Phone: 703.483.6383 Fax: 703.991.5341 www.controlcase.com

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

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.

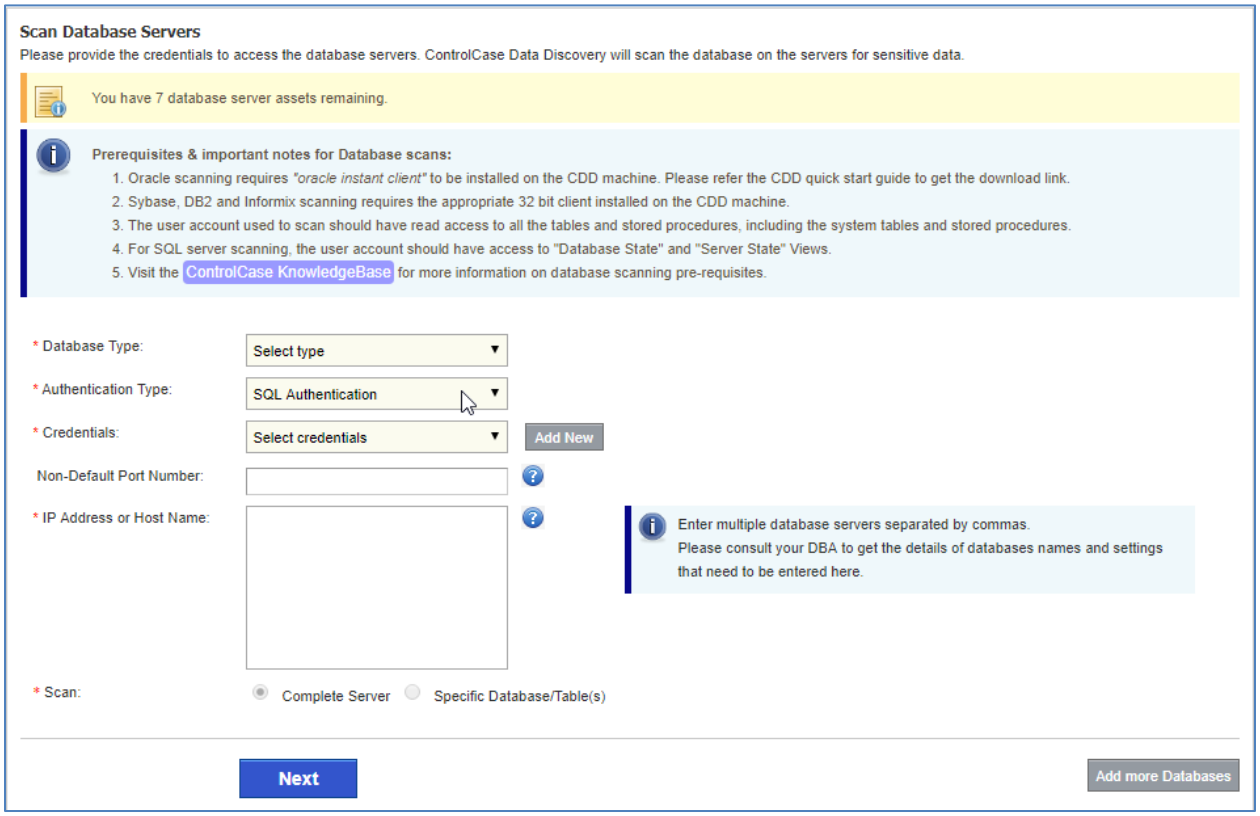
1. The Exchange management console and Windows PowerShell must be installed on the Exchange server.
2. **The 64-bit Outlook client must be installed on the Exchange server**.
3. The scanning user must have a mailbox on the Exchange server.
4. The scanning user must have the right to create a network 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:

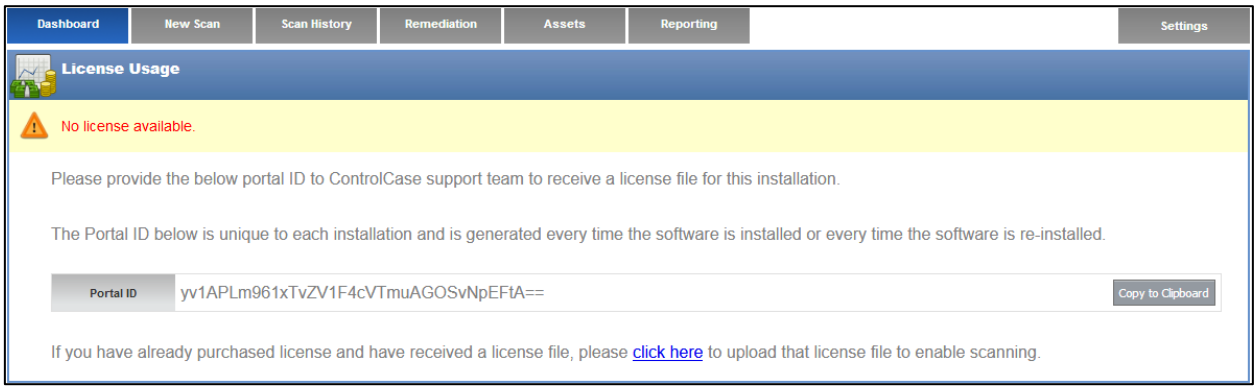


SCANNING DB2 AND SYBASE DATABASES (OPTIONAL)

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.

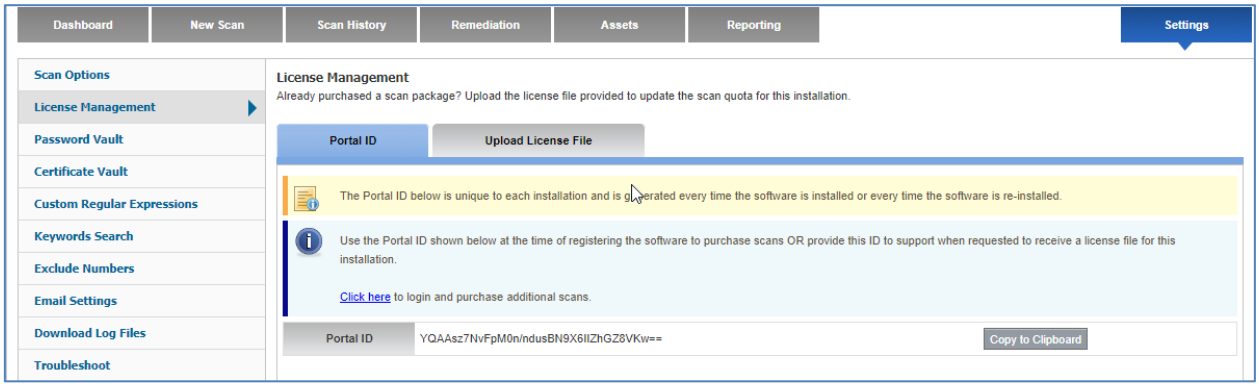
REGISTER A NEW INSTALLATION AND GET A LICENSE

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

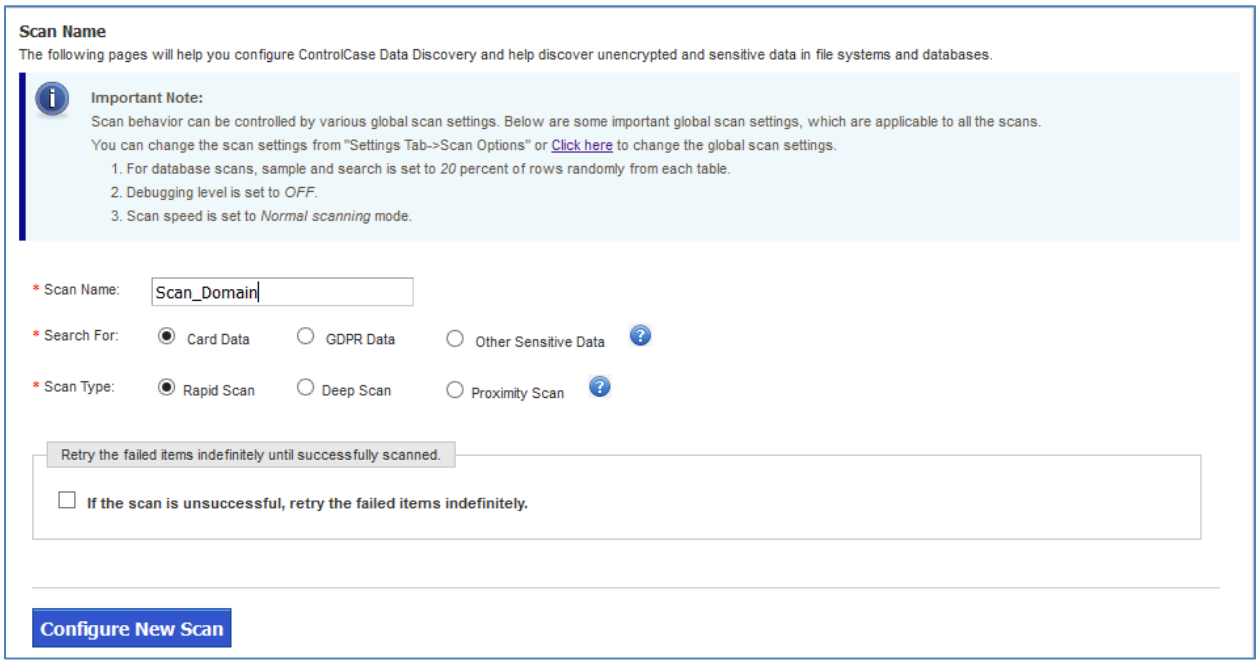
ControlCase will provide you a license file through email, which you will need to upload back to CDD using the Settings tab -> License Management and "Upload License File" page.
Save the file onto your hard disk and then select that file using the Browse. Button and click UPLOAD.



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.



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

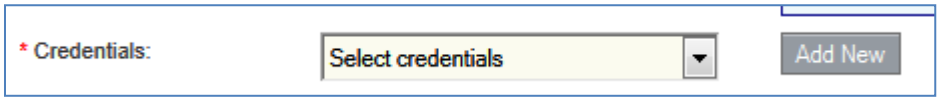
If you want to scan File systems, you can add 6 types of scans

- 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.

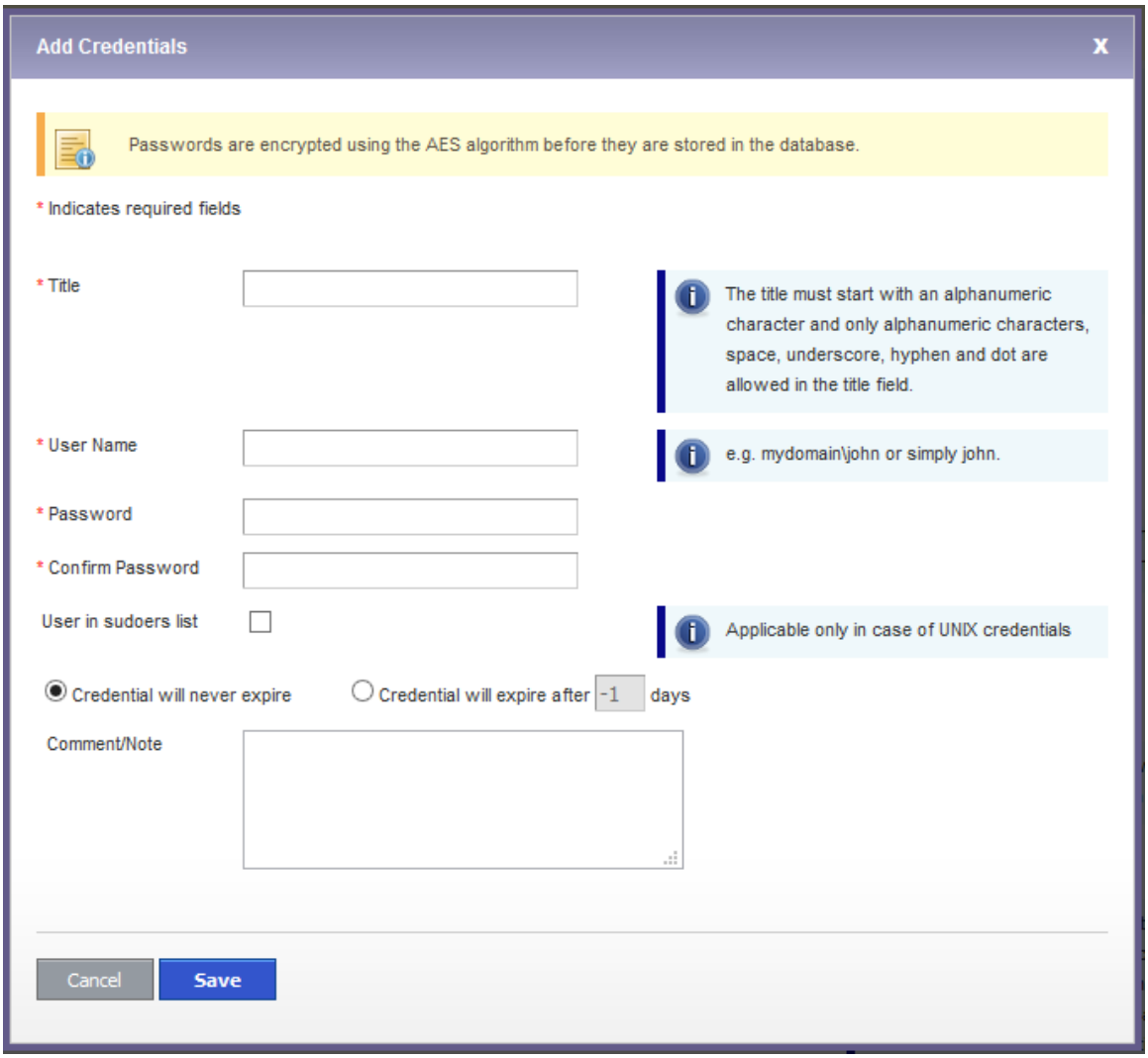
- Scan Mainframe files on a File Server (exported samples set of files)

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

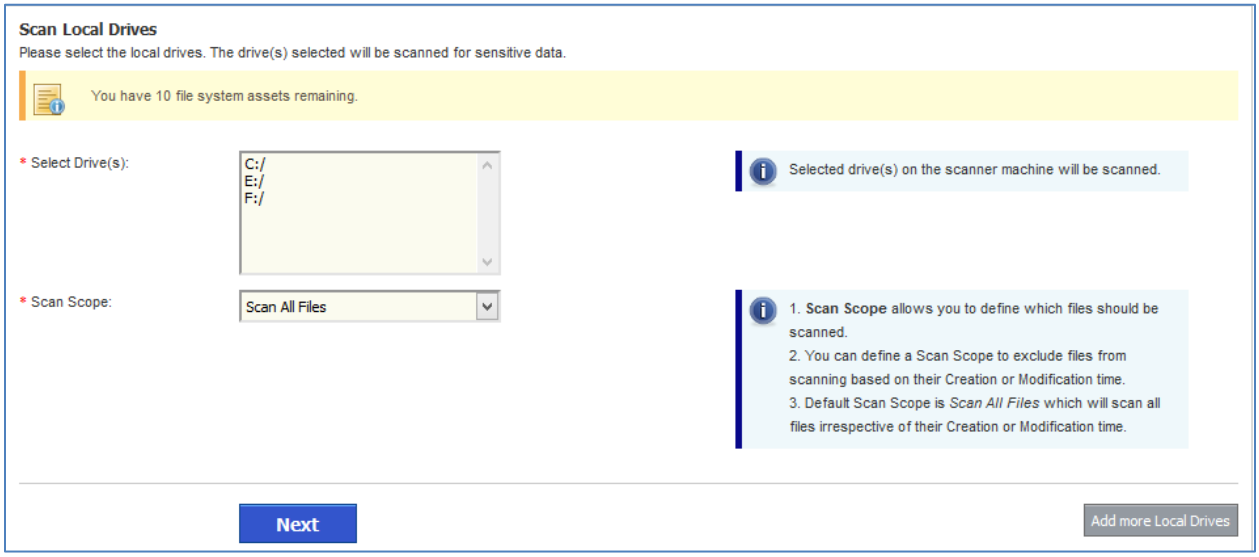
The credentials used to authenticate to the target machines to perform the scans are stored in the "Password Vault" in an encrypted state. When scanning a target for the first time, you will need to add the credentials to the Vault. This can be accomplished by clicking the ADD NEW button next to the Credentials



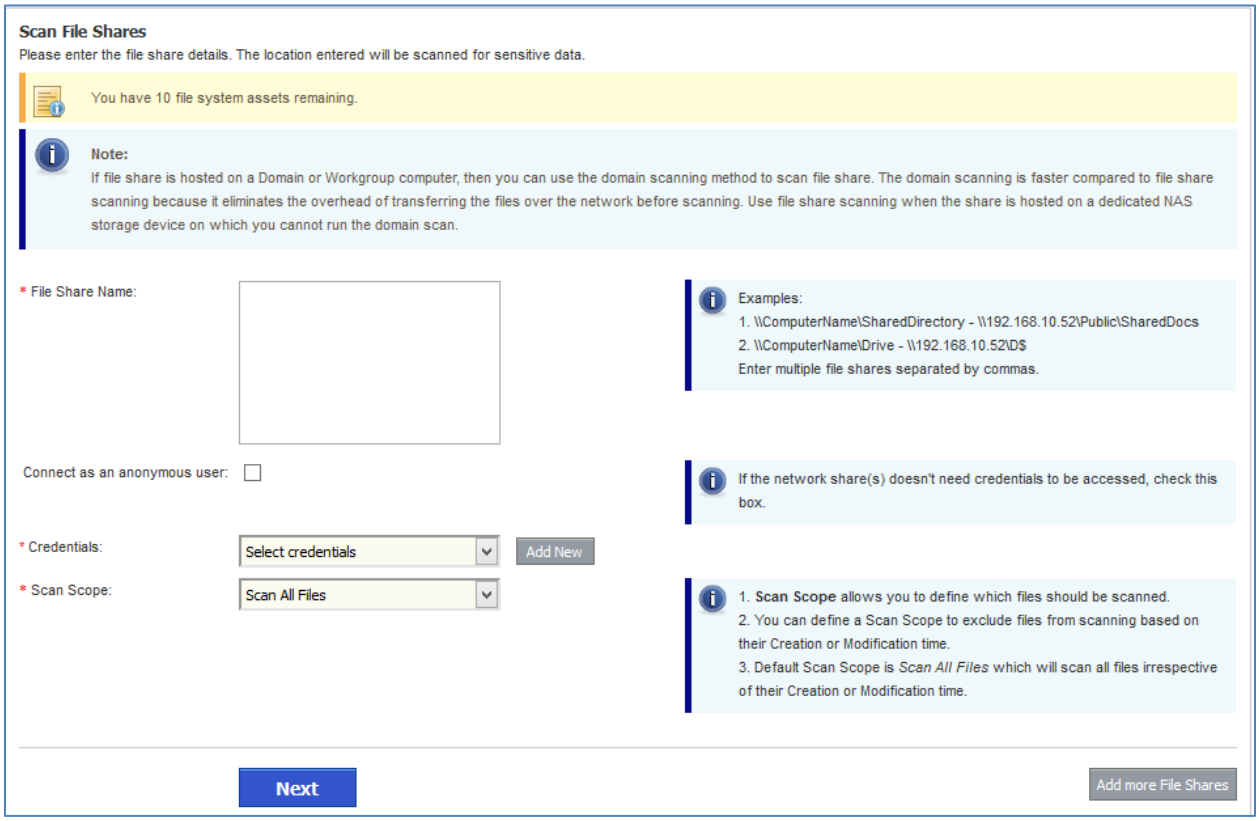
This will bring up another screen where you can add the credentials



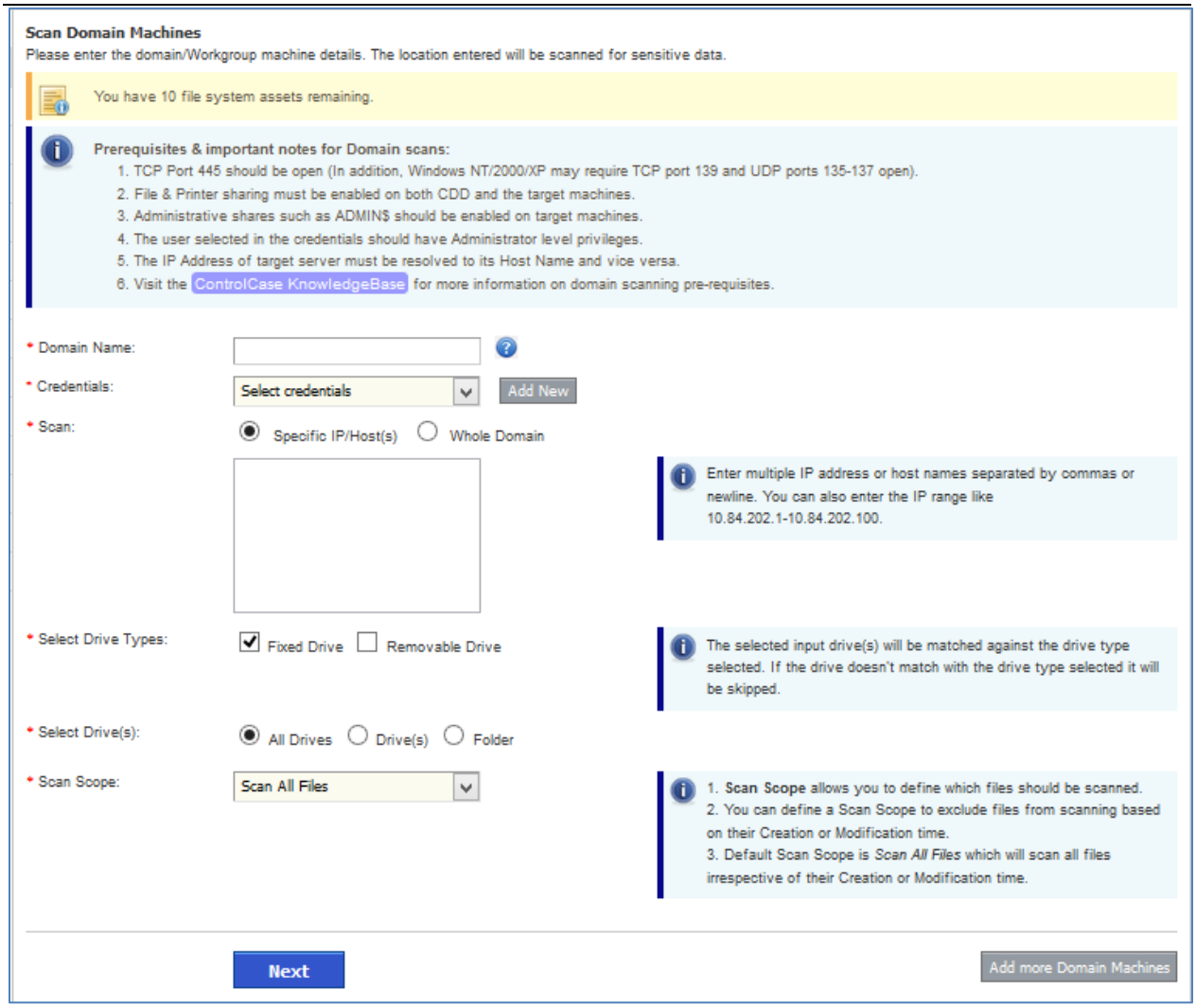
Local Drive/Disk



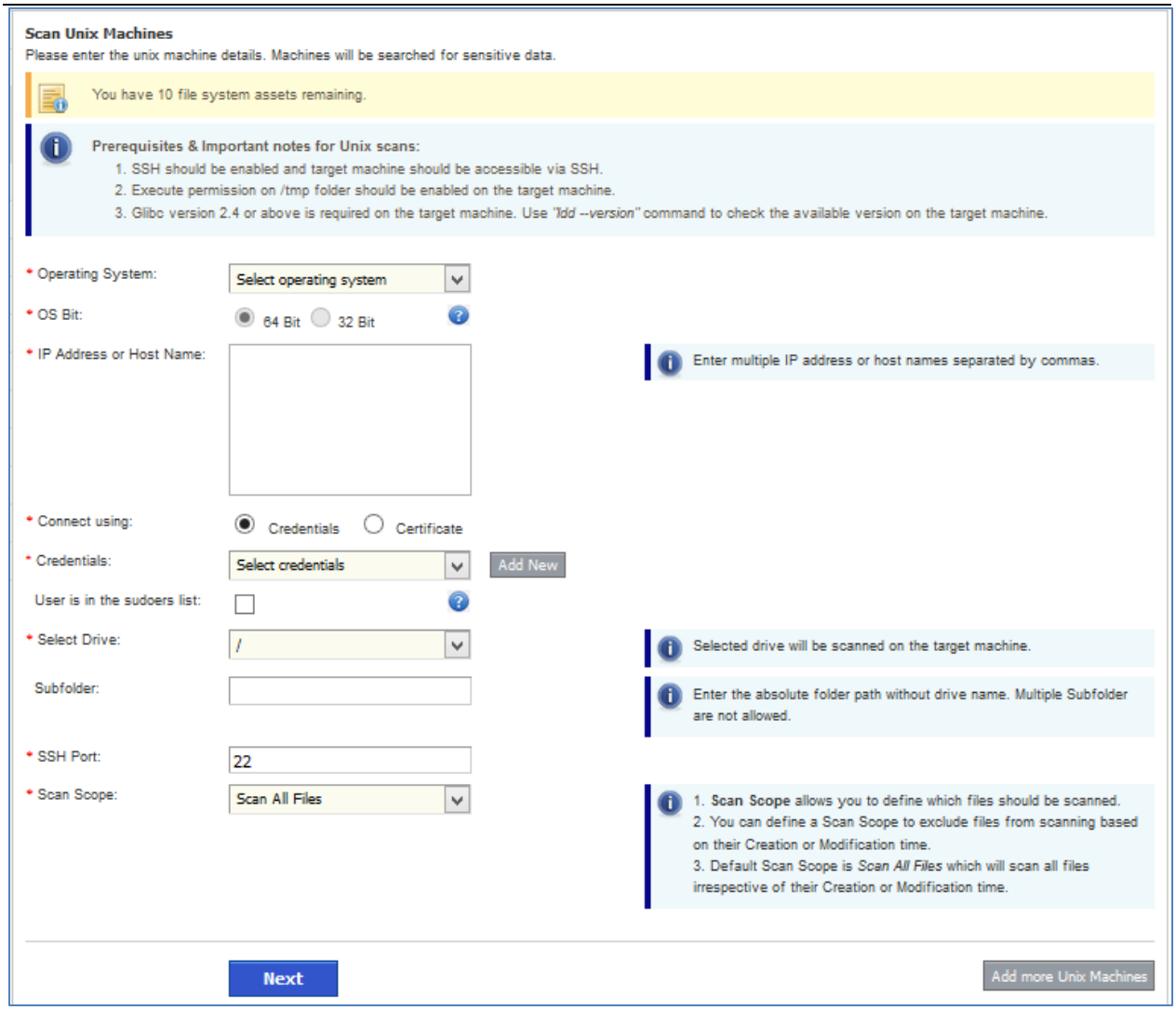
File Share (Network Drive)



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:
Select credentials
Add New
* Scan:
Specific IP/Host(s)
Whole Domain
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
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.
* Select Drive(s):
All Drives
Drive(s)
Folder
* Scan Scope:
Scan All Files
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

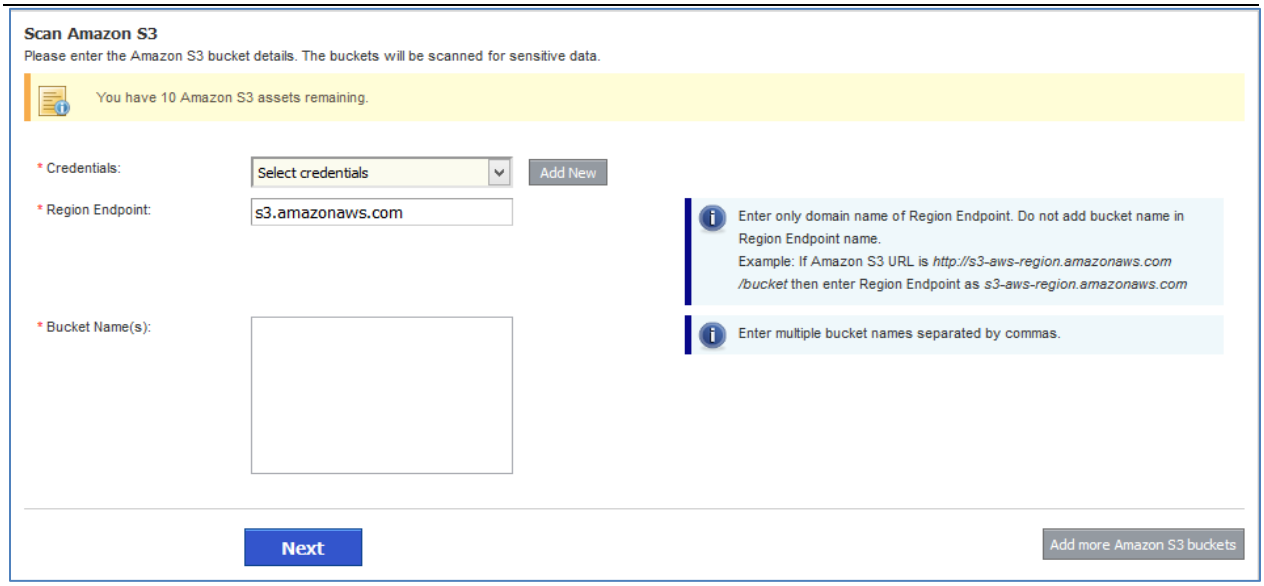


You can add the following types of Operating Systems

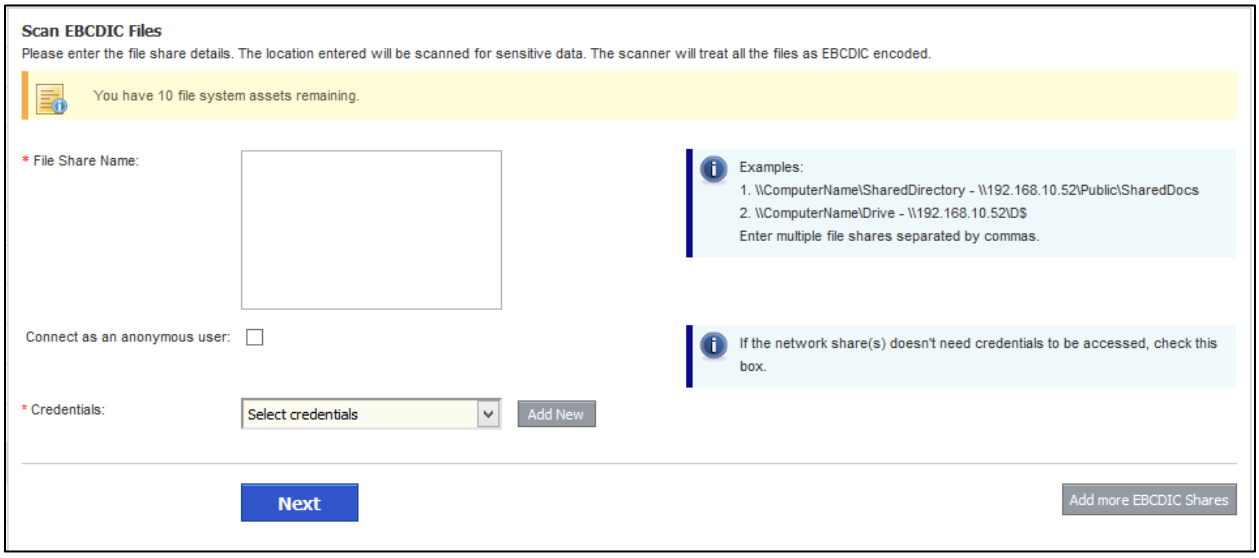
1. Linux/Unix and variants
2. MAC OS
3. Solaris X86 and Sparc
4. HP UX
5. AIX
6. FreeBSD

You can keep adding more File system scans by click the Add more … button

Amazon S3



Mainframe file formatted files (EBCDIC)

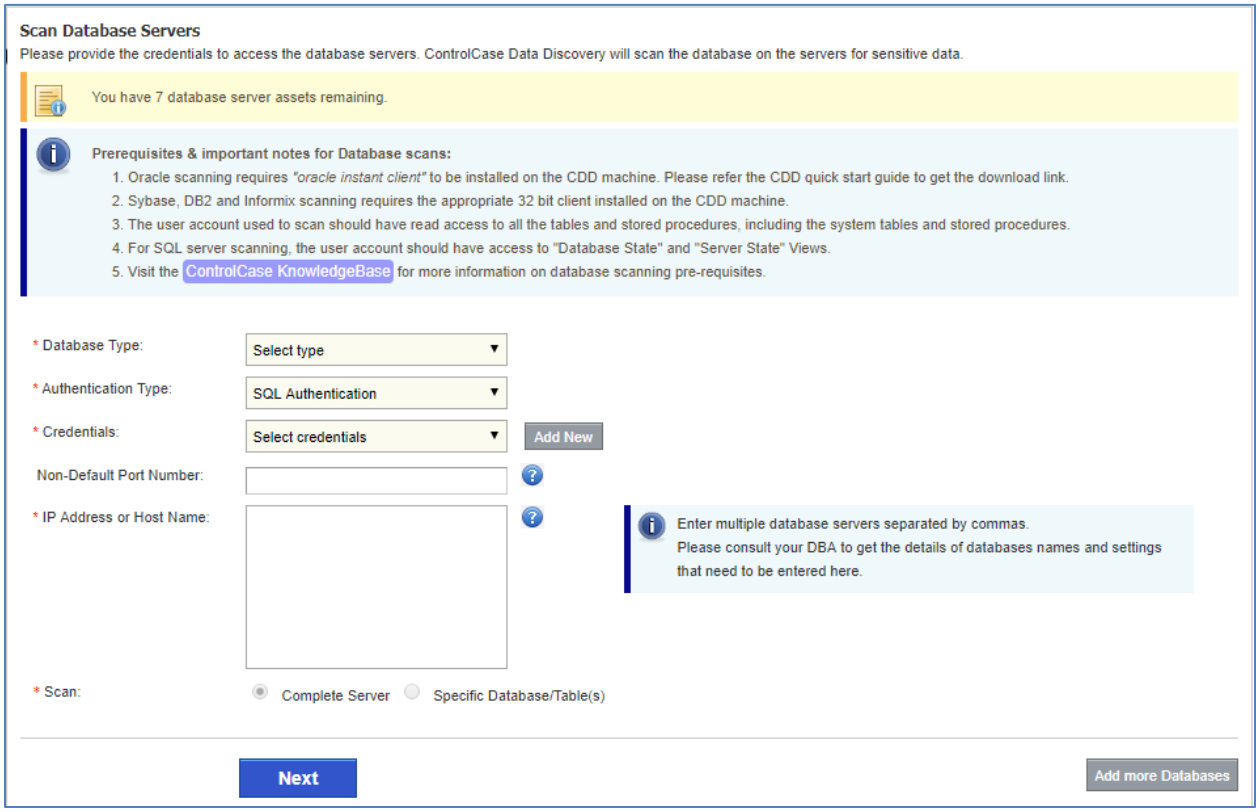


CDD cannot directly scan Mainframe computers, but a sample set of files exported from the mainframes in EBCDIC format can be placed on a file share and then CDD can scan those files.

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.

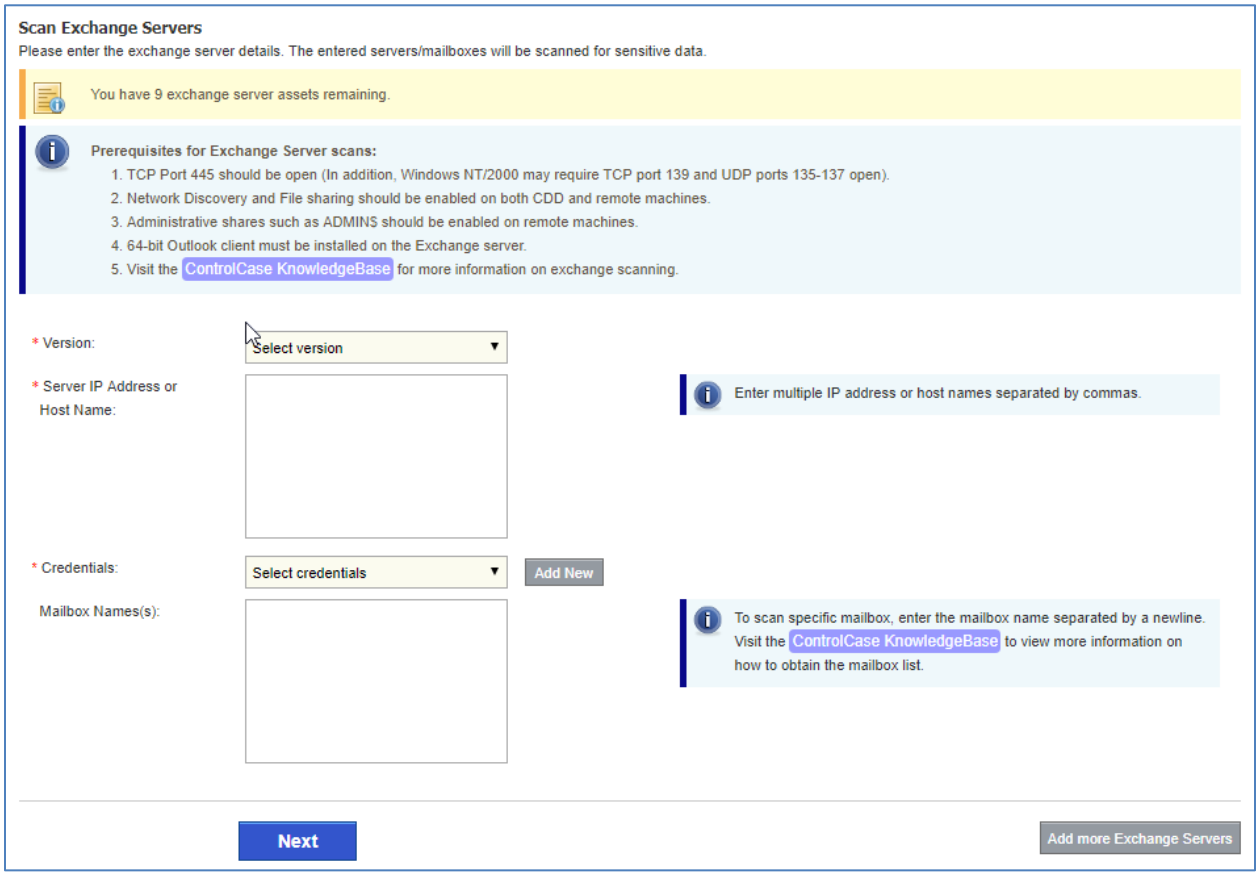


You can keep adding more Database scans by click the “Add more Databases” button, when you are done (or if you don’t want to scan any databases, just click the Scan Configuration Summary to start the scan)

Email Servers scans

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.

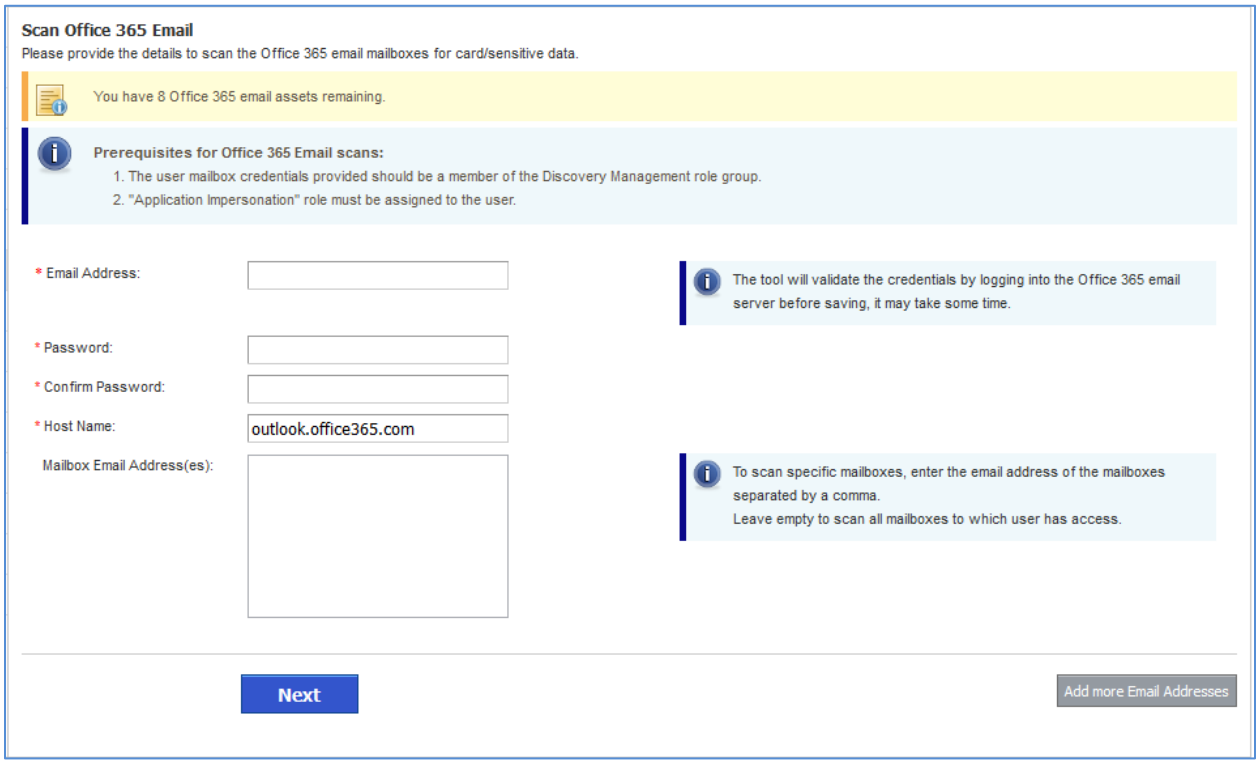


Office 365 Email Scanning

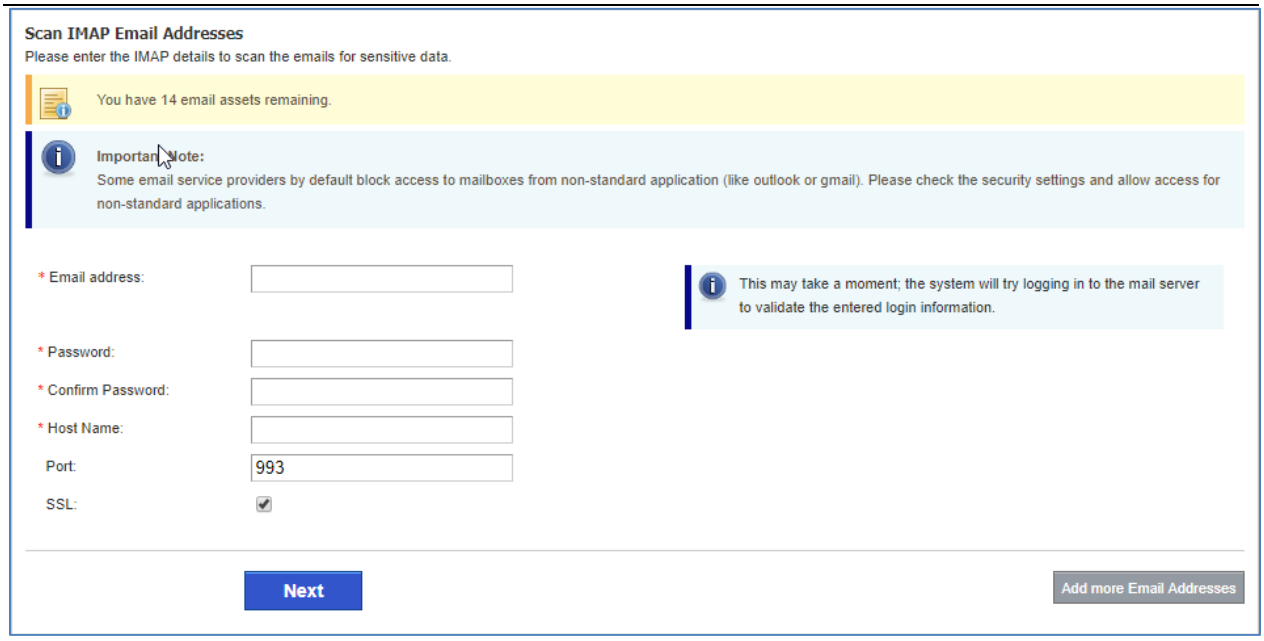
Due to the hosted nature of the Office 365 on Microsoft's servers, there are some limitations in the way the scans can occur.

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.

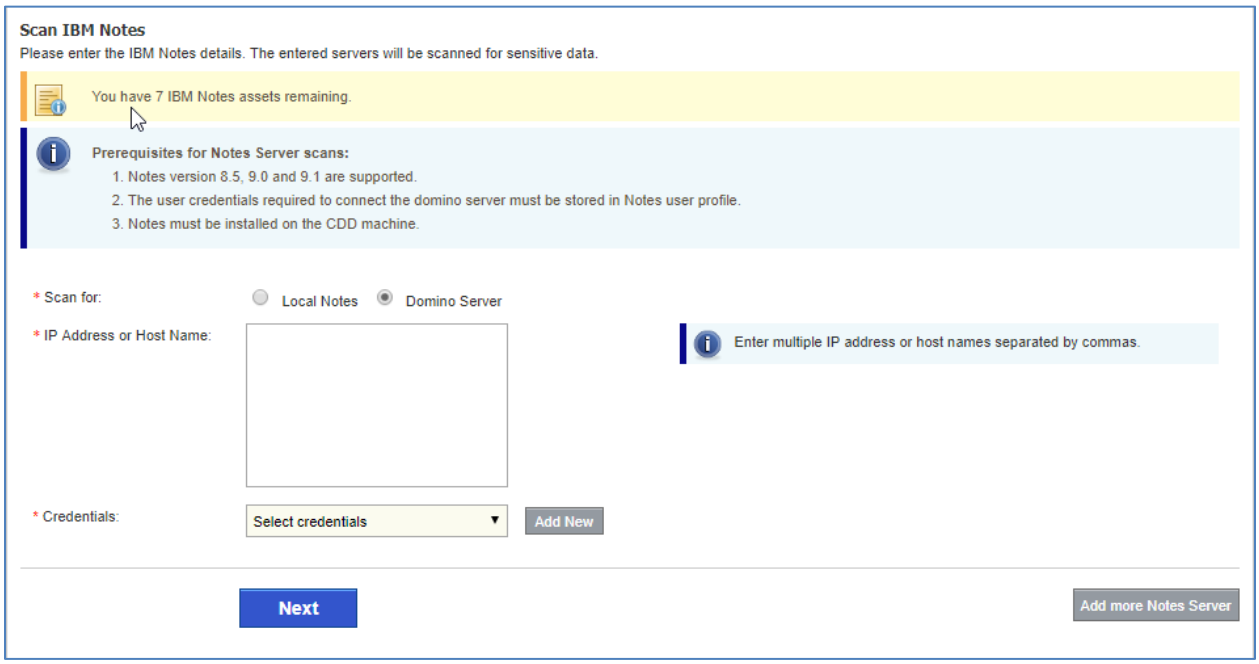
We have to use a sampling based approach for mailboxes and emails and those settings can be configured in the Settings area.



IMAP based Servers



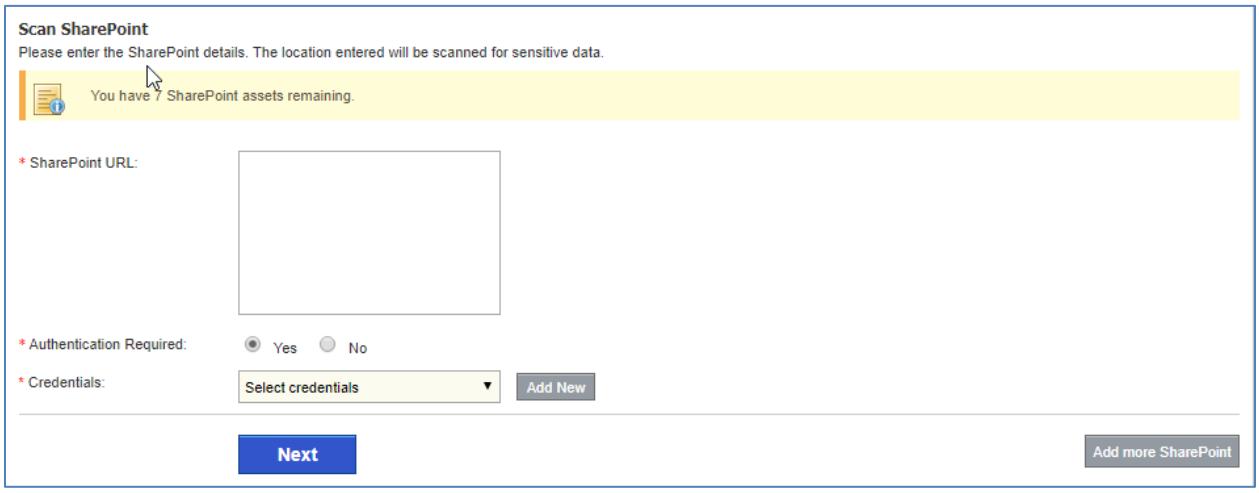
IBM Notes Servers



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

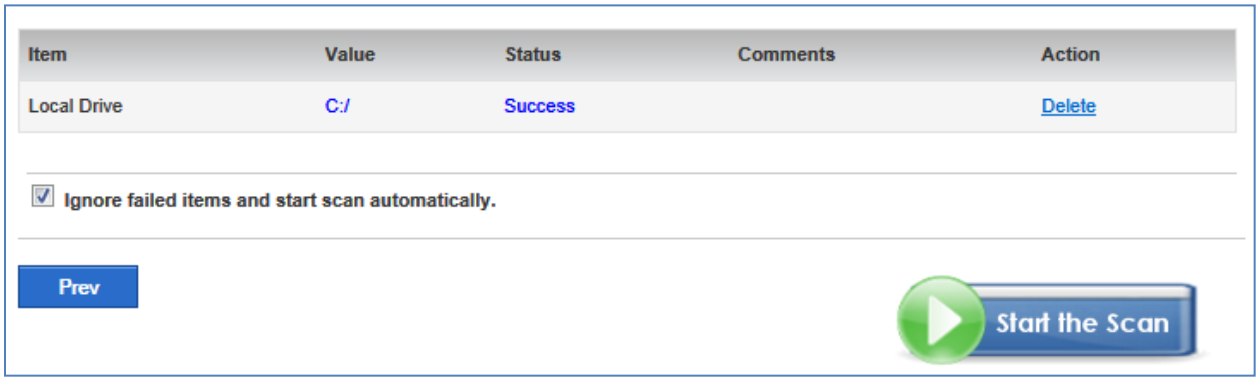
Microsoft SharePoint scans

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.



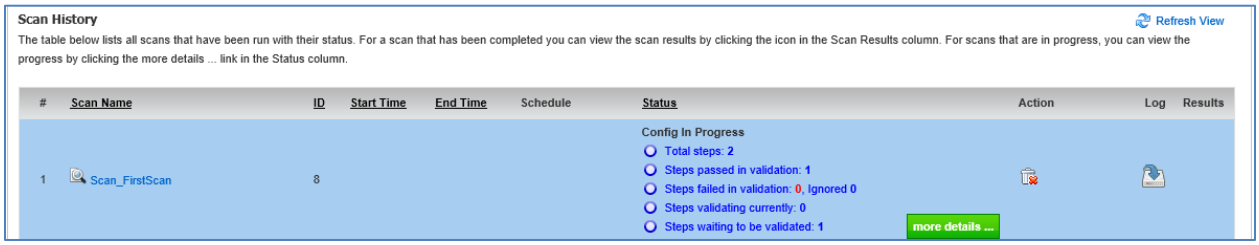
Start the scan

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.



Scan Status

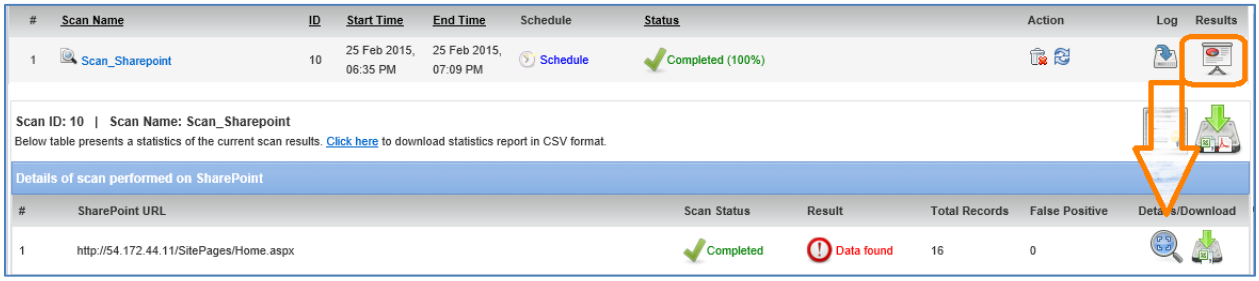
The progress of the scan can be seen on the next page or by clicking the SCAN HISTORY tab

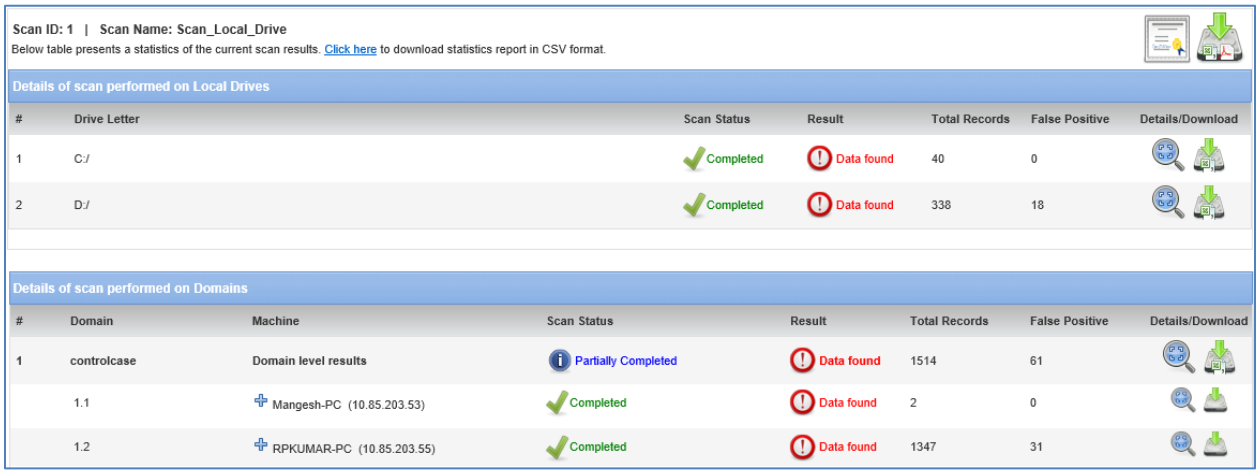


Additional details can be seen by clicking the MORE DETAILS… button

View Scan Results

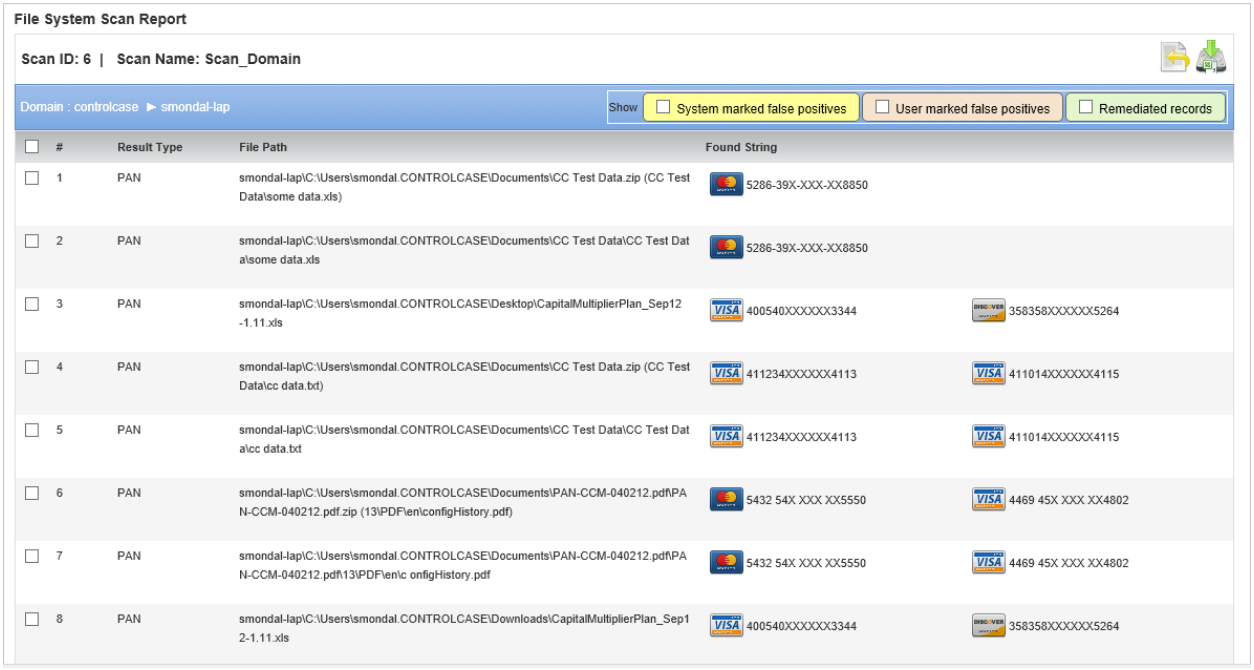
Once the scan is completed, the results can be seen from the SCAN HISTORY tab or through the DASHBOARD tab





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

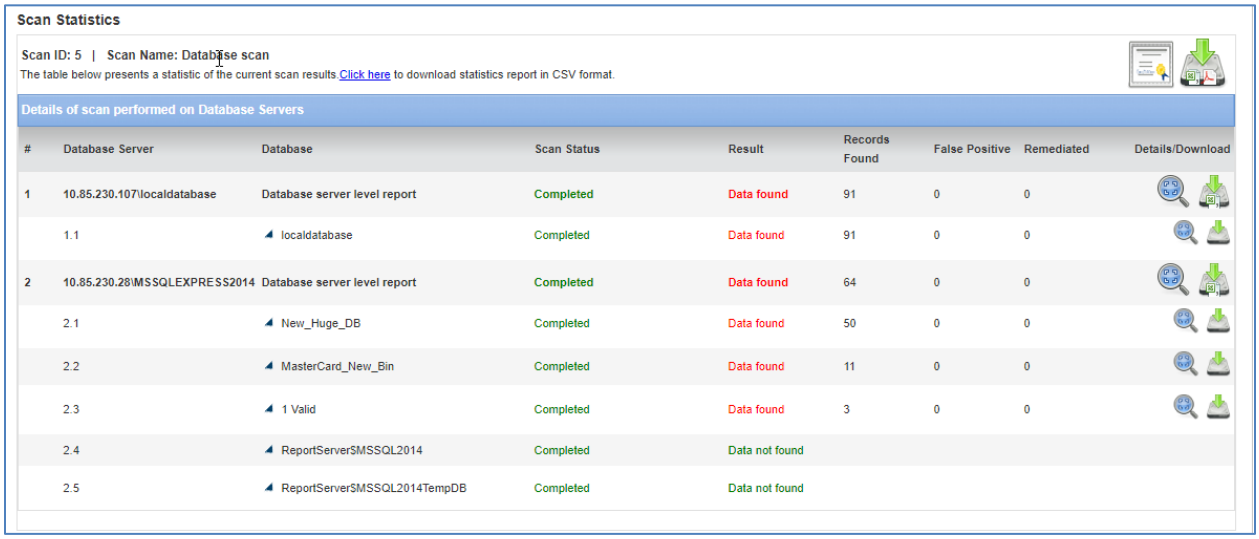
Scan ID: 6 | Scan Name: Scan_Domain

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.txt)	411234XXXXXX4113	411014XXXXXX4115
5	PAN	smondal-lap\C:\Users\smondal.CONTROLCASE\Documents\CC Test Data\CC Test Data\cc data.txt	411234XXXXXX4113	411014XXXXXX4115
6	PAN	smondal-lap\C:\Users\smondal.CONTROLCASE\Documents\PAN-CCM-040212.pdf\PAN-CCM-040212.pdf.zip (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\c onfigHistory.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



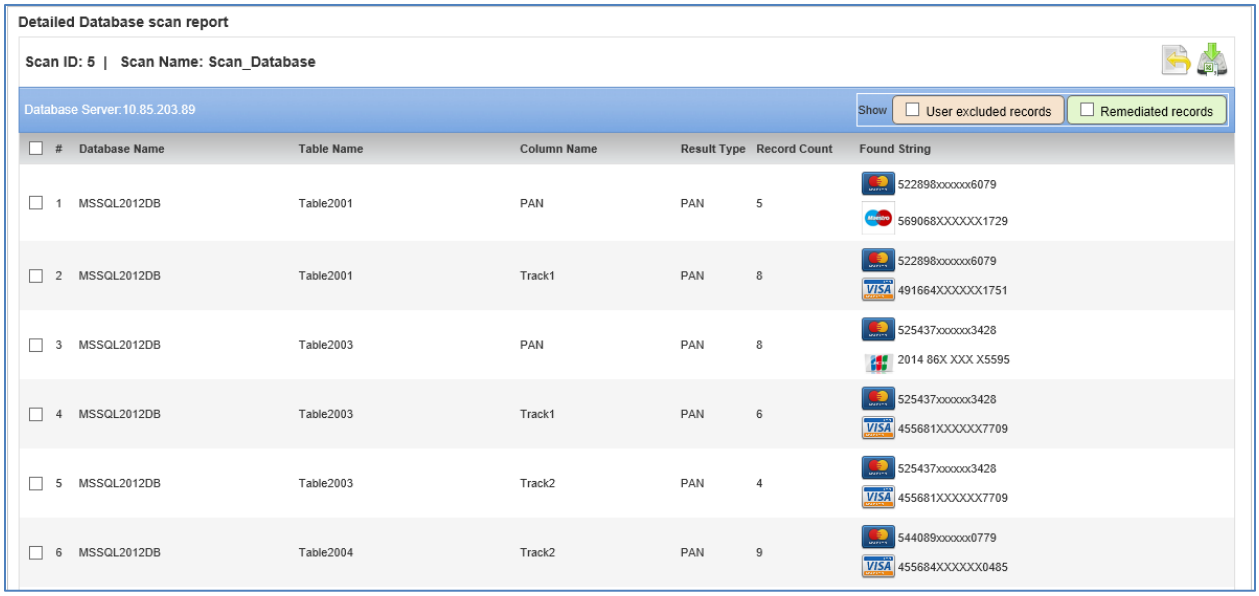
Scan Statistics

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	
1.1		localdatabase	Completed	Data found	91	0	0	
2	10.85.230.28\MSSQLEXPRESS2014	Database server level report	Completed	Data found	64	0	0	
2.1		New_Huge_DB	Completed	Data found	50	0	0	
2.2		MasterCard_New_Bin	Completed	Data found	11	0	0	
2.3		1 Valid	Completed	Data found	3	0	0	
2.4		ReportServerSMSSQL2014	Completed	Data not found				
2.5		ReportServerSMSSQL2014TempDB	Completed	Data not found				



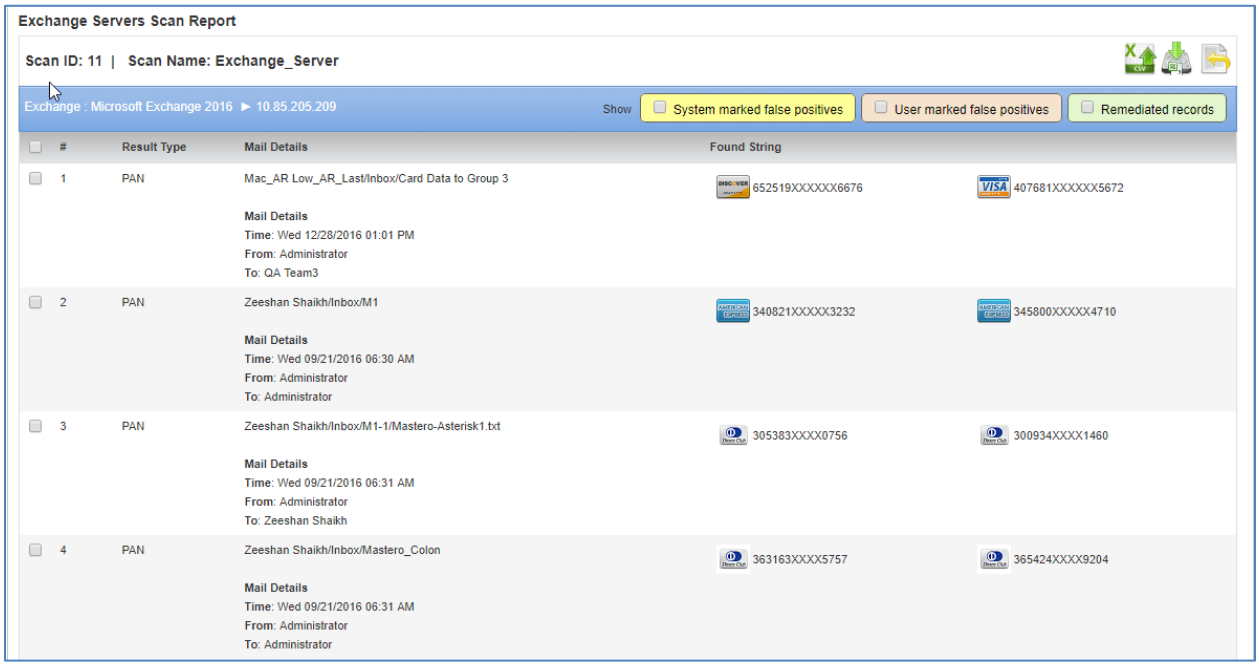
Detailed Database scan report

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
1	MSSQL2012DB	Table2001	PAN	PAN	5	522898xxxxxx6079 569068XXXXXX1729
2	MSSQL2012DB	Table2001	Track1	PAN	8	522898xxxxxx6079 491664XXXXXX1751
3	MSSQL2012DB	Table2003	PAN	PAN	8	525437xxxxxx3428 2014 86X XXX X5595
4	MSSQL2012DB	Table2003	Track1	PAN	6	525437xxxxxx3428 455681XXXXXX7709
5	MSSQL2012DB	Table2003	Track2	PAN	4	525437xxxxxx3428 455681XXXXXX7709
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	
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
2	PAN	Zeeshan Shaikh/Inbox/M1 **Mail Details** **Time**: Wed 09/21/2016 06:30 AM **From**: Administrator **To**: Administrator	340821XXXXX3232	345800XXXXX4710
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	305383XXXX0756	300934XXXX1460
4	PAN	Zeeshan Shaikh/Inbox/Mastero_Colon **Mail Details** **Time**: Wed 09/21/2016 06:31 AM **From**: Administrator **To**: Administrator	363163XXXX5757	365424XXXX9204

Office 365 Email scan results

Office 365 Email Scan Status

Scan ID: 5 | Scan Name: Scan_office365

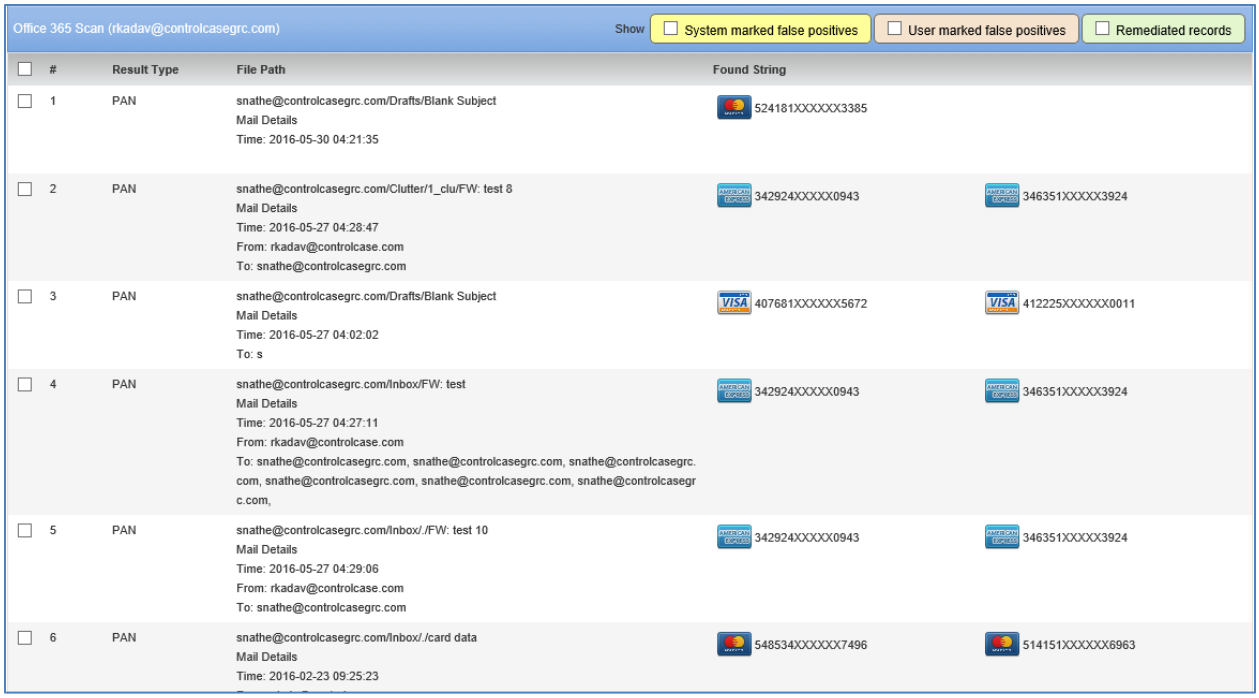
Process	Details	Status
Office 365 Email Search	rkadav@controlcasegrc.com - outlook.office365.com	Total Mailbox: 15 Pending: 0 Scanned: 15 Failed: 0 Terminated: 0 Ignored: 0

Detailed Status Show: All

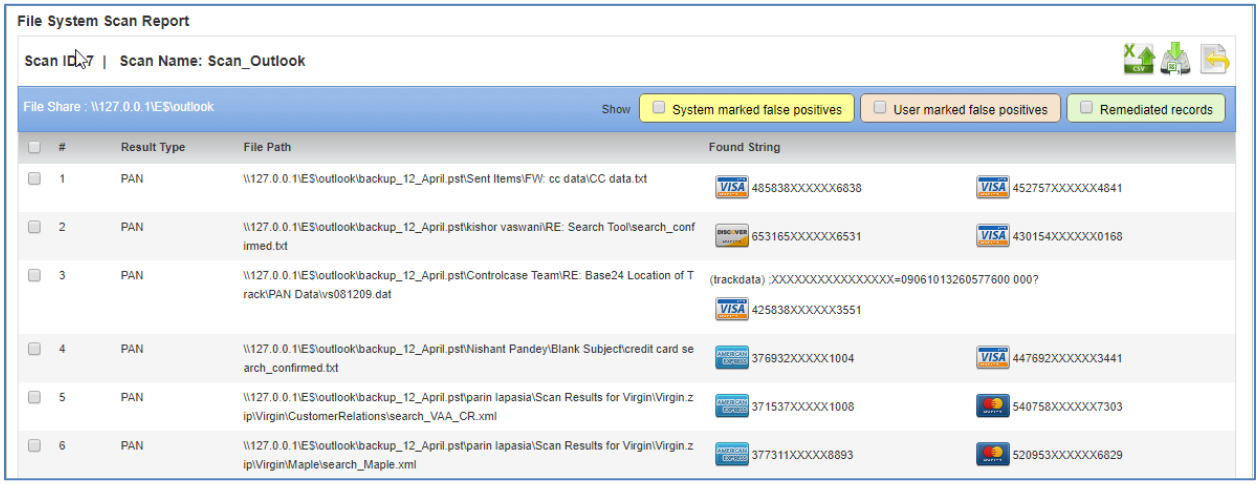
#	Email Address	Mailbox	Status	Comments
1	rkadav@controlcasegrc.com	-	Completed	Data found
1.1		arana@controlcasegrc.com	Emails Scanned: 5478 100%	Scan Completed Successfully
1.2		cddmeetingroom@controlcasegrc.com	Emails Scanned: 5189 100%	Scan Completed Successfully
1.3		cddsharedmailboxe@Controlcasetest.onmicrosoft.com	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	cddsharedmailboxe@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	



Outlook PST file scan results



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/