DataSecurity Plus

Quick start guide

ManageEngine
DataSecurity Plus

Table of contents

1. Introduction

1.1 What is DataSecurity Plus

ManageEngine DataSecurity Plus is a unified data visibility and security platform. It audits file changes in real time, triggers instant responses to critical events, shuts down ransomware intrusions, and helps organizations comply with numerous IT regulations. It also analyzes file storage and security permissions, deletes junk files, and detects file security vulnerabilities. Users can assess the risks associated with sensitive data storage by locating and classifying files containing PII, PCI, and ePHI. It also prevents data leaks via USBs, emails, printers, and web applications; monitors file integrity; and audits cloud application usage.

You can download and try our fully functional, free trial via the link below.

Download now

1.2 How DataSecurity Plus works

DataSecurity Plus caters to organizations of all sizes that are looking to enhance data visibility, strengthen security, and meet stringent data privacy mandates. A general overview of all the modules in DataSecurity Plus and its architecture diagram are given below.

Module	Core functionality	Licensing is based on
File Audit	Audit and report on all file accesses and modifications in real time.	Number of file servers
File Analysis	Identify file security vulnerabilities and manage inactive, junk, and duplicate data.	Scanned data size in terabytes (TB)
Risk Analysis	Discover files containing sensitive data and classify them based on their vulnerability.	Scanned data size in terabytes (TB)
Endpoint DLP	Detect, disrupt, and respond to sensitive data leaks via USBs, emails, printers, and other endpoints.	Number of workstations
Cloud Protection	Track your organization's web traffic and identify and block malicious web applications.	Free add-on of the Endpoint DLP module

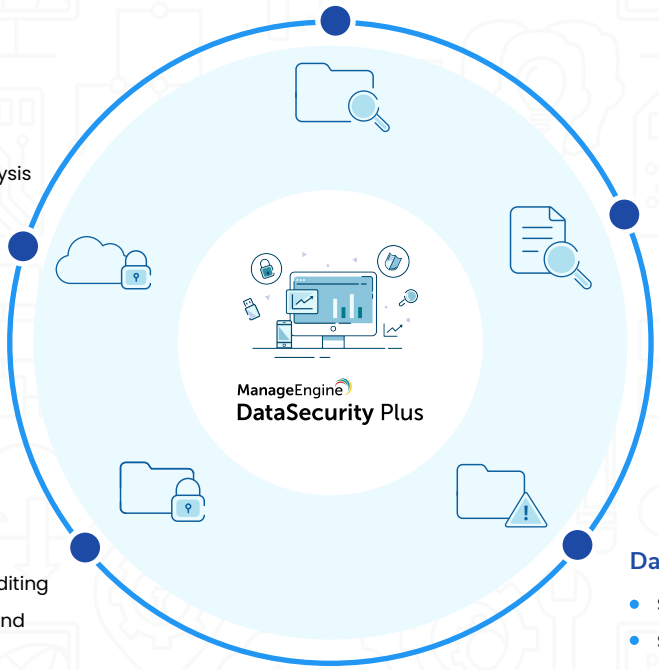
Architecture of the data visibility and security platform

File Audit

- Real-time file auditing and FIM
- Ransomware detection and response
- Compliance auditing and reporting

Cloud Protection

- Cloud app usage tracking
- Shadow IT discovery and analysis
- Application whitelisting and blacklisting



File Analysis

- Disk usage and permission analysis
- Permission vulnerability detection
- Junk file detection and deduplication

Data Leak Prevention

- Workstation and USB file auditing
- Data exfiltration detection and disruption
- Built-in DLP policies and strategies

Data Risk Assessment

- Sensitive data discovery
- Security analysis of sensitive files
- Dynamic risk scoring

DataSecurity Plus uses a lightweight agent to audit and analyze configured Windows file servers and failover clusters. The agent uses a Windows minifilter driver to audit file activities, and Windows APIs to analyze file properties.

DataSecurity Plus comes bundled with its default PostgresSQL and Lucene databases.

2. Setting up DataSecurity Plus

2.1 System requirements

Listed below are the hardware and software specifications required for the smooth functioning of DataSecurity Plus.

Hardware requirements

- Basic requirements

Component	Minimum	Recommended
Processor	2.4GHz	3GHz
Core	6	8 or more
RAM	12GB	16GB
Disk space	200GB*	1TB*
Network speed	100Mbps	1Gbps

*Some variations can be expected in these values depending on the environment and event details.

- Advanced requirements

The above recommended basic requirements might need to be supplemented with additional resources in some cases. Some of these are described below.

Case	Additional requirement
If you have a high event inflow from your file storage systems or your endpoints, you might need additional disk space.	• **Disk space:** To store reports and alerts for 1 million file events, you will need around 1.5GB of disk space and around 20MB of archive space.
If you have a huge number or volume of files and folders in disks in which you want to analyze file metadata and assess security permissions, you might need additional disk space.	• **Disk space:** As a general rule of thumb, allot around 2.5GB of disk space for every 10 million files or folders.
If you have configured data discovery and sensitive data reporting functions, in addition to the recommended basic requirements, you will need to add:	**Core:** Two or more depending on the desired scan speed. **Disk space:** Disk space requirements vary depending on the volume of files to be scanned and the number of rule-match content instances. Generally, 1 million files with 10 rule matches per file will take up 400MB of disk space. In terms of rule matches alone, 3 million matches take up around 100MB and 1 million incidents take up around 60MB of disk space.

Note: Some variation can be expected in these values, depending on the environment and event details.

2.2 Installing and setting up DataSecurity Plus

DataSecurity Plus can be installed on any machine in your network that satisfies the system requirements.

Installing DataSecurity Plus

By default, the product will be installed as an application. Once you've downloaded the ManageEngine_DataSecurity_Plus.exe file, run it, and follow these instructions:

1. Once the InstallShield Wizard opens, click Next.
2. Read the License Agreement, and click Yes.
3. Choose the destination folder for installation, and click Next. By default, DataSecurity Plus will be installed in C:\Program Files (x86)\ManageEngine\DataSecurity Plus.
4. Enter the port number that you wish to use for DataSecurity Plus, and click **Next.**

Note: The default port used by DataSecurity Plus is 8800. To customize it once installed, open DataSecurity Plus console, and navigate to **Admin** > **General Settings** > **Connection.** Type in the desired port number, and click **Save.**

5. Sign up for technical support. All you have to do is enter the required details, and click **Next.**
6. Click **Next** again to allow DataSecurity Plus to begin copying files to the installation directory. This process will take a few minutes.
7. Select **Start DataSecurity Plus,** and click **Finish.**

Starting DataSecurity Plus

There are two ways to start DataSecurity Plus:

1. As a service (recommended).
2. As an application.

Best practice: We strongly recommend running DataSecurity Plus as a service to ensure that event collection doesn't stop even after a user logs out.

Starting DataSecurity Plus as a service

1. To run DataSecurity Plus as a service, first install DataSecurity Plus as a Windows service.
    - Go to **Windows > DataSecurity Plus.**
    - Click **Install as a Service.**

Alternatively, you can also:

- Open the **Command Prompt.**
- Navigate to **<installation dir>\bin**

(Example: **C:\Program Files (x86)\ManageEngine\DataSecurity Plus)**

- Type **"InstallNTService.bat" and click Enter.**

2. Go to **Windows > Control Panel > System and Security > Administrative Tools > Services > ManageEngine DataSecurity Plus > Start the service.**

Note: By default, the DataSecurity Plus service uses the local system account. To use a different account that has the required minimum privileges, go to **Windows > Services,** and right-click **ManageEngine DataSecurity Plus.** Then select **Properties > Log on,** and provide the credentials of the account you want to use to run DataSecurity Plus as a service.

Starting DataSecurity Plus as an application

1. Install DataSecurity Plus.
2. Go to **Windows > DataSecurity Plus > Start DataSecurity Plus server.**

If you have any issues or errors, check out our troubleshooting guide to resolve it. You can also contact our support engineers who will be happy to assist you.

Launching DataSecurity Plus

1. Open a web browser and type **"http://<hostname>:<port number>"** in the address bar.
   The hostname is the name of the machine where DataSecurity Plus has been installed, and the port number is the web server port number that was specified during the installation.
   The default port used by DataSecurity Plus is 8800.

Note: To verify communication between DataSecurity Plus and your machine, go to **Windows > Command Prompt,** and enter in the command **"Ping <hostname>".**

2. If you're logging in for the first time, enter **admin** as the username and the password, and click **Login.**

Tips

1. After setting up DataSecurity Plus, change its default password by navigating to **Configuration > Admin > General Settings > Personalize > Change Password.**
2. Google Chrome is the recommended web browser for running DataSecurity Plus.

3. Configuring the File Audit module

3.1 About the File Audit module

DataSecurity Plus' File Audit module is a real-time Windows file server auditing and analysis solution that monitors, audits, alerts, and reports on all file accesses and modifications made in your file server environment. Further, it helps monitor file integrity, detect and contain ransomware attacks, and meet multiple compliance requirements.

3.2 Supported platforms

DataSecurity Plus performs file auditing across Windows file servers, failover clusters, and workgroup environments.

File Audit supports the following Microsoft Windows Server versions:

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008
- Windows Server 2003 R2

Volume type supported:

- Mounted volume

Share types supported are:

- SMB
- CIFS
- DFS
- DFSR

3.3 Domain configuration

Configure a domain only when you need to audit domain-based Windows file servers and failover clusters.

1. Select **Admin** from the application drop-down menu at the top.
2. Navigate to **Administration** > **Domain Settings**. Click + **Add Domain** in the top-right corner of the page.
3. Enter the domain name.
4. Check the box next to **Authentication**, and provide the domain user credentials.

Note: If the Authentication checkbox is unchecked, DataSecurity Plus will use the credentials of the account that is being used to run the product.

Tip: Use an account with domain admin credentials to ensure that the product has sufficient permissions to automatically install the agent. If you don't want to provide domain admin credentials, follow the steps listed here to install the agent manually using group policy.

5. Click the + symbol in the **Add Domain Controllers** field, and choose the desired one.
6. Click **Save.**

Tip: When configuring multiple domains, choose a default domain based on the primary view you need.

3.4 File server configuration

Configure the required file servers using the steps below:

1. Configure the domain in which the file server you want to audit is located.
2. Select **File Audit** from the application drop-down menu at the top. Go to **Configuration** > **Source** > **Windows File Server.**
3. Choose the appropriate domain.
4. Click + **Add File Server** in the top-right corner.
5. Once you've selected the domain, you'll see a list of the available servers within that domain.
6. Select the server to be audited.
7. Select objects to be monitored.

To audit shares: Choose one or more shares to be audited.

To audit subfolders, local folders, or local files: Enter their respective paths.

8. Finally, click **Install Agent and Finish.**

3.5 Cluster configuration

Configure the cluster servers for file auditing using the steps below:

1. Configure the domain in which the cluster you want to audit is present.
2. Select **File Audit** from the applications drop-down menu at the top. Go to **Configuration** > **Source** > **Windows File Cluster.**
3. Choose the appropriate domain.
4. Click + **Add Cluster** in the top-right corner.
5. Enter the **Cluster Name,** and click **Next.**
6. Choose the **Cluster Nodes** to be monitored. Click **Next.**
7. Choose the cluster **Client Access Point (CAP).** Click **Next.**
8. Select all the shares you want to audit. Click **Review.**
9. Review the settings that you just configured, and click **Configure.**
10. Once the cluster is successfully configured, its status will be displayed in the cluster configuration window.

3.6 Workgroup configuration

Configure the workgroup servers for file auditing using the steps below:

1. Select **Admin** from the applications drop-down menu at the top. Navigate to **Administration** > **Workgroup Settings.**
2. Click + **Add Workgroup** in the top-right corner.
3. Enter the **Host Name.**
4. Check the box next to **Authentication,** and provide the necessary user credentials.

Note: If the Authentication checkbox is unchecked, DataSecurity Plus will use the credentials of the account the product is using to run.

5. Select **File Audit** from the applications drop-down menu at the top. Go to **Configuration** > **Source** > **Workgroup Server.**
6. Click + **Add Workgroup** in the top-right corner.
7. Select the server to be audited.
8. Select objects to be monitored.

To audit shares: Choose one or more shares to be audited.

To audit subfolders, local folders, or local files: Enter their respective paths.

9. Finally, click **Install Agent and Finish.**

4. Configuring the File Analysis module

4.1 About the File Analysis module

DataSecurity Plus' File Analysis helps analyze data storage space, deduplicate files, discard junk data, and control unwanted data growth. Further, it helps review effective permissions, unearth file security vulnerabilities, such as files with open access and broken inheritance, and much more.

4.2 Supported platforms

DataSecurity Plus performs file analysis across Windows file servers, failover clusters, and workgroup environments.

File Analysis supports the following Microsoft Windows Server versions:

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008
- Windows Server 2003 R2

Volume type supported:

- Mounted volume

Share types supported are:

- SMB
- CIFS
- DFS
- DFSR

4.3 Domain configuration

Configure a domain only when you need to audit domain-based Windows file servers and failover clusters.
For in-depth steps on how to configure a domain for analyzing file servers, click here.

4.4 File server configuration

Configure the required file servers using the steps below:

1. Configure the domain in which the file server you want to configure is located.
2. Select **File Analysis** from the application drop-down menu at the top. Go to **Configuration > Source > Windows File Server.**
3. Choose the appropriate domain.
4. Click **+ Add File Server** in the top-right corner.
5. Once you've selected the domain, you'll see a list of the available servers within that domain.
6. Select the server to be audited.
7. Select drives to be monitored.
8. Finally, click **Install Agent and Finish.**

4.5 Failover cluster configuration

Configure the required clusters using the steps below:

1. Configure the domain in which the file server you want to configure is located.
2. Select **File Analysis** from the application drop-down menu at the top. Go to **Configuration > Source > Windows File Server.**
3. Choose the appropriate domain.
4. Click **+ Add Server** in the top-right corner.
5. Once you have selected the domain, select **Enter server name.**
6. On the window that opens, select the primary cluster node name.
7. Select the drives that need to be analyzed.
8. Finally, click **Install Agent and Finish.**

4.6 Workgroup configuration

Configure the required workgroups using the steps below:

1. For in-depth steps on how to configure the workgroup servers for file analysis, click here.
2. Select **File Analysis** from the applications drop-down menu at the top. Go to **Configuration > Source > Workgroup Server.**
3. Click **+ Add Workgroup** in the top-right corner.

4. Select the server to be analyzed.

5. Select the type of drives that you want to analyze.

All drives: The entire drive will be analyzed.

Only specific drives: Choose the respective drive letter from the options.

Custom drives: Type in the respective drive path.

6. Finally, click **Add.**

5. Configuring the Endpoint DLP module

5.1 About the Endpoint DLP module

DataSecurity Plus' Endpoint Security solution protects sensitive data from being exposed or stolen across traditional and virtual endpoints.

5.2 Supported platforms

DataSecurity Plus helps prevent data leaks across workgroup- and domain-based workstations.

- Windows 10
- Windows 8
- Windows 7
- Windows Vista
- Windows XP

5.3 Domain configuration

Configure a domain only when you need to audit domain-based workstations.
For in-depth steps on how to configure a domain for auditing workstations, click here.

5.4 Workstation configuration

Configure the required workstations using the steps below:
1. Configure the domain in which the workstations you want to configure is located.
2. Select **Endpoint DLP** from the application drop-down menu at the top.
3. Go to **Configuration** > **Devices.**

Note: Workstations can either be configured individually or in groups.
Best practice: We recommend grouping workstations and applying policies to the group rather than applying it directly to the workstation.

4. To configure workstations individually, follow the steps listed below:
    a. In the **Configured Workstation(s)** page, select **Add Workstation(s)** in the top-right corner.
    b. Select your domain.

Note: To add a domain that is not listed, click **Add New Domain** and follow the steps on this page.

    c. Select the + symbol next to the **Select Workstation(s)** text box, and add the workstations you want to audit.
    d. Then, select the **Security Policies** you want to monitor in the selected workstation(s).
    e. Click **Install Agent and Finish.**
5. To configure workstations in groups, follow the below listed steps:
    a. In the **Configured Workstation(s)** page, select **Configured Groups** tab. Select **+ Create Group** at the top-right corner.
    b. Provide an appropriate group name and description.
    c. Select your domain.
    d. Select the + symbol next to the **Select Workstation(s)** text box, and add the workstations you want to audit.
    e. Then, select the **Security Policies** you want to monitor in the selected workstation(s).
    f. Click **Create Group.**

Notes:

1. A workstation can be a part of only one group.
2. The most restrictive policy applies when two or more policies are applied to the same workstation.

For more details on how to use predefined DLP policies, create new policies, and incidents check out our help center.

5.5 Workgroup configuration

For in-depth steps on how to configure the workgroup servers for DLP, click here.

To configure the required workgroup, follow these steps:

1. Select **Endpoint DLP** from the applications drop-down menu at the top.
2. Go to **Configuration > Devices.**
3. Click **+ Add Workstation(s)** in the top-right corner.
4. If you have already configured the desired workgroup, you can choose it from the Select the Domain drop-down menu. If not, click **Workgroup** next to the Select the Domain drop-down menu and follow the instructions listed here.
5. Choose the appropriate workgroup by clicking the **+** next to Select Workstation(s).
6. Select the security policies you want to monitor on the selected workstations.
7. Click **Install Agent and Finish.**

6. Configuring the Risk Analysis module

6.1 About the Risk Analysis module

DataSecurity Plus' Risk Analysis performs content inspection and contextual analysis to discover critical data, and classify it based on sensitivity and vulnerability.

6.2 Supported platforms

DataSecurity Plus performs risk analysis across Windows file server, failover cluster, and Microsoft SQL Server environments.

Data source	Supported versions
Windows file server	Windows Server 2022 Windows Server 2019 Windows Server 2016 Windows Server 2012 R2 Windows Server 2012 Windows Server 2008 R2 Windows Server 2008 Windows Server 2003 R2
Microsoft SQL Server	Microsoft SQL Server 2019 Microsoft SQL Server 2017 Microsoft SQL Server 2016 Microsoft SQL Server 2014 Microsoft SQL Server 2012 Microsoft SQL Server 2008 R2 Microsoft SQL Server 2008

6.3 Domain configuration

To scan for sensitive data on:

- Domain-based file servers and failover clusters, configure the target domain by following the steps listed here.

- Microsoft SQL servers, domain configuration is not necessary.

6.4 File server configuration

Configure the required file servers using the steps below:

1. Configure the domain in which the file server you want to configure is located.
2. Select **Risk Analysis** from the application drop-down menu at the top. Go to **Configuration** > **Data Source Configuration** > **File Server.**
3. Choose the appropriate domain.
4. Click + **Add File Server** in the top-right corner.
5. Once you've selected the domain, you'll see a list of the available servers within that domain.
6. Select the servers which contain the files to be scanned.

Note: To add a server that is not listed, click **Enter server name,** and type in the server name.

7. Select the objects to be scanned.

To scan shares: Choose one or more shares to be scanned.

To scan subfolders: Enter their respective paths.

8. Finally, click **Save.**

6.5 Cluster configuration

Configure the required clusters using the steps below:

1. Configure the domain in which the cluster you want to configure is located.
2. Select **Risk Analysis** from the application drop-down menu at the top. Go to **Configuration** > **Data Source Configuration** > **File Server.**
3. Choose the appropriate domain.
4. Click + **Add File Server** in the top-right corner.
5. Once you've selected the domain, select **Enter server name.**
6. Type in the cluster name.
7. Select the objects to be scanned.

To scan shares: Choose one or more shares to be scanned.

To scan subfolders: Enter their respective paths.

8. Finally, click **Save.**

6.6 Microsoft SQL Server configuration

To configure Microsoft SQL Server for data discovery scans, follow these steps:

1. Select **Risk Analysis** from the applications drop-down menu at the top.
2. Go to **Configuration > Data Source Configuration > SQL Server.**
3. Click **+ Add SQL Server instance.**
4. Enter the *Server Name.*
5. Enter the *Instance Name and Port Number.*
6. Choose the *Authentication Type.*
7. Provide the credentials of the user whose account will be used for the selected authentication type.
8. Click **Save.**

DataSecurity Plus will now automatically schedule data discovery scans for the configured servers.

Tips for choosing the authentication type:

- When choosing **Windows Authentication,** the user account chosen should be within the listed Active Directory domain. Choose a user account with the least possible privileges as it is used only to carry out domain-level authentication.

- When choosing **SQL Server Authentication,** the user account chosen should be configured within the target SQL Server instance and have a minimum of read permissions.
  Refer to the permissions and privileges guide for more details on setting up a user account with the least privileges required.

7. Miscellaneous

Find the additional information required for quick and efficient installation of DataSecurity Plus below.

7.1 Ports configuration

Listed below are details about ports that need to be open for the regular functioning of DataSecurity Plus.

Product ports

The table below lists the default ports used by DataSecurity Plus. These can be changed during or after installation.

Ports	Protocol	Purpose
8800	HTTP	Product web server/agent communication
9163	HTTPS	Product web server/agent communication

Note: To change the default ports after installation, open the **DataSecurity Plus console.** Select **Admin** from the application drop-down menu at the top. Under **General settings,** go to **Connection > Change port.**

System ports

The table below lists the ports on the destination computers that DataSecurity Plus uses. Ensure that these ports are to be kept opened on Windows or third-party firewalls for uninterrupted functioning of DataSecurity Plus.

Ports	Protocol	Destination	Service	Purpose	Direction
135	TCP	Monitored computers	RPC	Agent communication	Outbound
137	TCP and UDP	Monitored computers	RPC	Agent communication	Outbound
138	UDP	Monitored computers	RPC	Agent communication	Outbound
139	TCP	Monitored computers	RPC	Agent communication	Outbound

445	TCP and UDP	Monitored computers	RPC	For listing file shares	Outbound
389	TCP and UDP	Domain controllers	LDAP	For syncing AD objects with DataSecurity Plus	Outbound
636	TCP	Domain controllers	LDAP over SSL	For syncing AD objects with DataSecurity Plus	Outbound
3268	TCP	Domain controllers	Global catalog	For syncing AD objects with DataSecurity Plus	Outbound
3269	TCP	Domain controllers	Global catalog over SSL	For syncing AD objects with DataSecurity Plus	Outbound
88	TCP	Domain controllers	Kerberos	For syncing AD objects with DataSecurity Plus	Outbound
25	TCP	SMTP servers	SMTP	To send emails	Outbound
465	TCP	SMTP servers	SSL	To send emails	Outbound
587	TCP	SMTP servers	TLS	To send emails	Outbound
49152 - 65535	TCP	Monitored computers	RPC randomly allocated high TCP ports	For agent communication and cluster configuration	Outbound

Notes:

1. Remote registry services must be running on all machines that have the DataSecurity Plus agent installed to monitor the agent status.
2. If you're using Windows Firewall, you can open dynamic ports 49152 to 65535 on the monitored computers by enabling the outbound rules listed below.
    Remote Event Log Management (NP-In)
    Remote Event Log Management (RPC)
    Remote Event Log Management (RPC-EPMAP)

To enable the above rules: Open **Windows Firewall > Advanced settings > Inbound Rules,** right-click on the respective rules, and select **Enable Rule.**

7.2 SSL configuration

Applying Secure Sockets Layer (SSL) certificates ensures that all data transfers between users' web browsers and the DataSecurity Plus server remain secure. You can find the guide that explains the steps to enable SSL by clicking here.

7.3 Minimum privileges required

Once Domain Admin credentials are granted, DataSecurity Plus instantly starts auditing file activities and discovering sensitive data. If you don't want to provide Domain Admin credentials, follow the steps in this checklist to set up the service account with the least privileges required.

1. Privileges required commonly across all modules

The below steps list the privileges required by every edition and commonly across all three modules of DataSecurity Plus. These permissions should be granted first, before the permissions specific to each module are provided.

a. Grant the user Full Control over the product installation folder.

DataSecurity Plus requires **Full Control** access level over the product installation folder to write in the database.

Log in to the computer where DataSecurity Plus is installed with **Domain Admin** privileges, locate the product installation folder, right-click **Properties** > **Security** > **Edit,** add the DataSecurity Plus user, and provide **Full Control** permissions.

b. Grant the user Full Control over DataSecurity Plus' archive folder.

DataSecurity Plus requires **Full Control** over the archive folder for storing and retrieving archived data from the database.

To find the location of the archive folder, open **DataSecurity Plus** > **Admin** > **Configurations** > **Archive Configuration.**

Log into the target computer with **Domain Admin** privileges. Locate the folder, right-click **Properties** > **Security** > **Edit**, add the DataSecurity Plus user, and provide **Full Control** permission.

c. Grant the user Full control over all of DataSecurity Plus' Scheduled Reports folders.

DataSecurity Plus requires **Full Control** over the **Scheduled Reports** folder for saving scheduled reports in the specified location.

- To find the location of a Scheduled Reports folder, open **DataSecurity Plus** > **Admin** > **Schedule Reports** > **Modify Schedule Report.** You can see the location under **After Execution.**
- Log into the target computer with **Domain Admin** privileges. Locate the folder; right-click, go to **Properties** > **Security** > **Edit,** add the DataSecurity Plus user, and provide **Full Control** permission.

Repeat the steps on all destination folders for scheduled reports.

d. Grant the user Read and Execute permission over all of DataSecurity Plus' alert script folders.

The product requires **Read & Execute** permissions on each alert script folder to execute scripts once an alert gets triggered. If you have created custom scripts to be executed, provide the necessary permissions to ensure smooth functioning.

- To find the location of the alert scripts folder, open **DataSecurity Plus.** Select **File Audit** from the apps drop-down menu at the top. Navigate to **Configuration** > **Alerts** > **Modify Alert Profile.** You can see the location under Script file path.
- Log into the target computer with **Domain Admin** privileges. Locate the folder, right-click, go to **Properties** > **Security** > **Edit**, add the DataSecurity Plus user, and provide **Read & Execute** permission.

Repeat the steps on all alert script folders.

2. Privileges required for File Audit module

The steps below detail the procedure to assign the minimum privileges required by DataSecurity Plus' File Audit module.

a. Make the user a member of the Power Users group

- Log into your Domain Controller with **Domain Admin** privileges. Open the Group Policy Management Console, right-click on any domain-level Group Policy Object (GPO), and click **Edit.**
- In the **Group Policy Management Editor**, select **Computer Configuration** > **Preferences** > **Control Panel Settings.** Right-click on **Local Users and Groups** > **Add Local Group.**
- In the New Local Group Properties wizard, select **Update** under **Action.** Select **Power Users group** under **Group Name**, and add the DataSecurity Plus user.

3. Privileges required for Risk Analysis module

DataSecurity Plus requires a minimum of read permissions to locate sensitive data (such as PII, ePHI, and credit card details) across:

- Windows file servers.
- Microsoft SQL database servers.

Provide read permissions for users across Windows file servers by following the steps below:

There are two ways to grant a user read permissions for the required shares:

a. Make the user is a member of the Local Administrators group.

1. Log in to any computer with domain admin privileges.
2. Open the Microsoft Management Console **(MMC)** and go to **File > Add/Remove Snap-in.**
3. Click **Local Users and Groups > Add > Another computer.**
4. Select the target computer, then click **Finish.**
5. Open **Local Users and Groups.**
6. Select **Groups.**
7. Right-click **Administrators** and click **Properties > Add DataSecurity Plus user.**
8. Repeat the steps above for every Windows file server or cluster on which Risk Analysis is to be performed.

b. Grant the user read permissions for both shares and NTFS on every share scanned.

1. Log in to any computer with domain admin privileges.
2. Open **MMC** and go to **File > Add/Remove Snap-in.**
3. Click **Shared Folders > Add > Another computer.**
4. Select the target computer.
5. Click **Finish**. This will open the list of shares from the target computer, provided the user has the necessary privileges.
6. Right-click the desired share and click **Properties > Security > Edit.**
7. Add the DataSecurity Plus user to whom you want to grant read permissions.
8. Click **Enter** to provide read permissions for both shares and NTFS.
9. Repeat the steps above for every share scanned.

Provide read permissions for users across Microsoft SQL database servers by following the steps below:

a. Grant the SQL account used for monitoring the following roles.

1. Log in to any computer with system admin privileges.
2. Open the **SQL Server Management Studio.** If you do not have it installed, you can download it here.
3. Click **Logins.**
4. Right-click the appropriate user and click **Properties.**
5. Click **Server Roles** and select **public**. By default, the public role should have a minimum of access and read permissions for the databases.
6. Click **Logins.**
7. Right-click the appropriate user and click **Properties.**
8. Click **User Mapping.** For all databases, both the public and db_datareader roles should be assigned to the user.

7.4 Agent documentation

DataSecurity Plus uses a lightweight agent to audit and analyze configured Windows file servers and failover clusters. The agent uses a Windows minifilter driver to audit file activities, and Windows API to analyze file properties.

a. Installation prerequisites

To allow smooth installation and functioning of the agent on the targeted data source, the criteria below have to be met.

i. Software requirements

The DataSecurity Plus agent can only run on a Windows machine with .NET Framework version 4 or higher. It supports the following OS versions:

- Windows Vista, 7, 8, 8.1, and 10
- Windows Server 2008, 2008 R2, 2012, 2012 R2, 2016, and 2019

ii. Disk space requirements

A minimum disk space of 4GB is required.

b. Port configuration

- For server to agent communication: RPC ports 135, 137, 138, 139, and 445.
- For agent to server communication: Port on which the DataSecurity Plus server is running (by default, 8800).

c. Privileges

By default, the agent uses the privileges of the Local System account.

d. Installing the agent

Admin privileges are required for agent installation. For more information, refer to the Minimum Permissions and Privileges Guide.

i. Automatic installation

The agent is automatically installed when the target machine is added. It can then be managed from the web console on the Manage Agent page. Select **Admin** from the apps drop down menu at the top. Navigate to **Administration** > **Manage Agent.**

ii. Manual installation

To install the agent manually, download the agent by navigating to **Admin** > **Administration** > **Manage Agent,** and click on **Download Agent** in the top-right corner.

Deploying the agent manually via Group Policy

Use the following properties while creating an MSI file for silent installation:

- SERVERNAME — The name of the server where DataSecurity Plus is hosted.
- SERVERFQDN — The fully qualified domain name (FQDN) of the server where DataSecurity Plus is hosted.
- SERVERIP — The IP address of the server where DataSecurity Plus is hosted.
- PORT — The port number DataSecurity Plus uses for communication.
- PROTOCOL — The protocol used for communication.

Installing the agent by running the MSI file on client computers

Provide the details below while installing the agent:

- **Server name:** The name of the server where DataSecurity Plus is hosted.
- **Port:** The port number used to communicate with the DataSecurity Plus server.
- **Protocol:** The defined protocol for communicating with the DataSecurity Plus server.

e. Updating the agent

If there is a new version of the agent available, the existing version will be upgraded automatically when DataSecurity Plus is updated.

To update the agent manually, download the updated agent and install it by following the directions in this section.

To check for product updates, please refer to the Release Notes.

Tip: For secure, encrypted communication, please enable HTTPS communication by following the steps in this guide.