DefendX Software

# DefendX Software Mobility Release Notes

## Version 8.2

These Release Notes contain supplemental information about Mobility Version 8.2

# Table of Contents

## Upgrading and Backwards Compatibility

1. Before upgrading you should backup both Mobility databases.
2. The Mobility Admin, Access Portal, Recovery Portal and File Intranet components must all be upgraded to Mobility 7.5
3. During the upgrade of the Mobility Admin you must choose to upgrade both databases.
4. Customers that have a lot of task services may not want to or be able to upgrade all of them at once. Therefore, the Mobility 7.5 Admin is backwards compatible with 7.x/6.x/5.x Task Services and 7.x/6.x/5.x Core Tiering Engines.
5. Before upgrading a task service, you should stop the service first to prevent having to reboot the server.
6. When upgrading the task service or core tiering engine, the other, (i.e. both), must be upgraded.

## Primary File Servers Supported

**Mobility 8.2 Task Services support the following server types:**

1. Microsoft Windows
   - Includes support for Windows Cluster
2. NetApp
   - 7-Mode
   - C-Mode
3. EMC
   - VNX
   - Unity
   - Dell EMC PowerMax eNAS
4. Generic
   - EMC Isilon
   - Hitachi HNAS
   - Other NAS servers

## Secondary Storage

**Mobility 8.2 supports the following secondary stores**

1. CIFS
   - On NTFS file systems
   - On Strongbox LTFS
2. Microsoft Azure
3. Amazon S3
4. S3 Connector
   - EMC ECS (S3)
   - Data Domain (S3)
   - NetApp StorageGRID Webscale (S3)
   - Hitachi HCP (S3)
   - Other S3 Compatible (future untested S3 compatible clouds)
5. NFS
   - Amazon NFS gateway

# What's New in Mobility 8.2

## All Components

- The company name has been changed to "DefendX"
- The product name has been changed to "Mobility-VFM"

## VFM Admin Notes

- There is now only a single VFM Admin installer that supports all secondary stores. The install will no longer prompt for a serial number. The License Key Utility will no longer be used.
- The VFM Admin has a new dark look. After an upgrade it may be necessary to refresh your browser by holding the Ctrl key down while clicking on the browser's refresh icon.
- The License Information Summary tree menu item and its parent tree menu will now display as "Orange" when the license consumption is between 75% and 90%. It will display "Red" when between 90% and 100% and "Yellow" when over 100% to match the banner's color of yellow.
- The Primary Storage Status tree menu item and its parent tree menu will now be "Red" when one or more primary servers has an alert.
- If "Mail Settings" has not been configured, then the tree menu item will be displayed in orange.

## New Features

- During Admin setup, when creating the databases, the location of the data and log files will be determined by retrieving the default locations configured for the SQL Server instance. If these locations were not able to be retrieved, then the location of the master database will be used.
- Assessments have been added:
    - Home page will display an Assessment report for the entire enterprise.
    - Reports by Primary Server page will display an Assessment report for each primary server.
    - Primary Server's CTE page as a separate tab to configure assessment scans.
    - Assessments can be run on their own schedule.

- A new Alerts page has been added:
    - The “Notification Settings” page was updated to include additional options for alerts.
    - Alerts will optionally be written to the VFM Admin’s server event log controlled by the “Log alerts to the Windows Event Log” checkbox.
    - Alerts will optionally be sent to each e-mail address listed. This is controlled by the “E-mail Administrative Alerts” checkbox.
    - There are two checkboxes which can be used to alert whenever there is a short burst of auto-recalls occurring or failing.
    - An alert will be generated when the auto-recall connector disconnects, database connectivity or updates fail, insufficient disk space when recalling files, secondary store connectivity or updates fail, CTE scan fails, requests were placed on hold or release, the contract license limit was exceeded.
- Tiering Operations – Stub Settings page will no longer have options to enable the auto-recall connector. This option has been moved to the primary Server Settings page.
- Tiering Operations - File Attribute Settings page is new and exposes all tiering options based on file attributes. An attributes setting’s name can be assigned to a primary server on its settings page.
- Tiering Operations - Core Tiering Engine Scan Policy page has new date options to allow for the selection of “Day”, “Week” or “Month” instead of just month.
- Tiering Operations added support for encrypting file data within the secondary stores.
    - The VFM Admin’s “web.config” file must have the following “appSetting”

      **<add key="ShowEncryptCompressSettings" value="Yes"/>**
    - Under “Tiering Operations – Encryption” there are two new pages, “Encryption Settings” and “Generate Encryption Keys”.
    - The “Master Encryption Key” page remains the same.
    - Assign an encryption settings name to a secondary store group.
- Primary Server Settings page now supports a Failover Primary Server to support high availability for primary servers. A “Failover” task server can now be assigned to “NetApp” and “Generic” primary servers. EMC VNX and Unity primary servers will be supported in a future release. Windows primary servers already support this for Windows Clusters.

    - To **manually fail over a task service**, place a check mark in one or more of the checkboxes on the “Primary Servers” page and press the “Failover Task Servers” button. The task servers will switch roles within 5 minutes.
    - A **task server will be automatically failed over** by the VFM Admin when the task server that is currently assigned as the primary role does not contact the VFM Admin within 5 minutes.
    - To **prevent a task service from manually or automatically failing over**, possibly due to planned maintenance, select “Edit Server” on the “primary Servers” page and place a check mark in the “Disable Failover” checkbox and press the “Update” button.
- Primary Server Settings page contains a new Auto-Retier option
    - Added option to enable Auto-Retiering of files that have been recalled or recovered based on whether it was selected during a right-click, portals, or file intranet operation.
    - Files that were auto-recalled will always be auto-retiered if the option is enabled.
- Primary Server Settings page for NetApp C-Mode now contains an additional TCP FPolicy Port setting so that communications with FPolicy can be with a specific port instead of a dynamic one. This can be used to allow a specific port through a firewall.
- Primary Servers – Share Settings page will indicate whether if the CTE locations are a list of included or excluded ones.
- Primary Server Summary page has a separate CTE link to configure the Core Tiering Engine.
- Added additional scan options for Core Tiering Engine Settings for Primary Servers. These options correspond with settings defined on the Stub Settings page and Secondary Store Platform Settings page.
    - Stub Sync
    - Stub Deletion during deletion policy run
    - Stub Recreation when stub is missing
    - Secondary Store Deletion when stub is missing
    - Mass recall option.
- Primary Server Settings page has options to restore NFS permissions when recovering files back to NFS exports. When a file is recreated its NFS permissions will be set to what it was when the file was tiered. The task services will use SSH to set the permissions if

SSH is configured for each primary server. The setting of NFS permissions should only be done on volumes whose security style is set to UNIX. It should not be done on mixed volumes since permissions could be set incorrectly.

- Secondary Storage - Platforms Enable Page was added to allow you to choose the secondary stores you want to enable.
    - After a new install of the Admin, this page will initially display.
- Secondary Storage - S3 Connector secondary store platform page now has an option to support V4 Authentication.
- Secondary Storage - Azure secondary store platform page now has an option to allow for a bucket name.
- Enhanced Scheduling page:
    - Added support for “Recur Every”, “Days of the Week” and “Minutes of the Hour”.
- Database Config and Store Setting pages now has support for enabling SQL Server “Encrypted Connections” and “Trust Server Certificate” options. The newer SQL OLEDB driver "MSOLEDBSQL" is required.
- Account/Process Configuration page has a new Exempt Processes page which is applicable to the Task Service for Windows only. A process name can be added to exempt that process from being able to auto-recall files.
- Account/Process Configuration page – Exempt Accounts now supports exempting UNIX UIDs from being able to auto-recall files. The numeric UID of the user can be added.
- The License Summary Information page also has a new “Resize License” button. This will start a resize to calculate the license consumed size immediately. The application event viewer will indicate when the resize is complete.
- The About page will no longer contain the option to update the contract license. This option was moved to the License Summary Information page.

**Note**: Not all minor fixes are listed here only the ones considered mentionable are.

## Task Service Fixes

- Tiering a file to a secondary store which failed and resulted in an error 12019 (handle is not in correct state) has been resolved to its actual error of 12002, http timeout. Therefore, when timeouts occur, the request will automatically be placed on hold and retried at a later time. The former error 12019 would immediately fail the request. This was fixed in 7.5.0.1215.
- Windows deduplication: Tiering files which have been deduped on Windows file servers would fail by default due to those files having a reparse point. To allow these files to be tiered, check the option on the File Attributes page to allow Windows Deduped files.
- NetApp NTFS volumes can be mounted on Linux when the export policy rule is configured for NFS access; therefore, these volumes will now be included in the list of NFS exports for the primary server shares.
- When recalling or deleting secondary store objects that were tiered via NFS and being recalled via CIFS may fail as well as vice-versa. This has been corrected.
- When recovering stubs, via the portals, if the file was tiered to multiple stores using a combination of mirrored and non-mirrored selections then the recreated stub failed to contain either the mirrored or non-mirrored data. This has been corrected.

## VFM Admin Fixes

- For Amazon and S3 Connector, the Test button would fail to connect for v4 authentication when a non-standard http/https port number was configured. This has been corrected.
- Fixed an issue with Storage Group settings dropdown for the selection of the Secondary Store Name. Sometimes not all the store's names would be present in the drop down.

## Recovery Portal Fixes

- Changes to direct download feature to fully support downloads of files having Unicode characters in their file names.
- For Amazon and S3 Connector, the direct download would fail to connect for v4 authentication when a non-standard http/https port number was configured. This has been corrected.

- Files that were tiered from NFS Exports would previously fail to recover when using the File & Search page if the checkbox "Check here if the Shares listed are actually NFS Exports" was not checked. This has been resolved. Note: The checkbox is intended to be used as a filter when displaying a list of files only.

## Known Issues

- AWS bucket name cannot have any dots (.) in it.

*Note: If you suspect that you found an issue with this product version, please reach out to support at support@defendx.com.*

## About DefendX Software

DefendX Software helps organizations secure their critical business files and maximize the value of their enterprise file storage resources. From comprehensive intelligence, modeling, costing and chargeback to seamless file movement, protection and archiving, DefendX provides industry-leading capabilities to eliminate waste and align the value of files with the storage resources they consume. With DefendX, important file locations and the users who access them can be monitored to provide governance, protect against theft and enforce compliance policies. For more than 20 years, DefendX Software has been helping public and private sector customers around the world save money and eliminate risk every day.

## DefendX Software Professional Services

DefendX Software's Professional Services offers consulting, training, and design services to help customers with their storage management challenges. We have helped hundreds of customers to implement cost-effective solutions for managing their storage environments. Our services range from a simple assessment to in-depth financial analyses.

For further assistance in creating the most cost-effective Storage Management Infrastructure, please contact your DefendX Software Representative at 800-390-6937.

## Legal & Contact Information

The information contained in this document is believed to be accurate as of the date of publication. Because DefendX Software must constantly respond to changing market conditions, what is here should not be interpreted as a commitment on the part of DefendX Software, and DefendX Software cannot guarantee the accuracy of any information presented after the date of publication.

This user manual is for informational purposes only. DEFENDX SOFTWARE MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

DefendX Software and other marks are either registered trademarks or trademarks of DefendX Software in the United States and/or other countries. Other product and company names mentioned herein may be the trademarks of their respective owners.

DefendX Software products and technologies described in this document may be protected by United States and/or international patents.

DefendX Software
119 Drum Hill Road, #383
Chelmsford MA 01824
Phone: 1-800-390-6937
E-mail: info@DefendX.com
Web Site: http://www.DefendX.com

 Doc#DFX1209EF