ManageEngine
DataSecurity Plus

Security Hardening Guide

www.datasecurityplus.com

Table of contents

DataSecurity Plus security hardening guide

DataSecurity Plus is a unified data visibility and security platform that helps administrators ensure comprehensive protection of data at rest, in use, and in motion.

While no system is impenetrable, certain best practices can be followed to reduce the overall attack surface that can potentially be exploited. This guide shows users how to harden security for DataSecurity Plus to eliminate as many security risks as possible.

Security hardening for DataSecurity Plus

1 Follow the principle of least privilege

If a domain administrator account is used, DataSecurity Plus instantly begins auditing, analyzing, and scanning your file storage environment. However, a domain administrator account has several additional elevated rights and privileges that are not required by DataSecurity Plus.

This is why we recommend creating a dedicated user account that only has the privileges and permissions required for DataSecurity Plus to perform its functions. This way, even if the dedicated user account is compromised, the impact of the breach is innately contained.

For the privileges and permissions required for each DataSecurity Plus module you have licensed, refer to the Minimum privileges and permissions guide.

2 Secure the built-in admin account

DataSecurity Plus comes with a built-in admin account that has ultimate privileges. The default password for this account is the same for every DataSecurity Plus customer.

This means the first thing you need to do after installation is change this password. If you skip this step, you will leave your system vulnerable to attacks.

The new password must meet the below complexity rules:

- It must be between 8 and 15 characters long
- It must contain at least:
  - One upper case letter (A - Z)
  - One lower case letter (a - z)
  - One numeric digit (0 - 9)
  - And one of following special characters: ! # $ % & ( ) * - @ ^ _

After three failed attempts to log in with an incorrect username-password combination, the account will get locked out and will unlock automatically after two minutes.

For steps on how to change this password, refer to this guide.

3 Enable HTTPS for secure communication

We recommend that you use HTTPS to ensure that all data transfers between users' web browsers and the DataSecurity Plus server remain secure.

This guide provides the steps to obtaining a signed Secure Sockets Layer (SSL) certificate from your certifying authority and binding it with DataSecurity Plus.

These settings can be further optimized within the following XML file:

conf\server.xml > connector (find the HTTPS connector corresponding to your configured port number).

If you choose to allow only a particular version of Transport Layer Security (TLS) — namely TLSv1, TLSv1.1, or TLSv1.2 — you can disable the other versions by modifying the following parameter, keeping only the required TLS versions:

```
sslEnabledProtocols="TLSv1,TLSv1.1,TLSv1.2"
```

If you want to disable or restrict ciphers, modify the following parameter to contain only the required ciphers:

```
ciphers = "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,
```

TLS_RSA_WITH_AES_128_CBC_SHA256,
TLS_RSA_WITH_AES_128_CBC_SHA,
TLS_RSA_WITH_AES_256_CBC_SHA256,
TLS_RSA_WITH_AES_256_CBC_SHA"

With these changes, you can secure all communication through DataSecurity Plus.

4 Restrict logon access to the DataSecurity Plus server

To further secure your DataSecurity Plus installation, we recommend restricting logon access to the DataSecurity Plus server. You can define the local policy settings and apply different policies to specific sets of users. In the *User Rights Assignment* tab of the *Group Policy Management Editor,* you can choose to **Allow log on locally** or **Allow log on through Remote Desktop Services.** These restrictions will help reduce the attack surface of your infrastructure.

5 Restrict access to the DataSecurity Plus installation folder

Restrict access to the DataSecurity Plus installation folder by modifying the associated folder permissions. This ensures that no one except permitted users have access to DataSecurity Plus' installation files.

6 Audit changes to DataSecurity Plus' installation folder

We recommend that you enable file integrity monitoring on DataSecurity Plus' installation folder from the Data Leak Prevention module (if DataSecurity Plus is installed on a workstation), with the File Audit module (if DataSecurity Plus is installed on a file server), or with a third-party solution.

This will help you track every access to these critical files, identify unwarranted changes, and respond to internal and external threats.

7 Restrict access to the agent installation folder

We recommend restricting access to the folder (in the audited file server) where the DataSecurity Plus agent is installed. By modifying the associated permissions, you can ensure that only authorized users can access or modify this folder.

8 Password-protect your database

DataSecurity Plus comes with a built-in, password-protected PostgreSQL database, allowing access only to authorized personnel. By default, the PostgreSQL service creates a user account with unrestricted privileges—similar to a domain administrator account in AD—to perform various administrative actions.

DataSecurity Plus changes the default password of this account and creates another user account with limited privileges. This new account has restricted permission, is used to connect to the database, and has encrypted credentials to ensure security.

9 Restrict database access from within the UI

By default, database access is restricted from DataSecurity Plus' UI and can only be enabled by an administrative user. The administrator can also choose which accounts should have this privilege. This prevents other technician accounts from modifying or deleting information from the database.

10

Delegate and audit technicians

While configuring technician roles, you can limit their access by allowing them to view only the necessary reports. You can also restrict technicians from performing administrative functions such as adding or removing servers for auditing, modifying configuration settings, and more. In addition, you can keep an eye on the actions performed by each technician with DataSecurity Plus' detailed technician auditing report.

11

Secure archived data

In order to reduce storage space consumption within the database, historical audit data can be compressed and stored separately on routine schedules. These files can then be restored at a later point for further analysis as needed.

We recommend that you password protect these archived files to ensure security and stay compliant with data protection regulations. For an additional layer of protection, we recommend restricting access to the folders containing these files.

12

Protect exported and scheduled reports

When a user exports a report or sets up report delivery schedules, DataSecurity Plus administrators can ensure their security by configuring a password for these files.

We also recommend modifying the folder permissions for the folder that contains these files to prevent unwarranted access.

13 Run DataSecurity Plus as a service

To ensure that event collection doesn't stop even after a user logs out, install DataSecurity Plus as a Windows service. For steps on how to run DataSecurity Plus as a service, refer to this guide.

14 Restrict non-admin users from stopping the agent and product services

To prevent unwanted service downtime, we recommend providing permissions to start, stop, and pause the DataSecurity Plus agent and product services **(ManageEngineDataSecurityPlus - AgentService** and **DataSecurity Plus** respectively) only to a few trusted administrative users.

To do this, follow these steps:

i Log in to your domain controller with administrative privileges and create a new group called **DataSecurity trusted admins.** To this group, add the users to whom you want to provide permission to start and stop the agent and product services.

ii Open the **Group Policy Management** console. From the left pane, expand the **Forests** and **Domains** drop-downs and select your target domain.

iii Right-click the **domain** and select **Create a GPO in this domain and Link it here.**

iv Name the new GPO **DataSecurity Plus Service Control** and click **OK.**

v Right-click the **DataSecurity Plus Service Control GPO** and select **Edit** to open the *Group Policy Management Editor.*

vi Navigate to **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **System Services.**

vii Right-click **ManageEngineDataSecurityPlus - AgentService.** Select **Properties.**

Note: If the DataSecurity Plus agent service is not found in the list, try installing it in the server and retry the above steps.

viii Check the box for **Define this policy setting** and select **Automatic** as the service startup mode.

ix Click **Edit security** to open the **Security for Application Experience** window.

x Clear the users and groups in the existing list and add the **DataSecurity trusted admins** group.

xi Provide **Start, stop and pause** permission to the trusted admin users group.

Repeat steps v to xi for the product service named **DataSecurity Plus.**

15 Configure a mail server

Configuring a mail server enables you to get notified about DataSecurity-Plus-related events. All you need to do is specify a mail server, port, and credentials to authenticate, if required. Refer to this guide for the steps to set up a mail server.

16 Configure a password policy

To configure a password policy, you can set a minimum password length and password history settings as per your requirement. This way, you can strengthen the security of IT infrastructures, thereby improving the overall security posture of your organization. For steps on how to configure a password policy, check out this guide.

17 Configure an account lockout policy

The account lockout policy restricts access to user accounts after a few unsuccessful login attempts. To configure an account lockout policy, you need to provide the number of failed logons to lock accounts after, along with a lockout duration. You can refer to this help document for directions to configure your account lockout policy.

18 Configure two-factor authentication

In DataSecurity Plus, data protection is strengthened with the implementation of two-factor authentication. Two-factor authentication makes it mandatory for users to authenticate twice during logon. To enable two-factor authentication, you need to enable logon settings and choose one or more authentication methods. For steps to configure two-factor authentication, refer to this guide.

19 Enable notifications

To receive notifications related to the agent service, server, disk space, event collection, etc., configure a mail server and the time at which you want to receive notifications. This guide provides you the steps to enable notifications.

20 Install the product on a non-OS drive

We recommend installing DataSecurity Plus on a non-OS drive to mitigate issues related to data storage and event collection. Refer to this help document for steps to move your installation to a target drive.

Need help?

If you have any questions about the above settings, please contact us at support@datasecurityplus.com.

You can also schedule a free personalized demonstration to have a product expert help you with the configurations.

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

Our Products

AD360 | Log360 | ADAudit Plus | EventLog Analyzer

Exchange Reporter Plus | SharePoint Manager Plus