ControlCase™ Data Discovery

Version 10.10
Updated Aug 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 11
Domain Scan 14
Unix/Linux variants 15
Amazon S3 16
Database scans 18
Microsoft Exchange Server Scans 19
Office 365 Scanning 20
IMAP based Servers 24
Microsoft SharePoint scans (On-premise) 25
Start the scan 26
Scan Status 27
View Scan Results 28
CDD False Positive Management and Remediation Feature 33

Scanning tips 34
Troubleshooting Failed scans 35
Known Issues 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

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

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

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

Step 6 →
Then download and install CDD 10.10.3.0 Upgrade Patch from
https://home.controlcase.com/downloads/ControlCase_Data_Discovery_V10.10.3.0_Update.exe

Step 7 →
Then download and install CDD 10.10.4.0 Upgrade Patch from
https://home.controlcase.com/downloads/ControlCase_Data_Discovery_V10.10.4.0_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

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

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

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

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

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

Step 9 →

Then download and install CDD 10.10.3.0 Upgrade Patch from
https://home.controlcase.com/downloads/ControlCase_Data_Discovery_V10.10.3.0_Update.exe

Step 10 →

Then download and install CDD 10.10.4.0 Upgrade Patch from
https://home.controlcase.com/downloads/ControlCase_Data_Discovery_V10.10.4.0_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

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

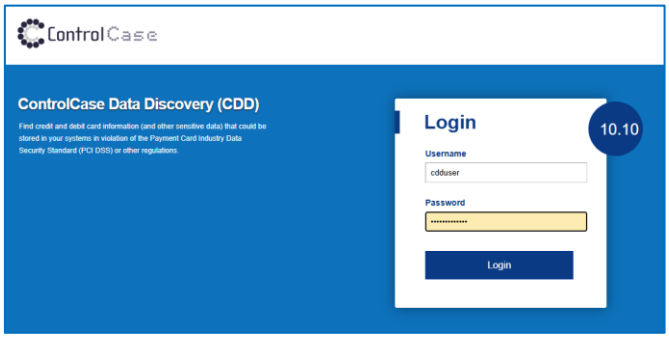
FIRST TIME LOGIN AFTER INSTALLTION

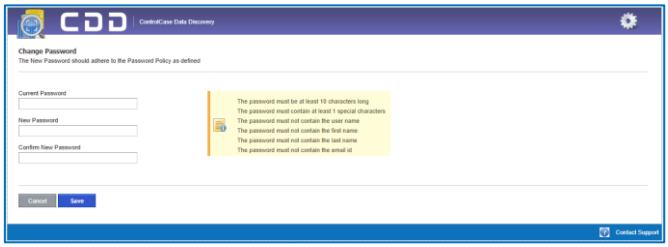
Once the **CDD Standalone version** is installed, you will be redirected to the CDD login page in your default browser. The URL http://localhost:845/ will open automatically.

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



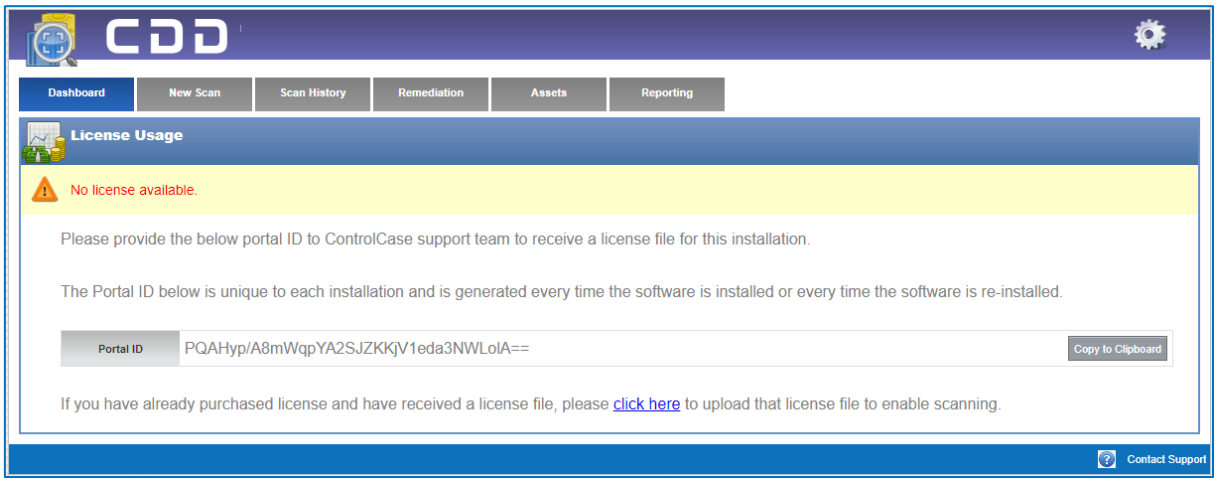


Note: The password must meet the following criteria:

- 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

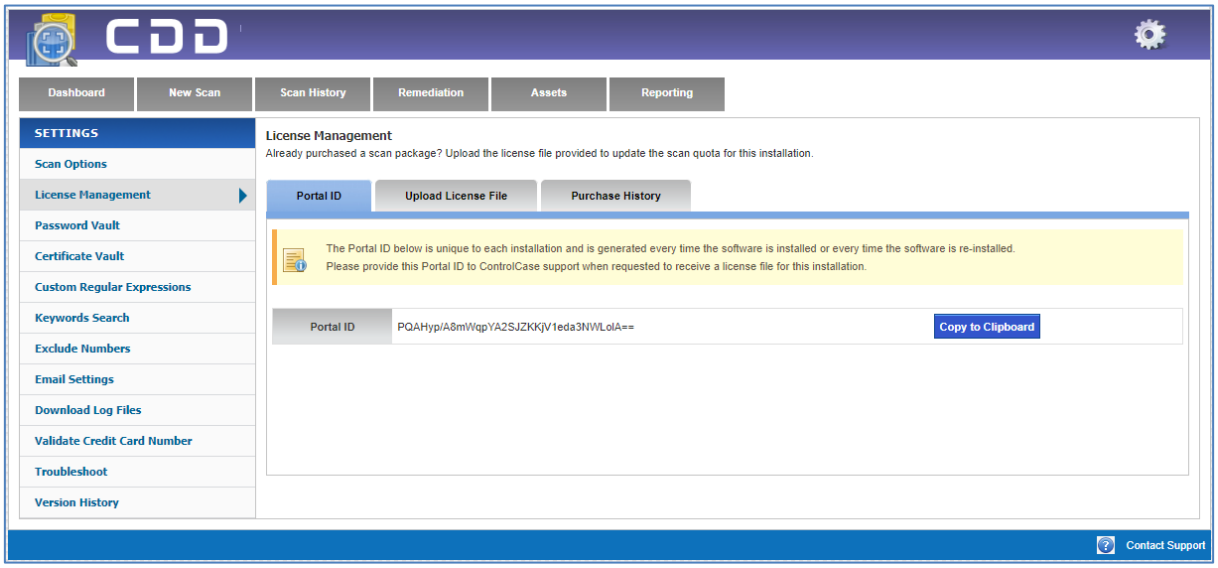
REGISTER A NEW INSTALLATION AND GET A LICENSE

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.



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.



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

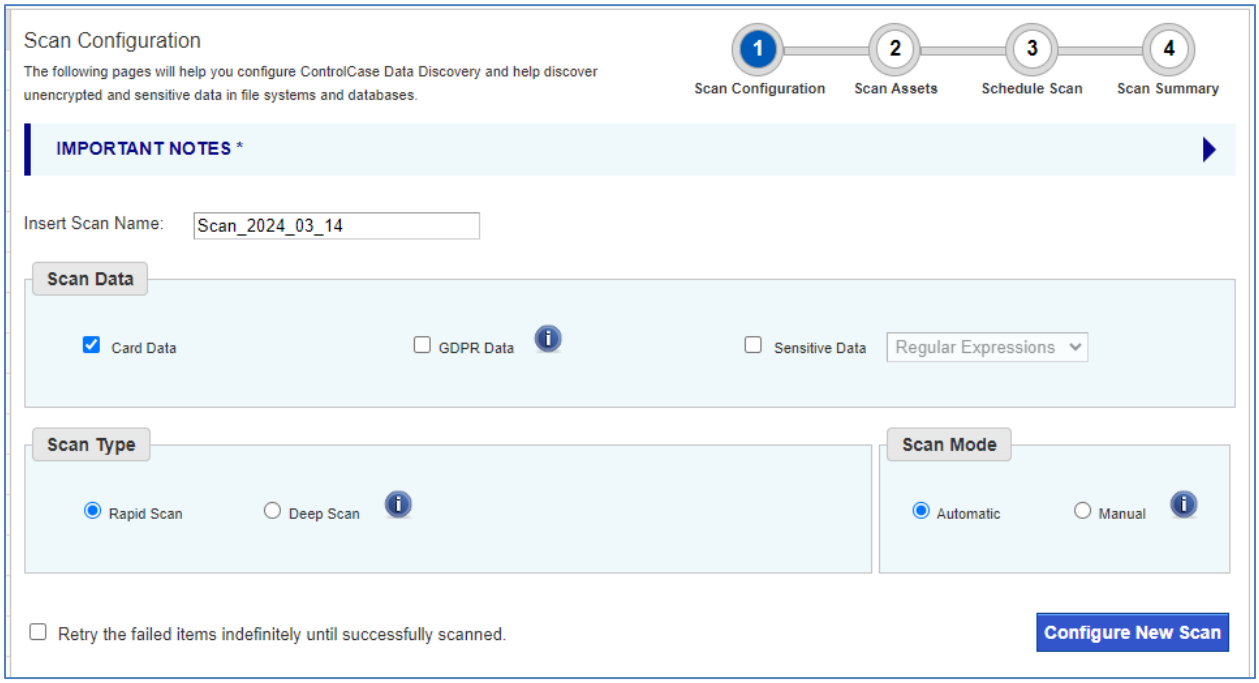
Scanning DB2, Sybase and Informix databases (Optional)

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.



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

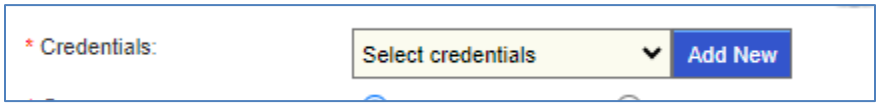
File System Scans

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

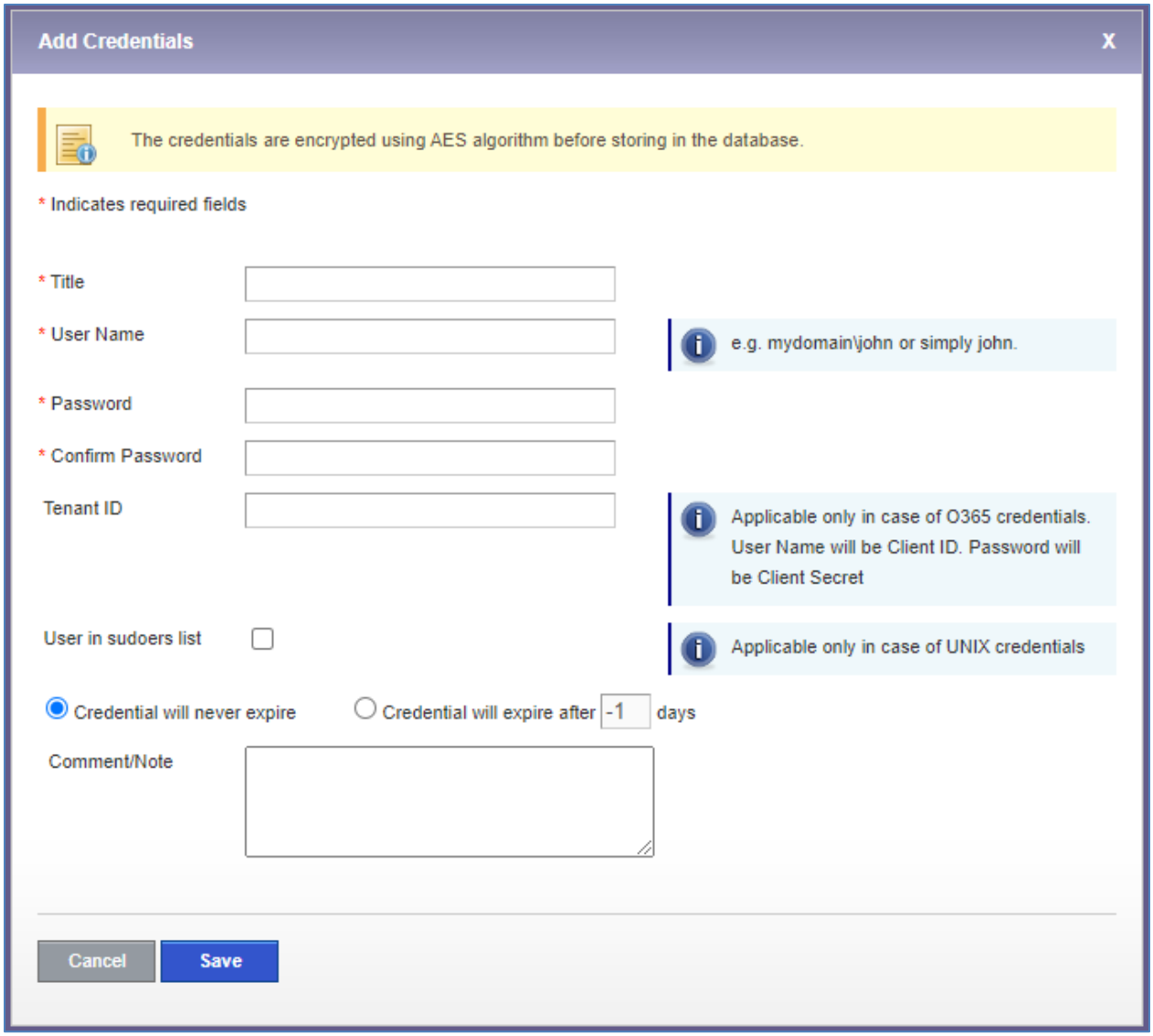
- Scan local hard disks (attached to the scanning computer)
- Scan File Shares/ Network drives (UNC scans)
- Scan the whole Windows Domain (Active Directory)
- Scan Unix/Linux variants, MAC machines
- Scan Amazon S3 buckets.
- Scan Mainframe files on a File Server (exported samples set of files)

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

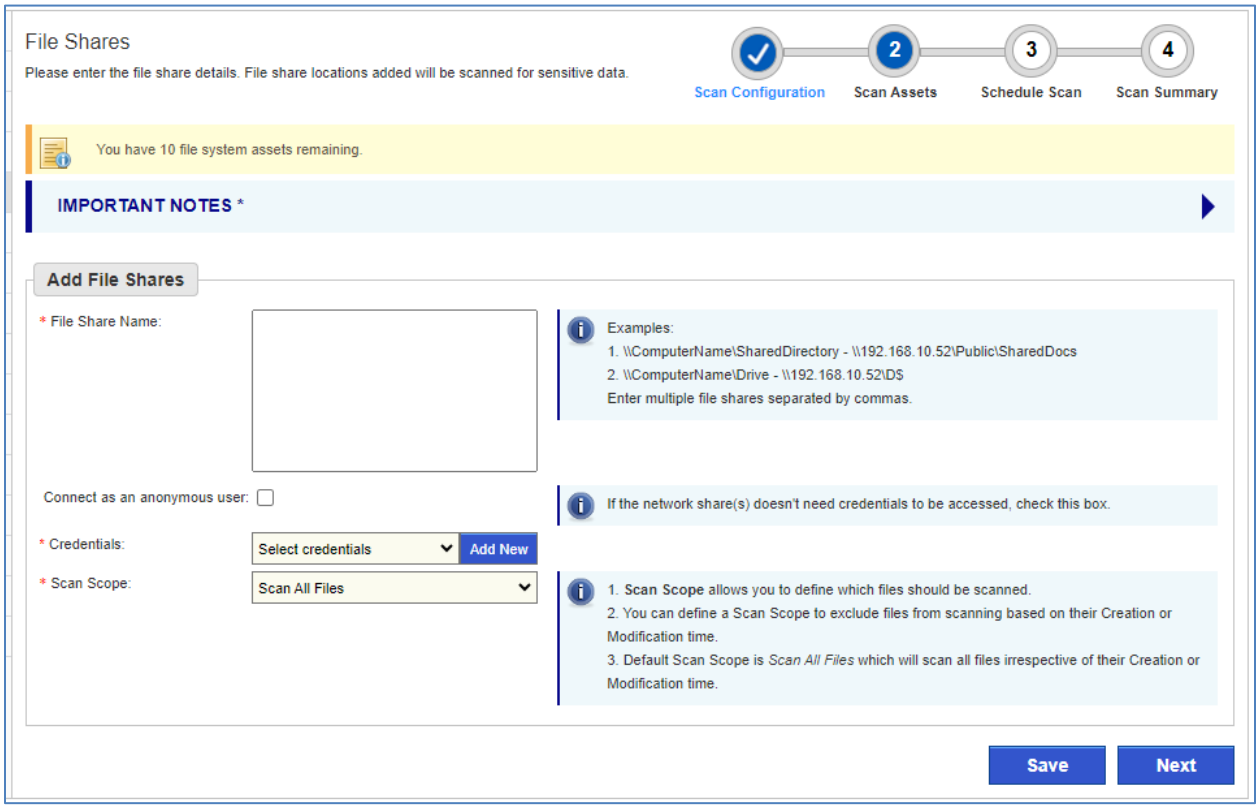
The credentials used to authenticate to the target machines to perform the scans are stored in the "Password Vault" in an encrypted state. When scanning a target for the first time, you will need to add the credentials to the Vault. This can be accomplished by clicking the ADD NEW button next to the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



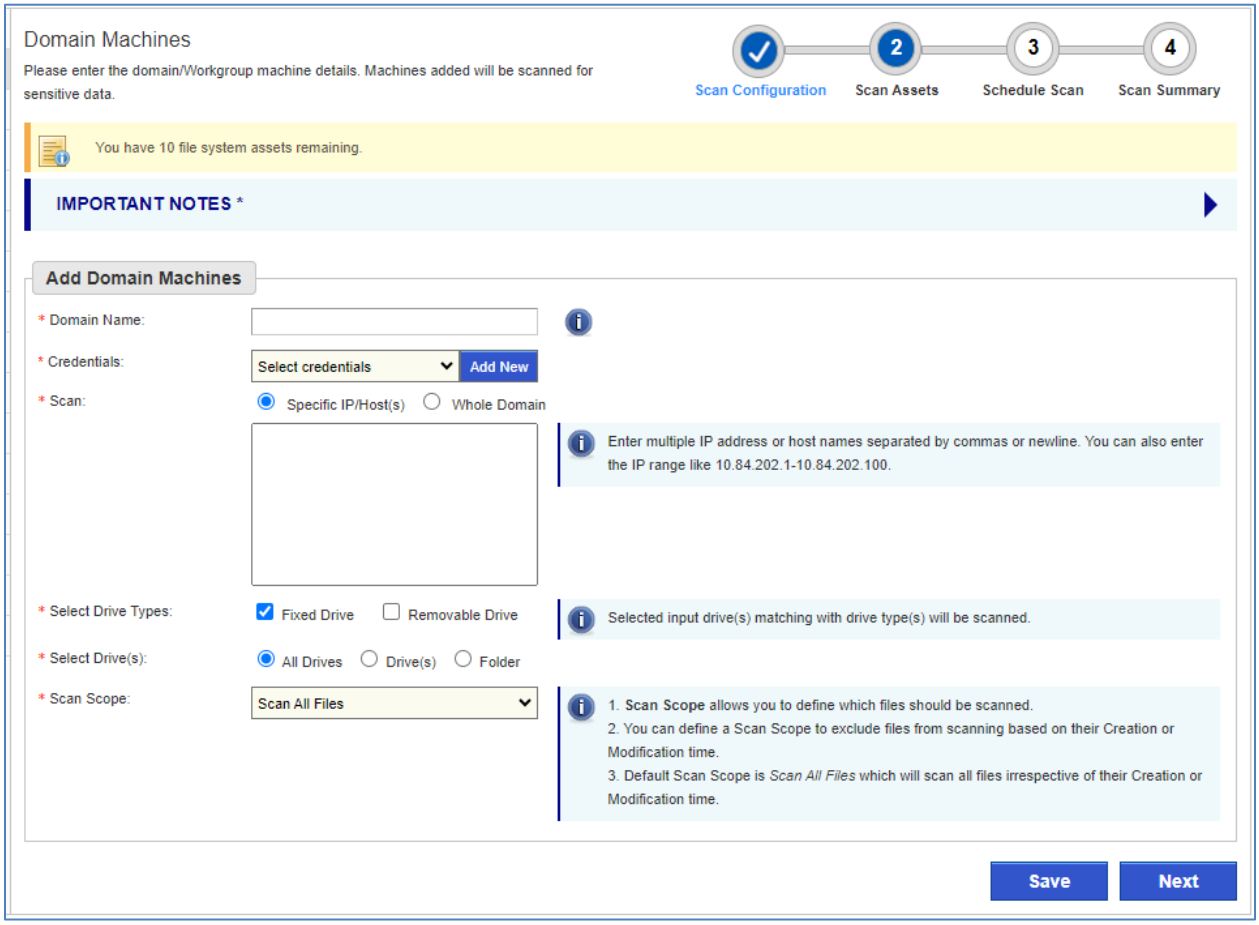
This will bring up another screen where you can add the credentials.


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 -1 days
Comment/Note
Cancel
Save

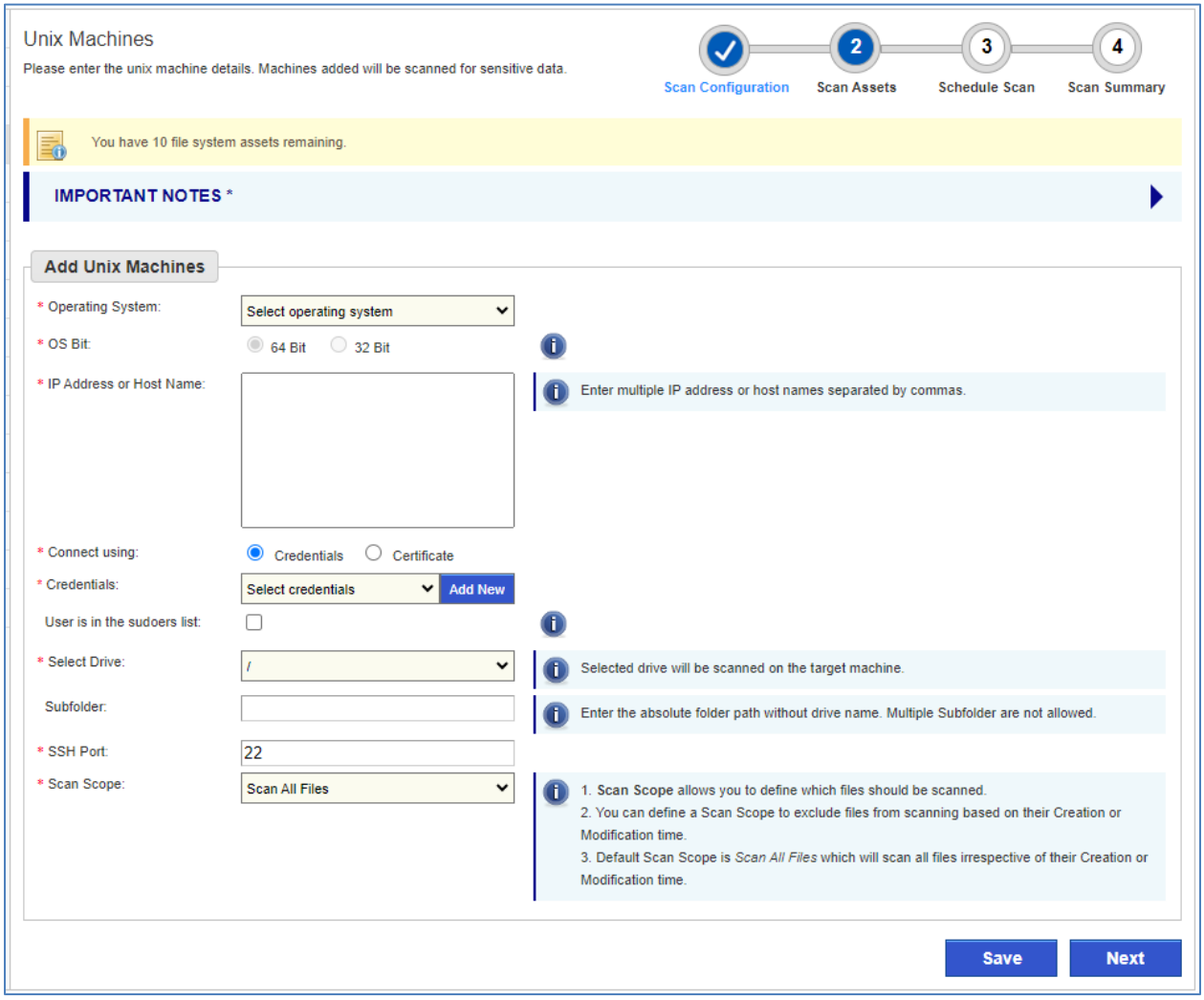
File Share (Network Drive)



Domain Scan


Domain Machines
Please enter the domain/Workgroup machine details. Machines added will be scanned for sensitive data.
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:
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
Selected input drive(s) matching with drive type(s) will be scanned.
* 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.
Save
Next

Unix/Linux variants

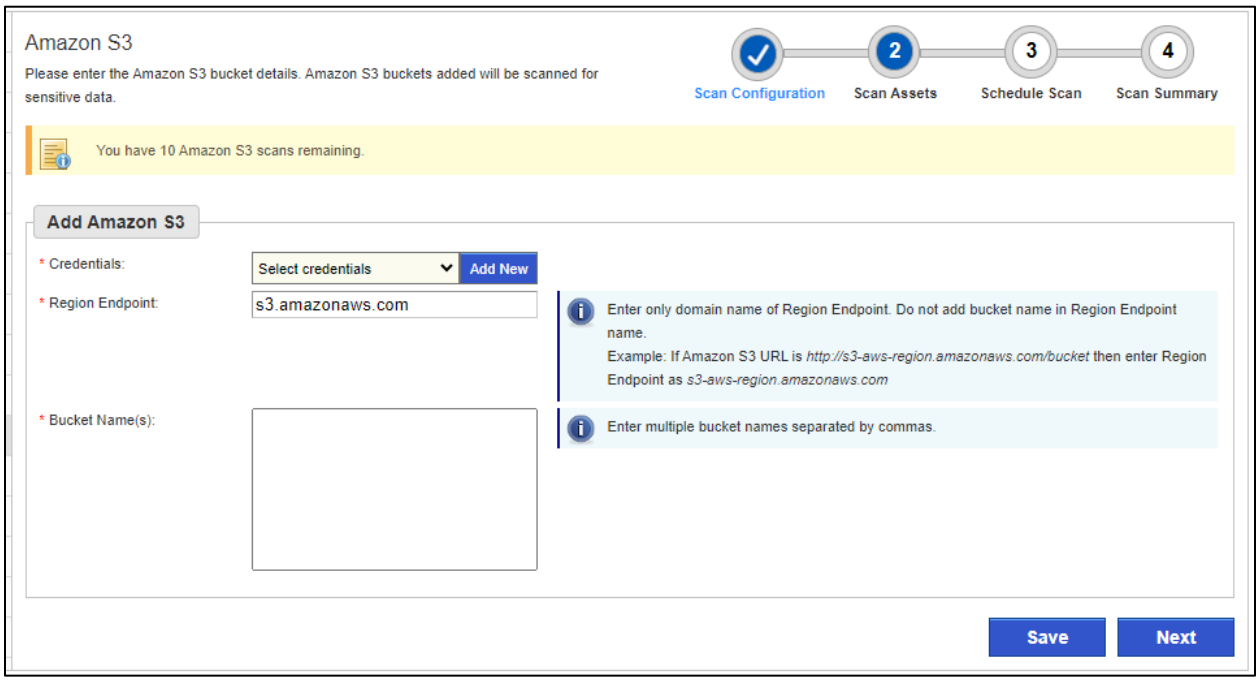


You can add the following types of Operating Systems

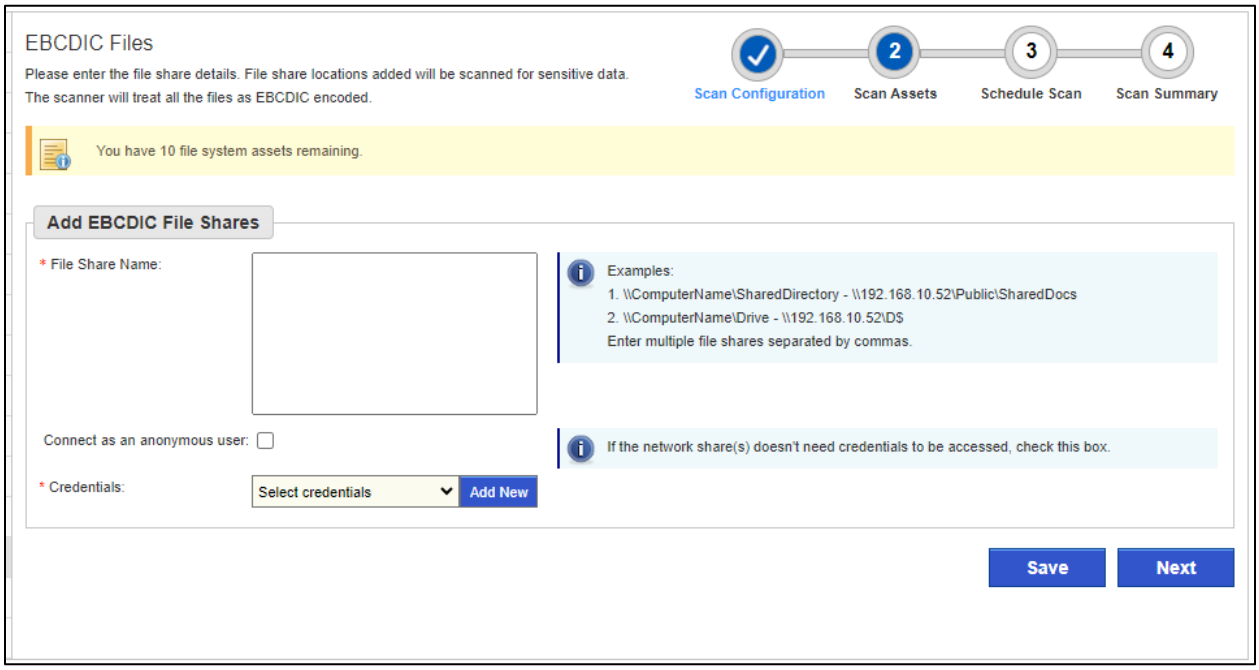
1. Linux/Unix and variants
2. MAC OS
3. Solaris X86 and Sparc
4. HP UX
5. AIX
6. FreeBSD

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

Amazon S3


Amazon S3
Please enter the Amazon S3 bucket details. Amazon S3 buckets added will be scanned for sensitive data.
Scan Configuration
Scan Assets
Schedule Scan
Scan Summary
You have 10 Amazon S3 scans remaining.
Add Amazon S3
* Credentials:
Select credentials
Add New
* Region Endpoint:
s3.amazonaws.com
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
* Bucket Name(s):
Enter multiple bucket names separated by commas.
Save
Next

Mainframe file formatted files (EBCDIC)

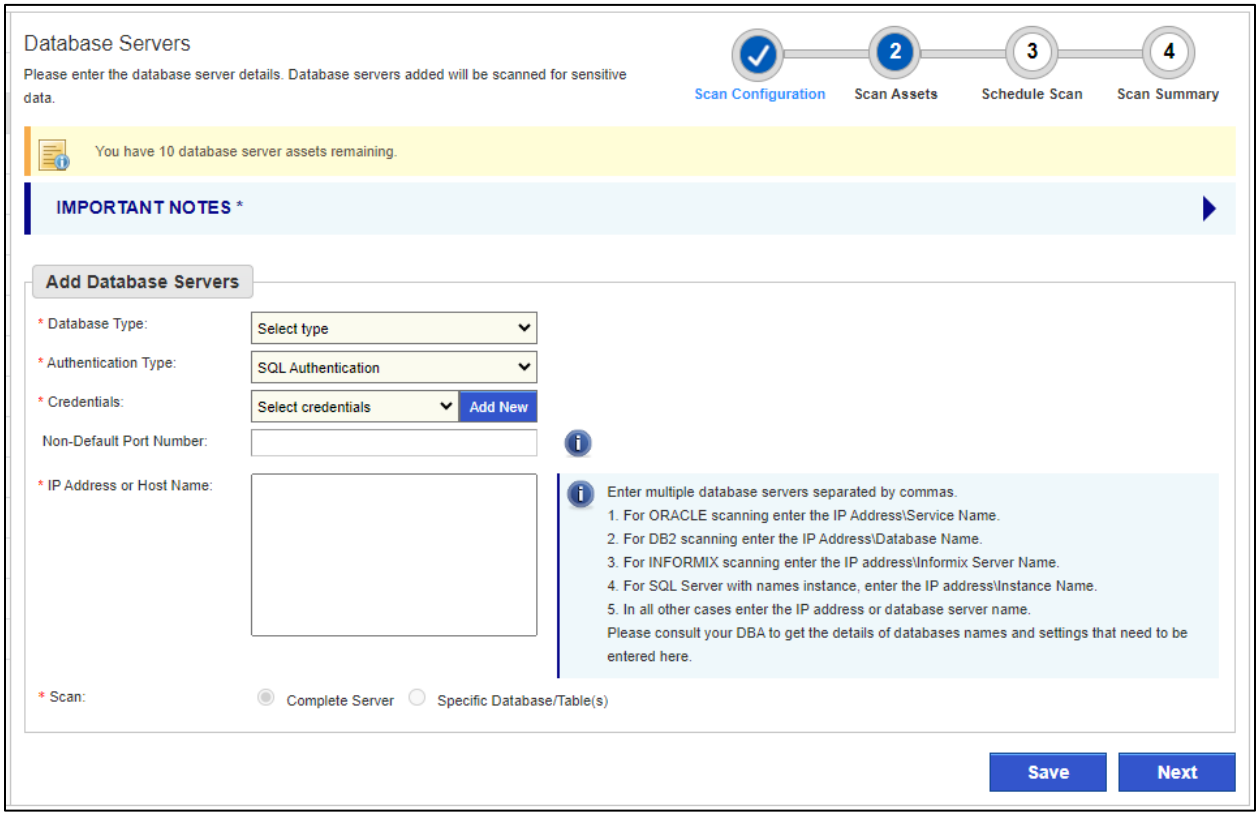


CDD cannot directly scan Mainframe computers, but a sample set of files exported from the mainframes in EBCDIC format can be placed on a file share and then CDD can scan those files.

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

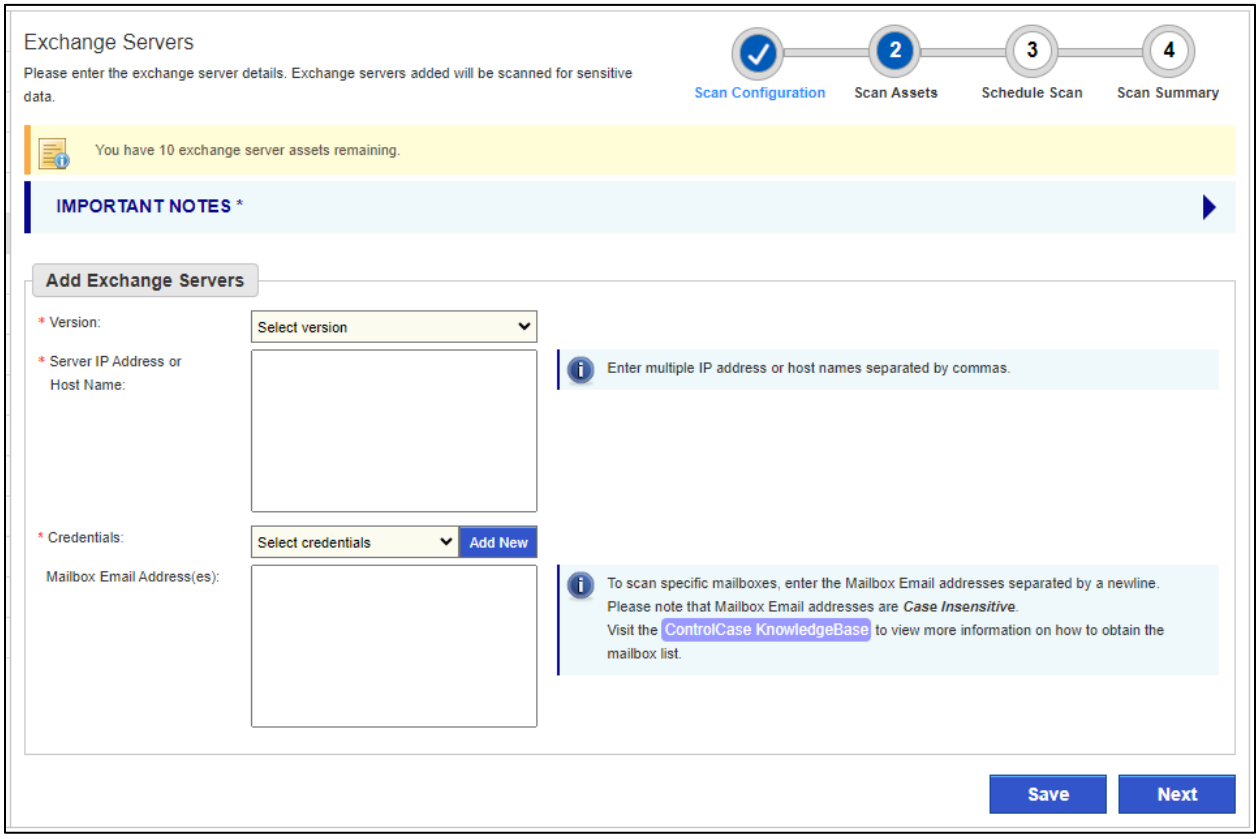
To add new database scans by entering the relevant details on the page. Please follow the instructions on each page for details.



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)

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.



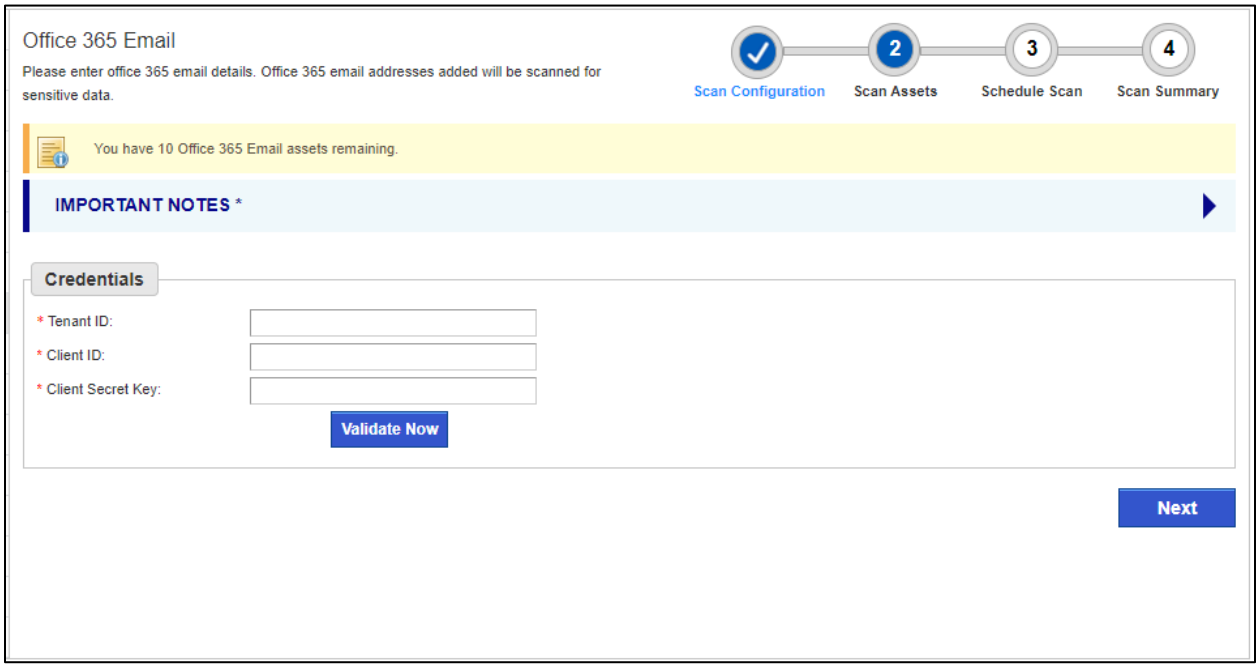
Office 365 Scanning

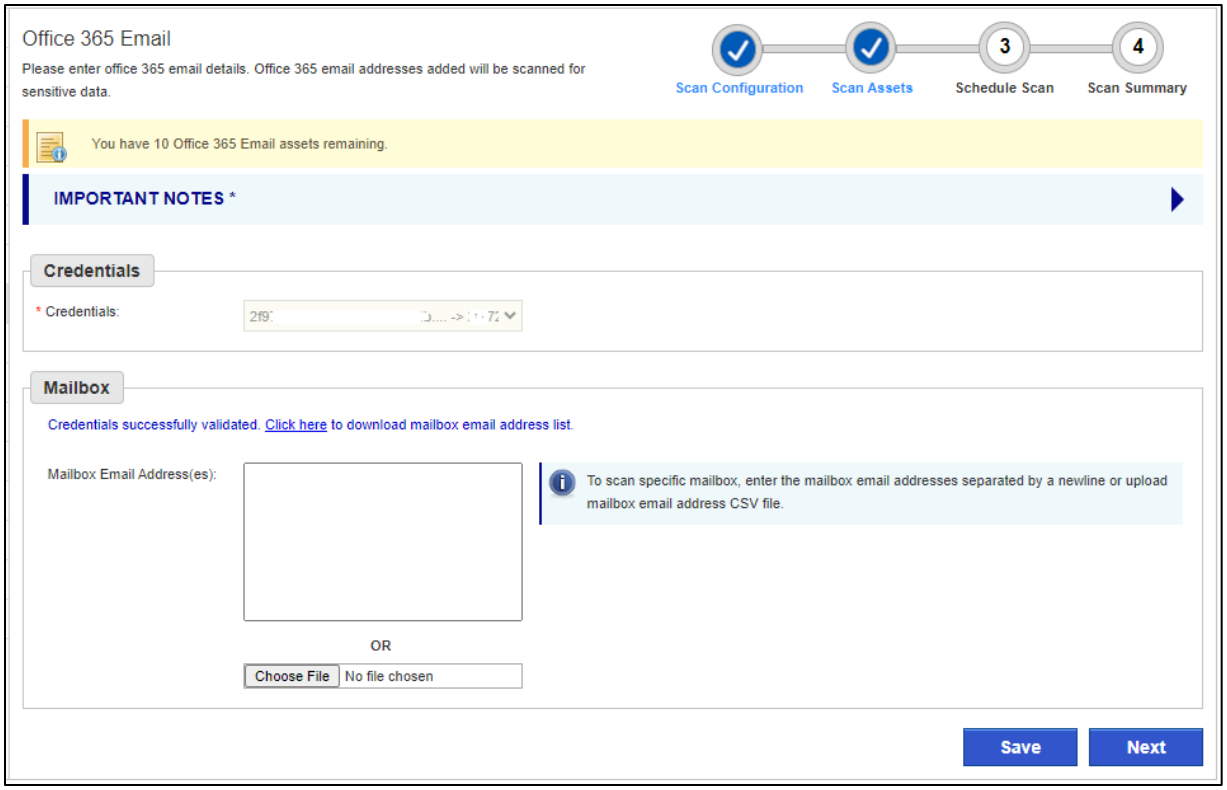
Due to the hosted nature of the Office 365 on Microsoft's servers, there are some limitations in the way the scans can occur.

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.

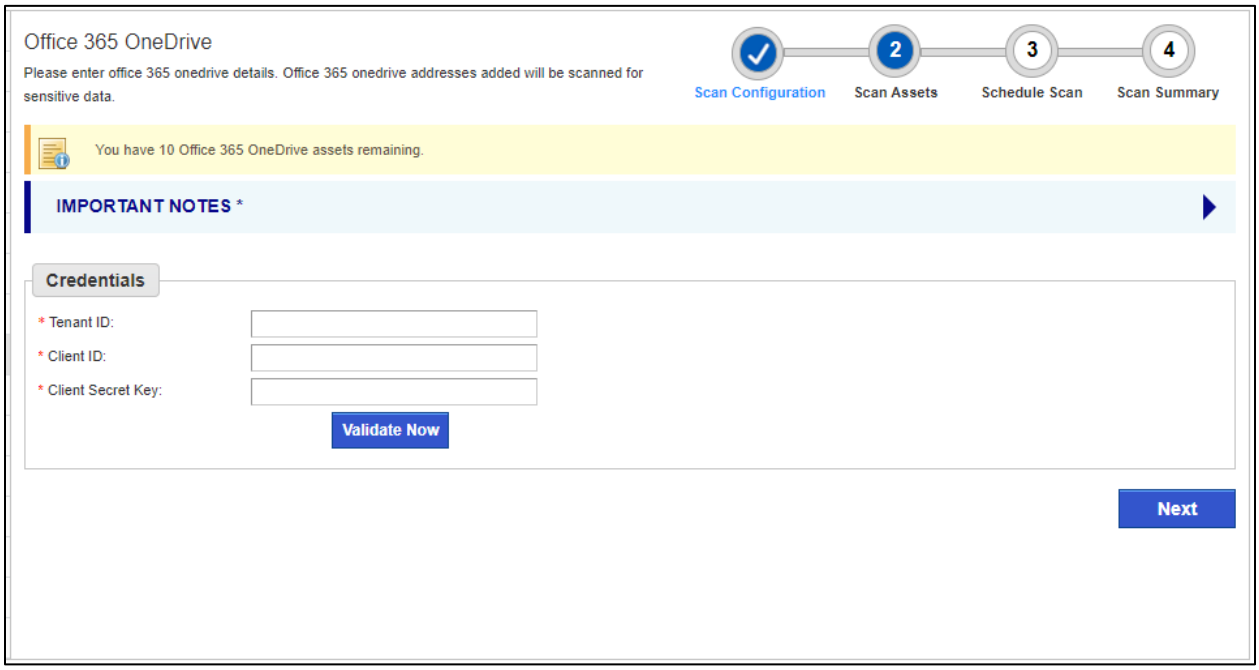
We have to use a sampling based approach for mailboxes and emails and those settings can be configured in the Settings area.

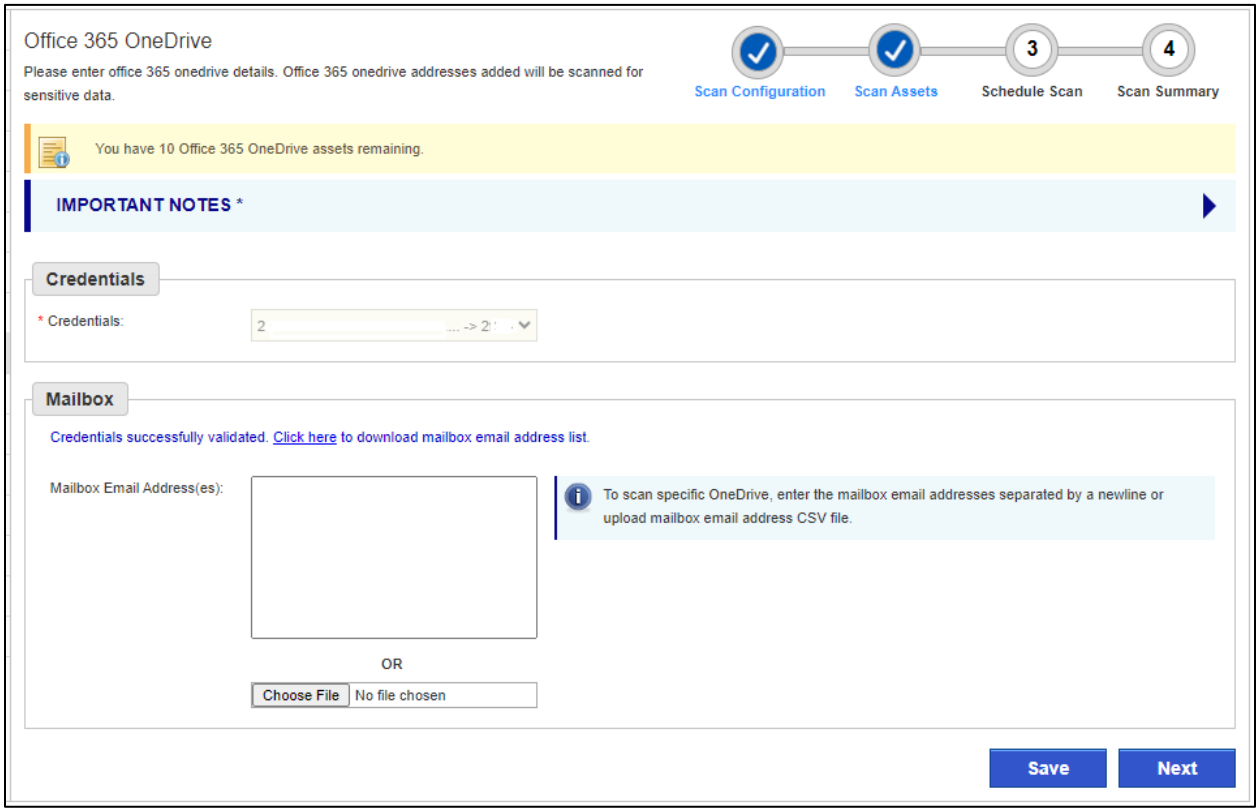
Office 365 Email



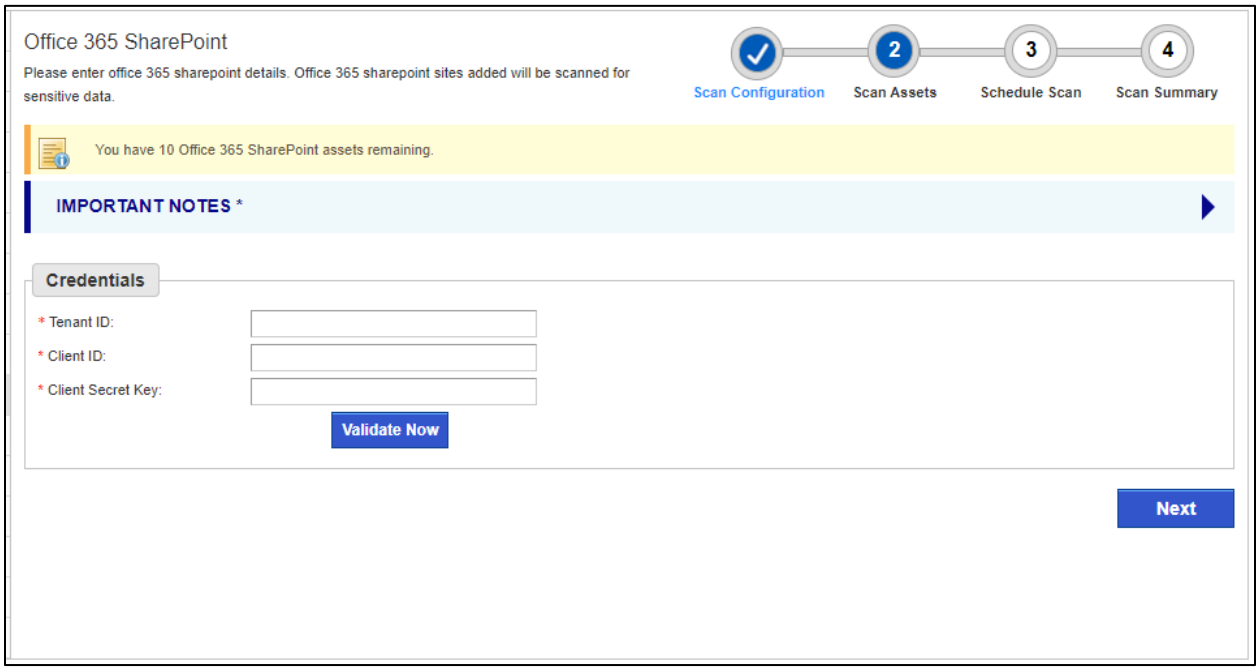

Office 365 Email
Please enter office 365 email details. Office 365 email addresses added will be scanned for sensitive data.
Scan Configuration
Scan Assets
3
Schedule Scan
4
Scan Summary
You have 10 Office 365 Email assets remaining.
IMPORTANT NOTES *
Credentials
* Credentials:
Mailbox
Credentials successfully validated. Click here to download mailbox email address list.
Mailbox Email Address(es):
To scan specific mailbox, enter the mailbox email addresses separated by a newline or upload mailbox email address CSV file.
OR
Choose File
No file chosen
Save
Next

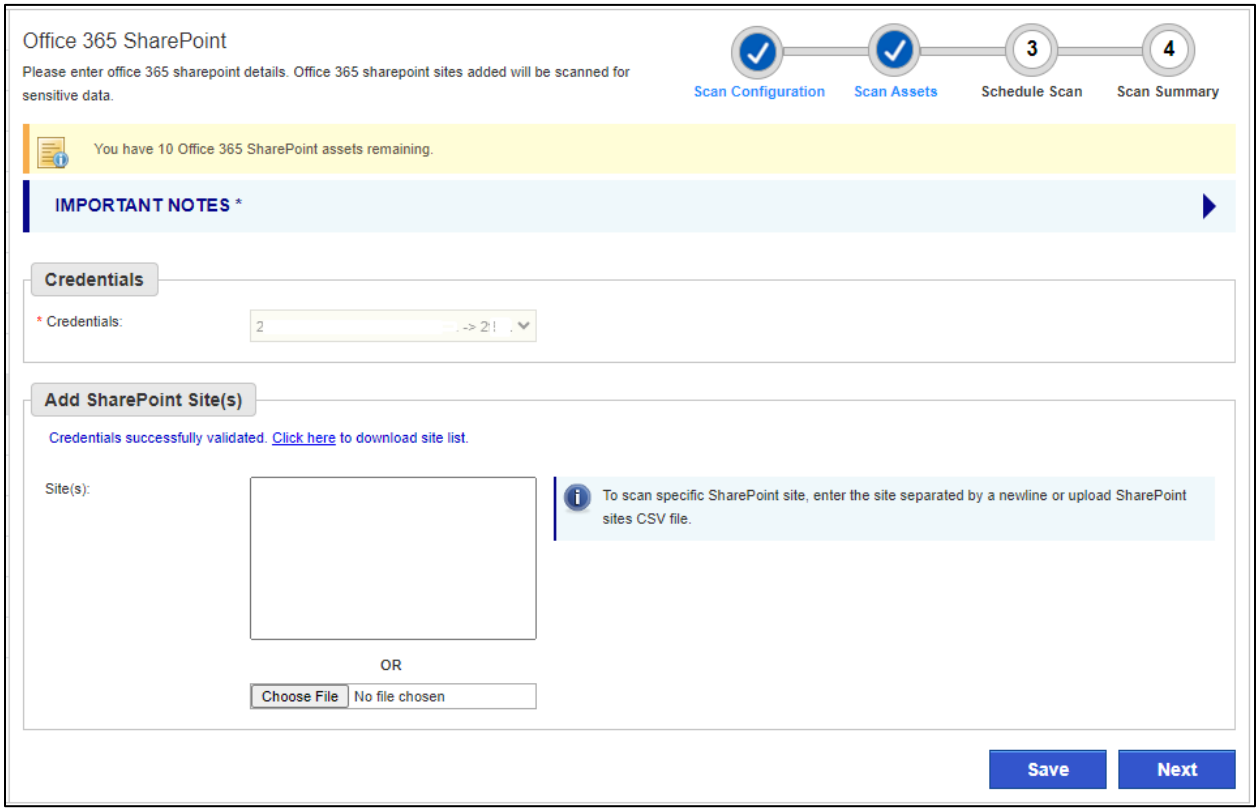
Office 365 OneDrive



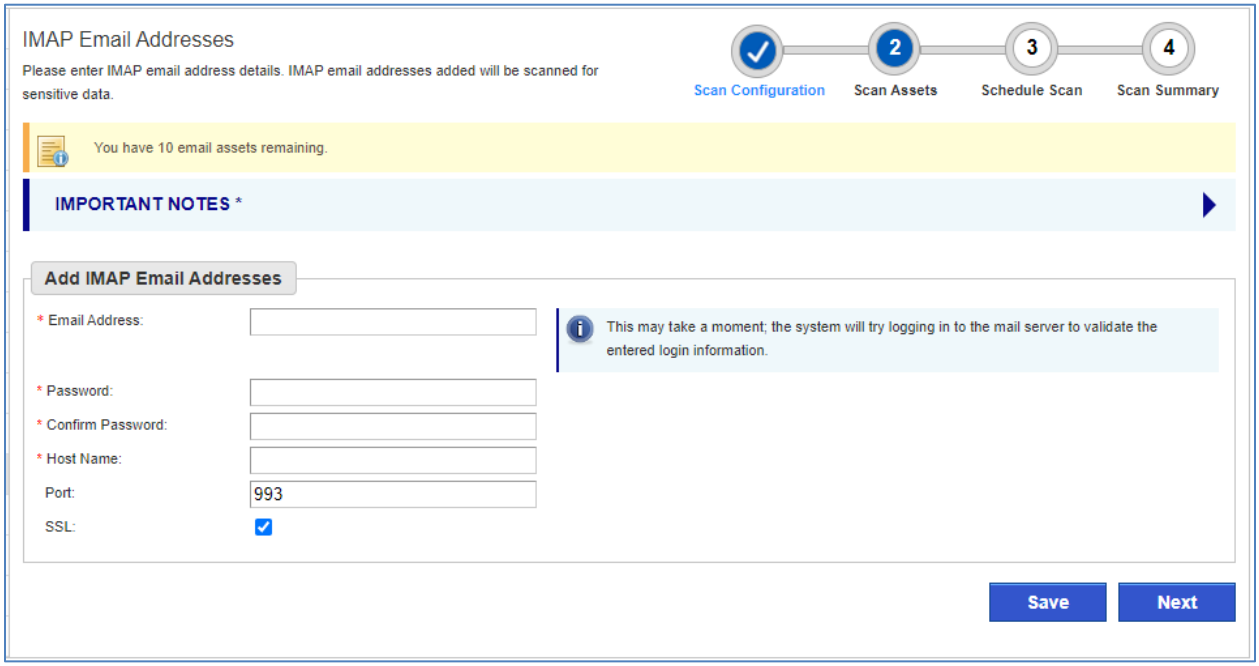


Office 365 SharePoint



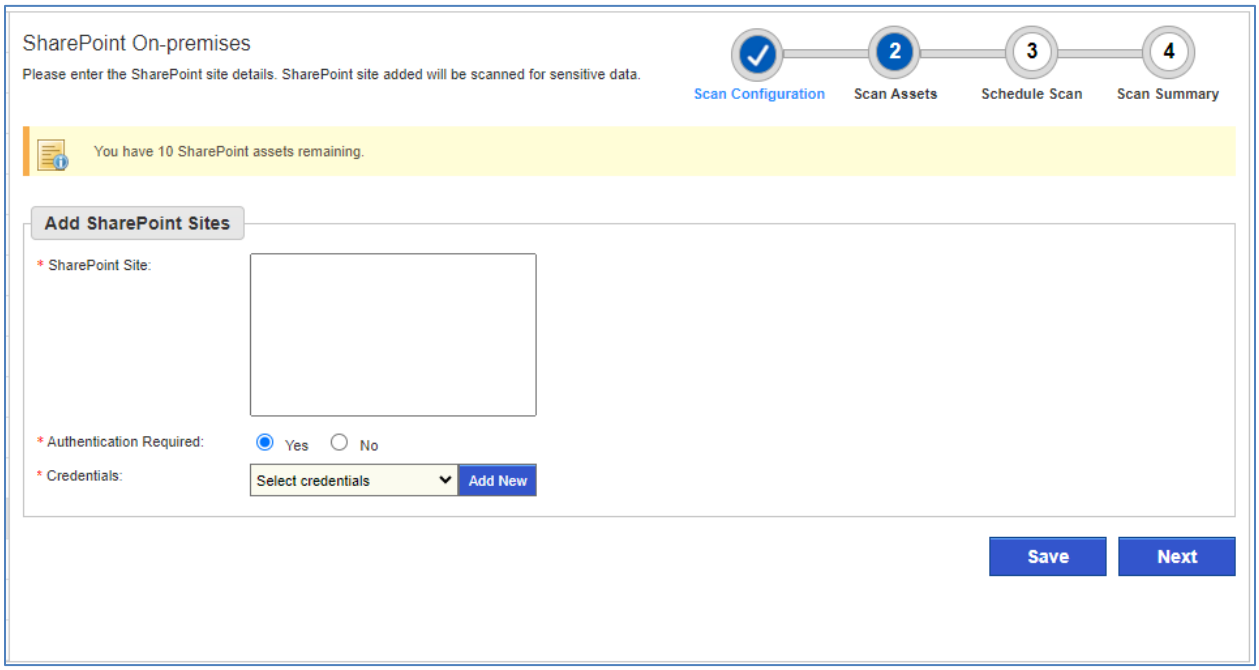


IMAP based Servers



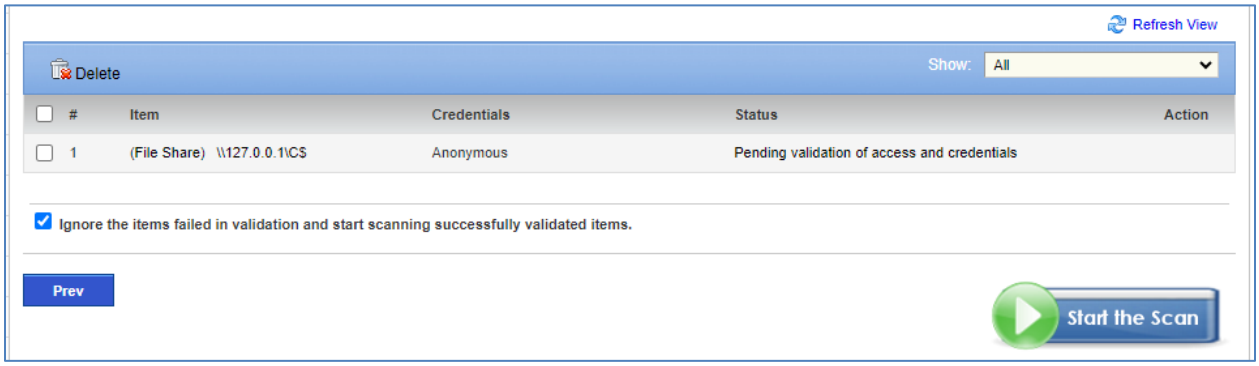
Microsoft SharePoint scans (On-premise)

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.



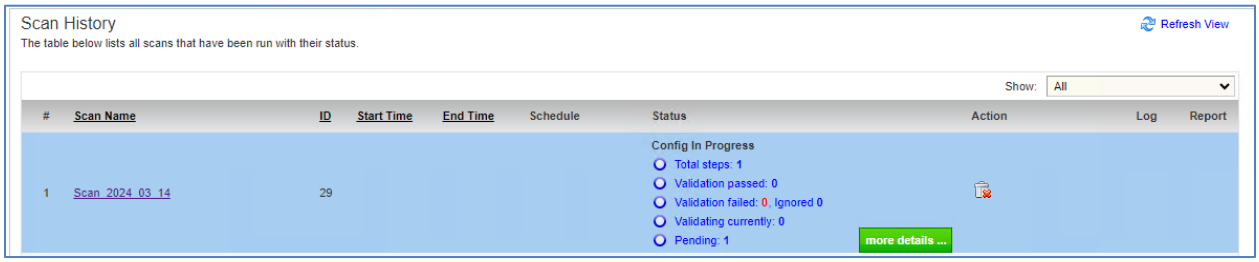
Start the scan

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.

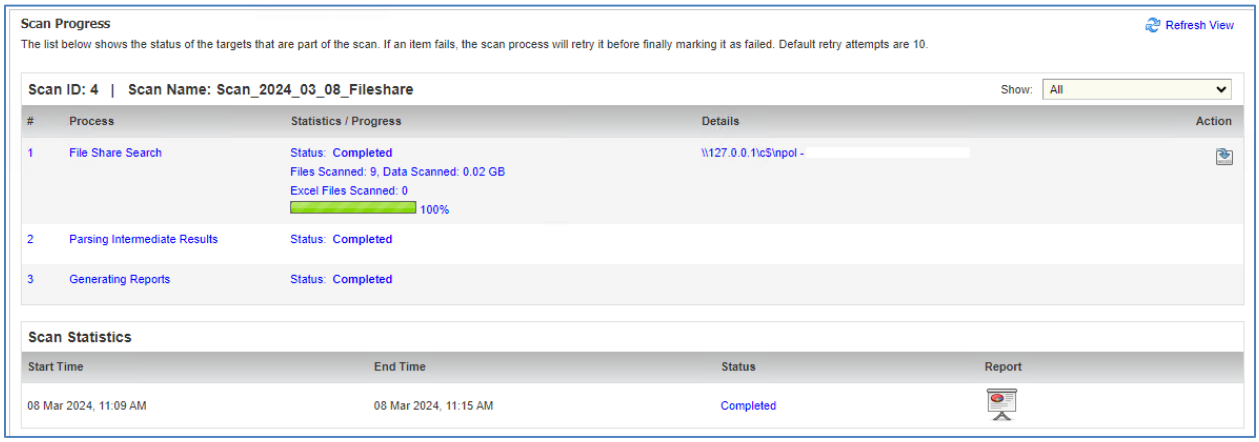


Scan Status

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

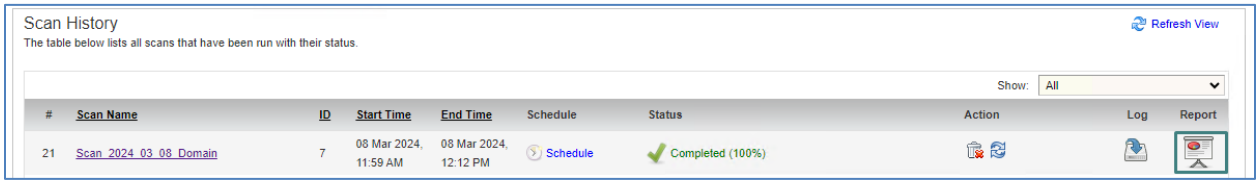


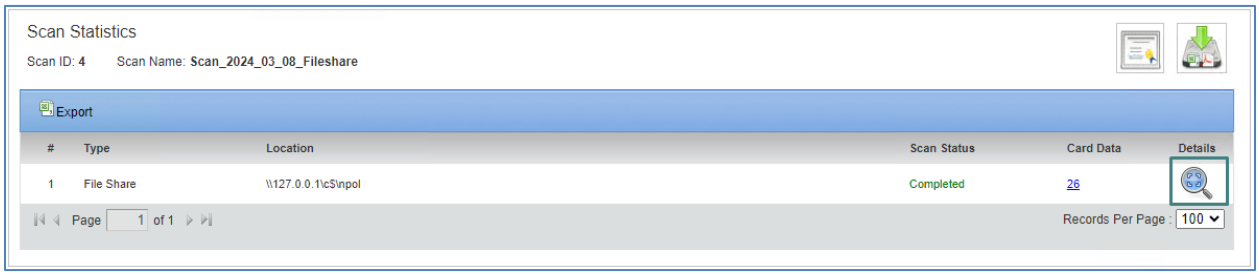
Additional details can be seen by clicking the MORE DETAILS… button

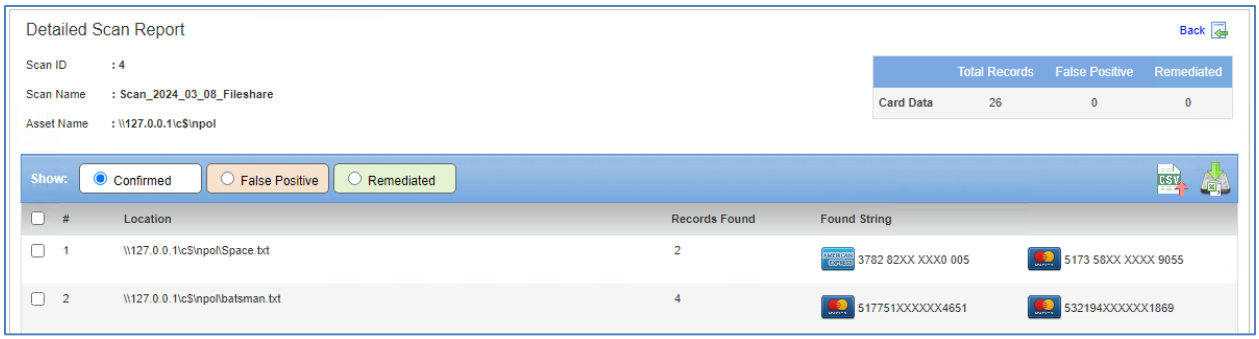


View Scan Results

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

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	
1	C:\npol\smallcddtestbed\exclude.txt	2	529196XXXXXX4320	511693XXXXXX4850
2	C:\npol\smallcddtestbed\include.txt	2	411096XXXXXX8385	469040XXXXXX0205
3	C:\npol\T.txt	4	521530XXXXXX4012	492994XXX3234
4	C:\npol\SmallCDDBed1FIle\Card_Data.csv	4	650601XXXXXX0993	554224XXXXXX3485
5	C:\npol\smallcddtestbed\small1file.txt	4	529196XXXXXX4320	511693XXXXXX4850

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	NBP_Test	Completed	8	

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	

#	Database	Scan Status	Card Data	Details
2	NPol_CDD_DB_1_Table_Only_9_Rows	Completed	1	

Sr. no	Table	Scan Status	Card Data	Details
1	Latest_C_NBP_CDD_TestBed_9_Rows	Completed	1	

#	Database	Scan Status	Card Data	Details
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	
1	QA_NPOL_Data	myTable	pan	270	(BRSolo) 633455 xxxxxx 6438	450 822xx xxxxx 866
2	QA_NPOL_Data	QA_NPOL_SDataTable1	pan	304	5038 47xxxx 1947	6759 38xx xxxx 9311
3	QA_NPOL_Data	QA_NPOL_SDataTable1	track1	47	(TrackData) %BXXXXXXXXXXXXXXXXX^EyvbffbCvirwp^33039029?2	(TrackData) %BXXXXXXXXXXXXXXXXX^HcjomdtPwykrz^5002271171?8
4	QA_NPOL_Data	QA_NPOL_SDataTable1	track2	53	(TrackData) XXXXXXXXXXXXXXXX=09091902161?	(TrackData) XXXXXXXXXXXXXXXX=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
1	zshaikh@ccawsqaex2016.com.pst/Inbox/JL_Diners Club US and Canada, 554089XXXXXX0420 **Mail Details** **Time**: Thu 05/09/2019 10:09 AM **From**: Jevita **To**: zshaikh	1	554089XXXXXX0420
2	zshaikh@ccawsqaex2016.com.pst/Outbox/RE: starts and ends with case sensi no/SOLO.CSV **Mail Details** **Time**: Thu 11/24/2022 11:39 AM **From**: zshaikh **To**: Jevita	1	(BRSolo) 633450XXXXXXXXX5503
3	zshaikh@ccawsqaex2016.com.pst/Outbox/CDD Data Test/SOLO.CSV **Mail Details** **Time**: Thu 11/24/2022 11:28 AM **From**: zshaikh **To**: npol; Jevita	1	(BRSolo) 633450XXXXXXXXX5503

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

#	Location	Records Found	Found String	
1	zshaikh@controlcasegrc.com/Inbox/Zip File Attached/smallcddtestbed.zip/exclude.txt **Mail Details** **Time**: 2023-10-04 07:27:33 **From**: zshaikh@controlcasegrc.com **To**: npol@controlcasegrc.com, anagare@controlcasegrc.com, anagare@controlcase.com, npol@controlcase.com, vdmello@controlcase.com, zshaikh@controlcasegrc.com,	2	529196XXXXXX4320	511693XXXXXX4850
2	zshaikh@controlcasegrc.com/Inbox/Zip File Attached/smallcddtestbed.zip/include.txt **Mail Details** **Time**: 2023-10-04 07:27:33 **From**: zshaikh@controlcasegrc.com **To**: npol@controlcasegrc.com, anagare@controlcasegrc.com, anagare@controlcase.com, npol@controlcase.com, vdmello@controlcase.com, zshaikh@controlcasegrc.com,	2	411096XXXXXX8385	469040XXXXXX0205
3	zshaikh@controlcasegrc.com/Inbox/FRT 516109XXXXXX1065 u8hukdndd 6759.3091.2213.2744 **Mail Details** **Time**: 2023-06-30 09:20:25 **From**: NPol@controlcase.com **To**: zshaikh@controlcasegrc.com,	2	516109XXXXXX1065	6759.30XX.XXXX.2744
4	zshaikh@controlcasegrc.com/Sent Items/Zip File Attached/smallcddtestbed.zip/exclude.txt **Mail Details** **Time**: 2023-10-04 07:27:30 **From**: zshaikh@controlcasegrc.com **To**: npol@controlcasegrc.com, anagare@controlcasegrc.com, anagare@controlcase.com, npol@controlcase.com, vdmello@controlcase.com, zshaikh@controlcasegrc.com,	2	529196XXXXXX4320	511693XXXXXX4850

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

#	Location	Found String	
1	\\Outlook_Mailbox\Allen.Stillwell@controlcase.org.com\Inbox\Re: Important Information about your reimbursement	376932XXXXX1004	376932XXXXX1004
2	\\Outlook_Mailbox\Allen.Stillwell@controlcase.org.comi\Inbox\RE: 225937 - 3175193 NS Ltd DBA Shine on Factory	656505XXXXXX6344	439901XXXXXX1390
3	\\Outlook_Mailbox\Allen.Stillwell@controlcase.org.com\Inbox\RE: one time cc\Misconduct_V3.txt	379733XXXXX4011	442142XXXXXX5661
4	\\Outlook_Mailbox\Allen.Stillwell@controlcase.org.com\Inbox\RE: IMEI Management Database	404970XXXXXX5716	404970XXXXXX5716
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/