Micro Focus File Dynamics 6.5 Release Notes

September 10, 2019

1 Platform and System Requirements

1.1 .NET Framework

The following packages now require .NET Framework 4.7.2 or later:

- Engine (Config) / File Viewer
- Event Monitor (Config)
- Admin Client
- Data Owner Client

The following packages still require .NET Framework 4.6.2 or later:

- File System Agent
- Phoenix Agent

1.2 Supported Platforms

Starting with File Dynamics 6.2, the following platform requirements have been updated:

- Engine now requires Windows Server 2012 R2 or later
- All components are supported on Windows Server 2019

Starting with File Dynamics 6.5, SQL Server 2012 and 2014 are now considered deprecated. Please note that support for these versions will most likely be removed in the next major release.

1.3 Desktop Applications are now 64-bit Only

Starting with File Dynamics 6.5 all desktop components are supported only with 64-bit operating systems. Prior release of the Admin Client and Data Owner Client would potentially operate on 32-bit systems.

Components which might have been installed in the standard `C:\Program Files (x86)` folder on 64-bit operating systems will now be installed by default in `C:\Program Files` instead.

2 New and Updated Security Policies

2.1 Updated Security Policy

The Security Notify policy has been updated and renamed to Security Notification policy.

2.1.1 Historical Reporting

Security Notification Policies now include time-based event records, and not just a single point-in-time differential snapshot. Based on the policy-defined retention period, historical reporting on security changes for a given path over a period of time is now possible.

2.1.2 Email Notifications

Email notifications for security event detection no longer contain the event data itself. The content of the email contains only the given target path for which security changes were detected.

2.1.3 Assigned Data Owners

Security Notification Policies now make use of Data Owner assignments, similar to other Target-Driven policies such as Epoch and Workload.

Data Owners assigned to a Security Policy have access to all of the Security Notification records and reporting associated with the policy via the Data Owner Client.

2.2 New Security Policies

The following new security policies are being introduced in File Dynamics 6.5:

- Security Lockdown policy
- Security Fencing policy

2.2.1 Security Lockdown Policy

This policy allows administrators to capture a baseline snapshot of all direct-assigned permissions to a target path and its subordinate folders, then enforce that baseline by reverting any detected security changes to the file system permissions.

The Security Lockdown policy includes all the benefits of the Security Notification policy including assignment of Data Owners and event reporting. Data Owners can also be assigned a Policy Enable permission that allows the Data Owner to act as a Security Manager, giving them the ability to enable or disable the associated Security Lockdown policy, as well as reset its permissions baseline.

2.2.2 Security Fencing Policy

This policy allows administrators to define a set of criteria that determines which identities are allowed to participate as directly-assigned permissions holders to a given target path and its subfolders.

The Security Fencing policy includes all the benefits of the Security Notification Policy including assignment of Data Owners and event reporting.

3 Updated Identity-Driven Policies

3.1 Expanded Options for Path Owner

A number of Identity-Driven policies now have expanded options for assignment of path owner. These updates include direct selection of the Built-in Administrators group, and for Collaborative policies, the option to use the associated group’s Manager.

3.2 Improved Handling for Profile Path Policies

Due to the evolving nature of Windows profiles and the folder naming scheme used for profile storage, File Dynamics will no longer manage the actual profile folders themselves but rather, the per-user parent folder under which the various profile folders are kept.

File Dynamics will no longer attempt to create these folders for you, and will allow Windows to create the profile folder that it requires. Furthermore, Full Control permissions are now assigned to the managed folder allowing Windows to dynamically create the required profile folder as needed.

3.3 Defer Delete Source for Move Events

Identity-Driven policies now include a setting in the Move Schedule options for deferring the cleanup of source data. This option applies to Move events in which data is copied then deleted, such as Move operations that cross volumes or servers.

4 Required Updates

4.1 Product Updates

File Dynamics 6.5 only supports direct updates from File Dynamics 5.2 or later.

4.2 Required Agent Updates

File Dynamics 6.5 supports the following minimum version of File System and Phoenix Agents:

- File System Agent 6.2 (or later)
- Phoenix Agent 6.5

5 Known Issues

5.1 Active Directory to Active Directory Cross-Empire Data Migrations

The Active Directory to Active Directory Cross-Empire Data Migration functionality is currently broken in this release and will be fixed in a forthcoming update.