ManageEngine
Exchange Reporter Plus

Data integrity techniques and security measures adopted by Exchange Reporter Plus

www.exchangereporterplus.com

ManageEngine Exchange Reporter Plus has several mechanisms to ensure the security and integrity of your Exchange data. This document elaborates on the methods adopted by Exchange Reporter Plus to secure Exchange data that is collected and processed.

Log collection

Secure communication protocols such as WMI or Distributed Component Object Model (DCOM), TLS, and HTTPS (HTTP secured with SSL/TLS) are used to transmit log data from Exchange Server and Microsoft 365 to the Exchange Reporter Plus server. HTTPS is also used to secure the communication between PowerShell and Exchange Reporter Plus. Reliable delivery of log messages is ensured with the TCP communication protocol.

Exchange Reporter Plus employs different security and encryption techniques such as TLS, AES-256, SHA-256, and more to secure the logs in transit. Based on the type of log data, the techniques vary. Here are the security methods employed by Exchange Reporter Plus based on the mode of log collection and data type.

a. **WMI configuration**
   Windows event logs that are collected using WMI configuration are secured using RPC_C_AUTHN_LEVEL_PKT_INTEGRITY, which authenticates and verifies that no data transferred between the client and server has been modified.

b. **Elasticsearch data in-transit**
   The integrity of Elasticsearch data while transiting using TLS is ensured using the Search Guard Elasticsearch plug-in.

Other security measures

- **Secure web communication:** Exchange Reporter Plus is a web-based solution with a web client that can be accessed from anywhere in the network. Enabling HTTPS ensures that all web communication is secure.

- **Role-based access control (RBAC):** Exchange Reporter Plus allows you to compartmentalize your data among the product's technicians. Two access levels are provided: administrator and operator, in order to limit user access and control to specific features and device information. In addition to these built-in access levels, you can create customized access levels. This way, you can ensure that data is accessed only by authorized personnel.

- **Exchange Reporter Plus technician actions:** Exchange Reporter Plus provides a built-in option to generate the audit trail of all user actions performed in the product. This allows you to ensure accountability within the solution.

- **Session termination after idle time:** With Exchange Reporter Plus, you can set up a session expiry time and if the session is idle for more than 10 minutes (the minimum time), the session will be terminated.

- **Report export password:** Exchange Reporter Plus provides a built-in option to export reports in a zipped format and protecting it with a strong and unique password of your choice. This way, you can ensure that the report data is seen only by authorized personnel.

- **Two-factor authentication with backup verification code:** Exchange Reporter Plus allows you to set up an extra authentication factor. You can also set up a backup verification code in case technicians don't have access to their mobile device or face issues with certain authentication methods.

- **Enforce LDAP SSL:** Exchange Reporter Plus allows you to secure the LDAP connection between the Exchange Reporter Plus server and Active Directory with SSL.

- **Enforce GDPR compliance:** Enabling this option in Exchange Reporter Plus ensures that email and IP addresses are masked in the product.

- **Database password:** The database password is encrypted using CrypTag with the AES-256 algorithm.

- **Database encryption key:** The database encryption key is encrypted using CrypTag with the AES-256 algorithm.

- **Built-in technician password:** Built-in technician passwords are stored in the database as a hashed value.

- **Email server communication:** The JavaMail API used for email communication is encrypted using SSL and TLS algorithms.

- **Active Directory authentication:** Active Directory login is performed using Kerberos and NT LAN Manager (NTLM) authentication.

Securing the Exchange Reporter Plus installation directory

The Exchange Reporter Plus installation directory contains important files required for it to function properly, including files that are used to start and stop the product and the license file. By default, Exchange Reporter Plus will be installed in the C:\ManageEngine folder. This will grant even non-admin users belonging to the Authenticated Users group Full Control permission over the files and folders in the product's installation directory, meaning any domain user can access the folder and modify its contents, potentially making the product unusable. Simply removing Authenticated Users from the Access Control List (ACL) won't help, as this will render them unable to even start Exchange Reporter Plus as a service or application. To overcome this issue, follow the steps outlined below based on where Exchange Reporter Plus is installed.

1. **If Exchange Reporter Plus is installed in the C:\ManageEngine folder.**
2. **If Exchange Reporter Plus is installed in the C:\Program Files folder.**

1. Steps to perform if Exchange Reporter Plus is installed in the C:\ManageEngine folder.

By default, the C: directory in a Windows Client OS has **Authenticated Users** with the **Modify** permission for subfolders. However, the C: directory in a Windows Server OS does not have **Authenticated Users** in its ACL. So, based on the OS in which Exchange Reporter Plus is installed, the steps may vary.

a. **If Exchange Reporter Plus is installed in a client OS.**
b. **If Exchange Reporter Plus is installed in a server OS.**

a. **If Exchange Reporter Plus is installed in a client OS:**

1. **Disable Inheritance for the C:\ManageEngine\Exchange Reporter Plus** folder. Refer to the Appendix below for step-by-step instructions.
2. Remove **Authenticated Users** from the folder's ACL. Refer to the Appendix for step-by-step instructions.
3. Remove the **Authenticated Users** permission for the folders listed below from the product's installation directory.
   i. bin\license
   ii. temp
4. Assign the **Modify** permission for the **C:\ManageEngine\Exchange Reporter Plus** folder to users who can start the product. Refer to the Appendix for step-by-step instructions.
5. If the product is installed as a service, make sure that the account configured under the **Log On** tab of the service's properties has been assigned the **Modify** permission for the folder.

b. If Exchange Reporter Plus is installed in a server OS:

1. Remove the **Authenticated Users** permission for the folders listed below from the product's installation directory. Refer to the Appendix for step-by-step instructions.
   i. bin\license
   ii. temp
2. Assign the **Modify** permission for the **C:\ManageEngine\Exchange Reporter Plus** folder to users who can start the product. Refer to the Appendix for step-by-step instructions.
3. If the product is installed as a service, make sure that the account configured under the **Log On** tab of the service's properties has been assigned the **Modify** permission for the folder.

2. Steps to perform if Exchange Reporter Plus is installed in C:\Program Files folder.

1. Remove the **Authenticated Users** permission for the folders listed below from the product's installation directory. Refer to the Appendix for step-by-step instructions.
   i. bin\license
   ii. temp
2. Assign the **Modify** permission for the **C:\ManageEngine\Exchange Reporter Plus** folder to users who can start the product. Refer to the Appendix for step-by-step instructions.
3. If the product is installed as a service, make sure that the account configured under the **Log On** tab of the service's properties has been assigned the **Modify** permission for the folder.

Notes:

- Microsoft recommends that software be installed in the Program Files directory. Based on your specific needs or organizational policies, you can choose a different location.

- The steps mentioned in this document are applicable to all ManageEngine products installed in the C:\ManageEngine folder by default.

Appendix

Steps to disable inheritance

1. Right-click the **folder** and select **Properties.**
2. Go to the **Security** tab and click **Advanced.**
3. Click **Disable inheritance.**
4. Click **Apply** and then **OK.**

Steps to remove Authenticated Users from ACL

1. Right-click the **folder** and select **Properties.**
2. Go to the **Security** tab and click **Edit.**
3. Select the **Authenticated Users** group and click **Remove.**
4. Click **Apply** and then **OK.**

Steps to assign modify permissions to users

1. Right-click the **folder** and select **Properties.**
2. Go to the **Security** tab and click **Edit.**
3. Click **Add.**
4. Enter the name of the user or group, and click **OK.**
5. Under the ***Permission for Users*** section, check the box under the **Allow** column for the **Modify** permission.
6. Click **Apply** and then **OK.**

Contact support for more details

For further details, please contact support: support@exchangereporterplus.com.