



# DefendX Software Mobility Release Notes

Version 7.5

These Release Notes contain supplemental information about Mobility Version 7.5



## Table of Contents

Upgrading and Backwards Compatibility .....	3
Primary File Servers Supported .....	3
Secondary Storage .....	4
What's New in Mobility 7.5.....	4
TLS Feature Enhancement:.....	4
Components.....	4
Task Service.....	4
VFM Admin .....	6
Installers .....	6
Windows File Filter.....	8
Core Tiering Engine .....	8
Database: .....	9
Known Issues .....	9
About DefendX Software .....	10
DefendX Software Professional Services .....	10
Legal & Contact Information .....	11

## 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 7.5 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
4. Generic
  - EMC Isilon
  - Hitachi HNAS
  - Other NAS servers

## Secondary Storage

### **Mobility 7.5 supports the following secondary stores**

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

## What's New in Mobility 7.5

### TLS Feature Enhancement:

- Refer to the “Transport Layer Secure Protocols supported in VFM” document.

### Components

- Updated all EULAs to the new 2018 text. EULA's are displayed during setup when accepting the license agreement.

### Task Service

- Checking the first 64KB of a file to determine if it is empty will be done on the file's main stream and no longer on alternate streams, if they exist. The alternate streams can be empty.
- The “Thumbs.db” files are dynamically generated files when using thumb nails in Windows Explorer; therefore, these files will no longer be tiered. This also prevents

creating a "Thumbs.db.htm" stub and having Windows Explorer automatically re-create the Thumbs.db file.

- Changed the x-ms-version to "2017-04-17" to support both Azure and the Azure DataBox. The previous "2018-03-28" date was not yet supported by the DataBox.
- Creating entries into the TieredTarget table were not unique enough for Atmos and Azure. This has been corrected by prefixing the Tenant/Account to the store's address.
- When aging files, only set the FileAged column when it is NULL so existing dates won't be changed, which was a mistake in previous versions.
- Changed the retrieving of previous file meta-data by getting just the current one, i.e. where FileAged is NULL.
- When the task service is doing SQL via Web, it should not be providing the database provider to use to the Admin. The Admin should be determining the correct provider based on the ones installed on its server.
- Universal S3 - Fixed backing-up the databases to Universal S3. Previous 7.x versions failed on auth error 403 when creating the anchor stub.
- NetApp Task Service - Fixed a possible crash in the Task Service for NetApp when it cannot access its configuration information from the VFM Admin. Adding the task service account as an exempt account would cause the abort when VFM Admin was not available
- Removed Securable Routable Object (SRO) code since it is deprecated.
- Fixed backing-up the databases to any Universal S3 store. Previous 7.x versions failed on authentication error 403 when creating the anchor stub in the Universal S3 store.
- Fixed a crash during a CIFS secondary store delete where the header file location failed to be. This only occurs when the name of the primary server contains an underscore which is rare.
- Fixed a possible crash in the Task Service for NetApp when it could not access its configuration information from the VFM Admin. The crash occurred when attempting to exempt account the service account.
- Fixed possible out-of-memory condition when traversing file system folders and one or more folders contain more than 250,000 files. The cache would be 1 GB and this could

cause the other threads to exceed the 2 GB boundary for 32-bit. The cache was reduced to 25,000 to prevent this.

- Fixed possible out-of-memory condition when traversing database folders during a recovery portal folder recovery when a tiered folder contains more than 100,000 files. The cache will now consist of up to 25,000 files at a time.
- Task Service for NetApp Installer: The libeay32.dll and ssleay32.dll files will first be deleted before InstallShield copies in the new files. This is due to these files having the same or earlier versions than the current ones installed. Therefore these files within the installer will always be copied.

## VFM Admin

- Added "StorePolicyName" to the Next Task request xml. This is for store delete requests so that the correct store name can be attributed to the object being deleted with multiples of the same store platform are defined. This is seen only within the Completed Queue for store delete requests.
- The "Additional Configuration – Product Installer Settings" page will now default to "%PROGRAMFILES%" instead of "%PROGRAMFILES86%" now that the Task Services are 64-bit. Note: Refer to the Installers section below.
- During an upgrade, the dialog that displays the database name and server will now be read only.

## Installers

- All services will be created using double quotes around the service's executable name to prevent customers security vulnerability scans from reporting this service as vulnerable. The services are: All Task Services, the Remote Installer service, the Domain Agent service and the NAS Proxy service.

## Admin Installer

- During an upgrade the installer will now check that the SQL login has at least "db\_owner", "db\_datareader" and "db\_datawriter" roles to both VFM databases instead of requiring database create permissions; however, database create will still be

required for new installs. This is to help prevent customers from manually running the scripts when create database permissions are not allowed.

## Task Service for NetApp Installer

- The libeay32.dll and ssleay32.dll files will first be deleted before InstallShield copies in the new files. This is due to these files having the same or earlier versions than the current ones installed. Therefore these files within the installer will always be copied.

## Installers – 32 and 64-Bit Components

- **Components Remaining as 32-bit**
  - Core Tiering Engine (CTE)
  - NAS Proxy Service
- **Components Converted to 64-bit**
  - All Task Services
  - The Domain Agent Service
  - The Event Driven Data Mover (EDDM)
  - The VFM License Key Utility
- **Components that were already 64-bit**
  - The VFM Admin
  - The Access Portal
  - The Recovery Portal
  - The File Intranet
  - The Product Installer
- **Components that were already both 32 and 64-bit**
  - Right-Click Tiering Windows Explorer Add-on
- **“Program Files” versus “Program Files (x86)”**
  - **New installations that are manually installed using Setup.exe**
    - All 64-bit components will be installed, by default, to “Program Files”.
    - All 32-bit components will be installed, by default, to “Program Files (x86)”.
  - **New installations of the Task Services and Core Tiering Engines that are installed via the Product Installer**

- The “Default Program Files Location” setting in the “VFM Admin - Additional Configuration – Product Installer Settings” page will install both the Task Service and CTE to that location regardless of whether the component is 32 or 64 bit. The new default location specifies “%PROGRAMFILES%” which is the “Program Files” folder.
  - **Updating existing components**
    - All upgrades, regardless if the component is 32 or 64-bit, will upgrade in-place.
    - NOTE: If you want to change the folder location then you must uninstall and install new.
    - **WARNING:** Do not uninstall the VFM Admin without first exporting the master encryption key. Refer to the white paper on the procedure for moving the VFM Admin to a different location.
- **Registry - HKEY\_LOCAL\_MACHINE – “Software\NTPSoftware” versus “Software\WOW6432Node\NTPSoftware”**
  - All components, regardless if the component is 32 or 64-bit, will still install into the “WOW6432Node” portion of the registry due to InstallShield being 32-bit.
  - VFM uses XML and Web.Config files instead of the registry therefore the registry is basically only for InstallShield use.
    - NOTE: these components are still 32-bit so these will remain in the WOW regardless
      - The Core Tiering Engine
      - The NAS Proxy Service

## Windows File Filter

- Corrected the digital certificate for all Windows 2008 and 2012 Servers.

## Core Tiering Engine

- Corrected the specific locations scan policy name to be that of each of location. It was previously wrongly set to the All Location policy name. This had no effect on the actual scan settings. The xml just had the wrong policy name.
- During an Assessment scan, the VFM Admin will send down True for all “Allow” flags so CTE will scan the entire paths, for example scanning into hidden folders will be allowed by default without having to manually change the database.
- During an Assessment scan, the XML was fixed to account for special characters, such as “&” in the data.



## Database:

- Updated the Amazon Regions table.
- Determining the files to delete from a secondary store platform would wrongly retrieve files that were tiered to another platform. This occurs when multiple different platforms are configured in the storage group. This has been corrected.
- Added TargetName column to the TieredTarget table because the TieredAddress is not unique enough for Atmos and Azure. This has been corrected by prefixing the Tenant/Account with the store's address to form the TargetName
- If files were tiered to multiples of the same platform, like Azure, using different assigned storage platform names then the files would be wrongly deleted from both stores whenever either storage platform name runs a deletion policy. This has been corrected within the retention/deletion stored procedures.

## 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](mailto: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](mailto:info@DefendX.com)  
Web Site: <http://www.DefendX.com>

Copyright © 2019 DefendX Software. All rights reserved. All trademarks and registered trademarks are the property of their respective owners. Doc#DFX1209EF