Guide to secure your RecoveryManager Plus installation

If a user belongs to the Authenticated Users group, they can tamper with the RecoveryManager Plus installation directory. To circumvent this and improve the security of your RecoveryManager Plus deployment, follow the steps in this document.

Description

The RecoveryManager Plus installation directory contains important files required for it to function properly, including files that are used to start and stop the product, file containing database configuration information, and the license file. By default, RecoveryManager Plus will be installed in the *C:\ProgramFiles\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 RecoveryManager Plus as a service or application.

For new RecoveryManager Plus installations builds 6074 and above

For new installations of builds 6074 and above, only the following types of accounts are automatically provided access to the installation directory to ensure file security and integrity:
- Local system account
- User account used during product installation
- Domain Admins group
- Administrators group

Important:
- If the product is installed as a service, ensure that the account configured under the **Log On** tab of the service's properties has been assigned **Full Control** permission for the installation directory.

For existing RecoveryManager Plus instances

Unauthorized users can be prevented from accessing the ADSelfService Plus installation directory for builds lower than 6304 in two ways:
   i. Run the SetPermission.bat file
   ii. Remove unnecessary permissions manually

I. Run the SetPermission.bat file

By this method, access to the installation directory is automatically restricted to only the necessary accounts. There are two ways to do this:

Option 1: Update to build 6074. Open **Command Prompt** as an administrator and navigate to the *<installation directory>/bin* folder (by default *C:\ProgramFiles\ManageEngine\ RecoveryManager Plus\bin)*. Run the **SetPermission.bat** file.

Option 2: Download the file using this link and move it to the ***<installation directory>/bin*** folder. Open **Command Prompt** as an administrator and navigate to the ***<installation directory>/bin*** folder (by default **C:\ProgramFiles\ManageEngine\RecoveryManager Plus\bin).** Run the **SetPermission.bat** file.

```
C:\Program Files\ManageEngine\RecoveryManagerPlus\bin>setPermission.bat
Successfully processed 13243 files; Failed processing 0 files
Successfully processed 13243 files; Failed processing 0 files
          \Domain Admins: No mapping between account names and security IDs was done.
Successfully processed 0 files; Failed processing 1 files
Successfully processed 1 files; Failed processing 0 files
Successfully processed 13243 files; Failed processing 0 files
Successfully processed 13243 files; Failed processing 0 files

C:\Program Files\ManageEngine\RecoveryManagerPlus\bin>_
```

II. Modify required permissions manually

To manually remove access permissions for unnecessary groups, such as Authenticated Users and Domain Users, follow the steps outlined below.

1. Disable Inheritance for the installation directory (by default ***C:\Program Files\ManageEngine\ RecoveryManager Plus).*** Refer to the appendix for step-by-step instructions.

2. Remove access permissions for all the unnecessary groups. Refer to the Appendix for step-by-step instructions.

3. Provide Full Control permissions to the following for the product's installation directory:
   - Local system account
   - Domain Admins group
   - Administrators group

Refer to the Appendix for step-by-step instructions.

4. Assign the **Full Control** permission for the installation directory 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, ensure that the account configured under the **Log On** tab of the service's properties has been assigned the **Full Control** 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.

Appendix

Steps to disable inheritance

1. Right-click the folder and select **Properties.**

2. Navigate 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. Navigate to the **Security** tab and click **Edit.**

3. Select the **Authenticated Users** group and click **Remove.**

4. Click **Apply** and then **OK.**

To assign modify permissions to users

1. Right-click the folder and select **Properties.**

2. Navigate 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.**

Our Products

AD360 | Log360 | ADManager Plus | ADAudit Plus | ADSelfService Plus | M365 Manager Plus

ManageEngine
RecoveryManager Plus

ManageEngine RecoveryManager Plus is a comprehensive backup and recovery solution that empowers administrators to back up and restore their Active Directory, Entra ID, Microsoft 365, Google Workspace, on-premises Exchange and Zoho WorkDrive environments. With its incremental backups, flexible retention policies and multiple modes of restoration—such as domain controller recovery and object-, item- and attribute-level restoration—RecoveryManager Plus delivers a holistic solution for backing up data that is critical for your enterprise to function.

For more information, visit www.manageengine.com/ad-recovery-manager.

$ Get Quote   **⬇ Download**