ManageEngine
DataSecurity Plus

Agent Document

www.datasecurityplus.com

Table of contents

About DataSecurity Plus

ManageEngine DataSecurity Plus is a file server auditing, file analysis, data risk assessment, and data loss prevention solution. It can:

- Audit file activities, monitor file integrity, and track file movement across file servers, failover clusters, and workstations.
- Locate files containing sensitive personal data, including personally identifiable information (PII), payment card information (PCI), and electronic protected health information (ePHI) using built-in data discovery rules.
- Identify file security vulnerabilities, deduplicate files, and control storage growth.
- Detect and block data leaks via USBs, email, printers, web applications, and more.
- Monitor and control the use of cloud applications.
- Provide detailed audit reports that help organizations streamline compliance with multiple IT regulations, and more.

1. Overview of agent-based data collection

DataSecurity Plus uses a lightweight agent to audit users' file activities in real time. This agent is installed when every Windows file server, failover cluster, workgroup server, or workstation is configured. It uses a Windows minifilter driver to collect file activities, and Windows API to analyze file properties.

The collected event data is forwarded to the centralized DataSecurity Plus server, where it is processed, analyzed, and presented in user-friendly reports and charts. Then, this data is stored on a managed server, and a notification is triggered if it violates any configured alert policies.

The agents can store up to 2GB of data on the machine where they are installed, allowing monitoring to continue even if contact is temporarily lost with the central management server. Once the connection is re-established, the stored data is forwarded to the management server for analysis and reporting, ensuring a foolproof audit trail.

When the agent-server connection is broken for any reason, the software will attempt to reconnect at one minute intervals.

2. Installation prerequisites

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

2.1 Software requirements

The DataSecurity Plus agent can only function on a Windows machine with .**NET Framework version 4 or higher,** and running any of the below OS versions:

- Windows Vista, 7, 8, 8.1, or 10
- Windows Server 2003 R2, 2008, 2008 R2, 2012, 2012 R2, 2016, or 2019

2.2 Disk space requirements

A minimum of 4GB of free disk space is required.

2.3 Ports

Ensure that the below ports are open to allow the agent to communicate with the DataSecurity Plus server.

- For server to agent communication: RPC ports 135, 137, 138, 139, and 445.
- Transmission Control Protocol (TCP) ports 49152 to 65535.
- For agent to server communication: The port on which the DataSecurity Plus server is running (by default, it runs on port 8800).

Notes:

1. To check which port is being used for HTTP/HTTPS communication, open the web console and navigate to **Admin > General Settings > Connection.** You can also change the default port here.
2. For more information on the ports used by the software, refer to the Port configuration guide.

2.4 Privileges

The DataSecurity Plus user (created while deploying the solution) should be a member of the **Domain Admins group** to perform the below tasks automatically:

- Install, uninstall, or update the agent
- Create or delete the agent service
- Sync properties across the server and the agent

However, if you do not wish to provide domain admin privileges, you can provide the user with the minimum privileges required and perform these tasks manually.

Note:

For information on the minimum privileges required by the service account, refer to the Permissions and privileges guide.

2.5 Firewall exclusions

The HTTP port configured by you for communication between the agent and the server should be excluded from your firewall.

Port	Protocol	Destination	Direction	Purpose
8800 (this is the default HTTP port. If you are using a different port, exclude that port)	HTTP	Target computers	Outbound	Agent to server communication
8800 (this is the default HTTP port. If you are using a different port, exclude that port)	HTTP	DataSecurity Plus server	Inbound	Server to agent communication

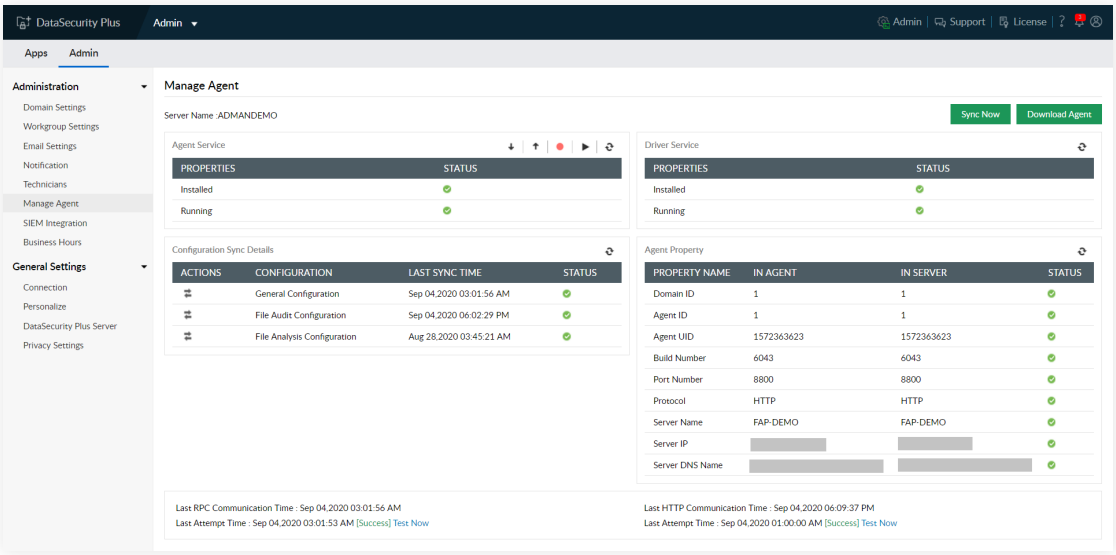
3. Installing the agent

The agent can be installed either automatically (if the service account has domain admin credentials) or manually (minimum privileges are sufficient for manual installation).

3.1 Automatic agent installation

The agent is automatically installed when the target machine is added in the DataSecurity Plus console.

It can then be managed from the Manage Agent page (**Admin > Administration > Manage Agent** > Click the **Manage Agent** link).



Note:
The service account used while configuring your domain in DataSecurity Plus has to be a member of the **Domain Admins group** to allow the application to install the agent automatically.

3.2 Manual agent installation

The agent can be installed manually by any of the four methods below:

A) Deploying the agent via Group Policy

B) Installing the agent by running the MSI file on client computers

C) Installing the agent via command line

D) Installing the agent via ManageEngine Desktop Central

Note:
During or after manual agent installation, event collection will begin only after the target machine is connected to the organization's network at least once, either directly or via VPN. This one-time step is required to sync agent configuration and validate that the machine where the agent is installed is a part of the domain.

3.2.1 Deploying the agent via Group Policy

Step 1: Create an MST file

An MST file is used by the Microsoft Windows Installer—a component of the Windows operating system that enables software installations. It is used to make changes to the MSI file provided by an application vendor during installation. An MST file needs to be created using the ORCA tool, which is available under Windows SDK Components for Windows Installer Developers.

i. Open the ORCA tool > **File** > **Open** > Select the MSI file.

Notes:

1. If the target computer is running a 32-bit operating system (OS), select **DataSecurityPlusAgent-x86.msi.** If the target computer is running a 64-bit OS, select **DataSecurityPlusAgent-x64.msi.**

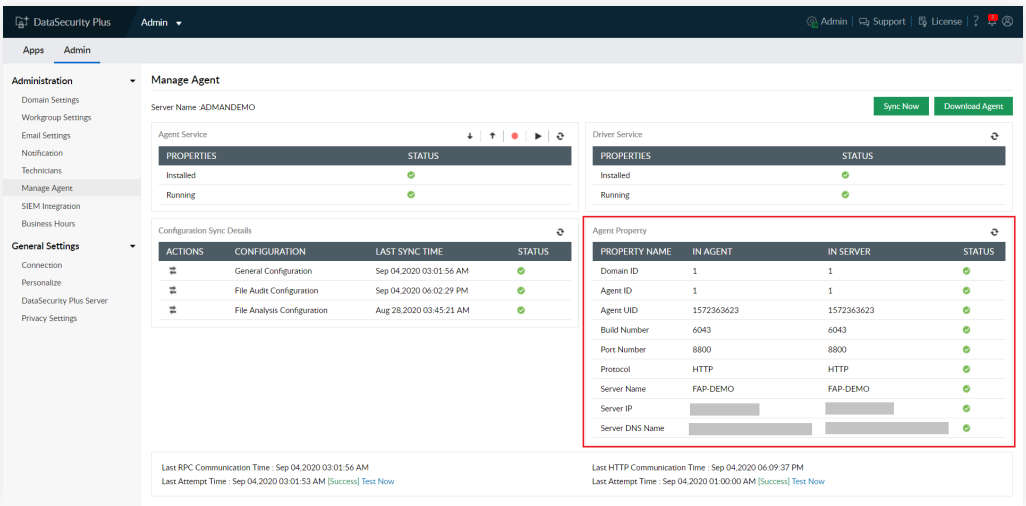
2. The necessary MSI file can be downloaded from the web console by clicking the **Download Agent** button located in the top-right corner of the Manage Agent page **(Admin > Administration > Manage Agent** > Click on the **Manage Agent** link). Alternatively, you can find both the MSI files at **<installation directory>\webapps\fap\agent.**

ii. Click the **Transform** menu > Select **New Transform** > Navigate to the panel on the left, select **Registry** > Enter appropriate values for the below fields:

- **SERVERNAME:** The name of the server where DataSecurity Plus is hosted.
- **SERVERFQDN:** The 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, i.e, HTTP or HTTPS.
- **IsEndpointAutoInstallRequired:** The agent is configured automatically with default policies when the value is set to true.

Note:

The values of these parameters will be displayed in the **Agent Property** table locate at **Admin > Administration > Manage Agent** > Click the **Manage Agent** link.



iii. Click the **Transform tab** > Select **Generate Transform** > Name the transformation file DSP.mst > Click Save.

iv. Copy both the MSI (**DataSecurityPlusAgent-x86.msi** or **DataSecurityPlusAgent-x64.msi**) and MST (**DSP.mst**) files to a new folder.

v. Right-click the newly-created folder, go to **Share with > Specific people** > Type **Domain Computers** in the search box > Provide **Read** permission > Click **Share.**

Step 2: Install the agent via GPO

i. Log in with domain admin credentials to any machine in your network that has the Group Policy Management Console (GPMC). Open the GPMC > Create a new Group Policy Object (GPO) named **DataSecurityPlusAgent** > Link this GPO to the audited computers.

ii. Right-click the **DataSecurityPlusAgent GPO** and select **Edit > Computer Configuration > Policies > Software Settings** > Right-click **Software Installation > New > Package** > In the dialog box, type the full Universal Naming Convention (UNC) path of your DataSecurity Plus **MSI file.**

iii. In the **Deploy Software** pop-up, select **Advanced > Modifications > Add** > Type the full UNC path of the DataSecurity Plus **MST file.**

> **Note:**
> In steps ii and iii, ensure that you enter the full UNC paths of the files as opposed to their local or network paths.

3.2.2 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 HTTP/HTTPS port number used to communicate with the DataSecurity Plus server.
- **Protocol:** The defined protocol for communicating with the DataSecurity Plus server, i.e, HTTP or HTTPS.
- **IsEndpointAutoInstallRequired:** Used for automatic configuration of the agent with default policies when the value is set to true.

Note:
The values of these parameters will be displayed in the **Agent Property** table located at **Admin > Administration > Manage Agent** > Click the **Manage Agent** link.

3.2.3 Installing the agent via command line

To install the agent via Command Prompt, follow the steps below:

i. Log in to the computer you wish to configure in DataSecurity Plus. Open an elevated Command Prompt (right-click Command Prompt and select **Run as administrator**) and type the below command:

msiexec /i "MSI_FILE_LOCATION" PROTOCOL=<PROTOCOL_USED> PORT=<PORT_NUMBER> SERVERNAME=<SERVER_NAME> FQDN=<SERVER_FQDN> SERVERIP=<SERVER_IP> /q

Replace the correct values in place of the below parameters:
<PROTOCOL_USED>: The defined protocol for communicating with the DataSecurity Plus server, i.e, HTTP or HTTPS.
<PORT_NUMBER>: The HTTP/HTTPS port number used to communicate with the DataSecurity Plus server.
<SERVER_NAME>: The name of the server where DataSecurity Plus is hosted.
<SERVER_FQDN>: The FQDN of the server where DataSecurity Plus is hosted.
<SERVER_IP>: The IP address of the server where DataSecurity Plus is hosted.

Notes:
1. The values of the above parameters will be displayed in the **Agent Property** table located at **Admin > Administration > Manage Agent** > Click the **Manage Agent** link.
2. If the target computer is running a 32-bit operating system (OS), provide the location of **DataSecurityPlusAgent-x86.msi.** If the target computer is running a 64-bit OS, provide the location of **DataSecurityPlusAgent-x64.msi.**

ii. Execute the command.

3.2.4 Installing the agent via ManageEngine Desktop Central

To install the DataSecurity Plus agent via Desktop Central, follow the steps below.

Step 1: Create an MSI package

MSI is an installer package file format used by Windows. It contains instructions for MSIEXEC.EXE to install a vendor's application.

i. Log in to the Desktop Central console as an administrator.

ii. Click **Software Deployment > Packages > Add Package** > Select **Windows** from the drop-down.

iii. Provide the below details:
Beside **Package Name,** enter **DSPAgent** or any other name of your choice.
Beside **Package Type,** select **MSI/MSP.**
Beside **License Type,** select **Commercial** from the drop-down.
Beside **Location installable,** select **From Shared Folder.**

iv. Install the package by following either of the methods below:

iv.a Install the package by using an MST file

An MST file is used by the Microsoft Windows Installer—a component of the Windows operating system that enables software installations. It is used to make changes to the MSI file provided by an application vendor during installation. An MST file needs to be created using the ORCA tool, which is available under Windows SDK Components for Windows Installer Developers.

- Open the ORCA tool > **File > Open** > Select the MSI file.

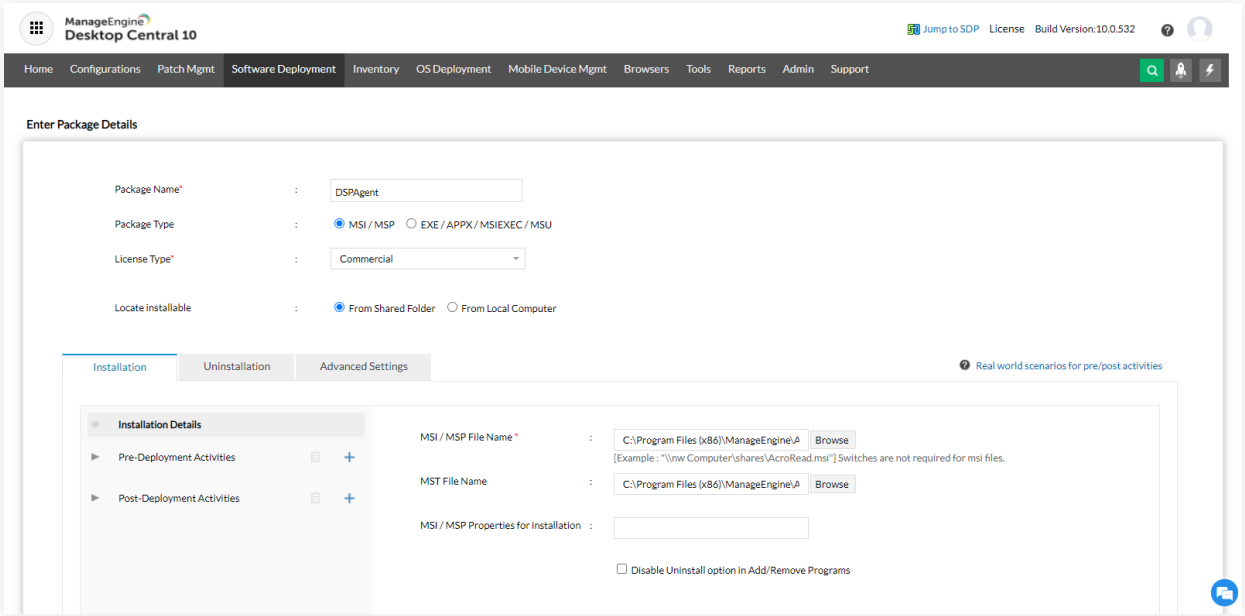
> **Notes:**
> 1. If you are running a 32-bit operating system (OS), select **DataSecurityPlusAgent -x86.msi**. If you are running a 64-bit OS, select **DataSecurityPlusAgent-x64.msi.**
> 2. The necessary MSI file can be downloaded from the web console in the top-right corner of the Manage Agent page (**Admin > Administration > Manage Agent** > Click the **Manage Agent** link). Alternatively, you can find both the MSI files at <**installation directory>\webapps\fap\agent.**

- Click the **Transform menu** > Select **New Transform** > Navigate to the panel on the left, select **Registry** > Enter appropriate values for the below fields:

- **SERVERNAME:** The name of the server where DataSecurity Plus is hosted.
- **SERVERFQDN:** The FQDN of the server where DataSecurity Plus is hosted.
- **SERVERIP:** The IP address of the server where DataSecurity Plus is hosted.
- **BUILD:** The build number of your DataSecurity Plus installation (can be verified by clicking the **License** link in your web console).
- **PORT:** The port number DataSecurity Plus uses for communication (can be verified under **Admin > General Settings > Connection).**
- **PROTOCOL:** The protocol used for communication.
- **IsEndpointAutoInstallRequired:** The agent is configured automatically with default policies when the value is set to true.

Note:
The values of these parameters will be displayed in DataSecurity Plus' web console in the **Agent Property** table located at **Admin > Administration > Manage Agent** > Click the **Manage Agent** link.

- Click the **Transform** tab > Select **Generate Transform** > Name the transformation file **DSP.mst** > Click **Save.**
- In the Desktop Central console, click **Browse**, and select the MSI and MST files.
- Click **Add Package.**



iv.b Install the package by using installation properties

To install the agent from Desktop Central using installation properties, follow the steps below:

- Under **Installation > MSI/MSP Properties for installation,** type the following command:

SERVERNAME="<SERVER_NAME>" PORT="<PORT_NUMBER>"
PROTOCOL="<PROTOCOL_USED>" SERVERFQDN="<SERVER_FQDN>"
SERVERIP="<SERVER_IP>"
SERVERNAME="<SERVER_NAME>" PORT="<PORT_NUMBER>"
PROTOCOL="<PROTOCOL_USED>" SERVERFQDN="<SERVER_FQDN>"
SERVERIP="<SERVER_IP>" IsEndpointAutoInstallRequired="True"

Replace the correct values in place of the below parameters:

<PROTOCOL_USED>: The defined protocol for communicating with the DataSecurity Plus server, i.e, HTTP or HTTPS.

<PORT_NUMBER>: The HTTP/HTTPS port number used to communicate with the DataSecurity Plus server.

<SERVER_NAME>: The name of the server where DataSecurity Plus is hosted.

<SERVER_FQDN>: The FQDN of the server where DataSecurity Plus is hosted.

<SERVER_IP>: The IP address of the server where DataSecurity Plus is hosted.

IsEndpointAutoInstallRequired: The agent is configured automatically with default policies when the value is set to true.

- Click **Add Package.**

Step 2: Deploy the MSI package

i. In the Desktop Central console, click **Software Deployment > Install/Uninstall Software > Windows > Computer Configuration.**

ii. Provide the below details:

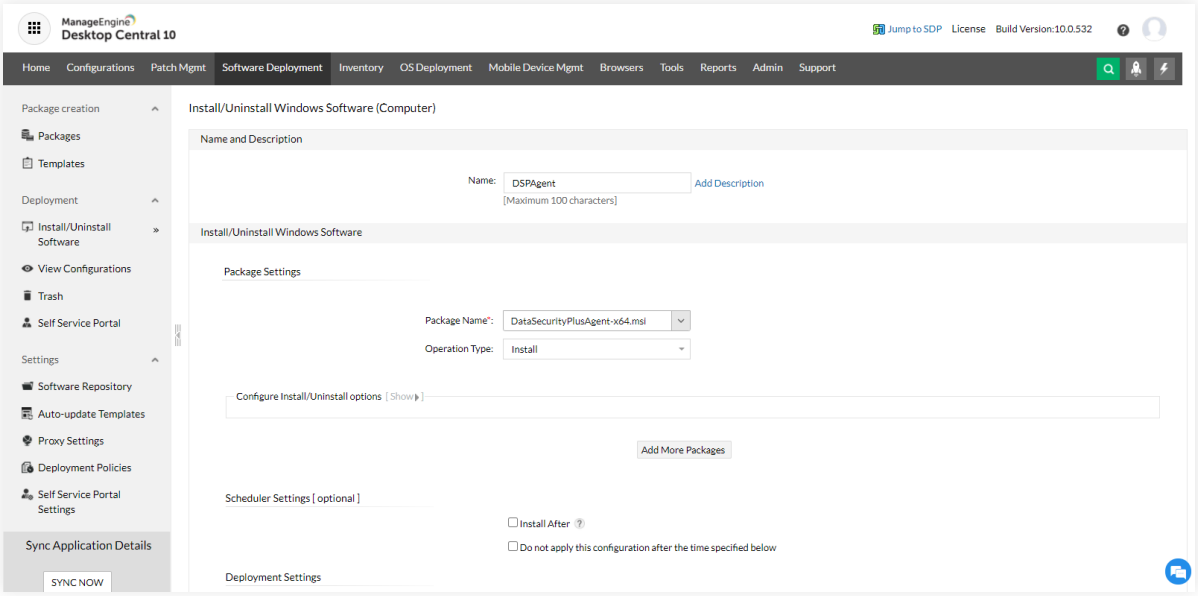
Beside **Name**, enter **DSPAgent** or any other name of your choice.

Beside **Package Name,** select the correct MSI file from the drop-down.

Beside **Operation Type**, select Install from the drop-down.

Beside **Define Target,** enter the name of the computer where the agent is to be installed.

iii. Click **Deploy Immediately.**



4. Syncing agent configuration

DataSecurity Plus attempts to sync agent-server configuration changes via remote procedure call (RPC) as soon as the changes are made.

The software also performs scheduled configuration checks via HTTP/HTTPS and syncs any variations between the agent and the server. Based on the module, these checks are performed at varying intervals.

File Audit: Once every 15 minutes
File Analysis: Once every 15 minutes
Endpoint DLP: Once every 3 hours

If the initial configuration sync via RPC fails, the subsequent scheduled checks will attempt to sync the changes via HTTP/HTTPS.

If the data source is offline, or if the agent-server communication is affected for any reason, up to 2GB of audit data will be stored locally. This data will be pushed to the DataSecurity Plus server once connection is re-established.

DataSecurity Plus also checks the agent service status every 30 minutes, and automatically restarts the service if it has stopped.

You can check the status of the agent and associated properties under **Admin > Administration > Manage Agent** > Click the **Manage Agent** link.

5. 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, provided the service account is a member of the **Domain Admins group.**

If you have only provided minimum privileges, you will have to update the agent manually. To do this, uninstall the existing agent, then download the updated agent and install it by following the directions in section 3.2.

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

6. Uninstalling the agent

To uninstall the DataSecurity Plus agent, go to **Control Panel > Programs > Uninstall a program.** Right-click **DataSecurity Plus Agent** and select **Uninstall.**

7. Troubleshooting agent installation errors

Below are some errors that may arise while installing the agent, as well as the the steps to resolve them.

7.1 The network path was not found

Causes

- The target computer cannot be contacted.
- The service account does not have sufficient privileges to access the admin share (\\Server_Name\admin$) on the target computer.

Solutions

- Ensure that the DataSecurity Plus server can contact the target computer.
- Check if the admin share is accessible by the service account. If not, provide the necessary permission to access the admin share on the target computer.

7.2 Couldn't copy DataSecurityPlus.msi / Access Denied: failed to connect to ADMIN$ share

Causes

- The service account does not have sufficient privileges to copy the MSI file to the admin share (\\Server_Name\admin$) on the target computer.
- The ADMIN$ share access limit has been exceeded.

Solutions

- Check if the service account has privileges to create files in the admin share. If not, provide the necessary permission to access the admin share on the target computer. Alternatively, you can use a different account with the necessary privileges by updating the **Domain User Name** and **Domain Password** under the **Admin** drop-down > **Admin > Administration > Domain Settings.** In either case, ensure that the provided user account is valid and has not been locked out.

- Navigate to **Shared Folders Microsoft Management Console** (MMC) snap-in > **Shares > ADMIN$ > Properties** > Set an appropriate value for **User limit.**

7.3 Another installation is already in progress (0x652)

Causes

- This error occurs when the installation of the DataSecurity Plus Agent MSI file is already in progress on the target computer.

Solutions

- Wait for a few minutes and try to install the agent again.
- If you have not initiated the installation of any software, you can also run the following command in Command Prompt: **taskkill /im /f msiexec.exe** to kill any MSI installation running on the target computer.

7.4 The system cannot find the file specified (0x2)

Causes

- This error occurs when the service account is unable to locate either the DataSecurityPlusAgent-x86.msi or DataSecurityPlusAgent-x64.msi files.

Solutions

- Ensure that either the **DataSecurityPlusAgent-x86.msi** or **DataSecurityPlusAgent-x64.msi** file is present in **SYSTEMDRIVE\Windows directory** on the target computer.

- Check if the admin share (\\Server_Name\admin$) is accessible by the service account. If not, provide the necessary permission to access the admin share on the target computer. Alternatively, you can use a different account with the necessary privileges by updating the **Domain User Name** and **Domain Password** under the **Admin drop-down > Admin > Administration > Domain Settings.** In either case, ensure that the provided user account is valid and has not been locked out.

7.5 Fatal error occurred (0x643)

Causes

This error could occur due to multiple reasons:

- The drive that contains the folder that you are trying to install the package to is accessed as a substitute drive.

- Windows Installer is attempting to install an app that is already installed on your PC.

- The SYSTEM account does not have Full Control permissions on the folder that you are trying to install the Windows Installer package to.

Solutions

- On the target computer, ensure that:
  - .NET 4 framework or above is installed.
  - DataSecurity Plus has not already been installed.

- Check if the admin share (\\Server_Name\admin$) is accessible by the service account. If not, provide the necessary permission to access the admin share on the target computer.

- Next, start and re-register Microsoft Installer Service on the target computer. To do this, press **Windows + R,** type **msiexec /unregister**, and hit **Enter.** Press **Windows + R** again, type **msiexec /register,** and hit **Enter.**

- If the issue persists, try to resolve it using the Program Install and Uninstall troubleshooter.

7.6 RemCom.exe is not recognized as an internal or external command, operable program or batch file

Causes

- This error occurs when the RemCom.exe file, which is used to install the agent on the target computer, has been flagged and deleted by an antivirus software.

Solutions

- Check if the RemCom.exe file exists in the bin folder of the Installation directory **(<installation directory>\bin**) on the target computer. Contact our support team at support@datasecurityplus.com for assistance.

7.7 Could not install client software

Causes

- This error occurs because of a network timeout while installing the agent.

- Agent installation might have been interrupted due to the target computer getting disconnected from the network while installation is in progress.

Solutions

- Ensure that the network connection is re-established and try to install the software again.

7.8 Could not connect to the machine

Causes

- This error occurs when the target computer cannot be contacted.

Solutions

- Check if you are able to ping the target computer from the server where DataSecurity Plus has been installed. If you are unable to fix any underlying connectivity issues, contact our support team at support@datasecurityplus.com.

7.9 Initiating connection to remote service failed

Causes

- This error occurs when the service cannot be created on the target computer.

Solutions

- Check if you are able to ping the target computer from the server where DataSecurity Plus has been installed. If you are unable to fix any underlying connectivity issues, contact our support team at support@datasecurityplus.com.

- Next, check if the admin share (\\Server_Name\admin$) is accessible by the service account. If not, provide the necessary permission to access the admin share on the target computer.

- If the issue persists, contact our support team at support@datasecurityplus.com.

7.10 Logon failure: The target account name is incorrect

Causes

- This error occurs when the service account used is locked, disabled, or its password has been changed.

Solutions

- Check if the admin share (\\Server_Name\admin$) is accessible by the service account. If not, provide the necessary permission to access the admin share on the target computer. Alternatively, you can use a different account with the necessary privileges by updating the **Domain User Name** and **Domain Password** under the **Admin drop-down > Admin > Administration > Domain Settings.** In either case, ensure that the provided user account is valid and has not been locked out.

7.11 Could not start remote service

Causes

- This error occurs when the service account does not have the privileges to start the service in the target computer.

Solutions

- Check if the admin share (\\Server_Name\admin$) is accessible by the service account. If not, provide the necessary permission to access the admin share on the target computer. Alternatively, you can use a different account with the necessary privileges by updating the **Domain User Name** and **Domain Password** under the **Admin drop-down > Admin > Administration > Domain Settings.** In either case, ensure that the provided user account is valid and has not been locked out.

7.12 Another version of the product is already installed (0x666)

Causes

- This error occurs when another version of the agent is already installed in the target computer.

Solutions

- Uninstall the existing agent from the target computer by following the steps in section 6, and retry the current installation.

7.13 Product is uninstalled (0x64E)

Causes

- This error occurs when the agent has already been uninstalled by some other method, such as manual uninstallation.

Solutions

- Install the agent by following the steps in section 3, and try to uninstall the agent again.

7.14 No communication available from agent to the server (initial profile fetch not happening)

Causes

- This error occurs when there is no communication from the agent to the server, immediately after installation.

Solutions

- On the target computer, check if you can access the web console via a browser. To do this, open any web browser and in the address bar, type: **Protocol://ServerName:Port**

- Here, **Protocol** refers to the protocol used for communication, i.e., HTTP or HTTPS. **ServerName** is the name (or IP address) of the server where DataSecurity Plus has been installed. **Port** refers to the port number over which DataSecurity Plus communicates. The default port number is 8800. If you are using a different port, please enter that value.

- If you can access the web console, contact our support team for further troubleshooting.

- If you cannot access the web console, check if the ports used by DataSecurity Plus are open. For more details on the ports used, refer to section 2.3.

7.15 Incorrect function

Causes

If the installation process quits abruptly, it could be due to the following two reasons:

- Shutdown/log off of the target computer has been initiated while the installation is in progress.
- There is insufficient space in the target computer to install the software.

Solutions

- Ensure shutdown/log off is not initiated in the target computer while the agent is getting installed.
- Ensure there is sufficient hard disk space available in the target computer before re-initiating agent installation.

8. Troubleshooting the agent

To monitor and manage the agent in a configured module, go to **Admin** > **Administration** > **Manage Agent** > Click the **Manage Agent** link.

Here, you will find the following details:

- The **Agent Service** table to check if the agent is installed and running. The agent can be installed/uninstalled and started/stopped using the buttons on this table.
- The **Driver Service** table to check if the driver service is installed and running.
- The **Configuration Sync** table to check the last sync time and the sync status of individual configurations. Each configuration can be synced using the corresponding buttons.
- The **Agent Property** table to compare the values of the agent properties in the agent itself and the server. If the properties match, the status is marked with a green check.
- The status of RPC and HTTP communication.

If an issue arises, a notification on the web console will prompt the user on how to resolve the problem.

While troubleshooting the agent service, perform the following checks:

A) Check if the agent service is installed and running on the desired computer.

- In the web console, navigate to the Manage Agent page **(Admin > Administration > Manage Agent >** Click the **Manage Agent** link).
- Refresh the **Agent Service** table.
- Check if the **Agent Service** table has green checks in the **Status** column against every property.
- If the service has stopped, start the service by clicking the appropriate icon.

> **Note:**
> The DataSecurity Plus service account should be a member of the **Domain Admins** group in order to get the service status.

B) Check if the agent is able to communicate with the DataSecurity Plus server.

On the Manage Agent page **(Admin > Administration > Manage Agent** > Click the **Manage Agent** link), refresh the **Agent Property** table.

Check if the Agent Property table has green checks in the **Status** column against every property.

> **Notes:**
> 1. Agent-server communication and configuration syncs occur via RPC.
> 2. The agent forwards event data to the DataSecurity Plus server via HTTP/HTTPS connection.
>
> - Check the status of the RPC and HTTP communication attempts at the end of the **Manage Agent** page.
> - Click **Test Now** to ensure that communication is established.

Below are some common issues that can occur, and the steps to resolve them:

8.1 Agent not installed/running

If you have provided domain admin privileges to the DataSecurity Plus user, the software will attempt auto-installation of the agent. If this fails, check if the user has the appropriate permission to perform this task.

However, if you have provided the minimum privileges, you will have to download the agent and install it manually by following the steps in section 3.2.

8.2 Driver service not installed/running

In case of an issue with the driver service, contact our support team at support@datasecurityplus.com, available 24x5.

8.3 RPC communication failure

DataSecurity Plus uses the RPC ports 135, 137, 138, 139, and 445. RPC communication failure occurs when the agent is unable to contact the server.

> **Note:**
> For more information on the ports used by DataSecurity Plus, refer to the Port configuration guide.

Solution:

In the event of a failure, check if the agent can successfully ping the server. If not, ensure that the RPC ports required for server-agent communication are opened.

If the issue persists, contact our support team at support@datasecurityplus.com.

8.4 HTTP communication failure

Issues in agent-server communication will trigger the "**No HTTP Communication available for more than 24 hours**" notification and cause a similar error message to be displayed on the product console's **Manage Agent** page **(Admin > Administration > Manage Agent >** Click the **Manage Agent** link).

Solution:

In the event of a HTTP communication failure, check if the configured HTTP/HTTPS port is available for use. If the ports are open, try following the steps in the HTTP communication troubleshooting guide.

Tip: For secure, encrypted communication, we strongly recommend enabling HTTPS communication by following the steps in the SSL configuration guide.

9. Limitation

On-demand reports cannot be generated for servers that are not connected to the organization's network.

10. Contacting the support team

For technical assistance, you can email us at support@datasecurityplus.com.

Kindly include the following details in your email to help us assist you better:

- Product edition (Free, Trial, or Standard Edition).
- Product build number.
- A brief description of the problem.

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 analyzes file storage and security permissions, deletes junk files, and detects security vulnerabilities. Users can assess the risks associated with sensitive data storage by locating and classifying files containing personally identifiable information (PII), payment card information (PCI), and electronic protected health information (ePHI). It also prevents data leaks via USBs, email, printers, and web applications; monitors file integrity; and audits cloud application usage. Together, these capabilities ensure the all-round protection of data at rest, data in use, and data in motion.

To explore these features and see DataSecurity Plus in action, check out the online demo.
To learn more about DataSecurity Plus, visit www.datasecurityplus.com.

Download free trial $ Get a quote

Explore **DataSecurity Plus' capabilities**

File server auditing
Audit and report on file accesses and modifications, with real-time alerts and automated responses for critical file activities.

Learn more

File analysis
Analyze file security and storage, manage junk files, optimize disk space usage, and identify permission vulnerabilities.

Learn more

Data risk assessment
Discover and classify files containing sensitive data such as PII, PCI, and ePHI by combining content inspection and contextual analysis.

Learn more

Data leak prevention
Detect and disrupt data leaks via USBs, email, web applications, and printers; monitor endpoint file activity; and more.

Learn more

Cloud protection
Track enterprise web traffic and enforce policies to block the use of inappropriate, risky, or malicious web applications.

Learn more