





















ControlCase™ Data Discovery





Version 8.6
Updated Nov 2021

CDD 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

	Prerequisites.....	4
	Download and Install.....	5
	Scanning Oracle Databases :: Oracle client download (Optional).....	7
	Scanning DB2 and Sybase databases (Optional)	7
	Register a new installation and get a License.....	8
	Scanning for Card Data – Running a new scan	9
	File System Scans	9
	Domain Scan	12
	Unix/Linux variants.....	13
	Amazon S3.....	14
	Database scans.....	15
	Email Servers scans	16
	Office 365 Email Scanning	17
	IMAP based Servers.....	18
	Microsoft SharePoint scans.....	19
	Start the scan.....	20
	Scan Status.....	21
	View Scan Results	22
	Scanning tips.....	27
	Troubleshooting Failed scans	28

	Known Issues	28
	What is new or changed in CDD 8.6.....	29
	What is new or changed in CDD 8.0	29
	Support and help.....	30


 **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 Server,**
 - b. **Windows Server 2012 R2 Service Pack 1,**
 - c. **Windows 8.1**
 - d. **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 4 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. 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-supportedvisual-c-downloads>
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 Installs

Please download and install CDD 8.0 from

https://home.controlcase.com/downloads/CDD_8.0.exe

Then download and install the Upgrade to 8.6 using

https://home.controlcase.com/downloads/Upgrade_CDD_8.6.exe

Then download and install the Latest updates for 8.6 using

https://home.controlcase.com/downloads/CDD_8.6_updates.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 instead of installing a new version.

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 the sufficient amount of 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.

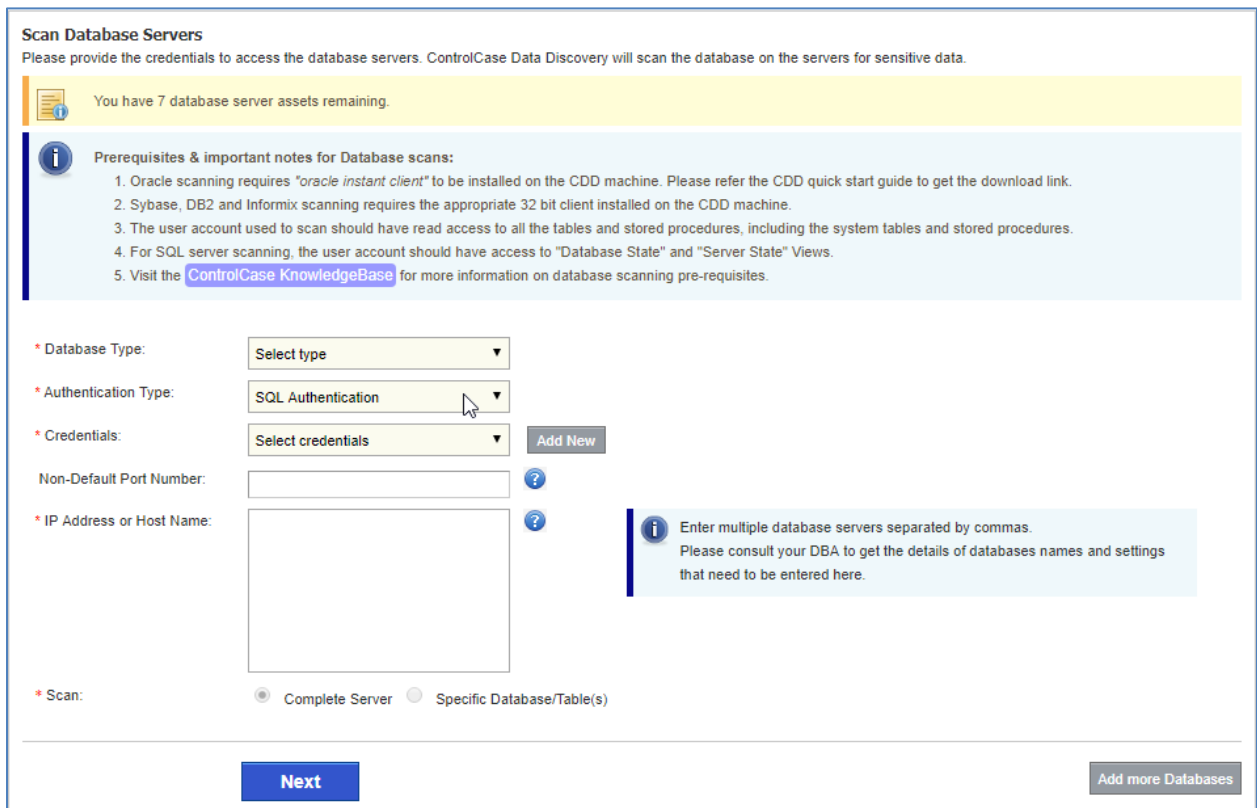
If you plan to scan Oracle databases, CDD now uses the Oracle Instant Client, which immensely simplifies the process of connecting to Oracle databases.

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 and run it to install and please accept the default prompts.

To enter the details of the database, please see the following screenshot:



Scan Database Servers
Please provide the credentials to access the database servers. ControlCase Data Discovery will scan the database on the servers for sensitive data.

You have 7 database server assets remaining.

Prerequisites & important notes for Database scans:

1. Oracle scanning requires "oracle instant client" to be installed on the CDD machine. Please refer the CDD quick start guide to get the download link.
2. Sybase, DB2 and Informix scanning requires the appropriate 32 bit client installed on the CDD machine.
3. The user account used to scan should have read access to all the tables and stored procedures, including the system tables and stored procedures.
4. For SQL server scanning, the user account should have access to "Database State" and "Server State" Views.
5. Visit the [ControlCase KnowledgeBase](#) for more information on database scanning pre-requisites.

* Database Type:

* Authentication Type:

* Credentials:

Non-Default Port Number:

* IP Address or Host Name:

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

Info: Enter multiple database servers separated by commas. Please consult your DBA to get the details of databases names and settings that need to be entered here.

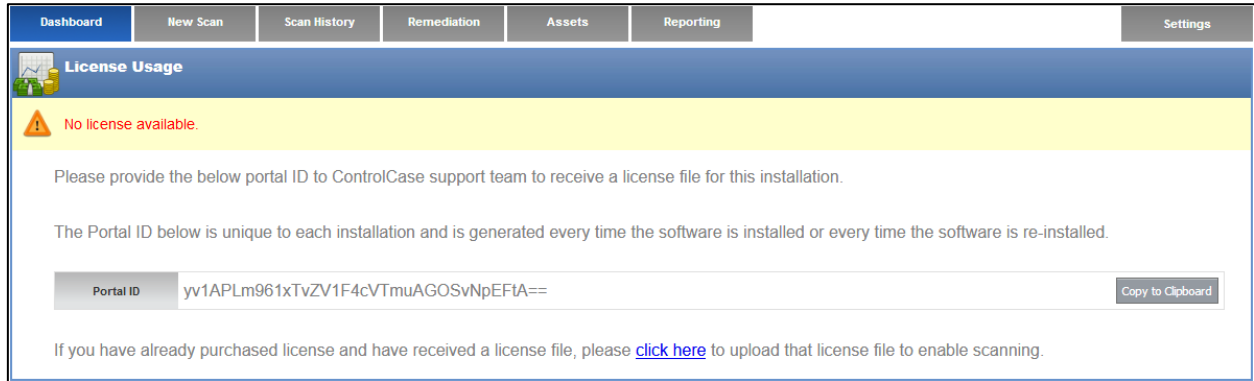


SCANNING DB2 AND SYBASE DATABASES (OPTIONAL)


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.

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.



License Usage

 No license available.

Please provide the below portal ID to ControlCase support team to receive a license file for this installation.

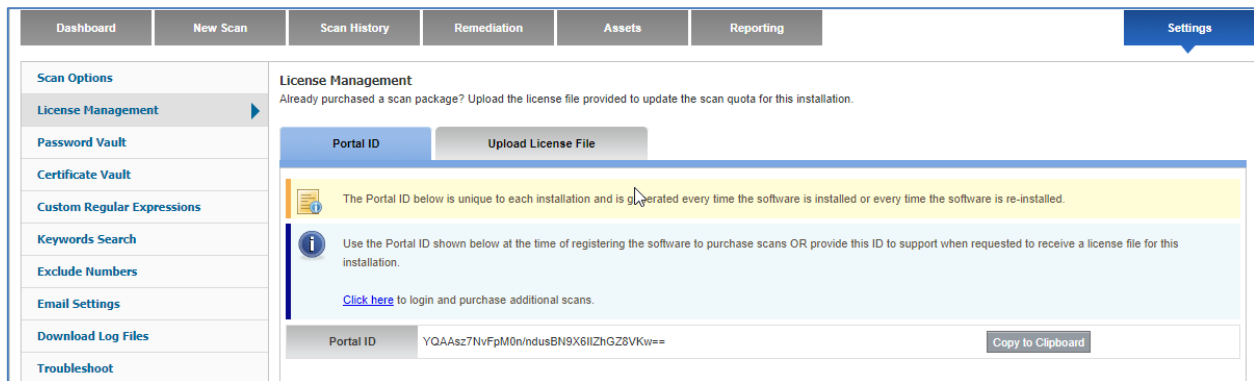
The Portal ID below is unique to each installation and is generated every time the software is installed or every time the software is re-installed.

Portal ID

If you have already purchased license and have received a license file, please [click here](#) to upload that license file to enable scanning.

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



License Management

Already purchased a scan package? Upload the license file provided to update the scan quota for this installation.

Portal ID

The Portal ID below is unique to each installation and is generated every time the software is installed or every time the software is re-installed.

Use the Portal ID shown below at the time of registering the software to purchase scans OR provide this ID to support when requested to receive a license file for this installation.

[Click here](#) to login and purchase additional scans.



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

Important Note:
Scan behavior can be controlled by various global scan settings. Below are some important global scan settings, which are applicable to all the scans.
You can change the scan settings from “Settings Tab->Scan Options” or [Click here](#) to change the global scan settings.

1. For database scans, sample and search is set to 20 percent of rows randomly from each table.
2. Debugging level is set to *OFF*.
3. Scan speed is set to *Normal scanning mode*.

* Scan Name:

* Search For: Card Data GDPR Data Other Sensitive Data [?](#)

* Scan Type: Rapid Scan Deep Scan Proximity Scan [?](#)

Retry the failed items indefinitely until successfully scanned.

If the scan is unsuccessful, retry the failed items indefinitely.

[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

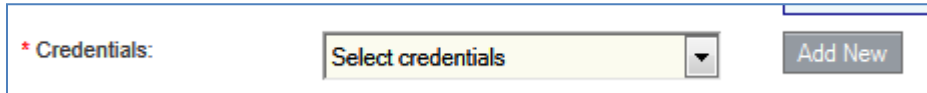
If you want to scan File systems, you can add 6 types of scans

- 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)

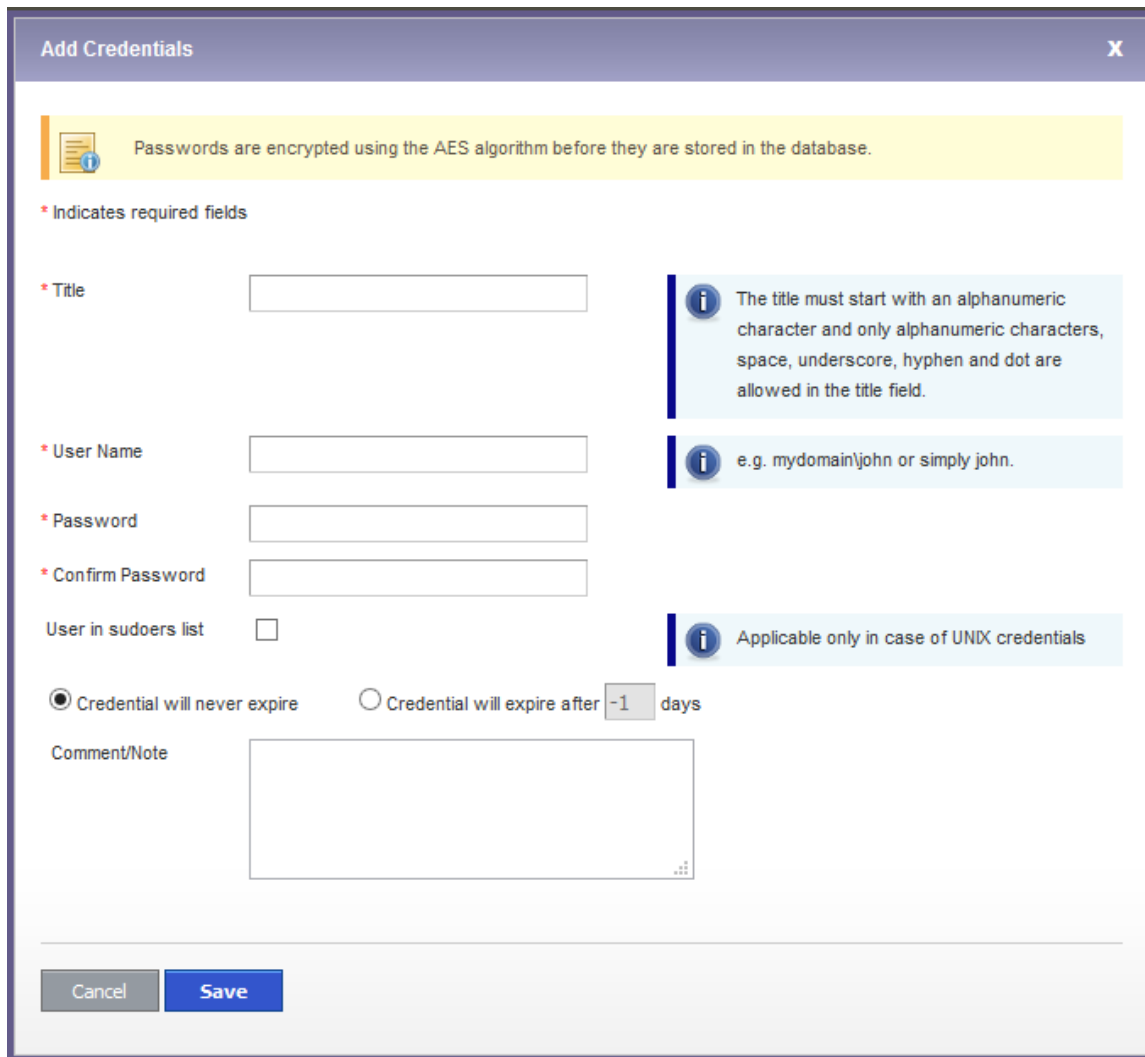
Please select any of the types as needed and enter the relevant data, the screens provide instructions on what information needs to be entered.

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



A screenshot of a web interface showing a dropdown menu for credentials. The label is "* Credentials:". The dropdown menu is open, showing "Select credentials" and a downward arrow. To the right of the dropdown is a button labeled "Add New".

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



A screenshot of the "Add Credentials" dialog box. The title bar says "Add Credentials" with a close button (X). Below the title bar is a yellow information banner: "Passwords are encrypted using the AES algorithm before they are stored in the database." Below this is a legend: "* Indicates required fields". The form contains the following fields and options:


- * Title: Text input field. Information: "The title must start with an alphanumeric character and only alphanumeric characters, space, underscore, hyphen and dot are allowed in the title field."
- * User Name: Text input field. Information: "e.g. mydomain\john or simply john."
- * Password: Text input field.
- * Confirm Password: Text input field.
- User in sudoers list:
- Expiration: Credential will never expire Credential will expire after days. Information: "Applicable only in case of UNIX credentials"
- Comment/Note: Text area.

At the bottom are "Cancel" and "Save" buttons.

Local Drive/Disk

Scan Local Drives

Please select the local drives. The drive(s) selected will be scanned for sensitive data.


 You have 10 file system assets remaining.


* Select Drive(s):

C:/
E:/
F:/

* Scan Scope:

Scan All Files

 Selected drive(s) on the scanner machine will be scanned.



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.


Next


Add more Local Drives

File Share (Network Drive)

Scan File Shares

Please enter the file share details. The location entered will be scanned for sensitive data.

 You have 10 file system assets remaining.

 **Note:**
 If file share is hosted on a Domain or Workgroup computer, then you can use the domain scanning method to scan file share. The domain scanning is faster compared to file share scanning because it eliminates the overhead of transferring the files over the network before scanning. Use file share scanning when the share is hosted on a dedicated NAS storage device on which you cannot run the domain scan.

* File Share Name:

Connect as an anonymous user:


* Credentials:


Select credentials


Add New

* Scan Scope:

Scan All Files

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

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



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.

Next

Add more File Shares

Domain Scan

Scan Domain Machines

Please enter the domain/Workgroup machine details. The location entered will be scanned for sensitive data.



You have 10 file system assets remaining.



Prerequisites & important notes for Domain scans:

1. TCP Port 445 should be open (In addition, Windows NT/2000/XP may require TCP port 139 and UDP ports 135-137 open).
2. File & Printer sharing must be enabled on both CDD and the target machines.
3. Administrative shares such as ADMIN\$ should be enabled on target machines.
4. The user selected in the credentials should have Administrator level privileges.
5. The IP Address of target server must be resolved to its Host Name and vice versa.
6. Visit the [ControlCase KnowledgeBase](#) for more information on domain scanning pre-requisites.

* Domain Name: ?

* Credentials:

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

* Select Drive Types: Fixed Drive Removable Drive

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

* Scan Scope:



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.



The selected input drive(s) will be matched against the drive type selected. If the drive doesn't match with the drive type selected it will be skipped.



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.

Next

Add more Domain Machines

 **Unix/Linux variants**

Scan Unix Machines

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

You have 10 file system assets remaining.

Prerequisites & Important notes for Unix scans:

1. SSH should be enabled and target machine should be accessible via SSH.
2. Execute permission on /tmp folder should be enabled on the target machine.
3. Glibc version 2.4 or above is required on the target machine. Use "ldd --version" command to check the available version on the target machine.

* Operating System:

* OS Bit: 64 Bit 32 Bit [?](#)

* IP Address or Host Name:

[?](#) Enter multiple IP address or host names separated by commas.

* Connect using: Credentials Certificate

* Credentials: [Add New](#)

User is in the sudoers list: [?](#)

* Select Drive:

[?](#) Selected drive will be scanned on the target machine.

Subfolder:

[?](#) Enter the absolute folder path without drive name. Multiple Subfolder are not allowed.

* SSH Port:

* Scan Scope:

[?](#) 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.

[Next](#) [Add more Unix Machines](#)

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

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

You have 10 Amazon S3 assets remaining.

* Credentials:

* Region Endpoint:

* Bucket Name(s):

i 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`

i Enter multiple bucket names separated by commas.

Mainframe file formatted files (EBCDIC)

Scan EBCDIC Files
Please enter the file share details. The location entered will be scanned for sensitive data. The scanner will treat all the files as EBCDIC encoded.

You have 10 file system assets remaining.

* File Share Name:

Connect as an anonymous user:

* Credentials:

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

i 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.

Scan Database Servers

Please provide the credentials to access the database servers. ControlCase Data Discovery will scan the database on the servers for sensitive data.

You have 7 database server assets remaining.

Prerequisites & important notes for Database scans:

1. Oracle scanning requires "oracle instant client" to be installed on the CDD machine. Please refer the CDD quick start guide to get the download link.
2. Sybase, DB2 and Informix scanning requires the appropriate 32 bit client installed on the CDD machine.
3. The user account used to scan should have read access to all the tables and stored procedures, including the system tables and stored procedures.
4. For SQL server scanning, the user account should have access to "Database State" and "Server State" Views.
5. Visit the [ControlCase KnowledgeBase](#) for more information on database scanning pre-requisites.

* Database Type:

* Authentication Type:

* Credentials:

Non-Default Port Number:

* IP Address or Host Name:

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

Enter multiple database servers separated by commas. 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

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.

Scan Exchange Servers

Please enter the exchange server details. The entered servers/mailboxes will be scanned for sensitive data.

You have 9 exchange server assets remaining.

Prerequisites for Exchange Server scans:

1. TCP Port 445 should be open (In addition, Windows NT/2000 may require TCP port 139 and UDP ports 135-137 open).
2. Network Discovery and File sharing should be enabled on both CDD and remote machines.
3. Administrative shares such as ADMIN\$ should be enabled on remote machines.
4. 64-bit Outlook client must be installed on the Exchange server.
5. Visit the [ControlCase KnowledgeBase](#) for more information on exchange scanning.

* Version:

* Server IP Address or Host Name:

* Credentials:

Mailbox Names(s):

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

Info: To scan specific mailbox, enter the mailbox name separated by a newline. Visit the [ControlCase KnowledgeBase](#) to view more information on how to obtain the mailbox list.

Office 365 Email 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.

Scan Office 365 Email

Please provide the details to scan the Office 365 email mailboxes for card/sensitive data.

 You have 8 Office 365 email assets remaining.

 **Prerequisites for Office 365 Email scans:**

1. The user mailbox credentials provided should be a member of the Discovery Management role group.
2. "Application Impersonation" role must be assigned to the user.


* Email Address:


* Password:

* Confirm Password:

* Host Name:

Mailbox Email Address(es):

 The tool will validate the credentials by logging into the Office 365 email server before saving, it may take some time.

 To scan specific mailboxes, enter the email address of the mailboxes separated by a comma.
Leave empty to scan all mailboxes to which user has access.

@ IMAP based Servers

Scan IMAP Email Addresses

Please enter the IMAP details to scan the emails for sensitive data.

You have 14 email assets remaining.

Important Note:
Some email service providers by default block access to mailboxes from non-standard application (like outlook or gmail). Please check the security settings and allow access for non-standard applications.

* Email address:

* Password:

* Confirm Password:

* Host Name:

Port:

SSL:

This may take a moment; the system will try logging in to the mail server to validate the entered login information.

Next Add more Email Addresses

IBM Notes Servers

Scan IBM Notes

Please enter the IBM Notes details. The entered servers will be scanned for sensitive data.

You have 7 IBM Notes assets remaining.

Prerequisites for Notes Server scans:

- Notes version 8.5, 9.0 and 9.1 are supported.
- The user credentials required to connect the domino server must be stored in Notes user profile.
- Notes must be installed on the CDD machine.

* Scan for: Local Notes Domino Server

* IP Address or Host Name:

Enter multiple IP address or host names separated by commas.

* Credentials:


Next Add more Notes Server

IBM Notes scans can be used to scan both, local Notes databases or Domino database servers.

Microsoft SharePoint scans

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.

Scan SharePoint
Please enter the SharePoint details. The location entered will be scanned for sensitive data.

 You have 7 SharePoint assets remaining.

* SharePoint URL:

* 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.

Item	Value	Status	Comments	Action
Local Drive	C:/	Success		Delete

Ignore failed items and start scan automatically.

[Prev](#) 







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. For a scan that has been completed you can view the scan results by clicking the icon in the Scan Results column. For scans that are in progress, you can view the progress by clicking the more details ... link in the Status column.

#	Scan Name	ID	Start Time	End Time	Schedule	Status	Action	Log	Results
1	 Scan_FirstScan	8				Config In Progress <input type="radio"/> Total steps: 2 <input type="radio"/> Steps passed in validation: 1 <input type="radio"/> Steps failed in validation: 0, Ignored 0 <input type="radio"/> Steps validating currently: 0 <input type="radio"/> Steps waiting to be validated: 1			

[more details ...](#)

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

Scan Name: Scan_c_drive

#	Process	Statistics / Progress	Details	Action
1	Filesystem Search - Local Drive	Status: In Progress Excel Files Scanned : 11 Files Scanned : 5899  0%	Total Size : 42.81 GB Scanned : 4.08 GB	C: Log



View Scan Results

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

#	Scan Name	ID	Start Time	End Time	Schedule	Status	Action	Log	Results
1	Scan_Sharepoint	10	25 Feb 2015, 06:35 PM	25 Feb 2015, 07:09 PM	Schedule	Completed (100%)			

Scan ID: 10 | Scan Name: Scan_Sharepoint
 Below table presents a statistics of the current scan results. [Click here](#) to download statistics report in CSV format.

Details of scan performed on SharePoint

#	SharePoint URL	Scan Status	Result	Total Records	False Positive	Details/Download
1	http://54.172.44.11/SitePages/Home.aspx	Completed	Data found	16	0	

Scan ID: 1 | Scan Name: Scan_Local_Drive
 Below table presents a statistics of the current scan results. [Click here](#) to download statistics report in CSV format.

Details of scan performed on Local Drives

#	Drive Letter	Scan Status	Result	Total Records	False Positive	Details/Download
1	C:/	Completed	Data found	40	0	
2	D:/	Completed	Data found	338	18	

Details of scan performed on Domains

#	Domain	Machine	Scan Status	Result	Total Records	False Positive	Details/Download
1	controlcase	Domain level results	Partially Completed	Data found	1514	61	
	1.1	Mangesh-PC (10.85.203.53)	Completed	Data found	2	0	
	1.2	RPKUMAR-PC (10.85.203.55)	Completed	Data found	1347	31	

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















Domain scan results

File System Scan Report

Scan ID: 6 | Scan Name: Scan_Domain

Domain: controlcase ▶ smondal-lap

Show System marked false positives User marked false positives Remediated records

#	Result Type	File Path	Found String
1	PAN	smondal-lap\C:\Users\smondal.CONTROLCASE\Documents\CC Test Data.zip (CC Test Data\some data.xls)	 5286-39X-XXX-XX8850
2	PAN	smondal-lap\C:\Users\smondal.CONTROLCASE\Documents\CC Test Data\CC Test Data\some data.xls	 5286-39X-XXX-XX8850
3	PAN	smondal-lap\C:\Users\smondal.CONTROLCASE\Desktop\CapitalMultiplierPlan_Sep12-1.11.xls	 400540XXXXXX3344  358358XXXXXX5264
4	PAN	smondal-lap\C:\Users\smondal.CONTROLCASE\Documents\CC Test Data.zip (CC Test Data\cc data.bt)	 411234XXXXXX4113  411014XXXXXX4115
5	PAN	smondal-lap\C:\Users\smondal.CONTROLCASE\Documents\CC Test Data\CC Test Data\alcc data.bt	 411234XXXXXX4113  411014XXXXXX4115
6	PAN	smondal-lap\C:\Users\smondal.CONTROLCASE\Documents\PAN-CCM-040212.pdf\PAN-CCM-040212.pdf\13\PDF\en\configHistory.pdf	 5432 54X XXX XX5550  4469 45X XXX XX4802
7	PAN	smondal-lap\C:\Users\smondal.CONTROLCASE\Documents\PAN-CCM-040212.pdf\PAN-CCM-040212.pdf\13\PDF\en\configHistory.pdf	 5432 54X XXX XX5550  4469 45X XXX XX4802
8	PAN	smondal-lap\C:\Users\smondal.CONTROLCASE\Downloads\CapitalMultiplierPlan_Sep12-1.11.xls	 400540XXXXXX3344  358358XXXXXX5264













Database scan results

Scan Statistics

Scan ID: 5 | Scan Name: Database scan

The table below presents a statistic of the current scan results. [Click here](#) to download statistics report in CSV format.

Details of scan performed on Database Servers













#	Database Server	Database	Scan Status	Result	Records Found	False Positive	Remediated	Details/Download
1	10.85.230.107/localdatabase	Database server level report	Completed	Data found	91	0	0	 
		localdatabase	Completed	Data found	91	0	0	 
2	10.85.230.28\MSSQLEXPRESS2014	Database server level report	Completed	Data found	64	0	0	 
		New_Huge_DB	Completed	Data found	50	0	0	 
		MasterCard_New_Bin	Completed	Data found	11	0	0	 
		1 Valid	Completed	Data found	3	0	0	 
		ReportServerMSSQL2014	Completed	Data not found				
		ReportServerMSSQL2014TempDB	Completed	Data not found				

Detailed Database scan report

Scan ID: 5 | Scan Name: Scan_Database

Database Server: 10.85.203.89

Show User excluded records Remediated records

#	Database Name	Table Name	Column Name	Result Type	Record Count	Found String
<input type="checkbox"/> 1	MSSQL2012DB	Table2001	PAN	PAN	5	 522898xxxxxx6079  569068XXXXXX1729
<input type="checkbox"/> 2	MSSQL2012DB	Table2001	Track1	PAN	8	 522898xxxxxx6079  491664XXXXXX1751
<input type="checkbox"/> 3	MSSQL2012DB	Table2003	PAN	PAN	8	 525437xxxxxx3428  2014 86X XXX X5595
<input type="checkbox"/> 4	MSSQL2012DB	Table2003	Track1	PAN	6	 525437xxxxxx3428  455681XXXXXX7709
<input type="checkbox"/> 5	MSSQL2012DB	Table2003	Track2	PAN	4	 525437xxxxxx3428  455681XXXXXX7709
<input type="checkbox"/> 6	MSSQL2012DB	Table2004	Track2	PAN	9	 544089xxxxxx0779  455684XXXXXX0485









MS Exchange scan results

Exchange Servers Scan Report


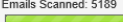



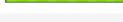
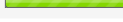
Scan ID: 11 | Scan Name: Exchange_Server





Exchange : Microsoft Exchange 2016 ▶ 10.85.205.209

Show System marked false positives User marked false positives Remediated records

#	Result Type	Mail Details	Found String
<input type="checkbox"/> 1	PAN	Mac_AR Low_AR_Last/Inbox/Card Data to Group 3 Mail Details Time: Wed 12/28/2016 01:01 PM From: Administrator To: QA Team3	 652519XXXXXX6676  407681XXXXXX5672
<input type="checkbox"/> 2	PAN	Zeeshan Shaikh/Inbox/M1 Mail Details Time: Wed 09/21/2016 06:30 AM From: Administrator To: Administrator	 340821XXXXX3232  345800XXXXX4710
<input type="checkbox"/> 3	PAN	Zeeshan Shaikh/Inbox/M1-1/Mastero-Asterisk1.txt Mail Details Time: Wed 09/21/2016 06:31 AM From: Administrator To: Zeeshan Shaikh	 305383XXXXX0756  300934XXXXX1460
<input type="checkbox"/> 4	PAN	Zeeshan Shaikh/Inbox/Mastero_Colon Mail Details Time: Wed 09/21/2016 06:31 AM From: Administrator To: Administrator	 363163XXXXX5757  365424XXXXX9204

Office 365 Email scan results

Office 365 Email Scan Status				
Scan ID: 5 Scan Name: Scan_office365				
Process	Details		Status	
Office 365 Email Search	rkadav@controlcasegrc.com - outlook.office365.com		<ul style="list-style-type: none"> Total Mailbox: 15 Pending: 0 Scanned: 15 Failed: 0 Terminated: 0 Ignored: 0 	
Detailed Status				Show: All
#	Email Address	Mailbox	Status	Comments
1	rkadav@controlcasegrc.com	-	Completed	Data found
1.1	arana@controlcasegrc.com		Emails Scanned: 5478  100%	Scan Completed Successfully
1.2	cddmeetingroom@controlcasegrc.com		Emails Scanned: 5189  100%	Scan Completed Successfully
1.3	cddsharedmailbox@Controlcasetest.onmicrosoft.com		Emails Scanned: 132  100%	Scan Completed Successfully
1.4	CWDAdmin@controlcasegrc.com		Emails Scanned: 2367  100%	Scan Completed Successfully
1.5	gkale@controlcasegrc.com		Emails Scanned: 11321  100%	Scan Completed Successfully
1.6	kkarpe@controlcasegrc.com		Emails Scanned: 10567  100%	Scan Completed Successfully
1.7	kparthasarathy@controlcasegrc.com		Emails Scanned: 2898  100%	Scan Completed Successfully

Details of scan performed on Office 365 Email						
#	Email Address	Scan Status	Result	Records Found	False Positive	Details/Download
1	Office 365 Scan (rkadav@controlcasegrc.com)	Completed	Data found	65	0	
1.1	arana@controlcasegrc.com	Completed	Data not found	0	0	
1.2	cddmeetingroom@controlcasegrc.com	Completed	Data not found	0	0	
1.3	cddsharedmailbox@Controlcasetest.onmicrosoft.com	Completed	Data not found	0	0	
1.4	CWDAdmin@controlcasegrc.com	Completed	Data not found	0	0	
1.5	gkale@controlcasegrc.com	Completed	Data not found	0	0	
1.6	kkarpe@controlcasegrc.com	Completed	Data found	4	0	
1.7	kparthasarathy@controlcasegrc.com	Completed	Data not found	0	0	
1.8	migration_test1@controlcasegrc.com	Completed	Data not found	0	0	
1.9	rkadav@controlcasegrc.com	Completed	Data found	16	0	
1.10	rmishra@controlcasegrc.com	Completed	Data found	6	0	

Office 365 Scan (rkadav@controlcasegr.com) Show System marked false positives User marked false positives Remediated records

#	Result Type	File Path	Found String
1	PAN	snathe@controlcasegr.com/Drafts/Blank Subject Mail Details Time: 2016-05-30 04:21:35	524181XXXXXX3385
2	PAN	snathe@controlcasegr.com/Clutter/1_cdu/FW: test 8 Mail Details Time: 2016-05-27 04:28:47 From: rkadav@controlcase.com To: snathe@controlcasegr.com	342924XXXXXX0943 346351XXXXX3924
3	PAN	snathe@controlcasegr.com/Drafts/Blank Subject Mail Details Time: 2016-05-27 04:02:02 To: s	407681XXXXXX5672 412225XXXXXX0011
4	PAN	snathe@controlcasegr.com/Inbox/FW: test Mail Details Time: 2016-05-27 04:27:11 From: rkadav@controlcase.com To: snathe@controlcasegr.com, snathe@controlcasegr.com, snathe@controlcasegr.com, snathe@controlcasegr.com, snathe@controlcasegr.com, snathe@controlcasegr.com,	342924XXXXXX0943 346351XXXXX3924
5	PAN	snathe@controlcasegr.com/Inbox/./FW: test 10 Mail Details Time: 2016-05-27 04:29:06 From: rkadav@controlcase.com To: snathe@controlcasegr.com	342924XXXXXX0943 346351XXXXX3924
6	PAN	snathe@controlcasegr.com/Inbox/./card data Mail Details Time: 2016-02-23 09:25:23	548534XXXXXX7496 514151XXXXXX6963

Outlook PST file scan results

File System Scan Report

Scan ID: 7 | Scan Name: Scan_Outlook


File Share: \\127.0.0.1\ES\outlook Show System marked false positives User marked false positives Remediated records

#	Result Type	File Path	Found String
1	PAN	\\127.0.0.1\ES\outlook\backup_12_April.pst\Sent Items\FW: cc data\CC data.txt	485838XXXXXX6838 452757XXXXXX4841
2	PAN	\\127.0.0.1\ES\outlook\backup_12_April.pst\kishor vaswani\RE: Search Tool\search_confirmed.txt	653165XXXXXX6531 430154XXXXXX0168
3	PAN	\\127.0.0.1\ES\outlook\backup_12_April.pst\Controlcase Team\RE: Base24 Location of Track\PAN Data\vs081209.dat	(trackdata) .XXXXXXXXXXXXXXXX=09061013260577600 000? 425838XXXXXX3551
4	PAN	\\127.0.0.1\ES\outlook\backup_12_April.pst\Nishant Pandey\Blank Subject\credit card search_confirmed.txt	376932XXXXX1004 447692XXXXXX3441
5	PAN	\\127.0.0.1\ES\outlook\backup_12_April.pst\parin lapasia\Scan Results for Virgin\Virgin.zip\Virgin\CustomerRelations\search_VAA_CR.xml	371537XXXXX1008 540758XXXXXX7303
6	PAN	\\127.0.0.1\ES\outlook\backup_12_April.pst\parin lapasia\Scan Results for Virgin\Virgin.zip\Virgin\Maple\search_Maple.xml	377311XXXXX8893 520953XXXXXX6829

 **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 gets distorted if the Internet Explorer "compatibility mode" is on.

WHAT IS NEW OR CHANGED IN CDD 8.6

1. GDPR – Database Metadata Scanning support.
2. Support to scan only those files which are modified after a last scan.
3. SQL server scanning – TLS Protocol V1.2 is now supported.
4. Enhanced keyword lists management.

WHAT IS NEW OR CHANGED IN CDD 8.0

1. Amazon S3 bucket scanning support.
2. Cassandra database scanning support.
3. MongoDB database scanning support.
4. Rescan only failed targets.
5. Scan level email notification.
6. Ability to scan specific database/table(s).
7. Luhn's verification feature.
8. Improved Keyword searching.
 - a. Option to search exact keyword.
9. Improved the False Positive Management algorithm for lesser false positives.
10. CDD database backup/restore functionality.
11. Database scanning show primary Id of table in CSV reports.
12. Upgraded the Core packages (Apache/PHP/MySQL) to minimize the security risks.

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/>