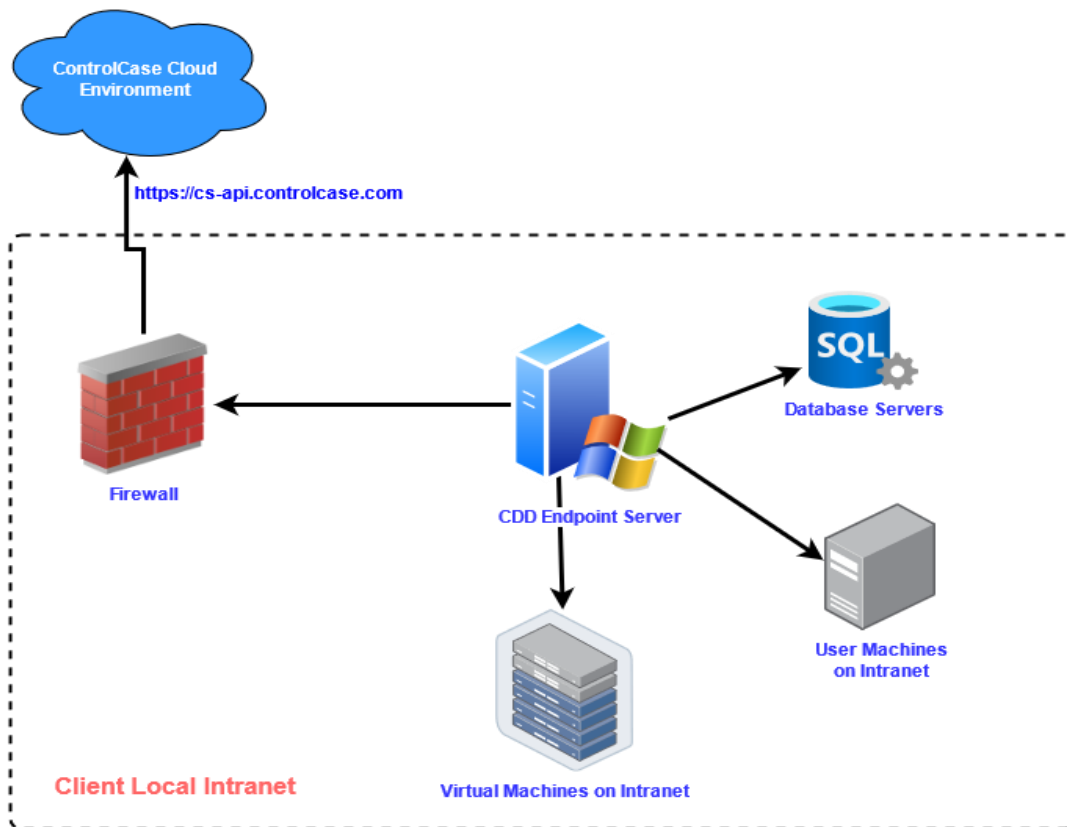
P a g e | **5**

3. FIREWALL RULES

Please open the firewall rule to access the ControlCase API server on port 443.

For more information on how to whitelist the API gateway URL check
https://help.controlcase.com/kb/how-to-whitelist-the-controlcase-api-gateway-url/

- Non-EU environment: https://cs-api.controlcase.com
- Europe (EU) environment: https://cs-api-eu.controlcase.com

Please check https://help.controlcase.com/kb/cdd-installation-guide/ for more details.

Please see below Image for overall data flow diagram.

CONTROLCASE   12015 Lee Jackson Memorial Hwy ● Suite 520 ● Fairfax, Virginia 22033 USA
Phone: +1.703.483.6383 (Support/Sales)   www.controlcase.com

P a g e | **6**

4. DATABASES CLIENTS

CDD has additional requirements for scanning Microsoft Exchange or Database servers. If you are planning to scan these systems, please download/install the appropriate software/Client.

4.1. Oracle

If you plan to scan Oracle databases, CDD now uses the Oracle Instant Client, which immensely simplifies the process of connecting to Oracle databases. You will need to download and install the Oracle Instant Client to scan Oracle databases.

Please download it from https://home.controlcase.com/downloads/Oracle_Instant_Client_11g_R2.exe and run it to install and please accept the default prompts.

4.2. MSSQL Server

If a SQL server is configured to use the protocol TLS version 1.2 or higher version, you need to install the 'SQL Server Native Client' for scanning. Click here to know about how to download, install and configure CDD to use the Native client.

4.3. DB2, Sybase and Informix databases

Sybase, DB2 and Informix scanning requires the appropriate 32-bit client must be installed on the CDD machine. Please visit the ControlCase https://help.controlcase.com/kb/database-prerequisites-and-settings/

CONTROLCASE   12015 Lee Jackson Memorial Hwy ● Suite 520 ● Fairfax, Virginia 22033 USA
Phone: +1.703.483.6383 (Support/Sales)   www.controlcase.com

P a g e | **7**

5. RUNNING A NEW SCAN

To run a scan, you have to login to the web-based console. Please contact the ControlCase to get the access to the ControlCase SkyCAM console.

1. Log into the ControlCase SkyCAM portal.

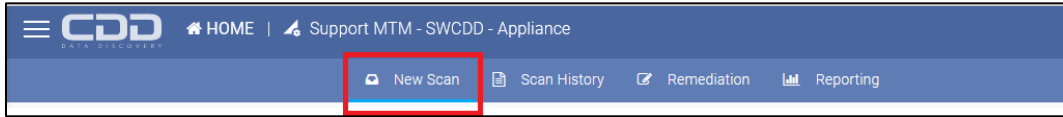2. Select the "Compliance Scanner" from the drop-down menu.
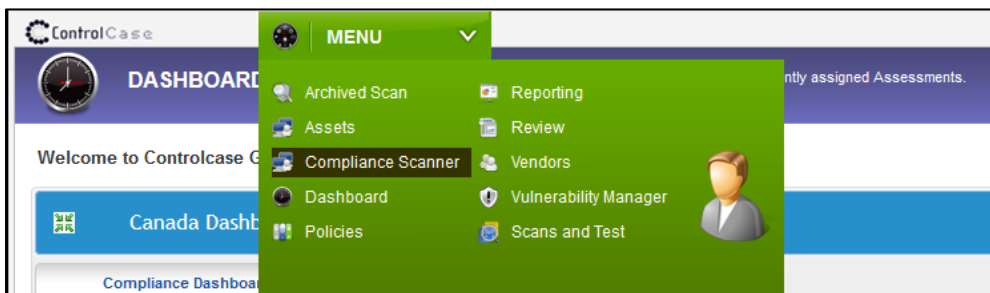
3. From the drop-down select the "CDD".
4. Select the Endpoint which you want to connect to and click Next.

CONTROLCASE   12015 Lee Jackson Memorial Hwy ● Suite 520 ● Fairfax, Virginia 22033 USA
Phone: +1.703.483.6383 (Support/Sales)   www.controlcase.com

P a g e | **8**

5. Select the "New Scan" tab from the top menu.

6. Enter a name (so that you can distinguish among various scans) for the scan and select what you want to scan and then click the "Next" button.
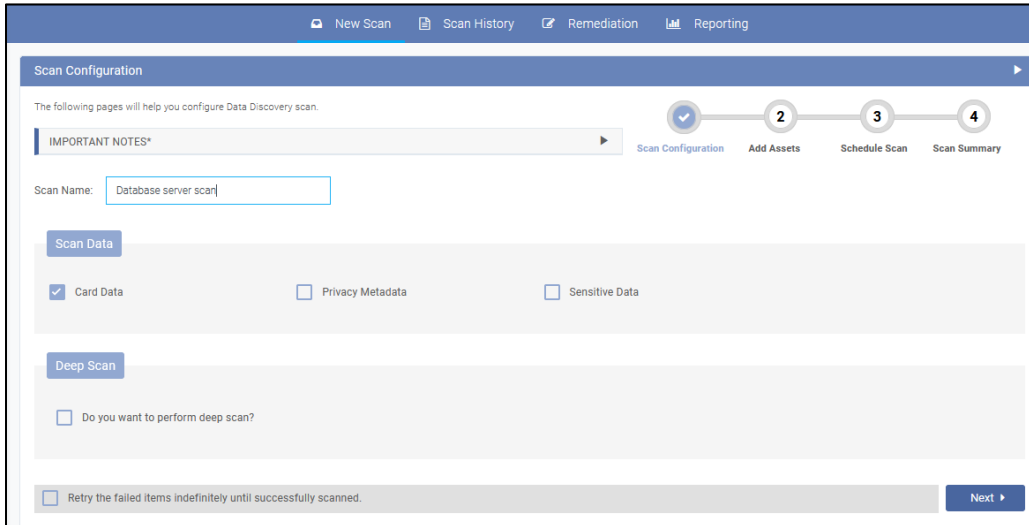
5.1 Supported target types

- **Domain Machines** – To scan hard drives on network computers.
- **Database Servers** – To scan database servers (SQL Server, Oracle, MySQL etc.)
- **Microsoft Exchange Server** –To scan Microsoft Exchange Server mailboxes.
- **Unix Machines** – To scan Unix based operating system machines (Linux, MAC, Sun Solaris etc.)
- **Office 365** – To scan Microsoft Office 365.
  - o **Email**
  - o **SharePoint**
  - o **OneDrive**
- **Amazon S3** – To scan Amazon S3 buckets**.**
- **File Shares** – To scan Files shares/Network drives.
- **IMAP Email Addresses** – To scan IMAP based email addresses like Gmail.
- **SharePoint On**-**Prem** – To scan on premise hosted Microsoft SharePoint.

Please select any of the types as needed and enter the relevant data, the screens provide instructions on what information needs to be entered.

CONTROLCASE   12015 Lee Jackson Memorial Hwy ● Suite 520 ● Fairfax, Virginia 22033 USA
Phone: +1.703.483.6383 (Support/Sales)   www.controlcase.com

P a g e | **9**

5.2 Credentials

The credentials used to authenticate to the target machines to perform the scans are stored in the "Password Vault" in an encrypted state. When scanning a target for the first time, you will need to add the credentials to the Vault.

There are 2 ways to add the credentials for scanning in "Password Vault".

5.2.1 Add credentials on the Skycam portal.

This can be accomplished by clicking the ADD NEW button next to the Credentials.
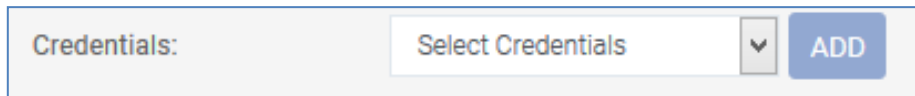
This will bring up another screen where you can add the credentials
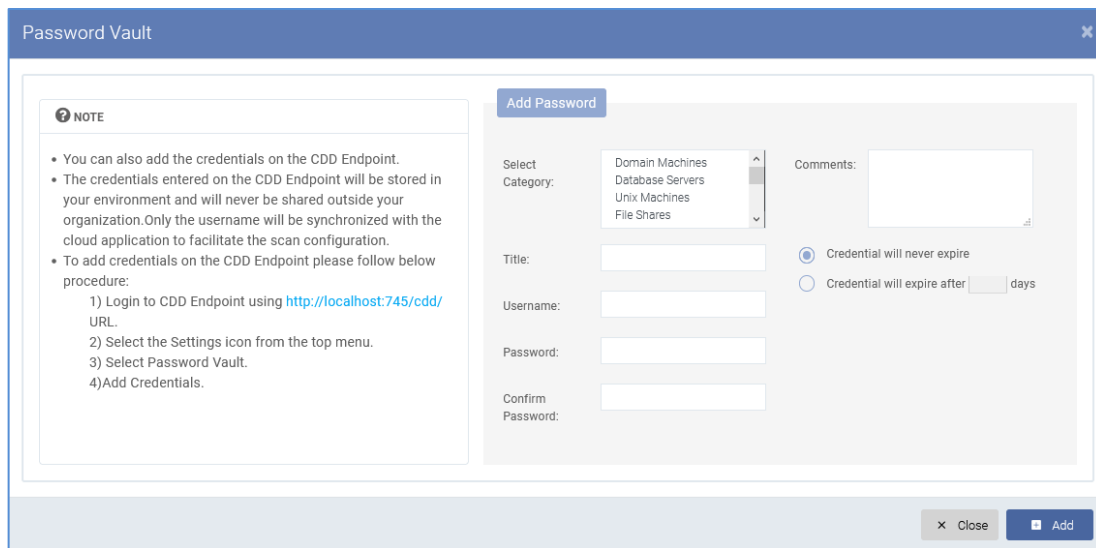
5.2.2 Add credentials on the CDD Endpoint.

If you add credentials to the CDD Endpoint, the credential remains in your environment and only the Title and Username fields synced with the Skycam portal to facilitate the configuration of scan.

To add credentials to the CDD Endpoint.

1. Log in to CDD Endpoint using the default credentials.
    a. Default Username: cdduser
    b. Default Password: cddpassword

CONTROLCASE   12015 Lee Jackson Memorial Hwy ● Suite 520 ● Fairfax, Virginia 22033 USA
Phone: +1.703.483.6383 (Support/Sales)   www.controlcase.com

P a g e | **10**

2. Select settings-> Password Vault and Click on Add button.
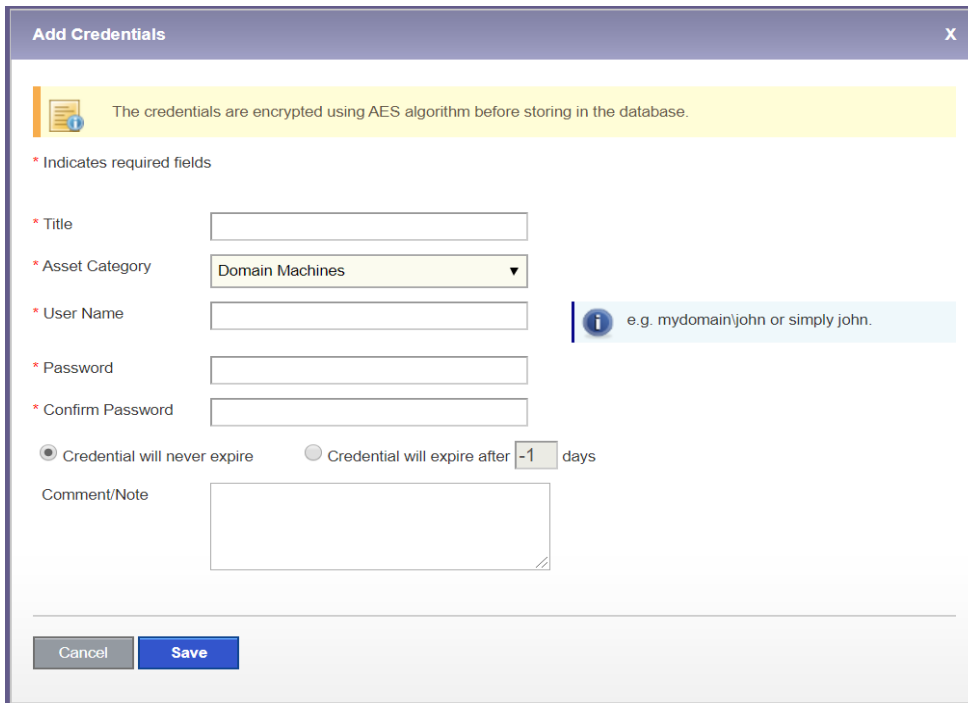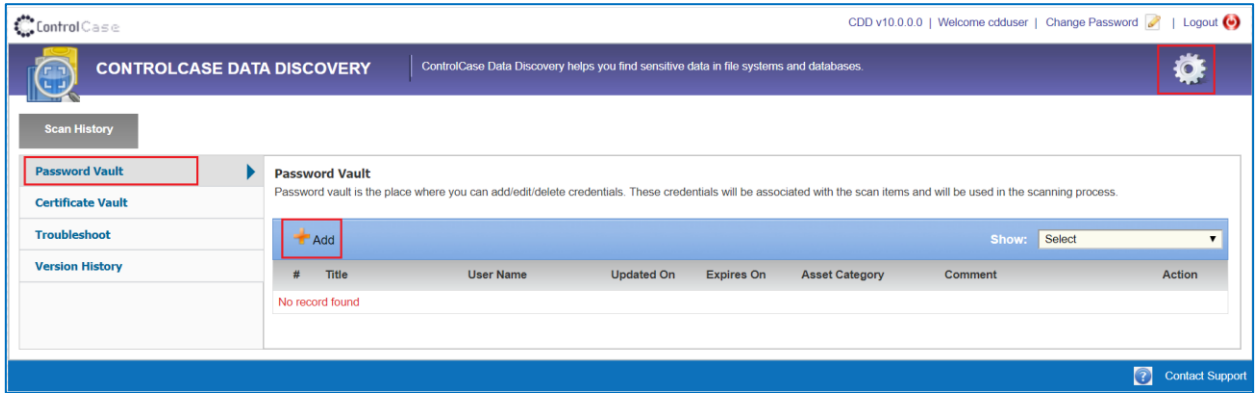
CONTROLCASE   12015 Lee Jackson Memorial Hwy ● Suite 520 ● Fairfax, Virginia 22033 USA
Phone: +1.703.483.6383 (Support/Sales)   www.controlcase.com

P a g e | **11**

5.3 Add Domain Machines

5.4 Add Database Servers

To add new database scans by entering the relevant details on the page. Please follow the instructions on each page for details.
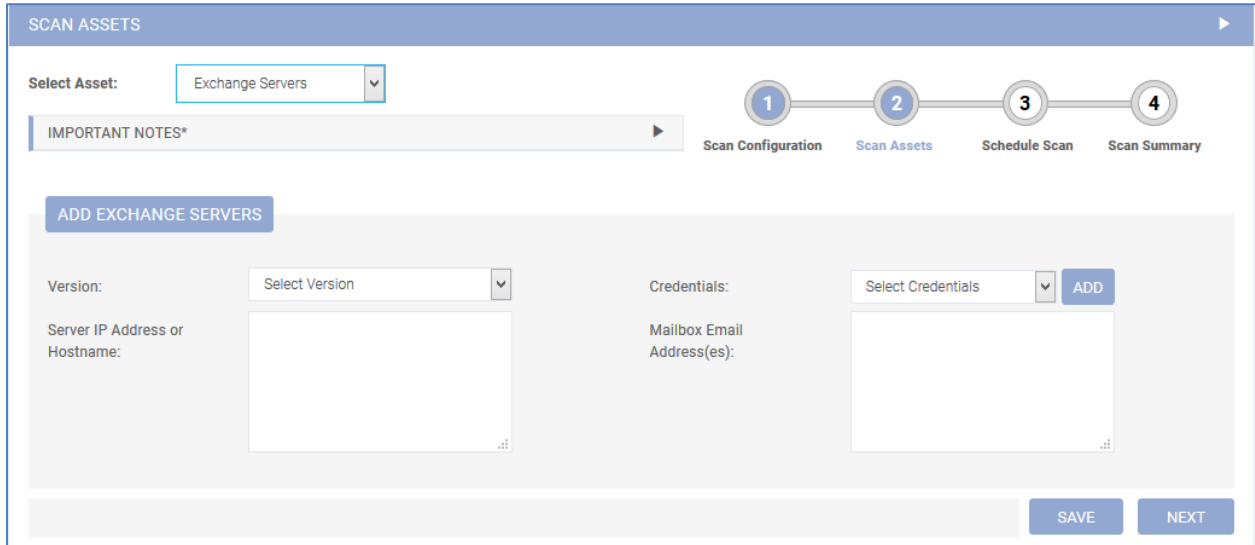
You can keep adding more Database scans by click the "Save" button When you are done, just click the Next button.

CONTROLCASE   12015 Lee Jackson Memorial Hwy ● Suite 520 ● Fairfax, Virginia 22033 USA
Phone: +1.703.483.6383 (Support/Sales)   www.controlcase.com

P a g e | **12**

5.5 Add Microsoft Exchange Servers

To add a new Microsoft Exchange Server scan by entering the relevant details on the page. Please follow the instructions on each page for details.

Please note that 64-bit Microsoft Outlook client must be installed on Exchange server for scanning.

CONTROLCASE   12015 Lee Jackson Memorial Hwy ● Suite 520 ● Fairfax, Virginia 22033 USA
Phone: +1.703.483.6383 (Support/Sales)   www.controlcase.com

P a g e | **13**

5.6 Add Unix Machines

You can add following types of Operating Systems.

1. Linux/Unix and variants
2. MAC OS
3. Solaris X86 and Sparc
4. HP UX
5. AIX
6. FreeBSD

You can keep adding more File system scans by clicking the Save button.

5.7 Add Amazon S3 Buckets

CONTROLCASE   12015 Lee Jackson Memorial Hwy ● Suite 520 ● Fairfax, Virginia 22033 USA
Phone: +1.703.483.6383 (Support/Sales)   www.controlcase.com

P a g e | **14**
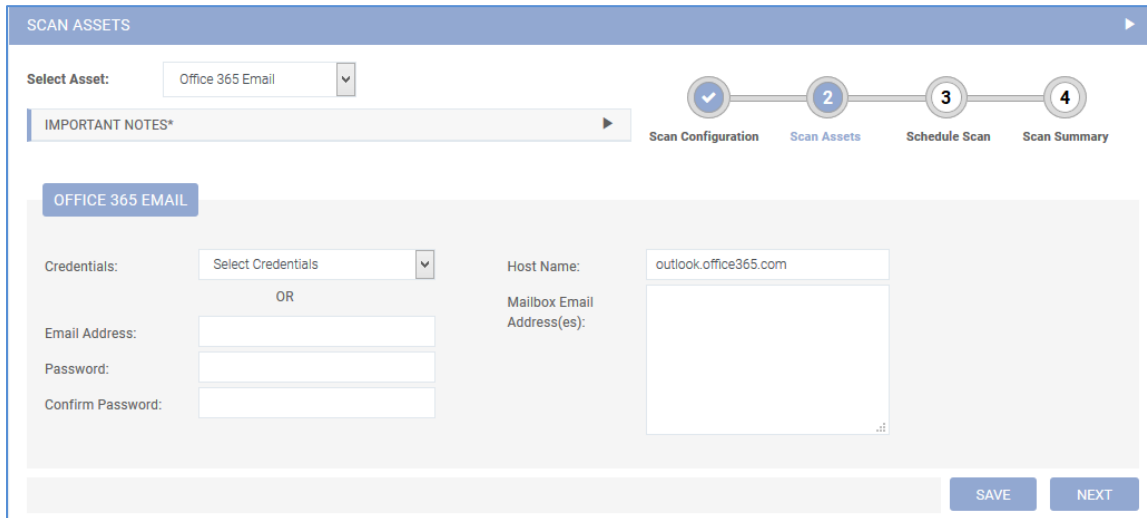
5.8 Add Office 365 targets

Due to the hosted nature of the Office 365 on Microsoft's servers, there are some limitations in the way the scans can occur.

We are unable to scan all mailboxes for all attachments and all sizes because that is not allowed by Microsoft. There are also throttling limits placed by Microsoft which prevent the scanning process.

We need to use a sampling-based approach for mailboxes and emails and those settings can be configured in the Settings area.

5.8.1 Add Office 365 Email

CONTROLCASE   12015 Lee Jackson Memorial Hwy ● Suite 520 ● Fairfax, Virginia 22033 USA
Phone: +1.703.483.6383 (Support/Sales)   www.controlcase.com

P a g e | **15**

5.8.2 Add Office 365 OneDrive

5.8.3 Add Office 365 SharePoint

CONTROLCASE   12015 Lee Jackson Memorial Hwy ● Suite 520 ● Fairfax, Virginia 22033 USA
Phone: +1.703.483.6383 (Support/Sales)   www.controlcase.com

P a g e | **16**
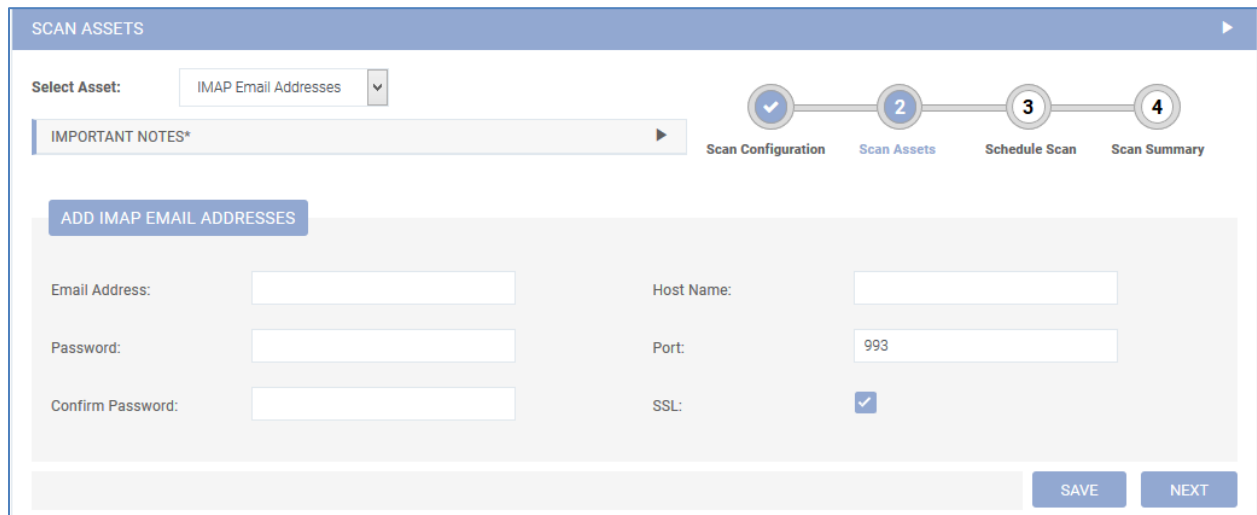
5.9 IMAP Email Addresses
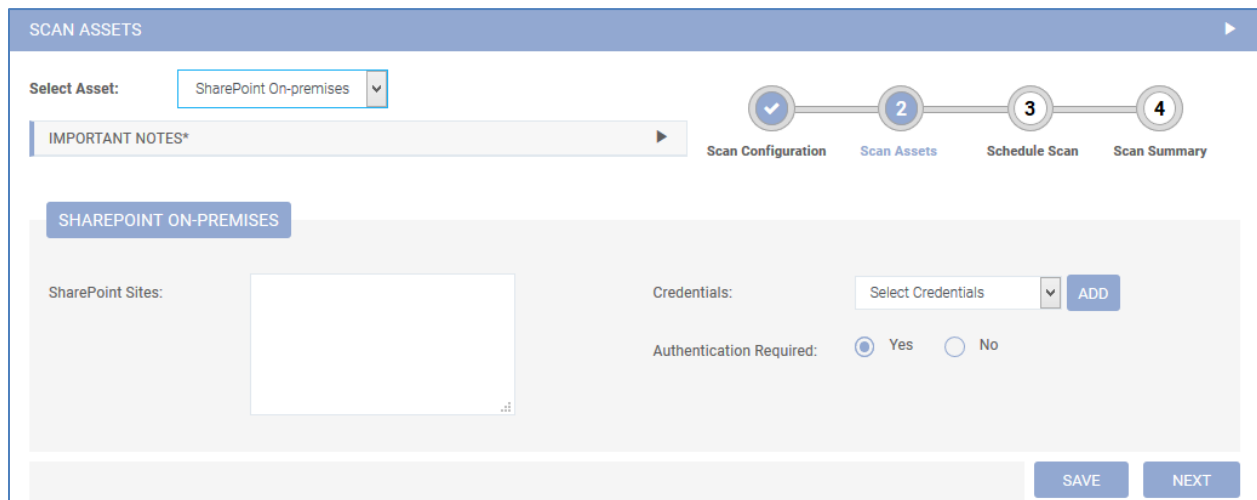
5.10 Add Microsoft SharePoint On-premise

To add a new Microsoft SharePoint On-Premise Server scan by entering the relevant details on the page.

CONTROLCASE   12015 Lee Jackson Memorial Hwy ● Suite 520 ● Fairfax, Virginia 22033 USA
Phone: +1.703.483.6383 (Support/Sales)   www.controlcase.com

P a g e | **17**

5.11 Add File Shares

6. SCHEDULE THE SCAN

You can run the scan now or schedule a scan to later. Please note that the schedule time is displayed in UTC time zone.

CONTROLCASE   12015 Lee Jackson Memorial Hwy ● Suite 520 ● Fairfax, Virginia 22033 USA
Phone: +1.703.483.6383 (Support/Sales)   www.controlcase.com

P a g e | **18**
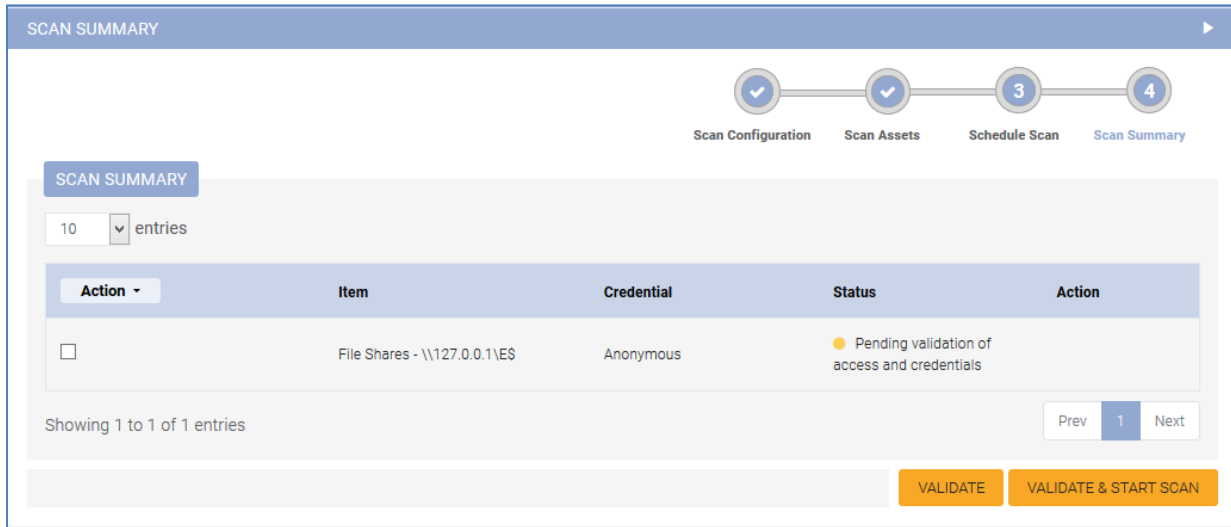
7. START THE SCAN

Click the "**Validate and Start Scan"** button. CDD will then verify the network access and credentials to these targets. Depending upon the number of targets of the scan this may take a few minutes.

If you just want to validate the credentials, click the "**Validate**" button.

CONTROLCASE   12015 Lee Jackson Memorial Hwy ● Suite 520 ● Fairfax, Virginia 22033 USA
Phone: +1.703.483.6383 (Support/Sales)   www.controlcase.com

P a g e | **19**
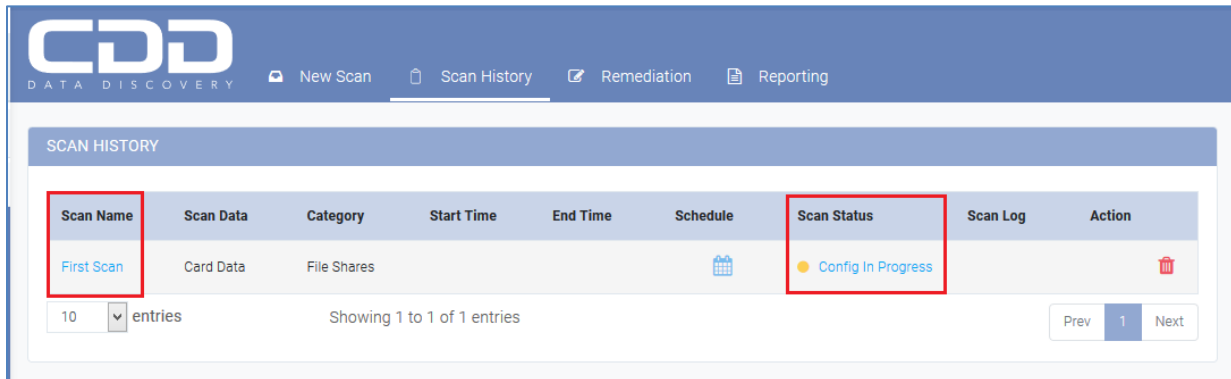
8. VIEW SCAN STATUS/PROGRESS

The progress of the scan can be seen on the next page or by clicking the Scan History tab

Additional details can be seen by clicking the link under the **Scan Status** column.

CONTROLCASE

12015 Lee Jackson Memorial Hwy ● Suite 520 ● Fairfax, Virginia 22033 USA
Phone: +1.703.483.6383 (Support/Sales)   www.controlcase.com

P a g e | **20**
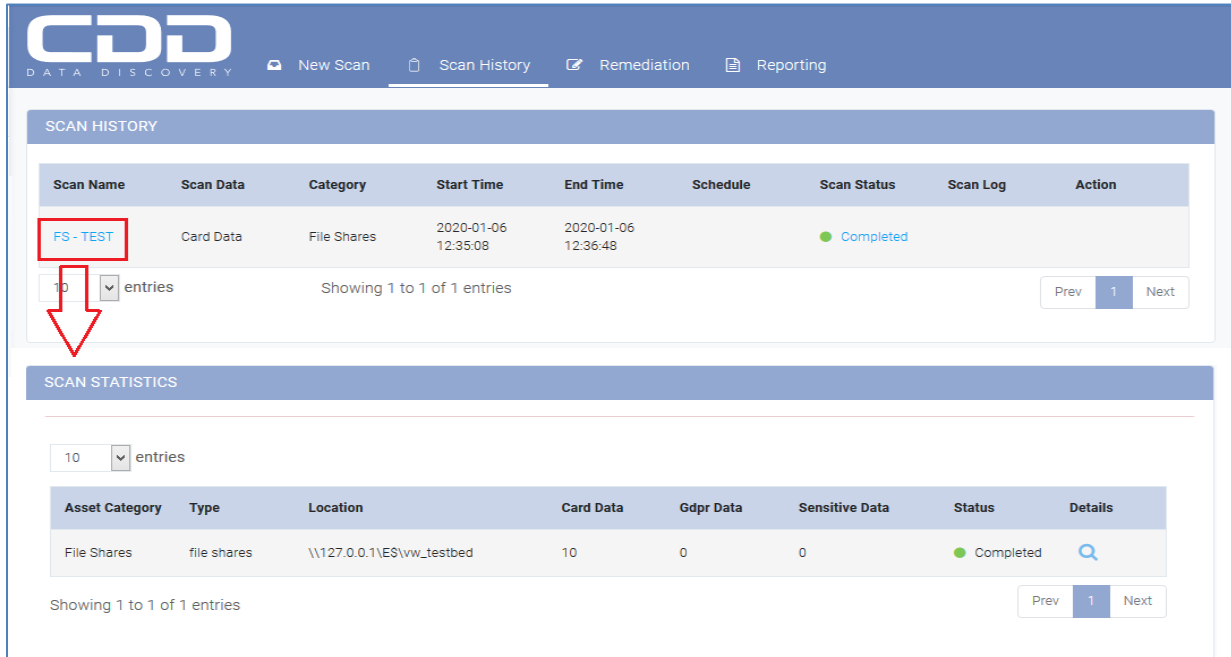
9. VIEW SCAN RESULTS

Once the scan is completed, the results can be seen from the **Scan History** tab. Click on the **Scan Name** to view the scan result.

You can export the result in CSV format by clicking on the **Export** button.

CONTROLCASE   12015 Lee Jackson Memorial Hwy ● Suite 520 ● Fairfax, Virginia 22033 USA
Phone: +1.703.483.6383 (Support/Sales)   www.controlcase.com

P a g e | **22**

10. REMEDIATION

CDD has a Remediation feature which facilitates you to see all the Card/Sensitive data and manage it from the single place. You can use the Remediation tab to export the result in the CSV format or mark the record as False Positive or Remediated.

The records marked as false positive will be excluded from the current and future scans.

The records marked as Remediated will be excluded from the current scan.
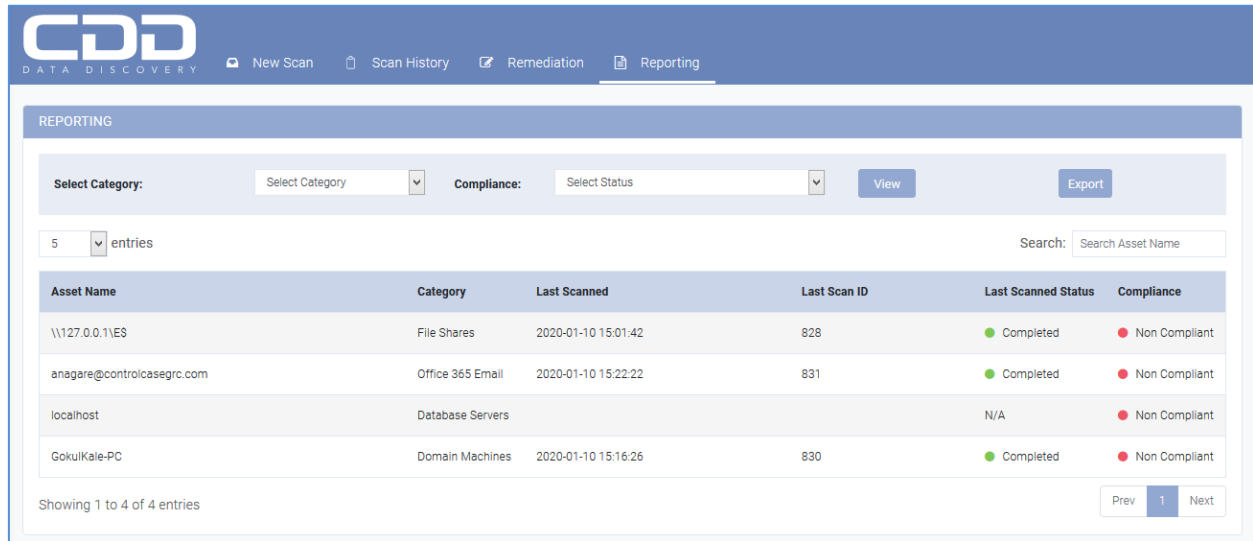
CONTROLCASE   12015 Lee Jackson Memorial Hwy ● Suite 520 ● Fairfax, Virginia 22033 USA
Phone: +1.703.483.6383 (Support/Sales)   www.controlcase.com

P a g e | **23**

11. REPORT GENERATION

We have simplified the compliance report generation process in this version. You can view the compliance status of Assets from the Reporting tab and generate the compliance report in PDF format to upload as an evidence.

CONTROLCASE   12015 Lee Jackson Memorial Hwy ● Suite 520 ● Fairfax, Virginia 22033 USA
Phone: +1.703.483.6383 (Support/Sales)   www.controlcase.com

P a g e | **24**

12. SCANNING TIPS

For successful scans please ensure the following:

<div style="border:1px solid black; text-align:center;">

PLEASE BE PATIENT

</div>

Scanning files and databases over a network does take time because we scan a significant amount of data character by character and the whole process comprises of multiple steps. Please allow the scans to finish rather than terminate them and start over. More information about the speed of scans can be found at 🌐 https://help.controlcase.com/kb/controlcase-data-discovery-performance-statistics/

FILE SCANS

1. For Domain level scans (i.e. scan an entire domain from our scanner) we need an account that has "Administrator" level privileges on target machine. We will need the domain name, username and password
2. For File Share/UNC scans (i.e. to scan only some computers and not the whole domain, or servers that are not part of a domain), we need an account that has local administrator privileges. Again, we will need the server name, username and password
3. Windows File Sharing and Network Discovery needs to be enabled on both the scanner and target machine
4. The scanner machine AND targets being scanned need to have the ADMIN$, C$, D$ etc enabled
5. For scanning MAC OS, SSH needs to be enabled on the MAC (System Preferences -> Sharing – Remote Login setting needs to be on). The scanning user must also have read, write and execute permission on /tmp directory

DATABASE SCANS

1. For SQL Server scans, we will need the credentials (username, password) for an account that has admin/sa level access to the database (In production, we can tweak and lower the access rights needed)

2. For Oracle scans, it is best to have an Oracle DBA available to provide you the correct configuration settings to scan the database (including but not limited to tnsnames files etc.). Please verify that you have the SQL Plus configuration working and you can connect to the database you are trying to scan through SQL Plus first

3. For Sybase scans, please verify that your Sybase client is working, and you can connect to the database using the Sybase client before you use CDD to scan the database. Again, it is best to have a DBA assist you in this process

More information on permissions, firewall ports, protocols etc. required by CDD can be found at 🌐 https://help.controlcase.com/kb/cddsettings/

CONTROLCASE   12015 Lee Jackson Memorial Hwy ● Suite 520 ● Fairfax, Virginia 22033 USA
Phone: +1.703.483.6383 (Support/Sales)   www.controlcase.com

P a g e | **25**

13. TROUBLESHOOTING FAILED SCANS

File Scan Failed? Here are the most common causes:

1. The scanner should be able to connect to the machines it is scanning (targets) using regular Windows networking. Please ensure that this access is possible at the TCP/IP and NetBIOS levels before we attempt scanning these machines with a scanner.

   A good way to test this is to type the target machine name \\target_machine_name\ADMIN$ in the Windows Run box. If that connects with the provided credentials, we will be able to scan the machine.

2. An antivirus/antimalware/application whitelisting or HIDS program on the target is not letting our scan process execute. Please verify that such programs are not interfering with our execution.

CONTROLCASE   12015 Lee Jackson Memorial Hwy ● Suite 520 ● Fairfax, Virginia 22033 USA
Phone: +1.703.483.6383 (Support/Sales)   www.controlcase.com

P a g e | **26**

14. SUPPORT AND HELP

More and latest support articles, tips and troubleshooting information can be found in the ControlCase Knowledge Base at
https://help.controlcase.com/kb/category/cdd/

OR

Contact ControlCase support at https://www.controlcase.com/contact-us/

CONTROLCASE   12015 Lee Jackson Memorial Hwy ● Suite 520 ● Fairfax, Virginia 22033 USA
Phone: +1.703.483.6383 (Support/Sales)   www.controlcase.com

P a g e | **27**