





















# ControlCase™ Data Discovery





Version 10.10  
Updated Jun 2026

## CDD Standalone 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

	Download and Install.....	5
	First Time Login After Installtion .....	7
	Register a new installation and get a License.....	8
	Microsoft Exchange Prerequisites.....	9
	Scanning Oracle Databases :: Oracle client download (Optional).....	9
	Scanning DB2, Sybase and Informix databases (Optional).....	9
	Scanning for Card Data – Running a new scan .....	10
	File System Scans .....	10
	Domain Scan .....	13
	Unix/Linux variants.....	14
	Amazon S3.....	15
	Database scans .....	17
	Microsoft Exchange Server Scans.....	18
	Office 365 Scanning.....	19
	IMAP based Servers.....	23
	Microsoft SharePoint scans (On-premise).....	24
	Start the scan.....	25
	Scan Status.....	26
	View Scan Results .....	27
	CDD False Positive Management and Remediation Feature.....	32

	Scanning tips.....	33
	Troubleshooting Failed scans .....	34
	Known Issues .....	34
	Support and help.....	35



## Prerequisites

Please ensure the following:


1. The CDD Installation machine (scanner machine) needs to be a “**brand new 64-bit**” machine of
  - a. **Windows 2016 or 2019 Server, Windows Server 2022, Windows Server 2025**
  - b. **Windows Server 2012 R2 Service Pack 1**

**We do not support any other operating systems, even if CDD may be installed 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 should be a “true” administrator and have ALL access rights to the machine including but not limited to “Run as Service”, “Install scheduled tasks”, “Access the network”, “RDP inbound”.
6. Visual C++ Redistributable (2015, 2017, 2019, and 2022) from Microsoft Please install **both x86 and x64 versions**.

<https://learn.microsoft.com/en-us/cpp/windows/latest-supported-vc-redist?view=msvc-170>

7. 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/>



## DOWNLOAD AND INSTALL

---

### ★ New Fresh Installation

**Step 1** →

Please download and install the Microsoft Visual C++ Redistributable packages. Kindly install both the x86 and x64 versions using the links provided on the previous page.

**Step 2** →

Please download and install CDD 10.9.3.0 from  
[https://home.controlcase.com/downloads/ControlCase\\_Data\\_Discovery\\_V10.9.3.0\\_Installer.exe](https://home.controlcase.com/downloads/ControlCase_Data_Discovery_V10.9.3.0_Installer.exe)

**Step 3** →

Then download and install CDD 10.10.0.0 Upgrade Patch from  
[https://home.controlcase.com/downloads/ControlCase\\_Data\\_Discovery\\_V10.10.0.0\\_Update.exe](https://home.controlcase.com/downloads/ControlCase_Data_Discovery_V10.10.0.0_Update.exe)

**Step 4** →

Then download and install CDD 10.10.1.0 Upgrade Patch from  
[https://home.controlcase.com/downloads/ControlCase\\_Data\\_Discovery\\_V10.10.1.0\\_Update.exe](https://home.controlcase.com/downloads/ControlCase_Data_Discovery_V10.10.1.0_Update.exe)

**Step 5** →

Then download and install CDD 10.10.2.0 Upgrade Patch from  
[https://home.controlcase.com/downloads/ControlCase\\_Data\\_Discovery\\_V10.10.2.0\\_Update.exe](https://home.controlcase.com/downloads/ControlCase_Data_Discovery_V10.10.2.0_Update.exe)

### ★ Upgrades and (New Installs with Migration)

**Step 1** →

Please download and install the Microsoft Visual C++ Redistributable packages. Kindly install both the x86 and x64 versions using the links provided on the previous page.

**Step 2** →

Please download and install CDD 10.9.0.1 from  
[https://home.controlcase.com/downloads/ControlCase\\_Data\\_Discovery\\_V10.9.0.1\\_Installer.exe](https://home.controlcase.com/downloads/ControlCase_Data_Discovery_V10.9.0.1_Installer.exe)

**Step 3** →

Then download and install CDD 10.9.2.0 Upgrade Patch from  
[https://home.controlcase.com/downloads/ControlCase\\_Data\\_Discovery\\_V10.9.2.0\\_Update.exe](https://home.controlcase.com/downloads/ControlCase_Data_Discovery_V10.9.2.0_Update.exe)

**Step 4** →

Perform the migration steps, confirm them by logging in, and then install the 10.9.3.0 patch mentioned below (**Note:** These steps must be performed when you have an existing older version (8.6 or 10.7) and need to migrate data from the older version to the newer version.)

**Step 5** →

Then download and install CDD 10.9.3.0 Upgrade Patch from  
[https://home.controlcase.com/downloads/ControlCase\\_Data\\_Discovery\\_V10.9.3.0\\_Update.exe](https://home.controlcase.com/downloads/ControlCase_Data_Discovery_V10.9.3.0_Update.exe)

**Step 6** →

Then download and install CDD 10.10.0.0 Upgrade Patch from  
[https://home.controlcase.com/downloads/ControlCase\\_Data\\_Discovery\\_V10.10.0.0\\_Update.exe](https://home.controlcase.com/downloads/ControlCase_Data_Discovery_V10.10.0.0_Update.exe)

**Step 7** →

Then download and install CDD 10.10.1.0 Upgrade Patch from  
[https://home.controlcase.com/downloads/ControlCase\\_Data\\_Discovery\\_V10.10.1.0\\_Update.exe](https://home.controlcase.com/downloads/ControlCase_Data_Discovery_V10.10.1.0_Update.exe)

**Step 8** →

Then download and install CDD 10.10.2.0 Upgrade Patch from  
[https://home.controlcase.com/downloads/ControlCase\\_Data\\_Discovery\\_V10.10.2.0\\_Update.exe](https://home.controlcase.com/downloads/ControlCase_Data_Discovery_V10.10.2.0_Update.exe)

## ★ Upgrades from Previous installed versions



Please DO NOT upgrade the CDD while a scan is running.

If you are upgrading from any other versions, please contact [ControlCase](#) support for instructions.



If you already have an older version of CDD installed and try to install a brand-new instance, you will be prompted to uninstall the older version. If you do so, you will LOSE all your existing CDD data.

To preserve your existing CDD data, please upgrade by installing a new version.

## ★ Migration Steps from CDD Standalone version v8.6 to v10.9

### Pre-requisites

- Verify if the CDD 8.6.10 is installed or not.
- Verify if the CDD 10.9.0.1 and 10.9.0.2 patch is installed or not.

Then download and install **CDD\_V8.6\_to\_10.9.2\_data\_migration** Patch from [https://s3.amazonaws.com/home.controlcase.com/downloads/CDD\\_V8.6\\_to\\_10.9.2\\_data\\_migration.exe](https://s3.amazonaws.com/home.controlcase.com/downloads/CDD_V8.6_to_10.9.2_data_migration.exe)

## ★ Migration Steps from CDD Standalone version v10.7 to v10.9

### Pre-requisites

- Verify if the CDD 10.7 is installed or not.

Then download and install **CDD\_V10.7\_to\_10.9.2\_Migration** Patch from [https://home.controlcase.com/downloads/CDD\\_V10.7\\_to\\_10.9.2\\_Migration.exe](https://home.controlcase.com/downloads/CDD_V10.7_to_10.9.2_Migration.exe)



## FIRST TIME LOGIN AFTER INSTALLTION

---

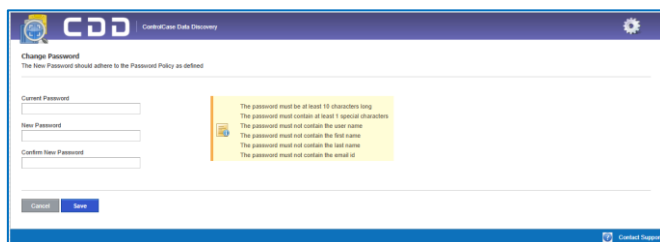
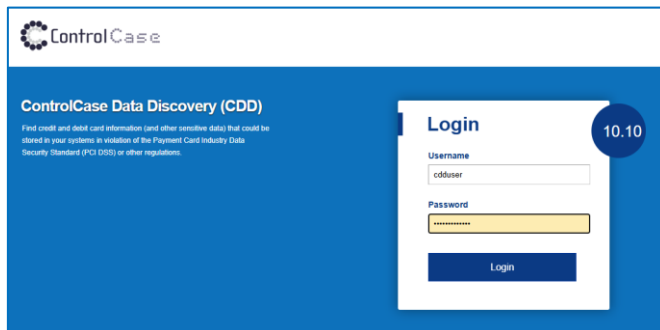
Once the **CDD Standalone version** is installed, you will be redirected to the CDD login page in your default browser. The URL <http://localhost:845/> will open automatically.

Log in using the default credentials provided below. After logging in for the first time, you will be prompted to set your desired credentials. Once the credentials are set, log in again using the newly created credentials.

The password will be valid for 90 days, after which it must be reset or changed. You will receive a notification before the password expires, and the reset must be performed using the same password reset method.

### Default Credentials:

- Default Username: cdduser
- Default Password: cddpassword

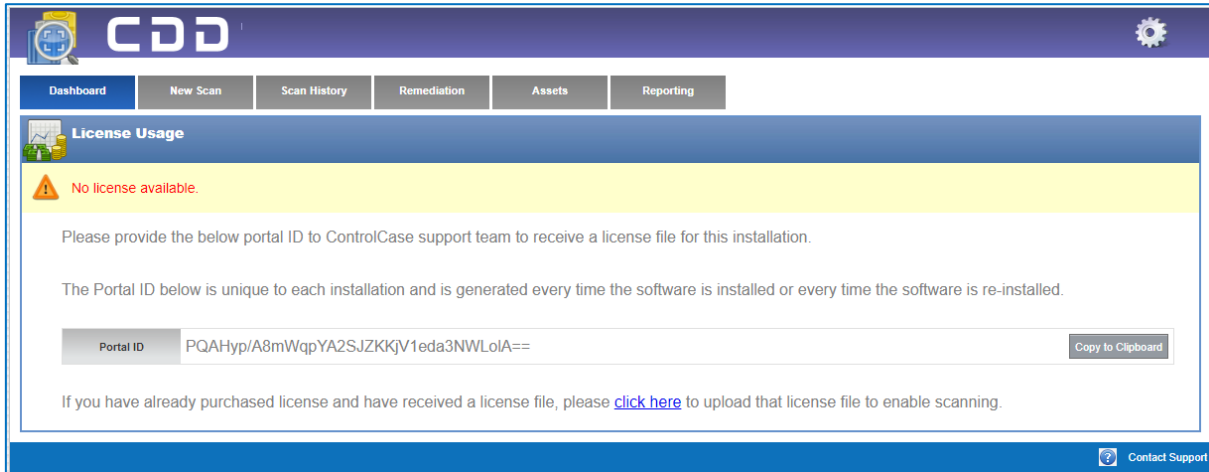


**Note:** The password must meet the following criteria:

- Must be at least 10 characters long
- Must include at least one special character
- Must not contain the username
- Must not contain the first name
- Must not contain the last name
- Must not contain the email ID

 **REGISTER A NEW INSTALLATION AND GET A LICENSE**

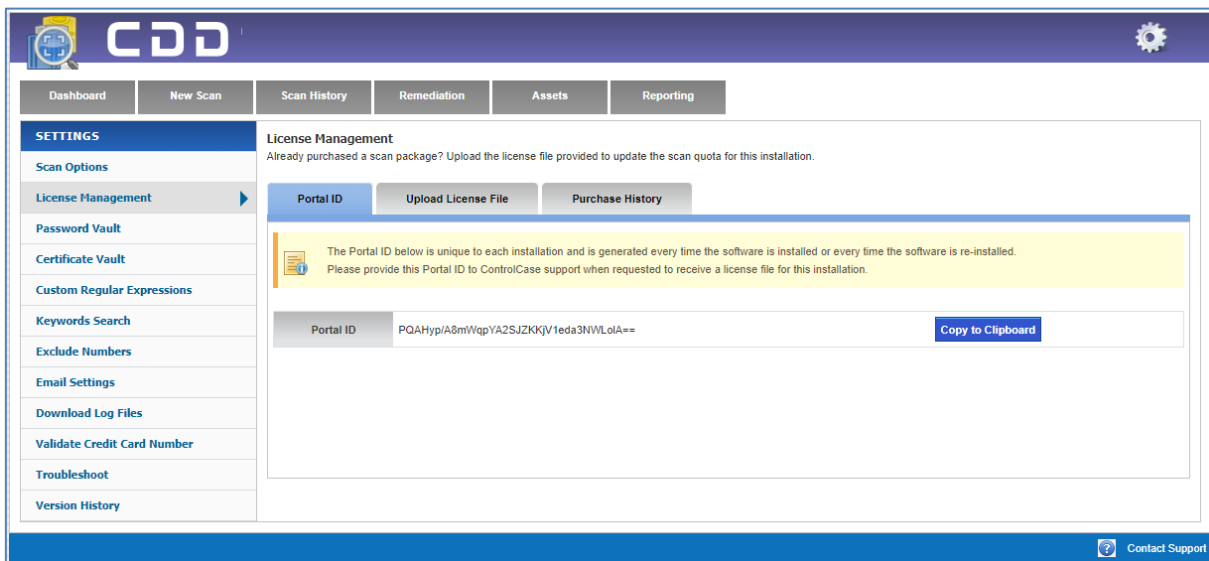
If you installed a new version of CDD (did not upgrade an existing install), you **will need a license key** to activate the product and start scanning. (see picture below). Please contact [ControlCase](#) to obtain the license key.



The screenshot shows the CDD web interface. At the top, there's a navigation bar with tabs: Dashboard, New Scan, Scan History, Remediation, Assets, and Reporting. Below this is a 'License Usage' section with a yellow warning banner that says 'No license available.' Below the banner, there's a text box with the Portal ID: PQAHyp/A8mWqpYA2SJZKQV1eda3NWLolA== and a 'Copy to Clipboard' button. A 'Contact Support' link is visible in the bottom right corner.

 **License keys are specific to every installation of CDD and are NOT portable. You will need a new license key if you reinstall CDD.**

ControlCase will provide you a license file through email, which you will need to upload back to CDD using the Settings tab -> License Management and "Upload License File" page. Save the file onto your hard disk and then select that file using the Browse. Button and click UPLOAD.



The screenshot shows the CDD web interface with the 'Settings' tab selected. Under 'Settings', the 'License Management' option is highlighted. The 'License Management' page has a sub-section 'License Management' with a text box asking to upload a license file. Below this, there's a yellow information banner with the same Portal ID: PQAHyp/A8mWqpYA2SJZKQV1eda3NWLolA== and a 'Copy to Clipboard' button. A 'Contact Support' link is visible in the bottom right corner.

## MICROSOFT EXCHANGE PREREQUISITES

---

Exchange comes with a specific list of prerequisites which need to be met fully for scans to work.

1. The Exchange management console and Windows PowerShell must be installed on the Exchange server.
2. **The 64-bit Outlook client must be installed on the Exchange server.**
3. The scanning user must have a mailbox on the Exchange server.
4. The scanning user must have the right to create a network share on the target machine.
5. The scanning user must have the right to retrieve the list of mailboxes. (Organization management, Exchange management and import/export mailbox).
6. The scanning user must have the right to export the mailboxes being scanned.
7. The scanning user must have a right to create a Windows Service and run the required executables on the Exchange server.
8. The Server must have enough empty hard disk/drive space on any local drive to export the mailbox (**At least 50GB of free space at a minimum and 100GB free space is recommended in most cases. However, extremely large mailboxes will need more space**).



## SCANNING ORACLE DATABASES :: ORACLE CLIENT DOWNLOAD (OPTIONAL)

---

If you do not plan to scan Oracle Databases, you can skip this download.

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](https://home.controlcase.com/downloads/Oracle_Instant_Client_11g_R2.exe) and run it to install and please accept the default prompts.



## SCANNING DB2, SYBASE AND INFORMIX DATABASES (OPTIONAL)

---

These databases also require a local DB client to be installed. Please contact [ControlCase](#) to get instructions on how to download and install the clients.



## SCANNING FOR CARD DATA – RUNNING A NEW SCAN

Once you are done uploading the license file, please click the New Scan tab to add new scans.

Enter a name (so that you can distinguish among various scans) for the scan and keep the default scan type “Rapid Scan” checked and then click the “Configure New Scan” button.

**Scan Configuration**

The following pages will help you configure ControlCase Data Discovery and help discover unencrypted and sensitive data in file systems and databases.

1 — 2 — 3 — 4  
 Scan Configuration   Scan Assets   Schedule Scan   Scan Summary

**IMPORTANT NOTES \***

Insert Scan Name:

**Scan Data**

Card Data    
  GDPR Data i    
  Sensitive Data

**Scan Type**

Rapid Scan    
  Deep Scan i

**Scan Mode**

Automatic    
  Manual i

Retry the failed items indefinitely until successfully scanned.

[Configure New Scan](#)

The major target types we scan are:

- **File System Scans** – Used to scan hard drives on local and network computers for many operating systems (Windows, Linux, MACs, Solaris etc.)
- **Database Scans** – Used to scan databases (SQL Server, Oracle etc.)
- **Email Server Scans** – Used to scan Microsoft Exchange Servers, Office 365, IBM Notes and IMAP
- **Application Servers** – Used to scan SharePoint servers



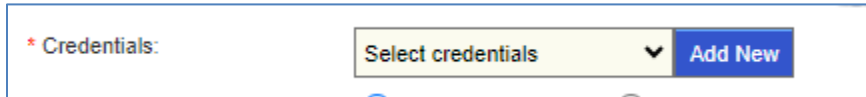
### File System Scans

If you want to scan File systems, you can add 6 types of scans

- Scan local hard disks (attached to the scanning computer)
- Scan File Shares/ Network drives (UNC scans)
- Scan the whole Windows Domain (Active Directory)
- Scan Unix/Linux variants, MAC machines
- Scan Amazon S3 buckets.
- Scan Mainframe files on a File Server (exported samples set of files)

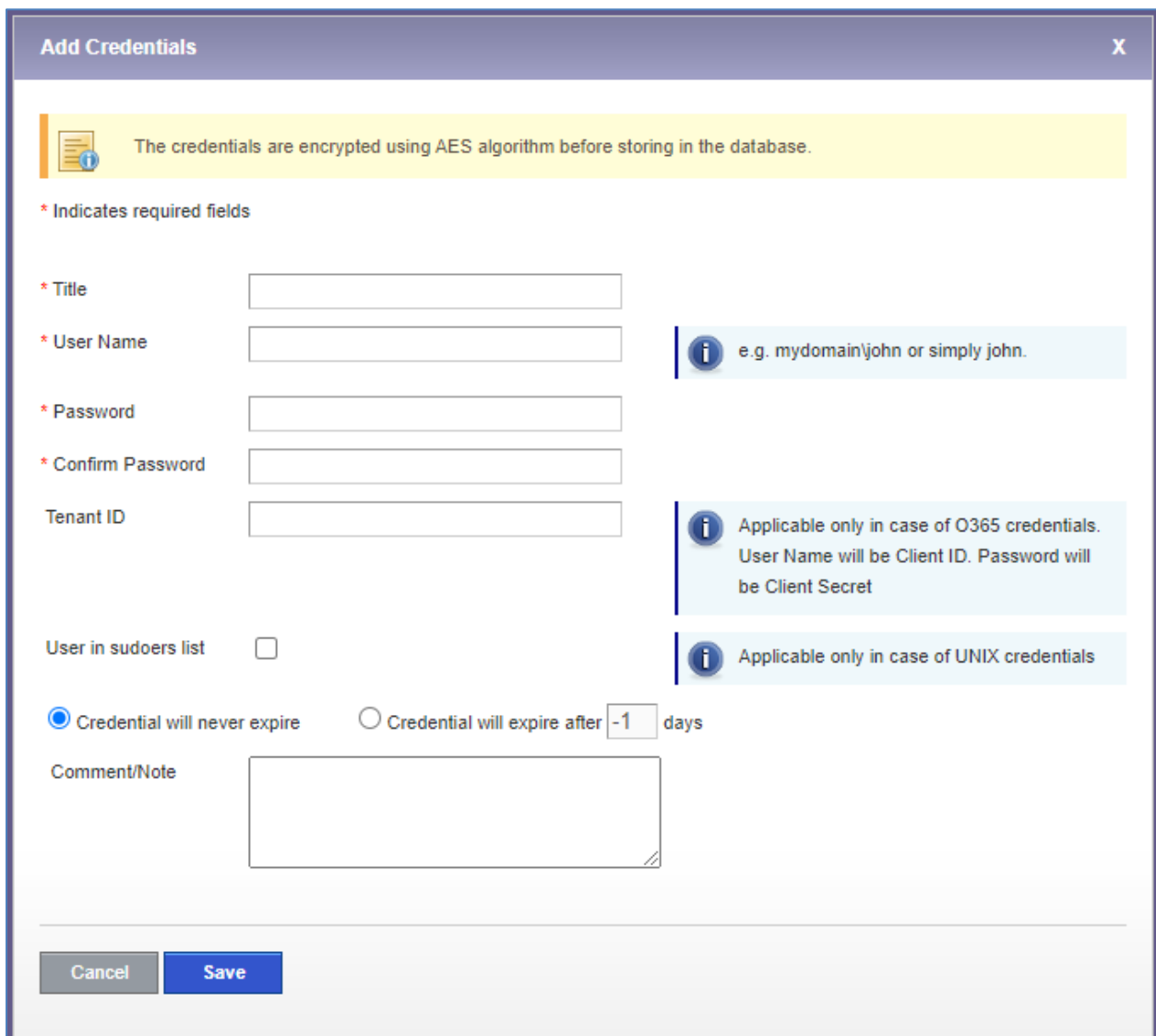
Please select any of the types as needed and enter the relevant data, the screens provide instructions on what information needs to be entered.

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. This can be accomplished by clicking the ADD NEW button next to the Credentials



\* Credentials: Select credentials Add New

This will bring up another screen where you can add the credentials.



**Add Credentials** [X]

The credentials are encrypted using AES algorithm before storing in the database.

\* Indicates required fields

\* Title

\* User Name  e.g. mydomain\john or simply john.

\* Password

\* Confirm Password

Tenant ID  Applicable only in case of O365 credentials. User Name will be Client ID. Password will be Client Secret

User in sudoers list  Applicable only in case of UNIX credentials

Credential will never expire  Credential will expire after  days

Comment/Note

Cancel Save

## File Share (Network Drive)

**File Shares**

Please enter the file share details. File share locations added will be scanned for sensitive data.

**1** Scan Configuration | **2** Scan Assets | **3** Schedule Scan | **4** Scan Summary

You have 10 file system assets remaining.

**IMPORTANT NOTES \***

**Add File Shares**

\* File Share Name:

Connect as an anonymous user:

\* Credentials:

\* Scan Scope:

**i** Examples:  
1. \\ComputerName\SharedDirectory - \\192.168.10.52\Public\SharedDocs  
2. \\ComputerName\Drive - \\192.168.10.52\DS  
Enter multiple file shares separated by commas.

**i** If the network share(s) doesn't need credentials to be accessed, check this box.

**i** 1. Scan Scope allows you to define which files should be scanned.  
2. You can define a Scan Scope to exclude files from scanning based on their Creation or Modification time.  
3. Default Scan Scope is *Scan All Files* which will scan all files irrespective of their Creation or Modification time.

## Domain Scan

### Domain Machines

Please enter the domain/Workgroup machine details. Machines added will be scanned for sensitive data.

**1** Scan Configuration   **2** Scan Assets   **3** Schedule Scan   **4** Scan Summary

You have 10 file system assets remaining.

**IMPORTANT NOTES \***

#### Add Domain Machines

\* Domain Name:

\* Credentials:

\* Scan:  Specific IP/Host(s)    Whole Domain

**i** Enter multiple IP address or host names separated by commas or newline. You can also enter the IP range like 10.84.202.1-10.84.202.100.

\* Select Drive Types:  Fixed Drive    Removable Drive

**i** Selected input drive(s) matching with drive type(s) will be scanned.

\* Select Drive(s):  All Drives    Drive(s)    Folder

\* Scan Scope:

**i** 1. Scan Scope allows you to define which files should be scanned.  
2. You can define a Scan Scope to exclude files from scanning based on their Creation or Modification time.  
3. Default Scan Scope is *Scan All Files* which will scan all files irrespective of their Creation or Modification time.

Unix Machines

Please enter the unix machine details. Machines added will be scanned for sensitive data.

**1** Scan Configuration   **2** Scan Assets   **3** Schedule Scan   **4** Scan Summary

You have 10 file system assets remaining.

**IMPORTANT NOTES**

**Add Unix Machines**

\* Operating System:

\* OS Bit:  64 Bit    32 Bit

\* IP Address or Host Name:

\* Connect using:  Credentials    Certificate

\* Credentials:

User is in the sudoers list:

\* Select Drive:

Subfolder:

\* SSH Port:

\* Scan Scope:

**Info:** Enter multiple IP address or host names separated by commas.

**Info:** Selected drive will be scanned on the target machine.

**Info:** Enter the absolute folder path without drive name. Multiple Subfolder are not allowed.

**Info:** 1. Scan Scope allows you to define which files should be scanned.  
2. You can define a Scan Scope to exclude files from scanning based on their Creation or Modification time.  
3. Default Scan Scope is *Scan All Files* which will scan all files irrespective of their Creation or Modification time.

You can add the 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 click the Add more ... button

### Amazon S3

Please enter the Amazon S3 bucket details. Amazon S3 buckets added will be scanned for sensitive data.

**1** Scan Configuration | **2** Scan Assets | **3** Schedule Scan | **4** Scan Summary


 You have 10 Amazon S3 scans remaining.


#### Add Amazon S3

\* Credentials:

\* Region Endpoint:

\* Bucket Name(s):

 Enter only domain name of Region Endpoint. Do not add bucket name in Region Endpoint name.  
Example: If Amazon S3 URL is `http://s3-aws-region.amazonaws.com/bucket` then enter Region Endpoint as `s3-aws-region.amazonaws.com`

 Enter multiple bucket names separated by commas.

## Mainframe file formatted files (EBCDIC)

**EBCDIC Files**

Please enter the file share details. File share locations added will be scanned for sensitive data. The scanner will treat all the files as EBCDIC encoded.

**1** Scan Configuration    **2** Scan Assets    **3** Schedule Scan    **4** Scan Summary

You have 10 file system assets remaining.

**Add EBCDIC File Shares**

\* File Share Name:

Connect as an anonymous user:

\* Credentials:

**Examples:**

- 1. \\ComputerName\SharedDirectory - \\192.168.10.52\Public\SharedDocs
- 2. \\ComputerName\Drive - \\192.168.10.52\DS

Enter multiple file shares separated by commas.

If the network share(s) doesn't need credentials to be accessed, check this box.

CDD cannot directly scan Mainframe computers, but a sample set of files exported from the mainframes in EBCDIC format can be placed on a file share and then CDD can scan those files.

When you are done (or if you don't want to add any file system scans, just click more targets on the Left navigation pane i.e. Database Servers or Scan Configuration Summary to add Databases scans or start the scan)



## Database scans

To add new database scans by entering the relevant details on the page. Please follow the instructions on each page for details.

Database Servers

Please enter the database server details. Database servers added will be scanned for sensitive data.

1 2 3 4  
Scan Configuration Scan Assets Schedule Scan Scan Summary

You have 10 database server assets remaining.

**IMPORTANT NOTES \***

**Add Database Servers**

\* Database Type:

\* Authentication Type:

\* Credentials:

Non-Default Port Number:

\* IP Address or Host Name:

\* Scan:  Complete Server  Specific Database/Table(s)

**i** Enter multiple database servers separated by commas.

1. For ORACLE scanning enter the IP Address\Service Name.
2. For DB2 scanning enter the IP Address/Database Name.
3. For INFORMIX scanning enter the IP address\Informix Server Name.
4. For SQL Server with names instance, enter the IP address\Instance Name.
5. In all other cases enter the IP address or database server name.

Please consult your DBA to get the details of databases names and settings that need to be entered here.

You can keep adding more Database scans by click the “Add more Databases” button, when you are done (or if you don’t want to scan any databases, just click the Scan Configuration Summary to start the scan)

## Microsoft Exchange Server Scans

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.

### Exchange Servers

Please enter the exchange server details. Exchange servers added will be scanned for sensitive data.

**1** Scan Configuration   **2** Scan Assets   **3** Schedule Scan   **4** Scan Summary

You have 10 exchange server assets remaining.

**IMPORTANT NOTES \***

#### Add Exchange Servers

\* Version:

\* Server IP Address or Host Name:

\* Credentials:

Mailbox Email Address(es):

**i** Enter multiple IP address or host names separated by commas.

**i** To scan specific mailboxes, enter the Mailbox Email addresses separated by a newline. Please note that Mailbox Email addresses are *Case Insensitive*. Visit the [ControlCase KnowledgeBase](#) to view more information on how to obtain the mailbox list.

## Office 365 Scanning

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

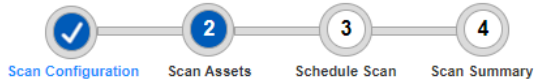
We are unable to scan all mailboxes for all attachments and all sizes because that is not allowed by Microsoft. There are also throttling limits placed by Microsoft which prevent the scanning process.


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


### Office 365 Email

Office 365 Email

Please enter office 365 email details. Office 365 email addresses added will be scanned for sensitive data.



 You have 10 Office 365 Email assets remaining.

**IMPORTANT NOTES \*** 

**Credentials**

\* Tenant ID:

\* Client ID:

\* Client Secret Key:

**Validate Now**

**Next**

### Office 365 Email

Please enter office 365 email details. Office 365 email addresses added will be scanned for sensitive data.

✓ ✓ **3** 4  
Scan Configuration   Scan Assets   Schedule Scan   Scan Summary

**You have 10 Office 365 Email assets remaining.**

**IMPORTANT NOTES \***

**Credentials**

\* Credentials:

**Mailbox**

Credentials successfully validated. [Click here](#) to download mailbox email address list.

Mailbox Email Address(es):

**i** To scan specific mailbox, enter the mailbox email addresses separated by a newline or upload mailbox email address CSV file.

OR

## Office 365 OneDrive

Office 365 OneDrive

Please enter office 365 onedrive details. Office 365 onedrive addresses added will be scanned for sensitive data.

✓

Scan Configuration

2

Scan Assets

3

Schedule Scan

4

Scan Summary

You have 10 Office 365 OneDrive assets remaining.

**IMPORTANT NOTES \*** ▶

**Credentials**

\* Tenant ID:

\* Client ID:

\* Client Secret Key:

[Validate Now](#)

[Next](#)

Office 365 OneDrive

Please enter office 365 onedrive details. Office 365 onedrive addresses added will be scanned for sensitive data.

✓

Scan Configuration

✓

Scan Assets

3

Schedule Scan

4

Scan Summary

You have 10 Office 365 OneDrive assets remaining.

**IMPORTANT NOTES \*** ▶

**Credentials**

\* Credentials:  ... -> 2:1 . v

**Mailbox**

Credentials successfully validated. [Click here](#) to download mailbox email address list.

Mailbox Email Address(es):

OR

To scan specific OneDrive, enter the mailbox email addresses separated by a newline or upload mailbox email address CSV file.


Save


Next

## Office 365 SharePoint

Office 365 SharePoint

Please enter office 365 sharepoint details. Office 365 sharepoint sites added will be scanned for sensitive data.



 You have 10 Office 365 SharePoint assets remaining.

**IMPORTANT NOTES \*** ▶

**Credentials**

\* Tenant ID:

\* Client ID:


\* Client Secret Key:


[Validate Now](#)

[Next](#)

Office 365 SharePoint

Please enter office 365 sharepoint details. Office 365 sharepoint sites added will be scanned for sensitive data.



 You have 10 Office 365 SharePoint assets remaining.

**IMPORTANT NOTES \*** ▶


**Credentials**

\* Credentials:  [-] [-> 2!]

**Add SharePoint Site(s)**

Credentials successfully validated. [Click here](#) to download site list.

Site(s):

 To scan specific SharePoint site, enter the site separated by a newline or upload SharePoint sites CSV file.

OR


[Save](#)
[Next](#)

## @ IMAP based Servers

### IMAP Email Addresses


Please enter IMAP email address details. IMAP email addresses added will be scanned for sensitive data.

**1** Scan Configuration   **2** Scan Assets   **3** Schedule Scan   **4** Scan Summary

 You have 10 email assets remaining.

**IMPORTANT NOTES \***

#### Add IMAP Email Addresses

* Email Address:	<input type="text"/>	 This may take a moment; the system will try logging in to the mail server to validate the entered login information.
* Password:	<input type="password"/>	
* Confirm Password:	<input type="password"/>	
* Host Name:	<input type="text"/>	
Port:	<input type="text" value="993"/>	
SSL:	<input checked="" type="checkbox"/>	

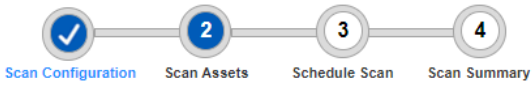
**Save**   **Next**


## Microsoft SharePoint scans (On-premise)

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

SharePoint On-premises

Please enter the SharePoint site details. SharePoint site added will be scanned for sensitive data.



 You have 10 SharePoint assets remaining.

### Add SharePoint Sites

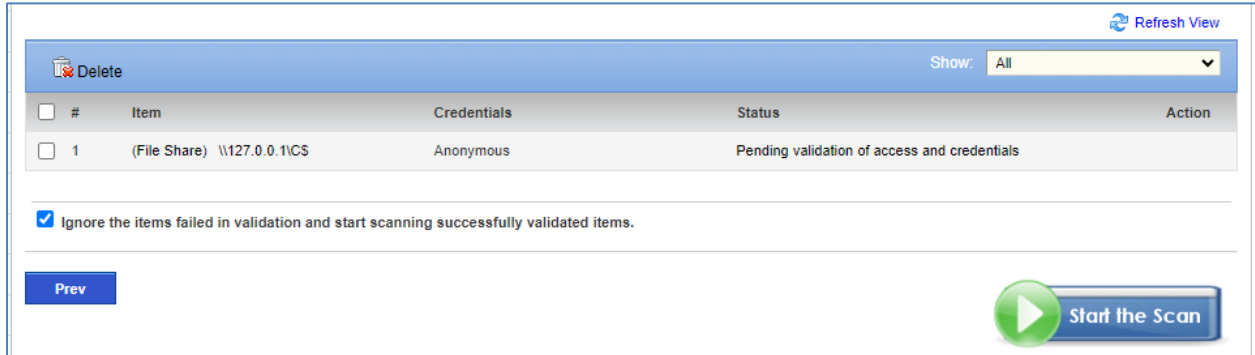
\* SharePoint Site:

\* Authentication Required:  Yes  No

\* Credentials:

 **Start the scan**

Finally, once you have added all the targets (File Systems, Databases etc. that need to be scanned), click the “Start the Scan” button. We will then verify the network access and credentials to these targets. Depending upon the size of the scan this may take a few minutes.



The screenshot shows a web interface for managing scan targets. At the top right, there is a "Refresh View" link. Below it is a "Delete" button with a trash icon and a "Show: All" dropdown menu. A table lists the scan targets with columns for selection, ID, Item, Credentials, Status, and Action.

<input type="checkbox"/>	#	Item	Credentials	Status	Action
<input type="checkbox"/>	1	(File Share) \\127.0.0.1\CS	Anonymous	Pending validation of access and credentials	

Below the table, there is a checkbox labeled "Ignore the items failed in validation and start scanning successfully validated items." which is checked. At the bottom left is a "Prev" button, and at the bottom right is a large green "Start the Scan" button with a play icon.



## Scan Status

The progress of the scan can be seen on the next page or by clicking the SCAN HISTORY tab

**Scan History** [Refresh View](#)

The table below lists all scans that have been run with their status.

#	Scan Name	ID	Start Time	End Time	Schedule	Status	Action	Log	Report
1	<a href="#">Scan_2024_03_14</a>	29				Config In Progress <input type="radio"/> Total steps: 1 <input type="radio"/> Validation passed: 0 <input type="radio"/> Validation failed: 0 Ignored 0 <input type="radio"/> Validating currently: 0 <input type="radio"/> Pending: 1			<a href="#">more details ...</a>

Additional details can be seen by clicking the MORE DETAILS... button

**Scan Progress** [Refresh View](#)

The list below shows the status of the targets that are part of the scan. If an item fails, the scan process will retry it before finally marking it as failed. Default retry attempts are 10.

Scan ID: 4 | Scan Name: Scan\_2024\_03\_08\_Fileshare Show: All

#	Process	Statistics / Progress	Details	Action
1	File Share Search	Status: <b>Completed</b> Files Scanned: 9, Data Scanned: 0.02 GB Excel Files Scanned: 0 <div style="width: 100%; background-color: green; height: 10px;"></div> 100%	\\127.0.0.1\c5\inpol -	
2	Parsing Intermediate Results	Status: <b>Completed</b>		
3	Generating Reports	Status: <b>Completed</b>		

**Scan Statistics**

Start Time	End Time	Status	Report
08 Mar 2024, 11:09 AM	08 Mar 2024, 11:15 AM	Completed	



## View Scan Results

Once the scan is completed, the results can be seen from the SCAN HISTORY tab or through the DASHBOARD tab

Scan History [Refresh View](#)

The table below lists all scans that have been run with their status.

Show: All

#	Scan Name	ID	Start Time	End Time	Schedule	Status	Action	Log	Report
21	<a href="#">Scan_2024_03_08_Domain</a>	7	08 Mar 2024, 11:59 AM	08 Mar 2024, 12:12 PM	<a href="#">Schedule</a>	<span style="color: green;">✔</span> Completed (100%)			

Scan Statistics

Scan ID: 4    Scan Name: Scan\_2024\_03\_08\_Fileshare

[Export](#)

#	Type	Location	Scan Status	Card Data	Details
1	File Share	\\127.0.0.1c\$inpol	Completed	26	

Page 1 of 1    Records Per Page: 100

Detailed Scan Report [Back](#)

Scan ID : 4

Scan Name : Scan\_2024\_03\_08\_Fileshare

Asset Name : \\127.0.0.1c\$inpol

	Total Records	False Positive	Remediated
Card Data	26	0	0

Show:  Confirmed    False Positive    Remediated

<input type="checkbox"/>	#	Location	Records Found	Found String
<input type="checkbox"/>	1	\\127.0.0.1c\$inpol\$Space.txt	2	3782 82XX XXXX 005    5173 58XX XXXX 9055
<input type="checkbox"/>	2	\\127.0.0.1c\$inpol\$batsman.txt	4	517751XXXXXX4651    532194XXXXXX1869

You can click the details icons to see additional details or download the results in a CSV file

## Domain scan results

Detailed Scan Report Back

Scan ID : 7

Scan Name : Scan\_2024\_03\_08\_Domain

Asset Name : QA-Candle.co.in ▶ 10.30.60.150

	Total Records	False Positive	Remediated
Card Data	16	0	0

Show:  Confirmed  False Positive  Remediated

#	Location	Records Found	Found String
<input type="checkbox"/> 1	C:\npol\smallddtestbed\exclude.txt	2	529196XXXXXXXX4320  511693XXXXXXXX4850
<input type="checkbox"/> 2	C:\npol\smallddtestbed\include.txt	2	411096XXXXXXXX8385  469040XXXXXXXX0205
<input type="checkbox"/> 3	C:\npol\T.txt	4	521530XXXXXXXX4012  492994XXX3234
<input type="checkbox"/> 4	C:\npol\SmallCDDBed1File\Card_Data.csv	4	650601XXXXXXXX0993  554224XXXXXXXX3485
<input type="checkbox"/> 5	C:\npol\smallddtestbed\smallfile.txt	4	529196XXXXXXXX4320  511693XXXXXXXX4850

Page 1 of 1 Records Per Page: 100


## Database scan results

Detailed Statistics for 10.30.60.250 Back

Scan ID: 2 Scan Name: Scan\_2024\_03\_08\_DB\_SQL

Export

#	Database	Scan Status	Card Data	Details																														
1	<ul style="list-style-type: none"> <li>NBP_Test               <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Sr. no</th> <th>Table</th> <th>Scan Status</th> <th>Card Data</th> <th>Details</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>table_name</td> <td>Completed</td> <td>0</td> <td></td> </tr> <tr> <td>2</td> <td>T2</td> <td>Completed</td> <td>1</td> <td></td> </tr> <tr> <td>3</td> <td>NPoL_CDD_TestBed_5</td> <td>Completed</td> <td>1</td> <td></td> </tr> <tr> <td>4</td> <td>C_NBP_CDD_TestBed_19_Rows</td> <td>Completed</td> <td>6</td> <td></td> </tr> <tr> <td>5</td> <td>cdd_dev</td> <td>Completed</td> <td>0</td> <td></td> </tr> </tbody> </table> </li> </ul>	Sr. no	Table	Scan Status	Card Data	Details	1	table_name	Completed	0		2	T2	Completed	1		3	NPoL_CDD_TestBed_5	Completed	1		4	C_NBP_CDD_TestBed_19_Rows	Completed	6		5	cdd_dev	Completed	0		Completed	9	
Sr. no	Table	Scan Status	Card Data	Details																														
1	table_name	Completed	0																															
2	T2	Completed	1																															
3	NPoL_CDD_TestBed_5	Completed	1																															
4	C_NBP_CDD_TestBed_19_Rows	Completed	6																															
5	cdd_dev	Completed	0																															
2	<ul style="list-style-type: none"> <li>NPoL_CDD_DB_1_Table_Only_9_Rows               <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Sr. no</th> <th>Table</th> <th>Scan Status</th> <th>Card Data</th> <th>Details</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Latest_C_NBP_CDD_TestBed_9_Rows</td> <td>Completed</td> <td>1</td> <td></td> </tr> </tbody> </table> </li> </ul>	Sr. no	Table	Scan Status	Card Data	Details	1	Latest_C_NBP_CDD_TestBed_9_Rows	Completed	1		Completed	1																					
Sr. no	Table	Scan Status	Card Data	Details																														
1	Latest_C_NBP_CDD_TestBed_9_Rows	Completed	1																															
3	cdd_dev	Completed	10																															
4	empty_db	Completed	0																															
5	empty_table	Completed	0																															

Detailed Scan Report Back 



Scan ID : 2




Scan Name : Scan\_2024\_03\_08\_DB\_SQL

Asset Name : 10.30.60.250 ▶ QA\_NPOL\_Data


	Total Records	False Positive	Remediated
Card Data	1876	50	818

Successfully marked the records as a false positive. These records will be excluded from future searches as well.

Show:  Confirmed  False Positive  Remediated  

#	Database	Table	Column	Records Found	Found String
<input type="checkbox"/> 1	QA_NPOL_Data	myTable	pan	270	(BRSolo) 633455 xxxxxx 6438  450 822:xx xxxxx 866
<input type="checkbox"/> 2	QA_NPOL_Data	QA_NPOL_SDataTable1	pan	304	 5038 47:xxxx 1947  6759 38:xx xxxxx 9311
<input type="checkbox"/> 3	QA_NPOL_Data	QA_NPOL_SDataTable1	track1	47	(TrackData) %BXXXXXXXXXXXX (TrackData) %BXXXXXXXXXXXX XXXXX^EybfbCvirvp^3303902 XXXXX^HcjomdlPvykrz^500227 972 1171778
<input type="checkbox"/> 4	QA_NPOL_Data	QA_NPOL_SDataTable1	track2	53	(TrackData) XXXXXXXXXXXXXXX (TrackData) XXXXXXXXXXXXXXX XXX=09091902161? XXX=32068536?

### MS Exchange scan results

Detailed Scan Report Back 



Scan ID : 5


Scan Name : Scan\_2024\_03\_08\_Exchange

Asset Name : Exchange ▶ 10.30.60.206 ▶ zshaikh

	Total Records	False Positive	Remediated
Card Data	102	7	3

Successfully marked the records as remediated.

Show:  Confirmed  False Positive  Remediated  



#	Location	Records Found	Found String
<input type="checkbox"/> 1	zshaikh@ccawsqaex2016.com.pst\Inbox\JL_Diners Club US and Canada, 554089XXXXX0420	1	 554089XXXXX0420
<input type="checkbox"/> 2	zshaikh@ccawsqaex2016.com.pst\Outbox\RE: starts and ends with case sensi no/SOLO.CSV	1	(BRSolo) 633450XXXXXXXXXX5503
<input type="checkbox"/> 3	zshaikh@ccawsqaex2016.com.pst\Outbox\CDD Data Test/SOLO.CSV	1	(BRSolo) 633450XXXXXXXXXX5503

**Mail Details**  
 Time: Thu 05/09/2019 10:09 AM  
 From: Jevita  
 To: zshaikh

**Mail Details**  
 Time: Thu 11/24/2022 11:39 AM  
 From: zshaikh  
 To: Jevita

**Mail Details**  
 Time: Thu 11/24/2022 11:28 AM  
 From: zshaikh  
 To: npol; Jevita


## Office 365 scan results

**Scan Statistics**  


Scan ID: 12    Scan Name: Scan\_2024\_03\_08\_emailSmall

---

**Export** 

#	Type	Location	Scan Status	Card Data	Details
1	Office 365 Email	zshaikh@controlcasegrc.com	Completed	43	



Page 1 of 1    Records Per Page: 100









**Detailed Scan Report** Back 

Scan ID : 12  
 Scan Name : Scan\_2024\_03\_08\_emailSmall  
 Asset Name : zshaikh@controlcasegrc.com


	Total Records	False Positive	Remediated
Card Data	43	1	1

Successfully marked the records as remediated.

Show:  Confirmed     False Positive     Remediated  



<input type="checkbox"/>	#	Location	Records Found	Found String
<input type="checkbox"/>	1	zshaikh@controlcasegrc.com/Inbox/Zip File Attached/smallcddtestbed.zip/exclude.txt	2	 529196XXXXX4320  511693XXXXX4850
		<b>Mail Details</b> Time: 2023-10-04 07:27:33 From: zshaikh@controlcasegrc.com To: npol@controlcasegrc.com, anagare@controlcasegrc.com, anagare@controlcase.com, npol@controlase.com, vdmello@controlcase.com, zshaikh@controlcasegrc.com,		
<input type="checkbox"/>	2	zshaikh@controlcasegrc.com/Inbox/Zip File Attached/smallcddtestbed.zip/include.txt	2	 411096XXXXX8385  469040XXXXX0205
		<b>Mail Details</b> Time: 2023-10-04 07:27:33 From: zshaikh@controlcasegrc.com To: npol@controlcasegrc.com, anagare@controlcasegrc.com, anagare@controlcase.com, npol@controlase.com, vdmello@controlcase.com, zshaikh@controlcasegrc.com,		
<input type="checkbox"/>	3	zshaikh@controlcasegrc.com/Inbox/FRT 516109XXXXX1065 u8hukdndd 6759.3091.2213.2744	2	 516109XXXXX1065  6759.30XX.XXXX.2744
		<b>Mail Details</b> Time: 2023-06-30 09:20:25 From: NPOL@controlcase.com To: zshaikh@controlcasegrc.com,		
<input type="checkbox"/>	4	zshaikh@controlcasegrc.com/Sent Items/Zip File Attached/smallcddtestbed.zip/exclude.txt	2	 529196XXXXX4320  511693XXXXX4850
		<b>Mail Details</b> Time: 2023-10-04 07:27:30 From: zshaikh@controlcasegrc.com To: npol@controlcasegrc.com, anagare@controlcasegrc.com, anagare@controlcase.com, npol@controlase.com, vdmello@controlcase.com, zshaikh@controlcasegrc.com,		











## Outlook PST file scan results

Detailed Scan Report Back 

Scan ID : 7  
 Scan Name : Scan\_Outlook  
 Asset Name : \\Outlook\_Mailbox

	Total Records	False Positive	Remediated
Card Data	145	10	4

Show:  Confirmed  False Positive  Remediated  

<input type="checkbox"/>	#	Location	Found String
<input type="checkbox"/>	1	\\Outlook_Mailbox\Allen.Stillwell@controlcase.org.com\Inbox\Re: Important Information about your reimbursement	 376932XXXXX1004  376932XXXXX1004
<input type="checkbox"/>	2	\\Outlook_Mailbox\Allen.Stillwell@controlcase.org.com\Inbox\RE: 225937 - 3175193 NS Ltd DBA Shine on Factory	 656505XXXXXX6344  439901XXXXXX1390
<input type="checkbox"/>	3	\\Outlook_Mailbox\Allen.Stillwell@controlcase.org.com\Inbox\RE: one time cd\Misconduct_V3.txt	 379733XXXXX4011  442142XXXXXX5681
<input type="checkbox"/>	4	\\Outlook_Mailbox\Allen.Stillwell@controlcase.org.com\Inbox\RE: IMEI Management Database	 404970XXXXXX5716  404970XXXXXX5716
<input type="checkbox"/>	5	\\Outlook_Mailbox\Allen.Stillwell@controlcase.org.com\Inbox\reversal of credit	 404970XXXXXX5716  404970XXXXXX5716



## CDD False Positive Management and Remediation Feature

---

CDD has a Remediation feature which facilitates you to see all the Card/Sensitive data and manage it from the single place.


The following process explains the steps involved in the typical Remediation process:

1. **Configure and Run the new scan to find the Card Holder/Sensitive data.** For more information on how to configure and run the scan please refer the CDD quick start guide.
2. **Use the Remediation Tab to obtain the CSV report or Mark the Record as false positives.**
  - a. Go to the “**Remediation Tab**”.
  - b. Select the scan record or search filters and Click on “**Search**” button to view the records.
  - c. Click on the export icon on the right hand side of the screen to export the report in the CSV format.
  - d. The CSV report will contain 3 types of records.
    - **Confirmed** – Records having high possibility of valid card data.
    - **False Positive** - The records which are marked as false positives by the end user (You will most likely ignore these records). You can see the false positive records by selecting the “User Marked False Positives” checkbox.
3. **Verify the findings and Mark the false positives.**
  - a. Inspect the records manually and check if it is a false positive or valid card data.
  - b. If it is false positive then go to the Remediation tab and mark it as a false positive.
  - c. If you marked the file as false positive then the tool will mark it as a false positive in subsequent scans automatically and will remove the records from the default view.
  - d. Remediate the other finding by manually removing/deleting/encrypting the data.
4. We have **Mark as Remediation tab** features for those finding to whom you have removed/deleted/encrypted. Once you done with remediation please regenerate reports to get compliant report.

 **SCANNING TIPS**

For successful scans please ensure the following:

## PLEASE BE PATIENT


**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/>



## 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.



## KNOWN ISSUES

---

- Special characters such as "`+\" - \" ^></ # \$ ~" etc. in Database object names, Any Passwords, Machine names, File Share Paths may result in failed scans.
- The UI layout becomes distorted if Internet Explorer's "compatibility mode" is enabled. The supported browsers are limited to Edge, Chrome, and Mozilla Firefox.

 **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/>**