DefendX Software Mobility ™ Administration Web Site

User Manual

Version 8.2

This guide details the method for using DefendX Software Mobility™ Administration Web Site, from an administrator's perspective. Upon completion of the steps within this document, DefendX Software Mobility™ can be used to manage your enterprise community

Table of Contents

Executive Summary

Thank you for your interest in DefendX Software Mobility™ VFM, hereafter referred to as DefendX Mobility VFM. The latest addition to the DefendX Software® product portfolio, DefendX Mobility VFM enables employees to tier files; users can select from a predefined set of criteria such as file size, age of last access, or other criteria (Right-Click Data Movement™), and organizations can also establish policies that automatically tier files as users reach their storage limits (Event-Driven Data Movement™). Both methods enable companies to control storage and operating costs and to expedite backups.

DefendX Mobility VFM makes it much easier for customers to control costs and consolidate data so that it can be searched and leveraged as needed. DefendX Software continues its innovation in file-based storage management with the ultimate objective of helping customers reduce storage capital and operating costs.

System Overview

Your goal is to categorize your data, properly manage it, and move the right data to the most appropriate storage tier to reduce costs, address compliance issues, and perform electronic discovery. However, most archival solutions require expensive, repeated scans of the entire file system. Even worse, large, infrequently used files can reside in your primary storage for months! DefendX Mobility VFM allows for flexibility in your approach to data migration with automated policy-driven movement, manual user driven movement, or a combination of both. You decide what is best for your organization. DefendX Mobility VFM redefines the economics of data movement by being event- and policy- driven in real time, rather than requiring repeated scans of the entire file system, thus greatly helping to reduce storage-related costs.

Browser Settings

You need to have the "Allow Active Scripting" under

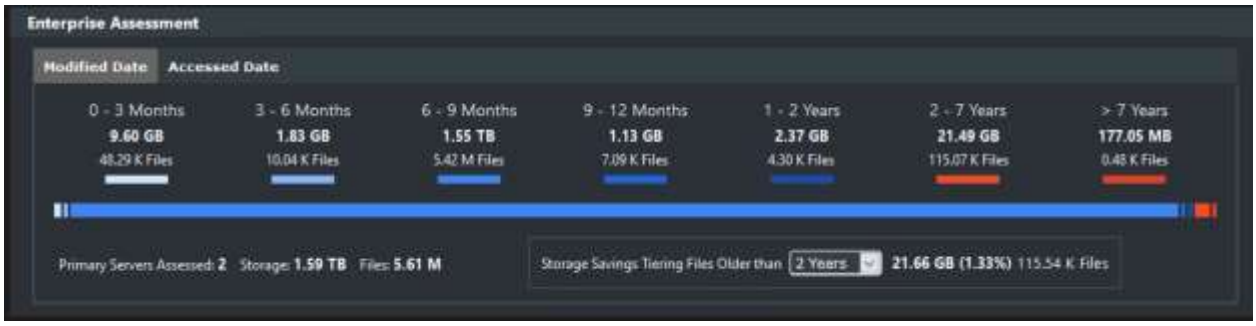
Properties>**Security**>**LocalIntranet**>**CustomSecurity** enabled. This may require you to add the DefendX Mobility VFM Admin server to your local intranet sites. If this option is disabled, then the DefendX Mobility VFM Admin site's left-hand main menu will not be able to expand.

DefendX Mobility VFM Home Page

The Home menu provides a quick view into the current status of the environment and statistics on the operation of the software.

Enterprise Assessment

The enterprise assessment section provides a quick view into the capacity that can be tiered in the environment. This is a result of the assessments for all primary servers that were configured in the environment. The Assessment report provides views of file aging by either "Accessed Date" or "Modified Date" of the files. The total number of files and their sizes are placed into date range buckets to allow for easy identification of how much capacity can be archived from the environment. The assessment widget also has a dropdown menu that allows for tallying all the files that are identified as happening after a specific time period.



Tiering Statistics

The Tiering statistics widget provides a view into the archiving activity of the software. The tiering statistics can be viewed as Daily activity for the past seven days or Monthly activity for the past six months. Both views provide the same tabular data which gives statistics for the number of tiering requests, the number of tiered files and the total Tiered size. It also provides a graphical view of the activity over the time period for the number of tiering requests, number of files tiered, primary storage savings, and tiering rate.

Auto-Recall Statistics

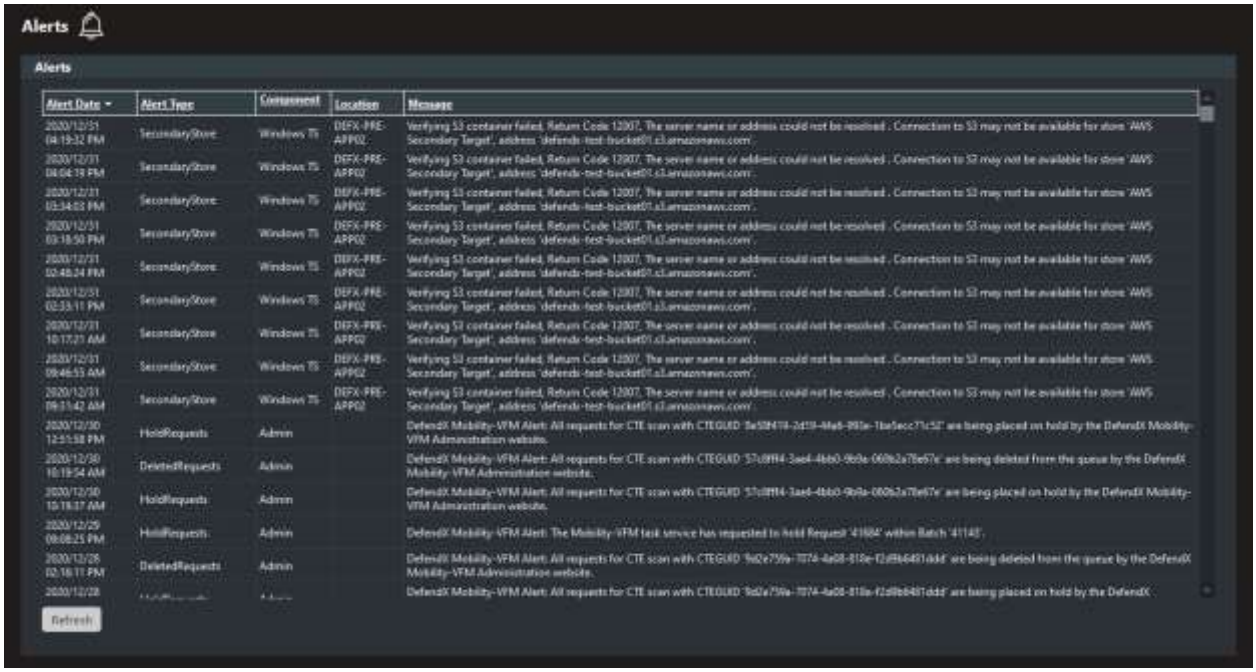
The auto-recall statistics give a view of the activity around auto-recalls. Auto-recalls are files that have been rehydrated back to a primary storage device during normal user operations such as double-clicking a file. The auto-recall statistics gives an overview of all auto-recall statistics grouped by daily, monthly, and all-time activity. Each of these tabs presents the number of requests per protocol (SMB or NFS) and a combined total. The tabs also provide statistics on successful and failed requests as well as a total capacity that was auto recalled. Finally, the widget provides a list of the top five users auto recalling files viewed by number of requests and capacity recalled.

DefendX Mobility VFM Alerts Page

The DefendX Mobility VFM Admin has a new “Alerts” item in the tree that provides a centralized repository of alerts from the system displayed in a table. Alerts will be retained in this table for 90 days, by default. This can be controlled within the DefendX Mobility VFM Admin “web.config” setting.

<add key="MaxDaysToKeepAlerts" value="90"/>

The Alerts table displays the date and time, type, DefendX VFM component generating the alert, the location or server where it occurred, and the message of the alert.



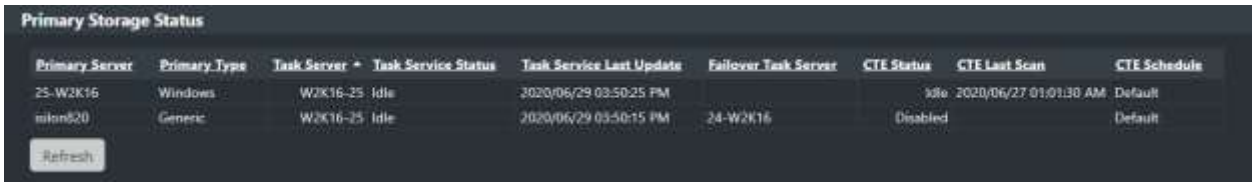
DefendX Mobility VFM Status Pages

The status pages provide details around the operational and activity status of the application components.

Primary Storage Status

This page displays the status of your DefendX Mobility VFM Task Servers and Core Tiering Engine (CTE) status.

To view the primary file server status, click **Primary File Severs Status** under the **Status** in the left-hand main menu. The **Primary File Server Status** page is displayed.



The page shows the name of the server and the status (whether it is idle or executing).

The Task Server Status states include:

- "**Idle**" – The Task Service has no requests to process. The Last Update date will be updated every 5 minutes so that there is an indication of whether the Task Service is in a normal operating state.
- "**Executing**" – The Task Service is currently executing a request. When the request is complete, its results can be viewed on the completed page.
- "**Disabled**" – The Task Service will no longer accept tier requests. Use the "Primary Servers" page to re-enable it.
- "**Stopped**" – The Task Service is currently stopped.

The CTE Status states include:

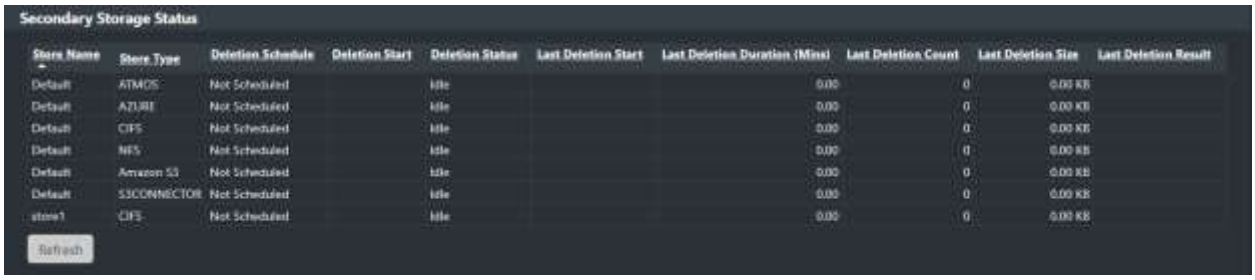
- **"Idle"** – A CTE scan is not running.
- **"Pending"** – A CTE scan has been manually initiated and will start executing within 5 minutes.
- **"Executing"** – A CTE scan is currently running.
- **"Executing Assessment"** – A CTE Assessment scan is currently running.
- **"Disabled"** – The CTE engine has been installed but scanning has not been enabled for the primary server. Refer to the Primary Server details page.
- **"Not Installed"** – The CTE engine has not been installed on the Task Server.
- **"Paused due to Operational Hours"** – Outside of hours of operation.

The CTE last tier scan displays the date of when the CTE engine last scanned the primary server.

The CTE last sync scan displays the date of when the CTE engine last synchronized stubs on the primary server.

Secondary Storage Status

The secondary storage status page displays all the configured secondary stores and related deletion statistics for the corresponding secondary store.



The table provides the name and type of each secondary store. For each store, it will outline if there is a deletion schedule configured, the next start time of the deletion schedule, the current status of the schedule, and the last time the schedule was started.

The Deletion Status states include:

- **"Idle"** – A deletion is not running.
- **"Pending"** – A deletion job has been initiated and will start executing within 5 minutes.
- **"Executing"** – A deletion job is currently running.

The table also provides statistic on the last deletion job that was run including the time to complete, the number of objects deleted, the total size of objects deleted and the results of the deletion.

Domain Storage Status

DefendX Mobility VFM has the ability to scan additional domain attributes to enhance the meta-data collected for the files tiered. The software stores meta-data related to the file both in the database and with the objects on the secondary store. With the domain agent,

additional domain attributes can be collected for the owner of the files and stored with the meta-data.

The domain storage status page displays all the configured domains and related statistics for the domain.

The table provides the domain name and type of directory service that was scanned. For each domain, the table shows the Task Service that was used to scan, the current Task Service status, the timestamp of the last update from the Task Service and the domain scan status.

The Domain Scan Status states include:

- **"Idle"** – A domain scan is not running.
- **"Pending"** – A domain scan has been initiated and will start executing within 5 minutes.
- **"Executing"** – A domain scan is currently running.
- **"Updating DB"** – A domain scan has completed, and the data is being uploaded to the database.
- **"Stopped"** – The domain agent service is currently stopped.

The table also provides statistic on the last scan job that was run including the time to complete, the number of objects scanned, what domain controller was scanned, the scan results, as well as the schedule (if any) assigned to the domain.

On-Demand Status

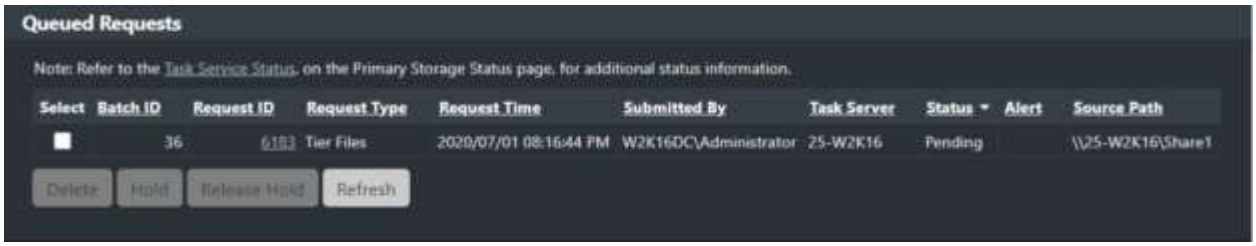
This page displays all the pending requests that have been submitted by the Right-Click Data Movement (RCDM) application, the Event-Driven Data Movement (EDDM) application, the Recovery Portal or the Access Portal. There are three types of requests, Tier, Recall, and Recover. Each request is assigned an ID for which you can drill into and view additional information. Requests are also stamped with the time it was submitted along with the primary

server the request was issued for. Pending requests can also be placed on hold until released and they can be removed.

Queued Requests

To view queued requests, perform the following steps:

1. Under **Status** in the left-hand main menu, click **On-Demand Status**>**Queued Requests**. The **Queued Requests** page is displayed.



2. To view the details of the request, click the link for the request ID. This will show the details of the request: the request ID, who submitted it, when it was submitted, the UNC path of the file, the file name, the file size, and the file owner.

NOTE: If the request type was to tier or recall specific files, then those file names, sizes, and owners will appear. If the request type was to tier or recall a folder, then the file grid will not appear.

NOTES:

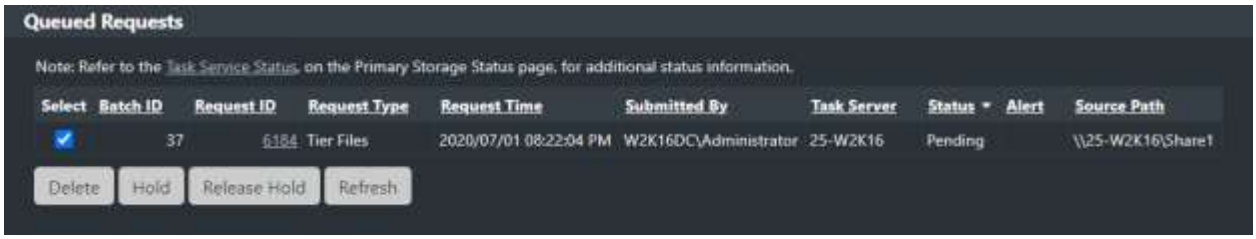
- **Queued** requests are sitting in a queue waiting to be serviced. Pending items will get processed in a sequential order.
- **On-hold (Manual)** means the item was placed on hold manually, i.e., by

using the Hold button. Items that are manually held will not be processed until the administrator releases the hold on the item.

- **On-hold (Network)** means the item was placed on hold by a Task Service due to a network issue while trying to tier or recall an item. When the network issue is resolved then these held items will automatically be released by the Task Service.

It is possible to place network held items on manual hold by selecting the items and pressing the hold button. When doing this then those items will be held until manually released.

3. To move an item from queued to on-hold, or to release an item from hold, simply check the **Select** column and then click either the **Hold** or **Release Hold** button. Administrators can put tiering requests on hold, release the hold, or delete the requests.



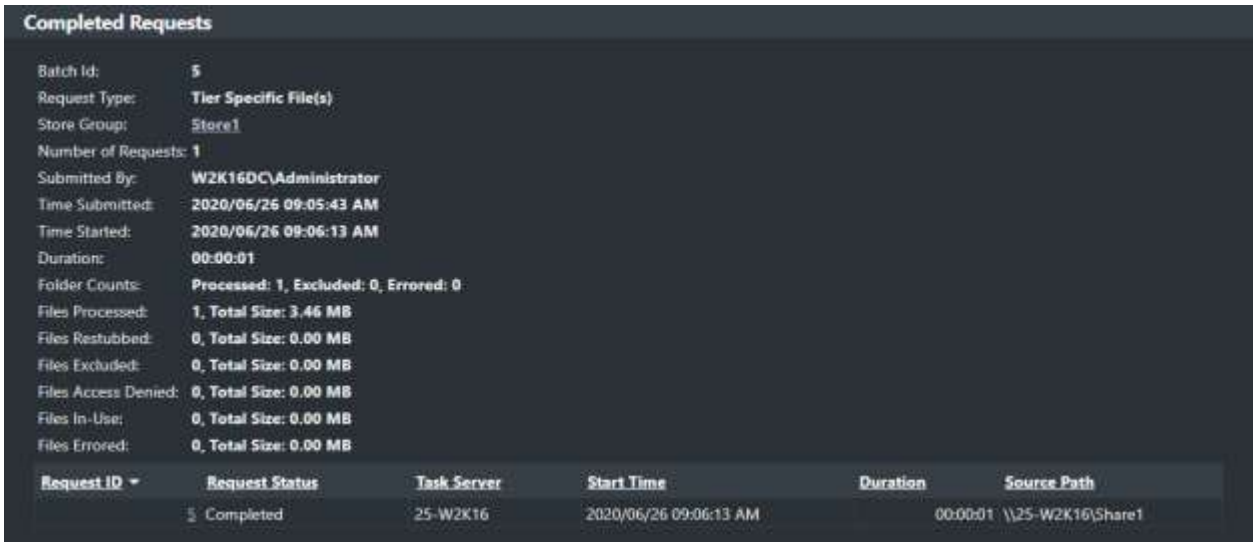
Completed Requests

This page displays all the most recent completed requests. The number of completed requests that will be displayed is 250 by default. This number is controlled by the *MaxCompletedRequestsToDisplay* value found in the web.config file. By clicking the Batch ID, you can drill into and view the results of the request.

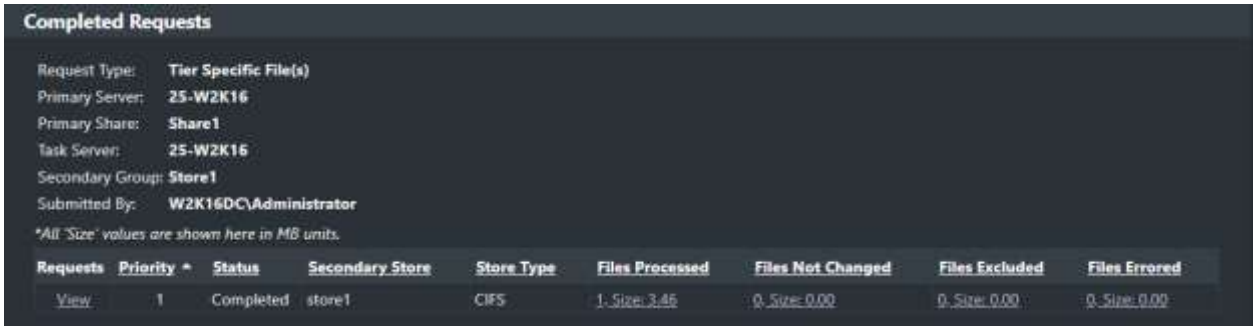
To view completed requests, perform the following steps:

1. Under **Status** in the left-hand main menu, click **On-Demand Status**>**Completed Requests**. The **Completed Requests** page is displayed.

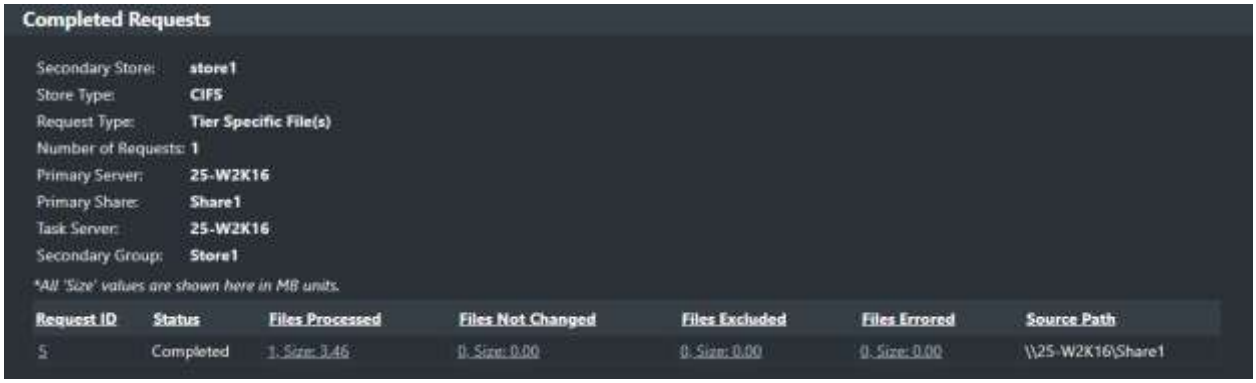
2. To view the details of the batch, click the link for the Batch ID. This will show the details of the batch.



3. To view the results of the files being tiered to each of the secondary stores defined in the storage group, click on the Store Group link.



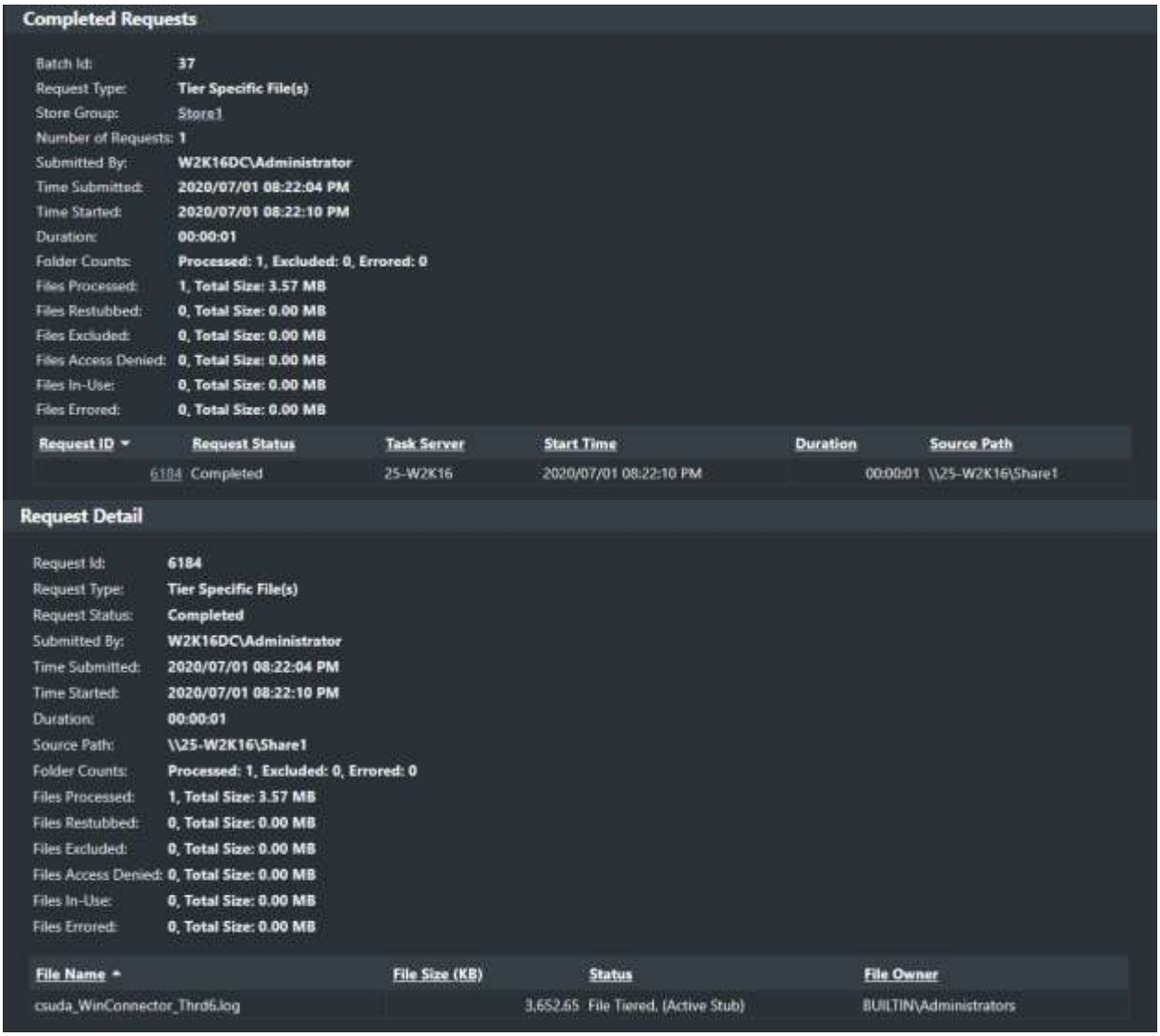
4. To dig further to the request within the specified batch, click the View link.



NOTES:

- If the request type was to tier or recall specific files, then those file names and sizes will appear.
- If the request type was to tier or recall a folder, then the file grid will not appear.

5. Navigate to the batch details page (as per step #2 of this section), you can drill into the Request ID in the file grid, you will be able to view the results of each file on primary storage. Whether the file was stubbed, for tiering requests, or restored for recall requests.



Scheduled Status

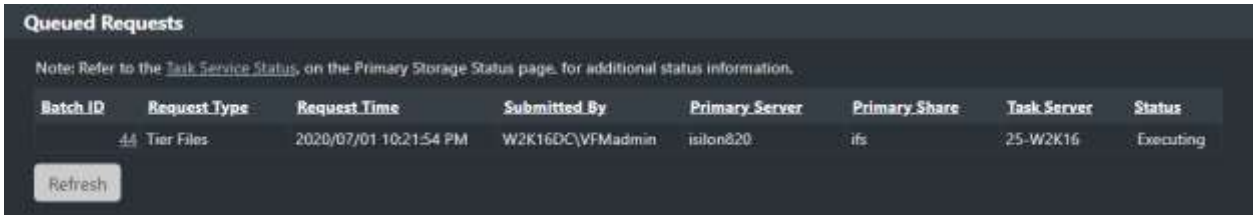
This page displays the requests that have been submitted by a Core Tiering Engine (CTE) scan or a secondary storage deletion. The requests are sorted by the date and time the Core Tiering Engine or secondary storage deletion was executed. The queued requests allow the user to drill into and view additional information.

Queued Requests

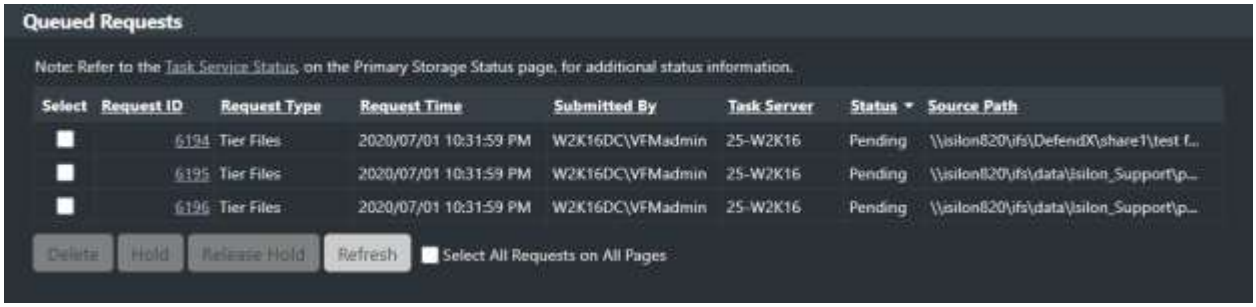
To view queued requests, perform the following steps:

1. Under **Status** in the left-hand main menu, click **Scheduled Status**>**Queued Requests**. The **Queued Scans** page is displayed.

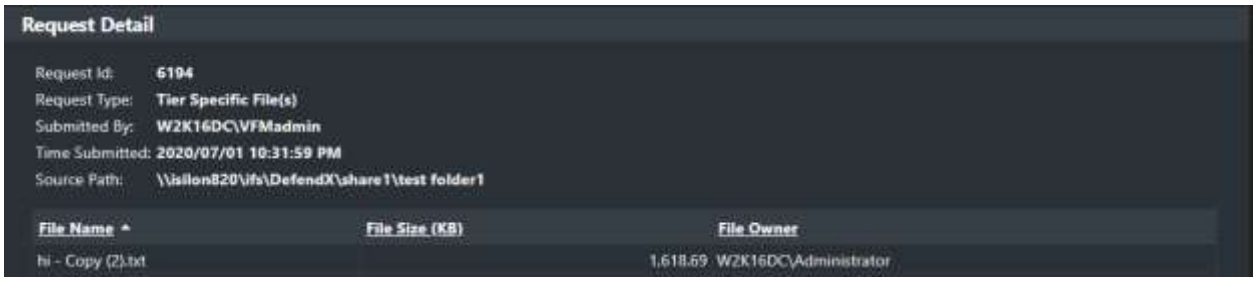
2. To view the details of the request, click the link for the Request Time. This will show the details of the request and the current status. The Core Tiering Engine divides a scan into multiple batches. Each batch contains multiple requests, and each request contains multiple files that will be tiered. By drilling into a Batch-ID, you can view all the requests for that batch, and then, by drilling into a Request-ID, you can view all of its files as shown by the following screen shots.



3. To view the requests within a certain Batch ID, click on the Batch ID link.



4. To view the request details, click on the Request ID.



Completed Requests

This page displays all the most recent completed requests. The number of completed requests that will be displayed is 250 by default. This number is controlled by the *MaxCompletedRequestsToDisplay* value found in the web.config file. By clicking the Date Time Stamp, you can drill into and view the results of the request.

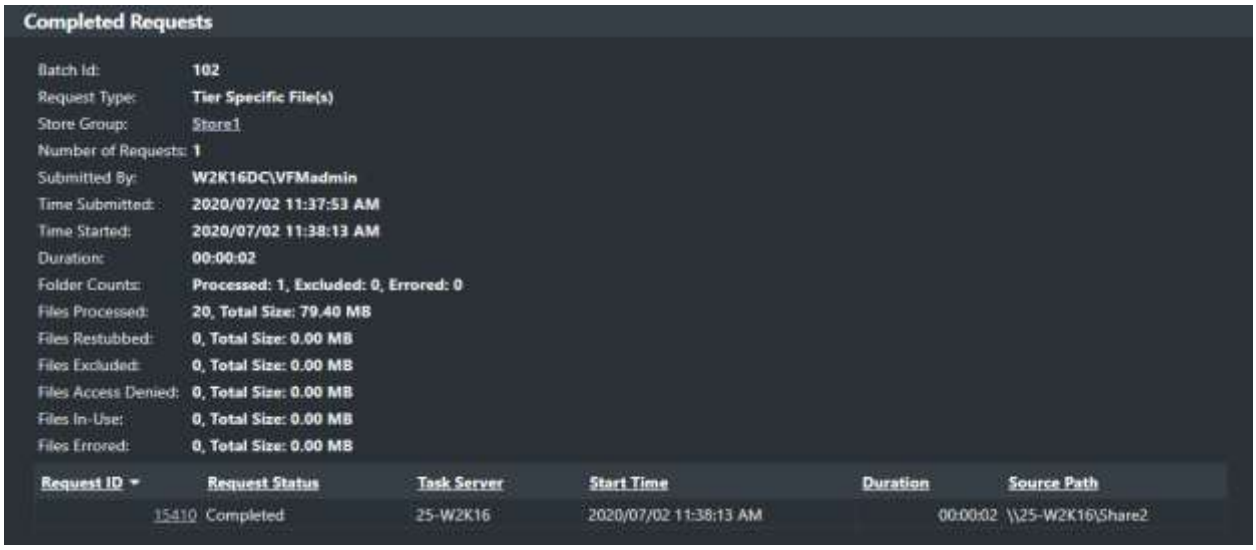
To view completed requests, perform the following steps:

1. Under **Status** in the left-hand main menu, click **Scheduled Status**>**Completed Requests**. The **Completed Requests** page is displayed. The requests are sorted by the date and time the Core Tiering Engine was executed.

2. The Core Tiering Engine divides a scan into multiple batches. Each batch contains multiple requests, and each request contains the results of files that were tiered. By drilling into a Batch-ID, you can view all the requests for that batch, and then, by drilling into a Request-ID, you can view the results of all of its files as shown by the following screen shots.

3. To view the details of the request, click the link for the Start Time. This will show the status for each batch.

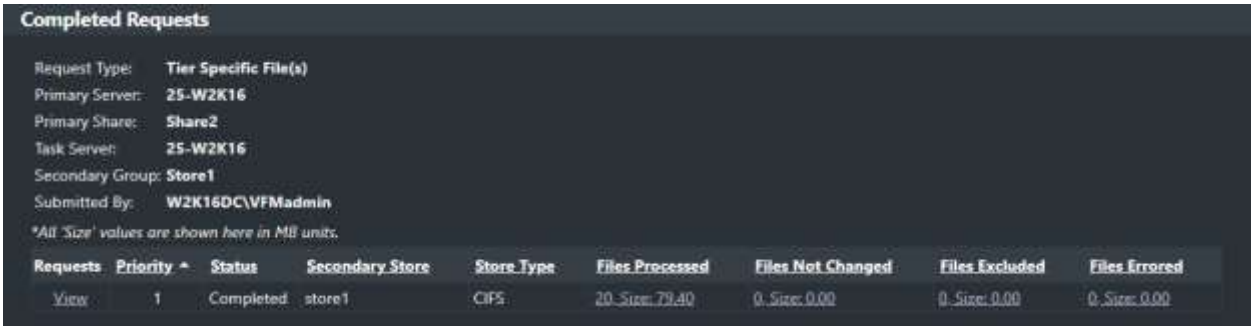
4. To view the requests within a certain Batch ID, click on the Batch ID link.



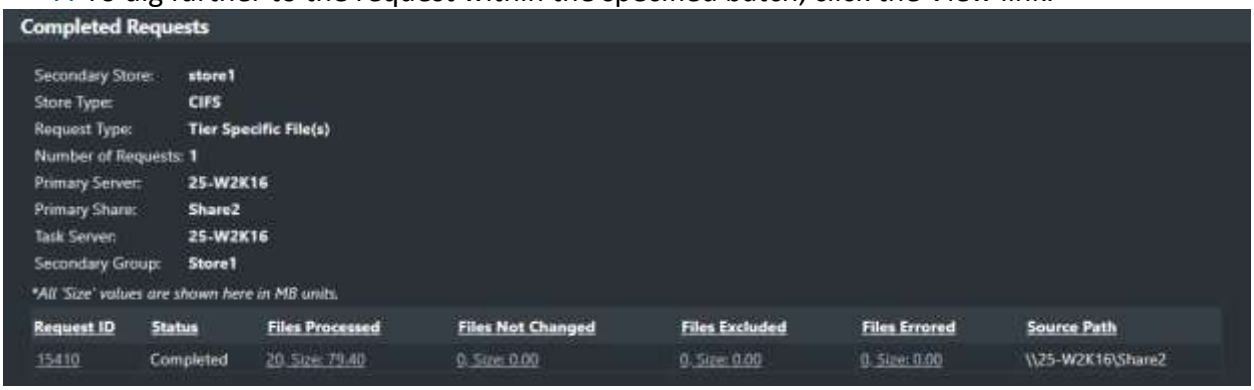
5. To view the Request Detail, Click on the Request ID

6. To view the results of the files being tiered to each of the secondary stores defined in the storage group, click on the Store Group link.

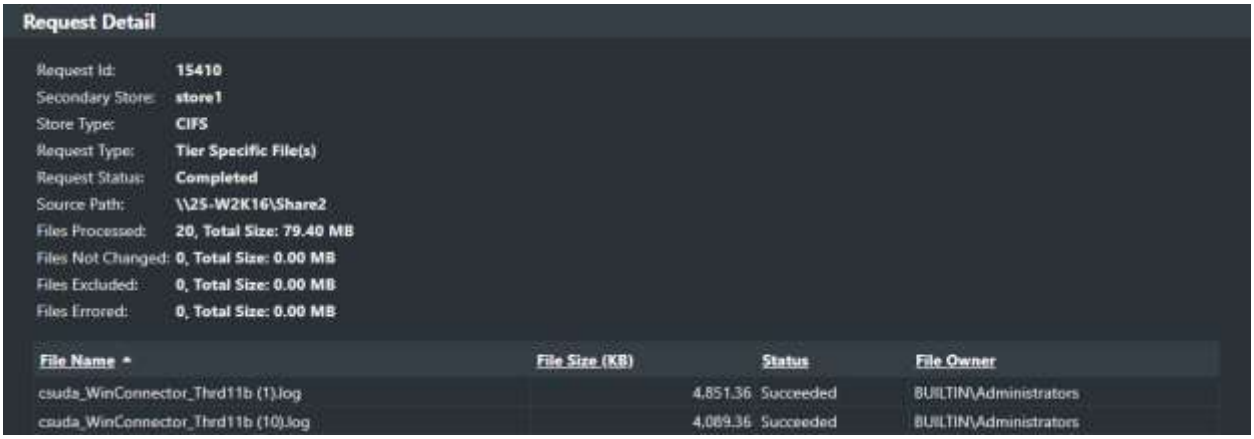
NOTE: If the request type was to tier specific files, then those file names, size, and owners will appear. If the request type was to tier a folder, then the file grid will not appear.



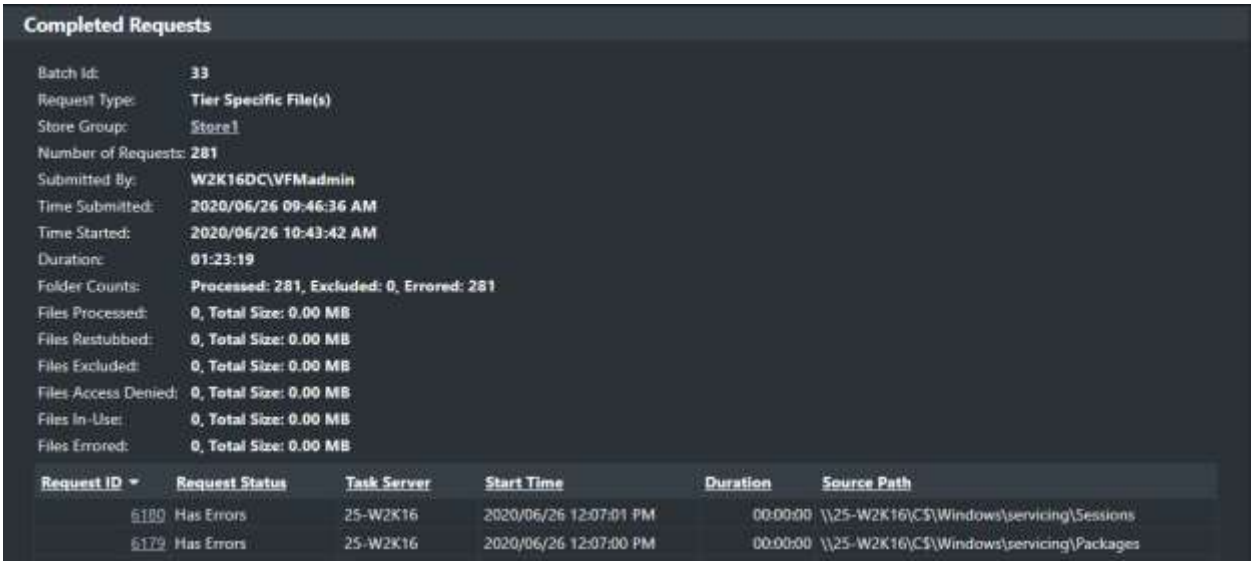
7. To dig further to the request within the specified batch, click the View link.

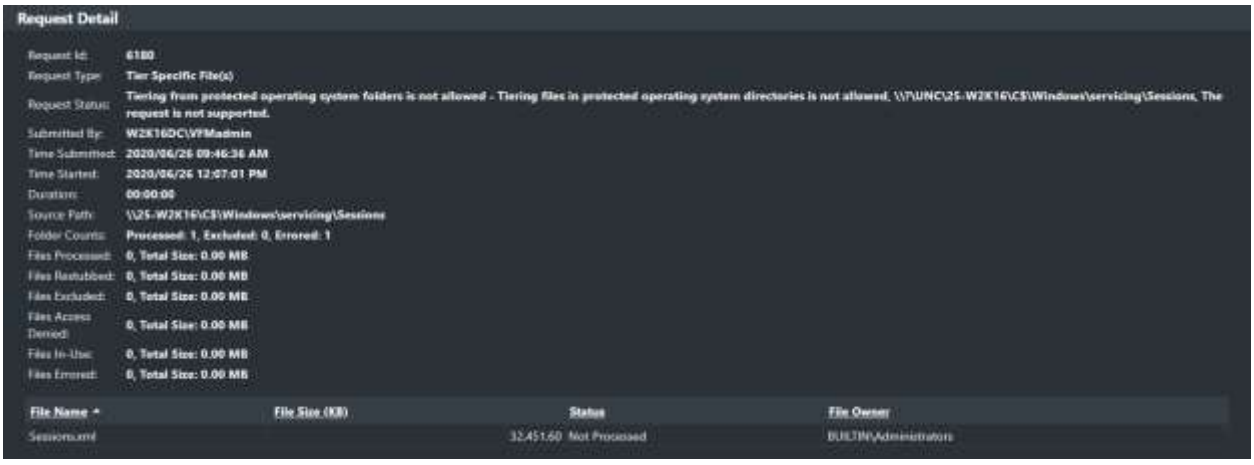


8. Drilling into the Request ID in the file grid, you will be able to view the results of each file on secondary storage.



9. Navigate to the batch details page (as per step #4 of this section), you can drill into the Request ID on this page to view the results of each file on primary storage and whether the file was stubbed, or a warning or error occurred.





DefendX Mobility VFM Reports Pages

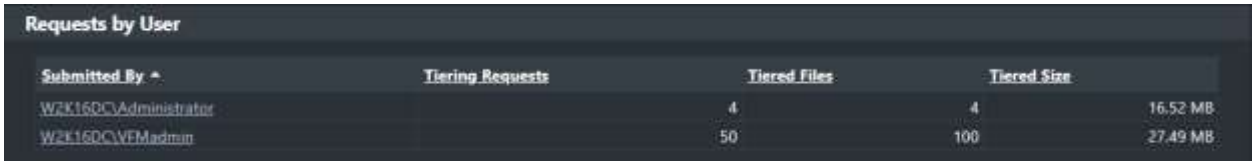
The reports pages provide high level reports on the users and primary servers of the system.

User Reports

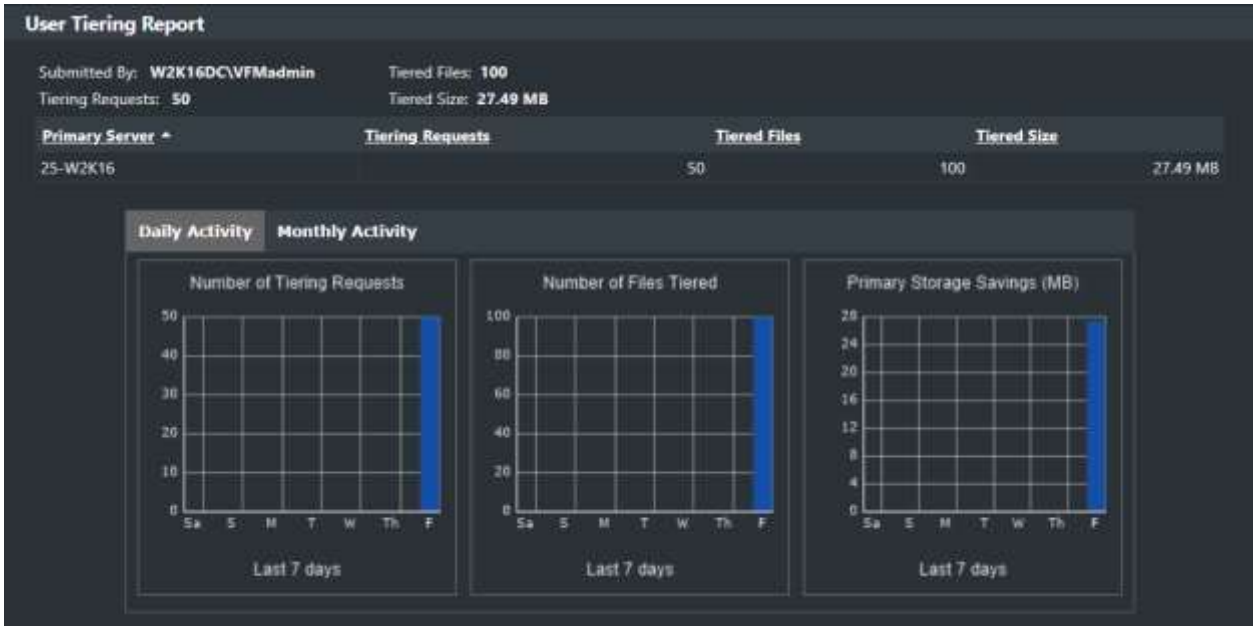
This page displays the number of tier requests for each user who submitted requests.

To view this report, perform the following steps:

1. Click **Requests by User** under **Reports** in the left-hand main menu. The **User Report** is displayed.



2. To display more detail, click the username. This page displays the number of requests for the selected user that were destined for each of the primary servers listed. This page also displays statistical information for the past 7 days as well as for the month (when the *Monthly Activity* tab is selected).



NOTE: Detailed information is only displayed for tier requests. Recall requests are not taken into consideration here.

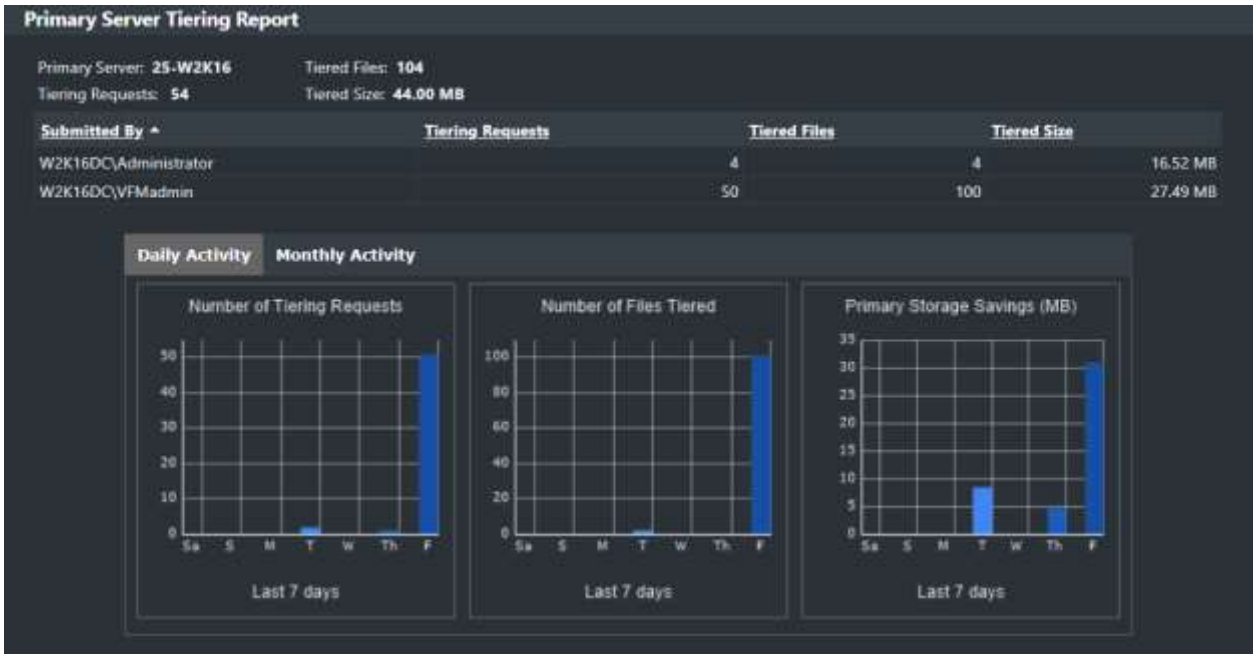
Primary Server Reports

This page displays the number of tier requests processed by each primary server.

To view this report, perform the following steps:

1. Click **Requests by Primary Server** under **Reports** in the left-hand main menu. The **Primary Server Report** is displayed.

2. To display more detail, click the primary server name. This page displays the number of tier requests for this selected server and each of the users who submitted requests for it. This page also displays statistical information for the past 7 days as well as for the month (when the *Monthly Activity* tab is selected).



NOTE: Detailed information is only displayed for tier requests. Recall requests are not taken into consideration here.

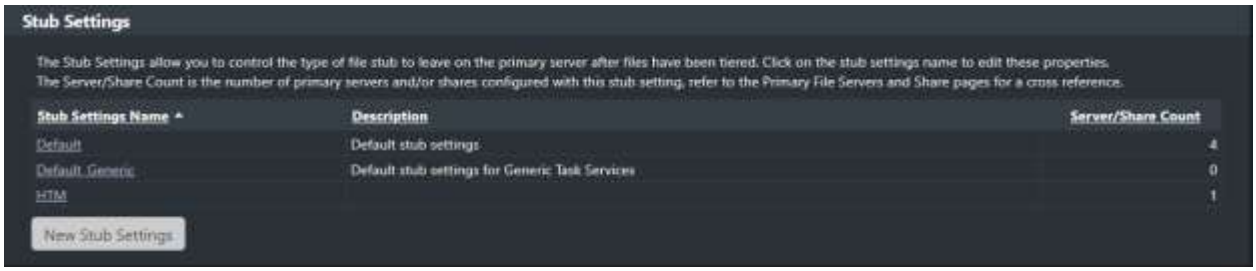
The assessment section provides a quick view into the capacity that can be tiered on this server. The Assessment report provides views of file aging by either “Accessed Date” or “Modified Date” of the files. The total number of files and their sizes are placed into date range buckets to allow for easy identification of how much capacity can be archived from this primary server. The assessment widget also has a dropdown menu that allows for tallying all the files that are identified as happening after a specific time period.

DefendX Mobility VFM Tiering Operations Pages

The tiering operations section of the system is where users can configure operational components of the application that can be used to create the tiering policies. These components are reusable across policies.

Stub Settings

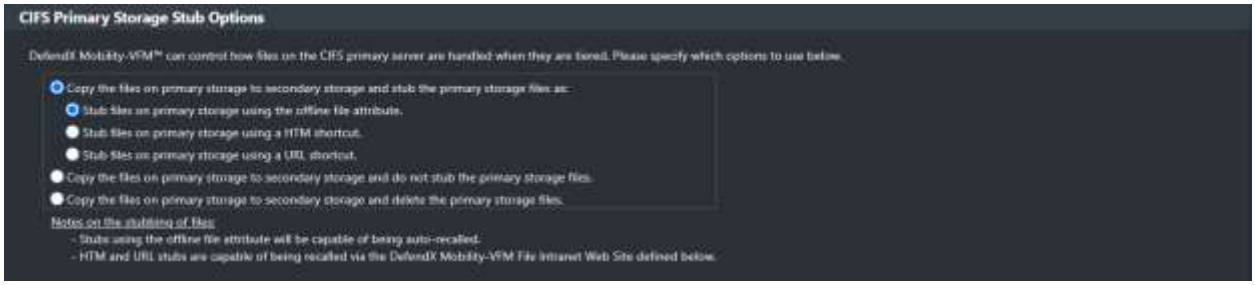
The Stub Settings allows users to control the type of file stub to leave on the primary server after files have been tiered. The stubs setting table shows the names, descriptions and counts of the stub settings. The Server/Share Count is the number of primary servers and/or shares configured with this stub setting, refer to the Primary File Servers and Share pages for a cross reference.



To create a new stub setting, click on the “New Stub Setting” button

1. In the **Name and Description** section, enter a name and description for the stub setting. The name can then be assigned to one or more primary servers.

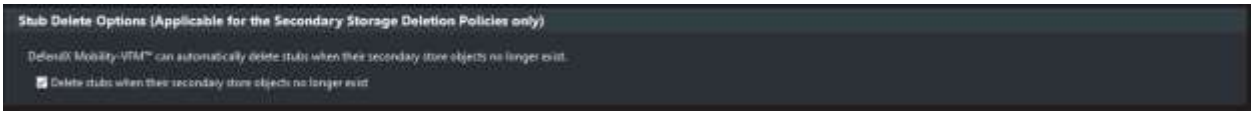
2. In the **CIFS Primary Storage Stub Options** section, specify the options through which you want DefendX Mobility VFM to handle files located on primary servers CIFS shares when they are tiered.



3. In the NFS Primary Storage Stub Options section, specify the options through which you want DefendX Mobility VFM to handle files located on primary servers NFS exports when they are tiered.

NOTE: Microsoft Services for NFS must be installed on the Task Servers if you want to tier files from NFS exports located on EMC VNX/Unity or Generic NAS devices. It is not necessary for NetApp.

4. In the Stub Delete options section, specify if you want stubs to be deleted when no more objects representing the files exist in any secondary stores. This option only applies to objects deleted by a secondary store deletion policy.



5. In the Missing Stub Options section, you can indicate how the application will behave when stub files are deleted. The Missing Stub Options are tied to the “Stub Sync” option for a primary server which is a batch operation. If no options are selected, when a stub file is deleted from the primary server, the file object(s) on secondary stores will not be

modified. Select the "Perform the following actions if a stub does not exist" checkbox to enable the Missing Stub options. Once enabled, you can select either:

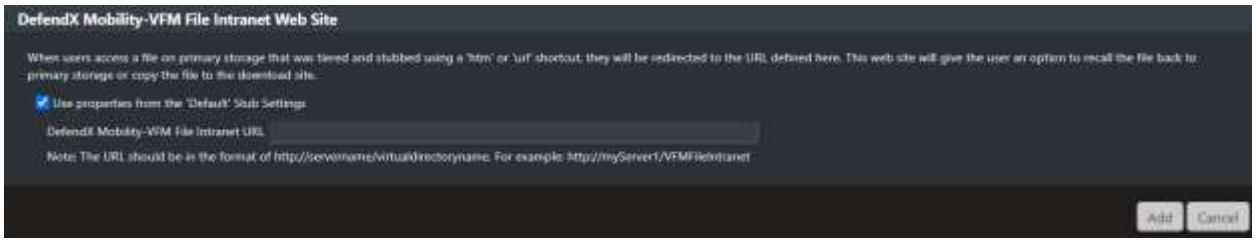
- Recreate the stub files if a secondary store object still exists OR
- Delete the secondary store object(s) for that file and set a time frame for that deletion from the secondary store

Additionally, the Missing Stub Option can be switched from batch processing (post-event) to near real-time operation by selecting the checkbox to perform the options only for real-time delete events.

NOTE: The real-time option is only available on NetApp storage arrays, EMC VNX, and EMC Unity arrays.

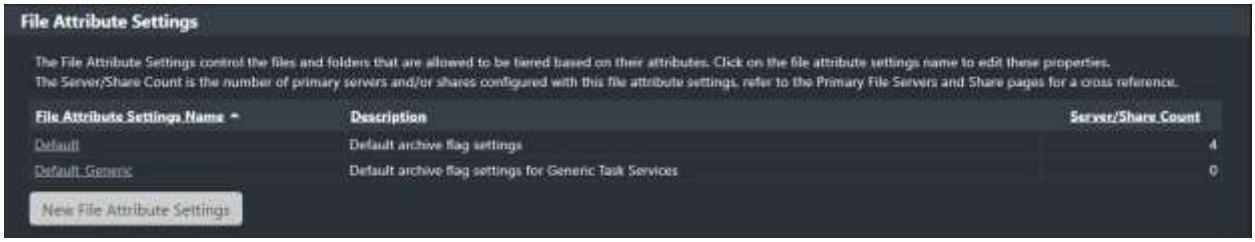
6. In the **DefendX Mobility VFM File Intranet Website** section, enter the URL of the website to which users are directed when they access a file on primary storage that was tiered and stubbed using either the URL or HTM stub options. This website allows users an option to recall files back to primary storage. The URL format is: "http://<server>/VFMFileIntranet".

Note: The DefendX Mobility VFM File Intranet must be installed on <server>.



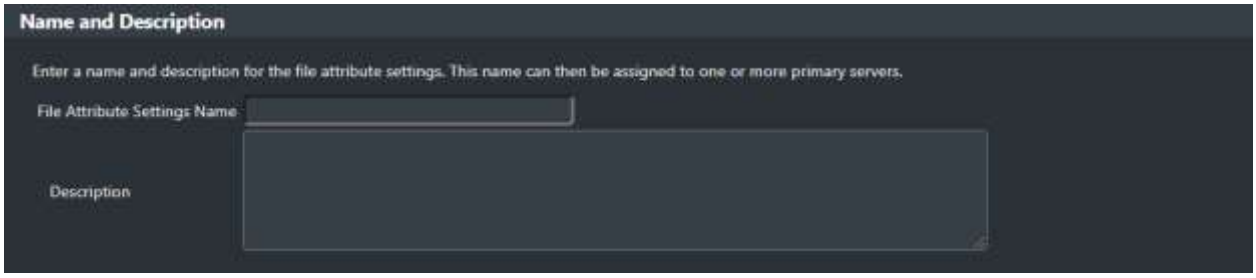
Configuring File Attribute Settings

File attribute settings are used by the Core Tiering Engine to include or exclude files that have special attributes. The File attribute settings page displays any configured file attribute setting groups and allows the creation of new file attribute settings.

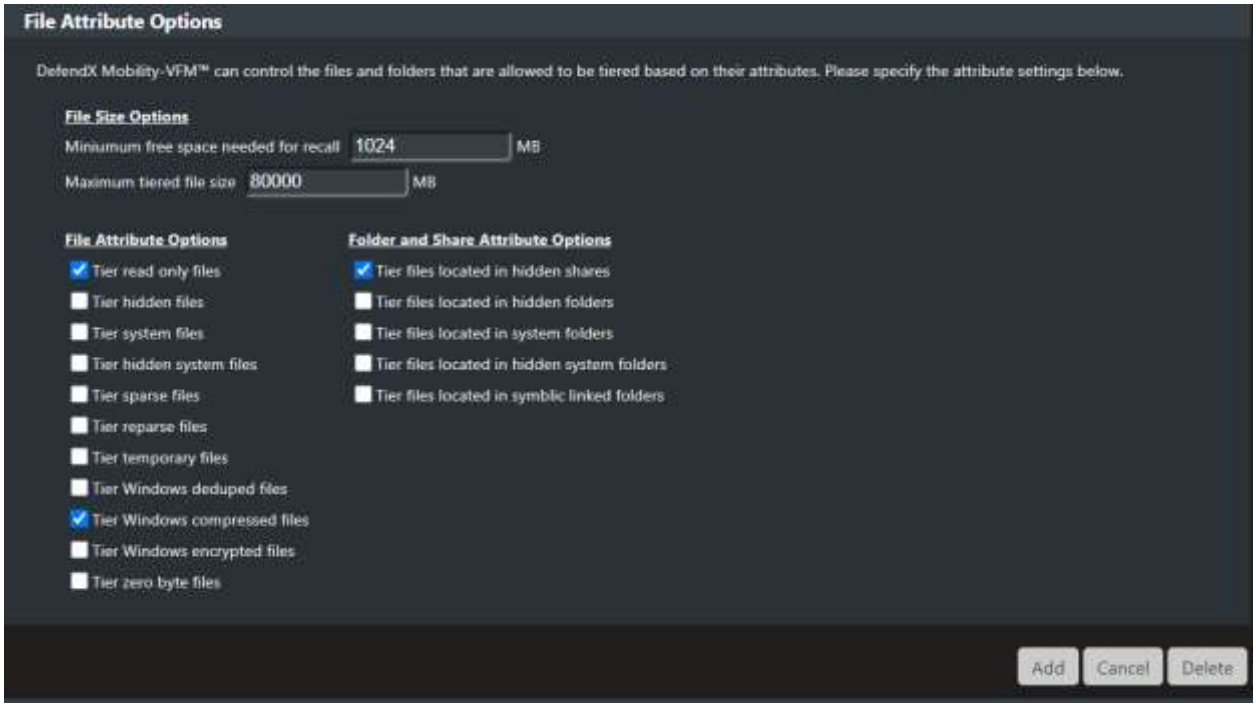


To create a new file attribute setting, click on the “New File Attribute Setting” button

1. In the **Name and Description** section, enter a name and description for the attribute settings group. The name can then be assigned to one or more primary servers.



2. In the **File Attribute Options** section, specify the options through which you want DefendX Mobility VFM to include (checked) or exclude (unchecked) in the scan.



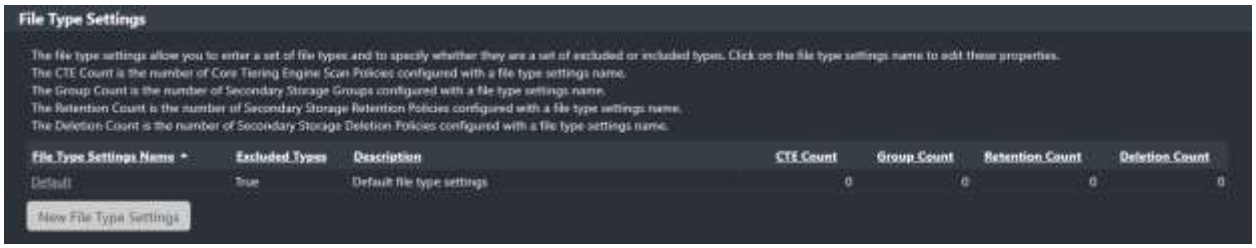
Configuring File Type Settings

The file type settings allow you to enter a set of file types and to specify whether they are a set of excluded or included types. These file type sets can be used in scan and deletion policies to further identify files that meet the criteria for the specified action.

To configure File Type settings, perform the following steps:

1. Under **Tiering Configuration** in the left-hand main menu, click **File Type Settings**.

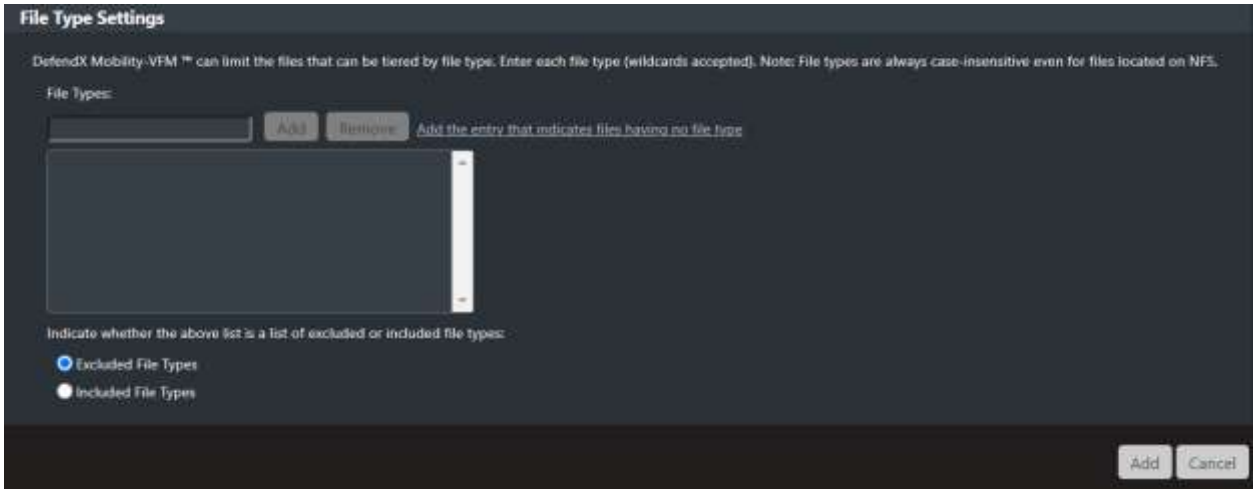
2. In the **File type Settings** section, click **New File Type Settings** or click the name of an already existing File Type Settings name to edit these properties.



3. In the **Name and Description** section, enter a name and description for the file type settings. The name can then be assigned to one or more secondary storage groups as well as the Core Tiering Engine policies and secondary storage groups.

4. In the **File Type Settings** section, enter one or more file types by which DefendX Mobility VFM can limit the files that can be tiered.

5. Indicate whether the listed file types are a list of excluded or included file types.



Core Tiering Engine

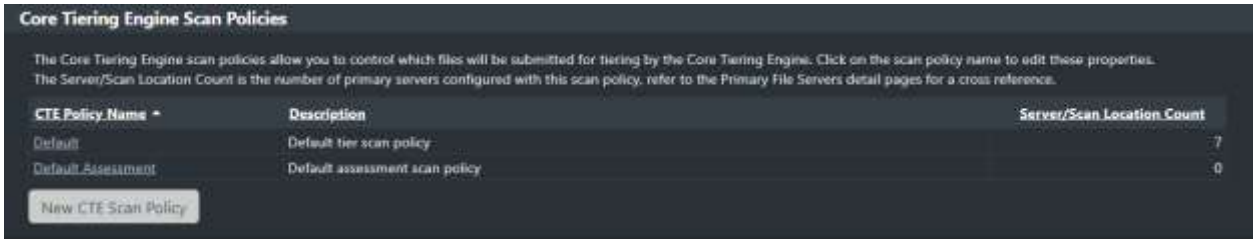
The Core Tiering Engine works in conjunction with DefendX Mobility VFM to tier files from one or more primary servers. As with RCDM, the Core Tiering Engine gives administrators a method to tier aged files from servers. The DefendX Mobility VFM Admin site and corresponding Task Services must be configured in order for the Core Tiering Engine to tier files. Based on the configuration, the engine can scan CIFS shares and NFS exports, identify files that meet the requirements to be tiered, then issue tier requests to DefendX Mobility VFM Admin (Administration web site). The corresponding Task Services will process the tier

requests that have been submitted to DefendX Mobility VFM as would occur in any standard DefendX Mobility VFM deployment.

NOTE: The Core Tiering Engine must be installed on the Windows server for which the DefendX Mobility VFM Task Service controls the tiering of the primary server's files. To assign a Core Tiering Engine schedule and policy, click on the *CTE link for* the primary server on the primary servers' page and enable *Scanning* for the Core Tiering Engine as well as assign the schedule. A policy can be assigned to each scan location added.

Scan Policies Page

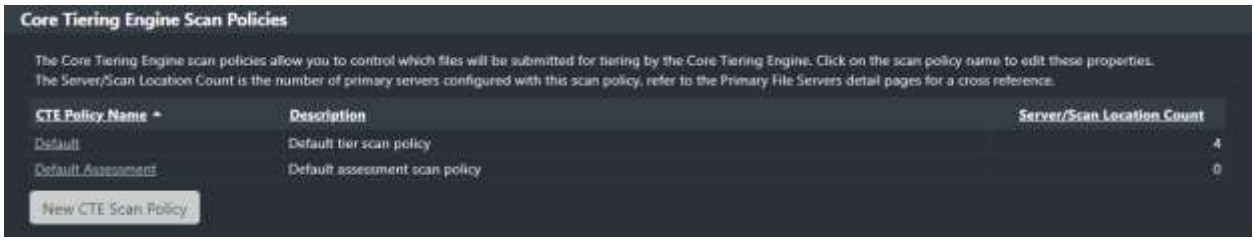
The **Core Tiering Engine Scan Policies** allows you to control which files will be submitted for tiering by the Core Tiering Engine. The Scan Policies page displays all the configured scan policies in the environment and allows the user to create a new policy. These policies can be applied to a share to define how files are identified for tiering. A scan policy can be used in multiple shares.



To configure a CTE Scan Policy, perform the following steps:

1. Under Core Tiering Engine Configuration in the left-hand main menu, click Scan Policies.

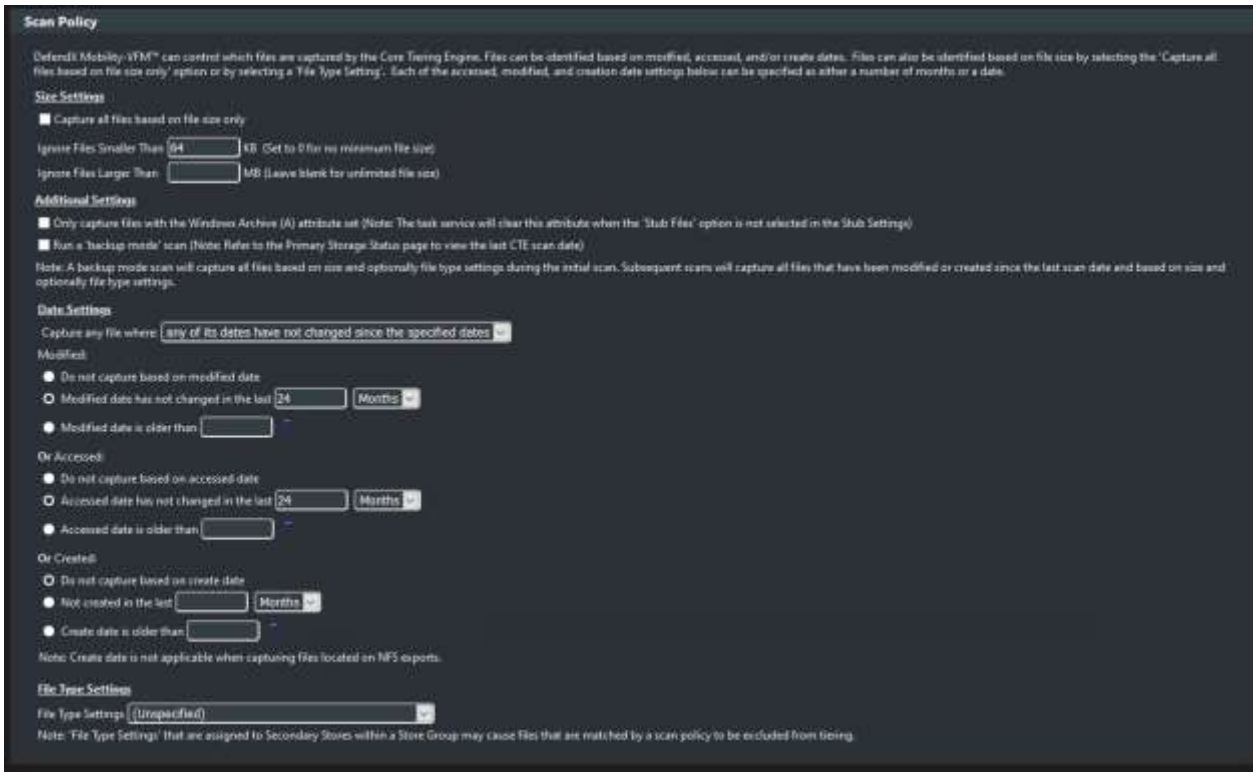
2. In the **Core Tiering Engine Scan Policies,** click **New CTE Scan Policy** or click the name of an already existing CTE Scan Policy to edit these properties.



3. In the **Name and Description** section, enter a name and description for the Scan Policy. The name can then be assigned to one or more primary servers.

4. In the **Scan Policy** section, specify the criteria by which DefendX Mobility VFM can identify which files are tiered by the CTE. Files can be identified for tiering based on modified, accessed and created dates. Files can also be identified by file size and by file type settings.

NOTE: DefendX Mobility VFM can control which files are tiered by the Core Tiering Engine. Files can be identified for tiering based on modified, accessed, and created dates. Files can also be identified for tiering based on file size by selecting the *Tier all files based on file size only* option. Each of the accessed, modified, and creation date settings below can be specified as either a number of months or a date.



Default Assessment Policy

Default Assessment: A new default assessment policy will be created during the upgrade and is assigned as the default Core Tiering Engine policy when the primary server is set to a scan type of assessment.

Note: Any scan policy can be used for assessments. The default assessment policy was created for convenience.

By default, the Default Assessment policy will scan all files based on file size only. Since the file size setting is set to zero, all files will be used in the assessment. However, this policy can be modified to assess files based on date and/or file types as well.

Encryption

Files tiered by DefendX Mobility VFM can be configured for data at rest encryption. Encryptions settings for data at rest as well as the master encryption key for the product are controlled by this section.

Encryption Settings

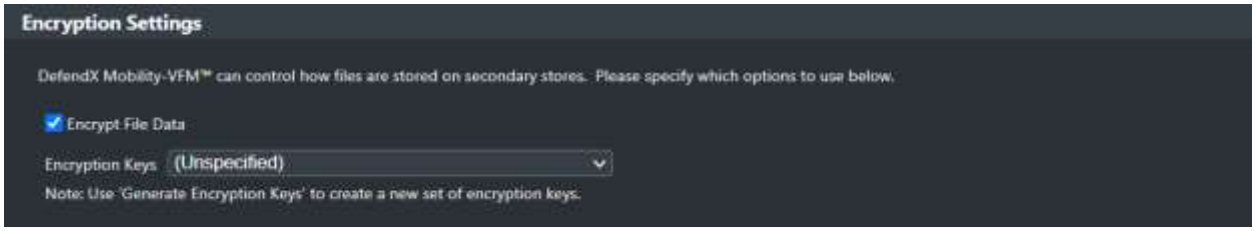
The Encryption Settings Page lists any encryption keys that have been configured in DefendX Mobility VFM and allows for the creation of new keys. Encryption keys are assigned to secondary data stores to configure data at rest encryption of tiered files

To configure Encryption settings, perform the following steps:

1. Under Encryption Settings, click New Settings or click the name of an already existing Encryption Setting to edit these properties

2. In the **Name and Description** section, enter a name and description for the Encryption settings. The name can then be assigned to one or more secondary storage groups.

3. In the **Encryption Settings** section, Select the checkmark to Encrypt File Data and select an Encryption key that was previously generated using the “Generate Encryption Keys” section.



Generate Encryption Keys

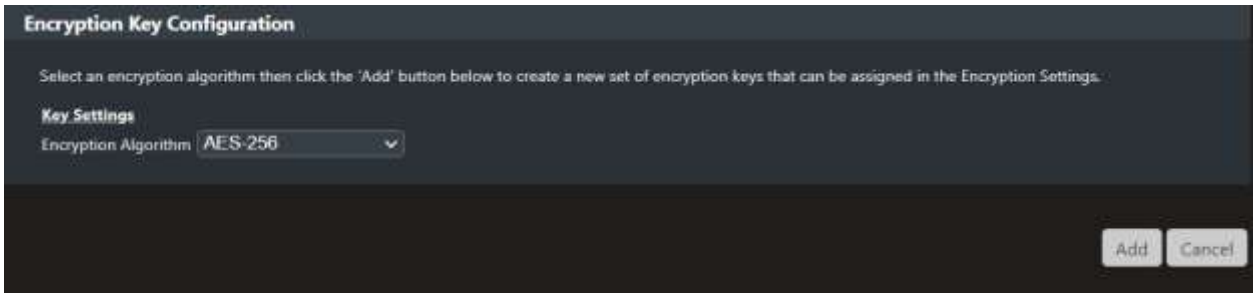
The Generate Encryption Keys section allows users to create encryption keys to be used in the Encryption Settings section. The system takes care of storing these encryption keys and managing them if they are changed over time.

To configure and Encryption Key, perform the following steps:

1. Under Encryption Key Configuration, click New Key Configuration or click the name of an already existing Encryption Key to edit these properties

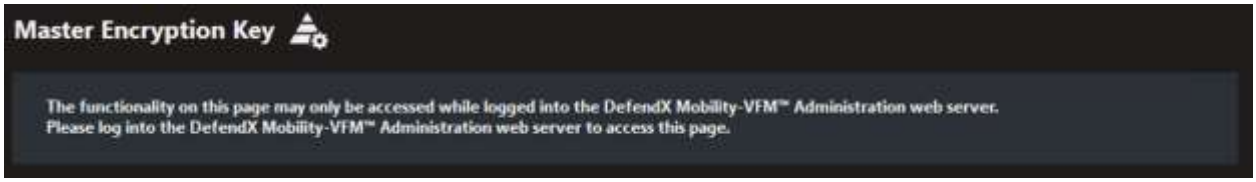
2. In the **Name and Description** section, enter a name and description for the Encryption Key. The name can then be assigned to one or more Encryption Settings.

3. In the **Key Settings** section, Select the encryption algorithm for the encryption key. Currently the system supports AES-128, AES-192, or AES-256.



Master Encryption Key

The Master Encryption key is used by DefendX Mobility VFM to encrypt sensitive configuration data such as passwords when they are stored in the database. The Master Encryption Key section allows for the backup, recovery, and generation of new Encryption keys. Performing of these operations is limited to access of the application from the server that is running the DefendX Mobility VFM Admin. If a user attempts to reach this section from any other location, they will see the following message.



When logged into the server running the DefendX Mobility VFM Admin component, the user will see the following options:

In this section the user can select to export the key to a text file. Please ensure that this key remains in a safe location as it can potentially be used to decrypt the database and reveal the contents of passwords stored in the system.

The Import section allows an encryption key that was previously exported to be added to the system to be able to access encrypted information on the database. This process is sometimes necessary when a re-installation of the DefendX Mobility VFM Admin has occurred.

Finally, the Modify section allows users to re-generate an encryption key for the system. The Master Encryption Key should only be replaced when it is necessary (i.e., when the current key has been compromised). To modify the key, the “Enable Modify Button” must be pressed. This will enable the modification button that will re-generate the encryption key. After modifying the Master Encryption Key use the 'Export' option above to save it to a file for backup purposes. Before modifying the Master Encryption Key, it is highly recommended to back-up the DefendX Mobility VFM Administration configuration and stores databases.

Configuring Primary Storage

A Primary Server is a source file server used to access primary storage. The Core Tiering Engine will scan the primary server's shares and select the files to be tiered based on the assigned policy's criteria. Users connecting to the primary server's shares will also be able to select files and folders for tiering using DefendX Software RCDM.

When a new Task Service is installed, the primary server entered during the Task Service installation will be automatically added to the primary servers' page within 60 seconds after the Task Service installation is complete. Primary servers that are automatically added will be configured to use the "Default" secondary storage group."

The **New Primary Server** button can be used to add additional NAS or generic servers to an already existing Task Service installation.

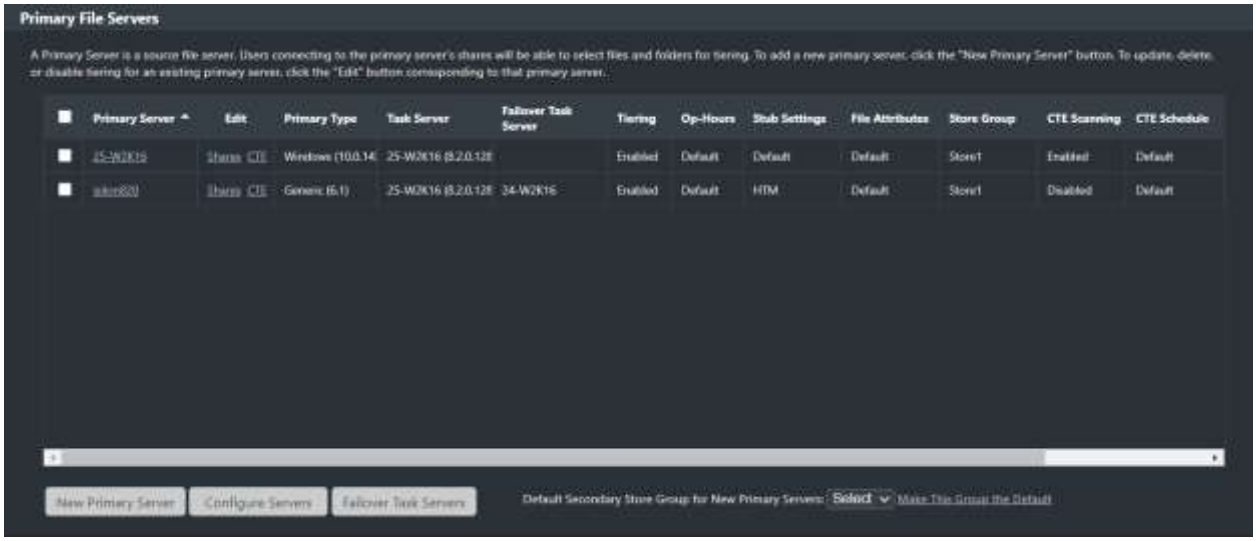
The **New Primary Server** button can also be used to re-add a primary server that was previously deleted in the DefendX Mobility VFM Admin. To undelete a primary server, click the **New Primary Server** button and type in the name of the primary server and choose the correct Task Server. You can also select a different Task Server having the same type if you want to move the primary server to another Task Server.

NOTES:

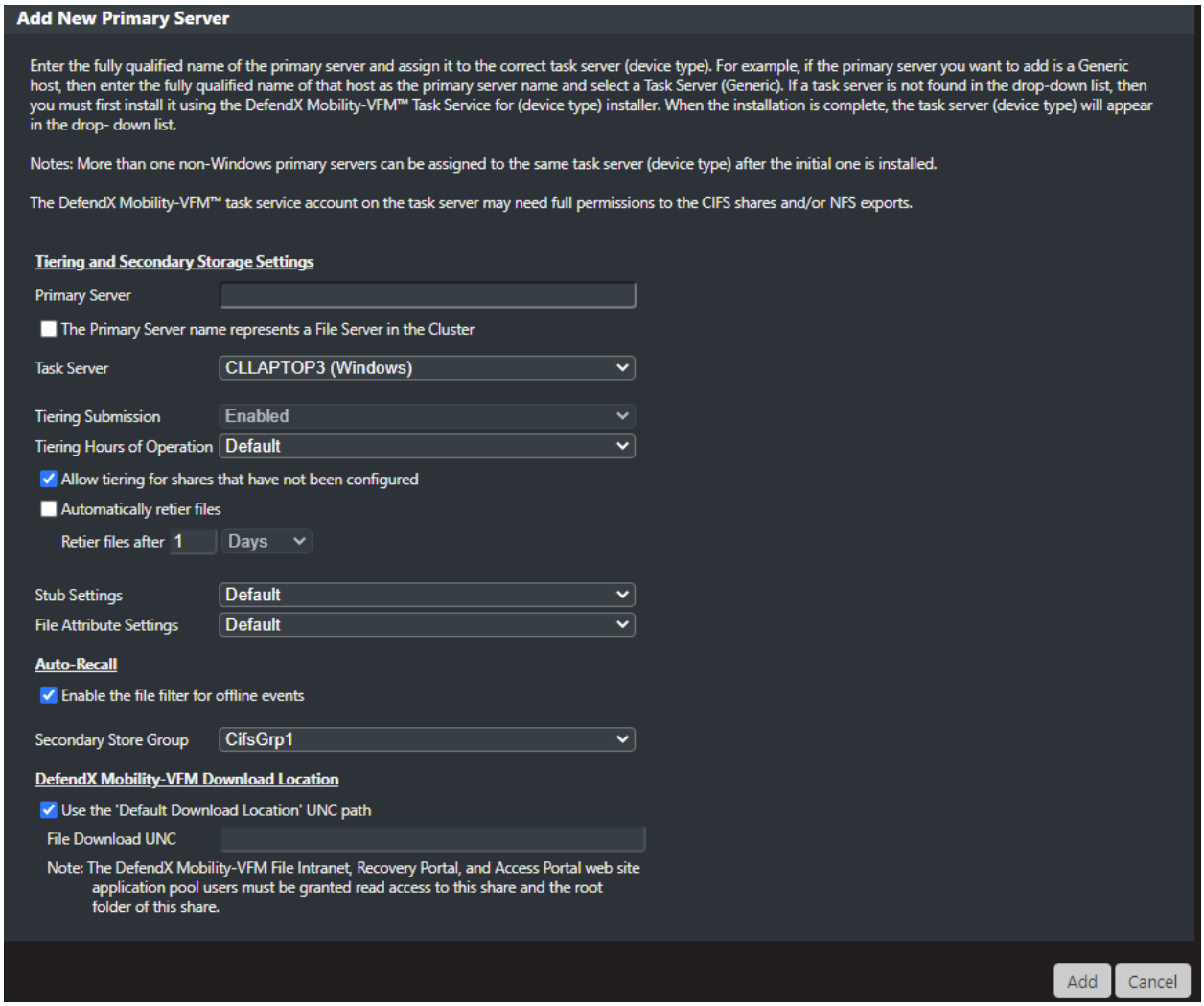
- The Task Service installer for a NAS or generic server will prompt for the initial NAS or generic host name. This host name will automatically be added to the primary servers, as described above.
- If you want the same Task Service to control more than one of the same types of NAS or generic server, then use the New Primary Server button.

To add a new primary server, perform the following steps:

1. Under **Primary Storage** in the left-hand main menu, click **Primary File Servers**.
2. In the **Primary File Servers** dialog box, click the **New Primary Server** button.



3. In the **Add New Primary Server** dialog box, enter the needed information. This dialog box enables you to assign the settings for Tiering, Stubbing, Secondary Storage Group to a primary server**.**



If a Task Server is not found in the drop-down list, then you must first install the Task Service using the DefendX Mobility VFM Task Service for the applicable primary server type. When the installation is complete, the Task Server will appear in the primary server drop- down list.

More than one primary server can be assigned to the same Task Service as long as the Task Service has full permissions to its shares and the primary server is the same type as the specified Task Server.

Value	Definition

Primary Server	The name of the primary server you want to tier files from. For new primary servers being added, you can enter either the fully qualified name or the NetBIOS name. When editing, the primary server name will always display the NetBIOS name and will not be editable.
The Primary Server name represents a File Server in the Cluster	This is only applicable for Windows primary servers. Refer to the Windows Cluster Server appendix.
Task Server	Select the appropriate Task Server that will be used to tier files from the primary server depending on the primary server's platform type.
Tiering Submission	Submitting tiering requests can be enabled or disabled. Primary servers that are disabled will continue to process all pending tiering requests; however, new tiering requests will be denied. Recall and Recovery requests are not affected and will always be accepted.
Tiering Hours of Operation	Select the name of a hours of operation settings that will control when tiering can occur.

Allow tiering for shares that have not been configured.	If checked then all the primary server's shares will be allowed to have files tiered from without being configured separately. If the share does not have an explicit configuration defined, then the primary server settings will be used. If not checked, then only the primary server's shares that are explicitly configured will be allowed to have their files tiered. Therefore, tiering can be restricted to certain shares. Refer to the section on *Configuring* Primary Server Shares for more details.
Automatically re-tier files	This allows for the automatic re-tiering of files which have been recalled. The re-tiering will occur after a specified period of time has elapsed.
Stub Settings	Choose a stub settings name that will control how a tiered file on primary storage is stubbed.
File Attribute Settings	Choose a file attribute settings name that will control what types of files on primary storage can be tiered based on file attributes.
Auto-Recall section.	Windows: Enable the file filer for offline events NetApp: Enable FPolicy for offline events. VNX/Unity: Enable CEE connector for offline events.

Secondary Store Group	Select the name of the secondary storage group, which contains one or more secondary storage locations, to tier the primary server's files to.

Use the Default Download Location UNC Path	If checked then all file download requests initiated from the Access Portal, Recovery Portal or FileIntranet sites will use the default download location defined in the *Additional Configuration – Default Download Location* page. If unchecked, then all file downloads will be stored in the location specified below.
File Download UNC	If the above checkbox is not checked, then specify the UNC path to be used to temporarily store the contents of tiered files being downloaded from secondary storage. Note: The Access Portal, Recovery Portal and FileIntranet sites application pool users must be granted read access to the share and directories in this UNC path.
Important Notes: • The following applies to Task Services for Windows ONLY. Primary server name represents a Cluster name. When checked indicates that the primary server name is the cluster which contains the shared resources. An additional text box will also appear for you to enter the name of the fail-over Task Server. Refer to the appendix for details on configuring tiering for a Microsoft Windows Cluster environment. • The following applies to Task Service for NetApp ONLY. Enable Pass-through Read when stubbing with the offline file attribute. If checked then when a user double clicks on a stubbed file containing the	

offline file attribute, the contents of the file stored in secondary storage will be passed through to the user keeping the stub file intact (i.e., without recalling the file back to primary storage).

If not checked, then when a user double clicks on the stubbed file, the file on secondary storage will be copied back to primary storage overwriting the stub.

NetApp Cluster Mode Settings require the IP address of the cluster as well as the login credentials for that cluster. **Note**: Leave this section empty for 7-Mode filers.

- The following applies to Task Service for VNX ONLY.
- VNX Control Station Settings: VNX hosts require the IP address of its control station as well as the login credentials for that control station.
- The name of the Proxy Server, where the Proxy Service is installed. The Proxy Service is required for Auto-Recall functionality.

- The following applies to Task Services for NetApp, VNX and Generic.

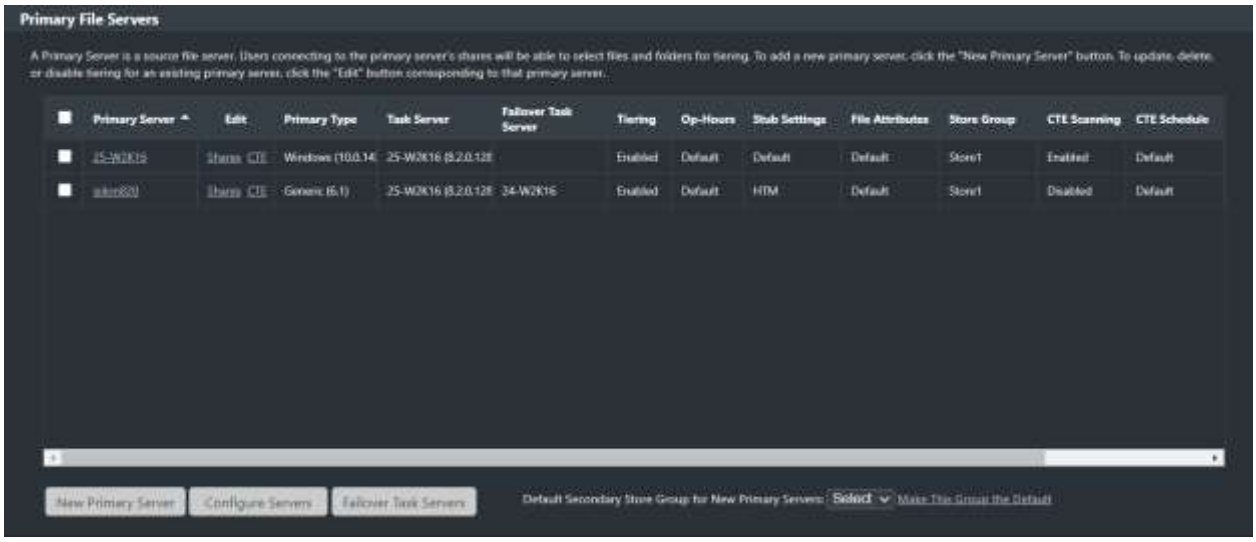
  The optional SSH settings can be used to set NFS permissions on UNIX only volumes.

Editing a Primary Server

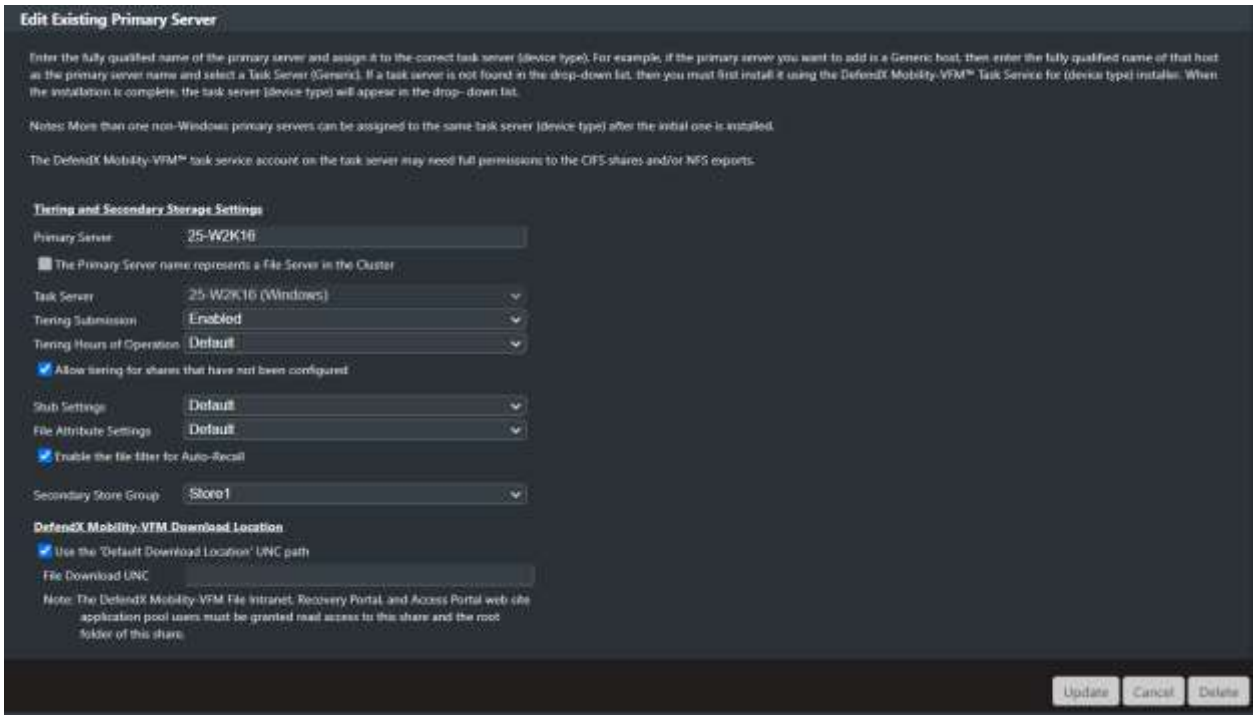
To edit an existing primary file server, perform the following steps:

1. Under **Primary Storage** in the left-hand main menu, click **Primary File Servers**.

2. In the **Primary File Servers** dialog box, click the **Primary Server** name of the primary server that you want to edit.



3. In the **Edit Existing Primary Server** dialog box, enter the changes/updates to the server information and then click the **Update** button. Please refer to the *Add a New Primary Server* section.



NOTE:

To remove a primary server:

- If the corresponding Task Service has more than one primary server assigned to it, then you can remove one of its primary servers by clicking on the **Delete** button in the **Edit Existing Primary Server** dialog box.
- If the corresponding Task Service only has one primary server assigned to it and you want to remove that primary server then:
- Uninstall the DefendX Mobility VFM Task Service first.
- Click the Delete button in the **Edit Existing Primary Server** dialog box.

Configuring Primary Server Shares

One or more shares and exports for a primary server can be configured with separate tiering options, stub and schedule settings and secondary storage group than the settings defined for the primary server itself.

NOTE:

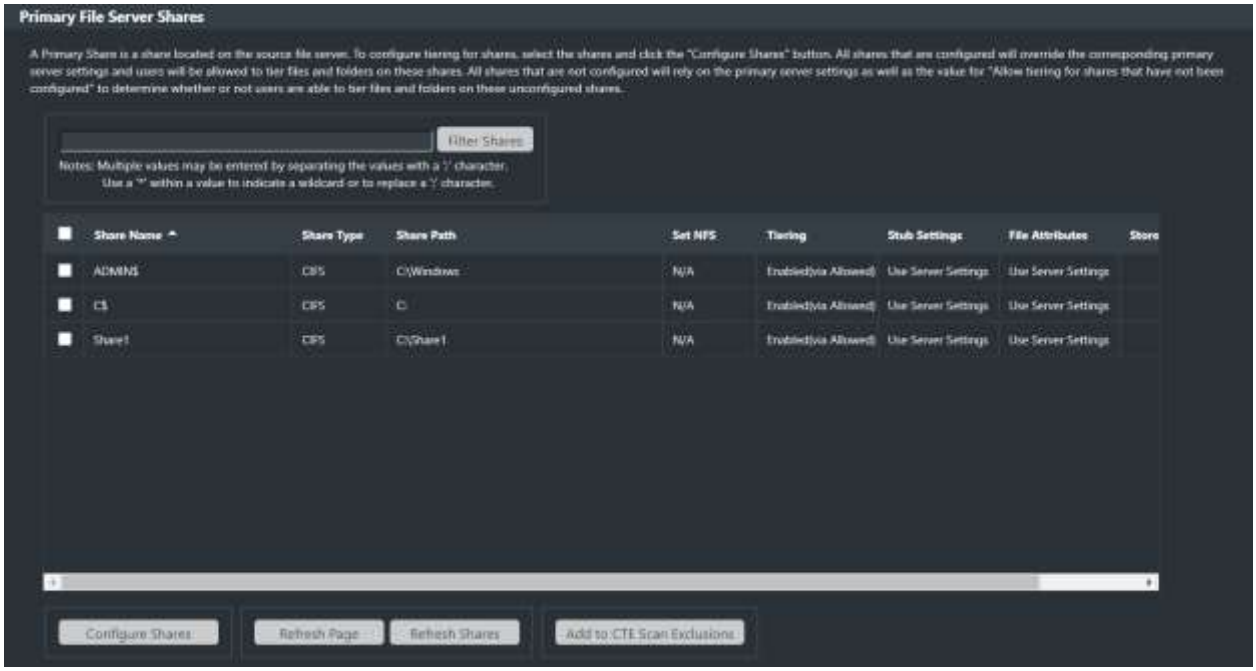
After a new primary server has been added, it may take several minutes for the shares to be populated; however, if the shares or exports continue to not display on this page, then the Task Service's login account may not have been made a member of the administrators' group or the account does have the proper permissions to the NAS device.

To configure one or more primary file server shares, perform the following steps:

1. Under **Primary Storage** in the left-hand main menu, click **Primary File Servers**.

2. In the **Primary File Servers** dialog box, click **Edit Shares** for the primary server name that you want to edit.

3. The **Primary File Server Shares** dialog box will be displayed.



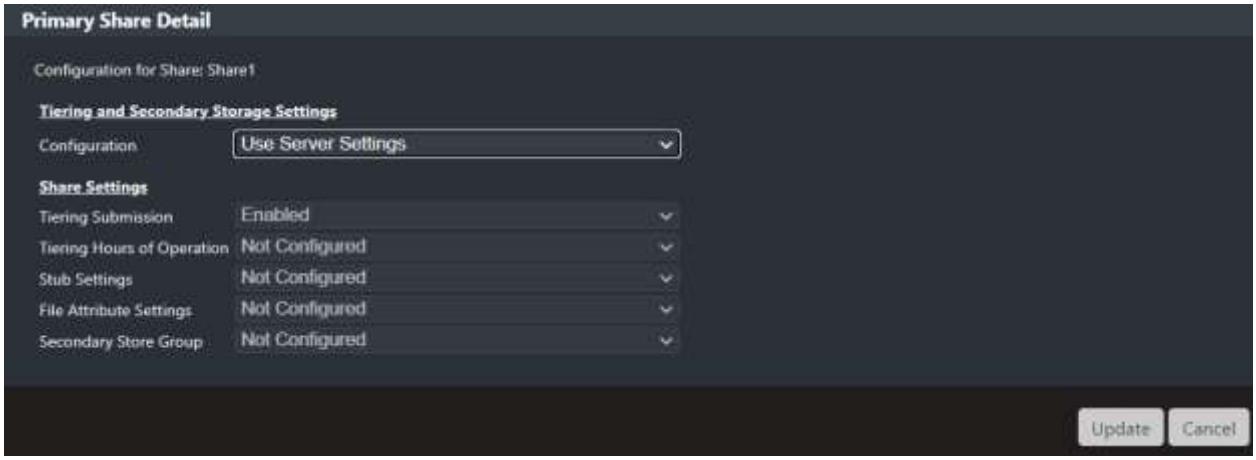
Field	Description
Filter Shares text box and button	Used to display share names using a wild card. This is useful when there are thousands of shares defined on the primary server.
Share Name column	Displays the name of the CIFS share or NFS export.
Share Type column	Indicates if the share name is CIFS or NFS
Share Path column	Shows CIFS share's path or NFS export's path.
Tiering column	Indicates whether the share is using the primary server settings, or it has been explicitly configured with its own settings.

Enabled (via Allowed)	Indicates the share is using the primary server settings and the *Allows tiering for shares that have not been configured* checkbox is checked.
Disabled (via Allowed)	Indicates the share is using the primary server settings and the *Allows tiering for shares that have not been configured* checkbox is not checked.
Enabled (via Share)	Indicates the share has been explicitly configured with its own settings and its *Tier* setting is set to enabled.
Disabled (via Share)	Indicates the share has been explicitly configured with its own settings and its *Tier* setting is set to disabled.
Stub and Schedule Settings column	Displays the name of this setting for shares that have been explicitly configured.
Secondary Store Group column	Displays the name of this setting for shares that have been explicitly configured.
Configure Shares button	Allows you to select one or more shares to explicitly configure. The Primary Share Detail page will be displayed when this
	button is pressed.
Refresh Page button	Redisplays all the shares. This is used in conjunction with the *Refresh Shares* button.

Refresh Shares button	This sends a message to the Task Service instructing it to reload all shares for this primary server into the database. The button will become disabled after pressing it. Use the *Refresh Page* button to redisplay the page from the shares in the database. After pressing Refresh Page, the Refresh Shares button will become enabled again. Note: Allow several minutes for the Task Service to re-populate the shares into the database. You can continue to press the Refresh Page button until the shares you are expecting to be shown appear. The Refresh Shares button is useful for when new shares are created on the primary server and you want them to appear within a short period of time.
Add to CTE Scan button	Allows you to select one or more shares to be included in a Core Tiering Engine (CTE) scan. Adding shares to the CTE from this menu will cause the CTE to scan the entire share. If you wish to scan certain directories within a share, then you must use the primary file server settings page to add the paths to CTE.
Scan Policy drop down	Used in conjunction with the *Add to CTE Scan* button. The selected shares being added to CTE will be assigned to the CTE Scan Policy selected in the drop down.

4. Click the **Configure Shares** button.

5. On the **Primary Share Detail** section, specify the configuration details.



The tabular form outlined below displays the Configuration Options:

Field	**Description**
Use Server Settings	Allows the shares to inherit their settings from the primary server settings. If the primary server setting that *Allows tiering for shares that have not been configured* is not checked, then tiering files from these shares will not be allowed. Therefore, selecting to *Use Server Settings* option unconfigures the share and resets it to use the primary server setting.
Use Share Settings	Allows you to explicitly configure the selected shares with its own set of tiering options for *Tiering*, *Stub and Schedule Settings* and *Secondary Store Group*. Using this option gives you the capability of tiering files located on different shares to different secondary stores.

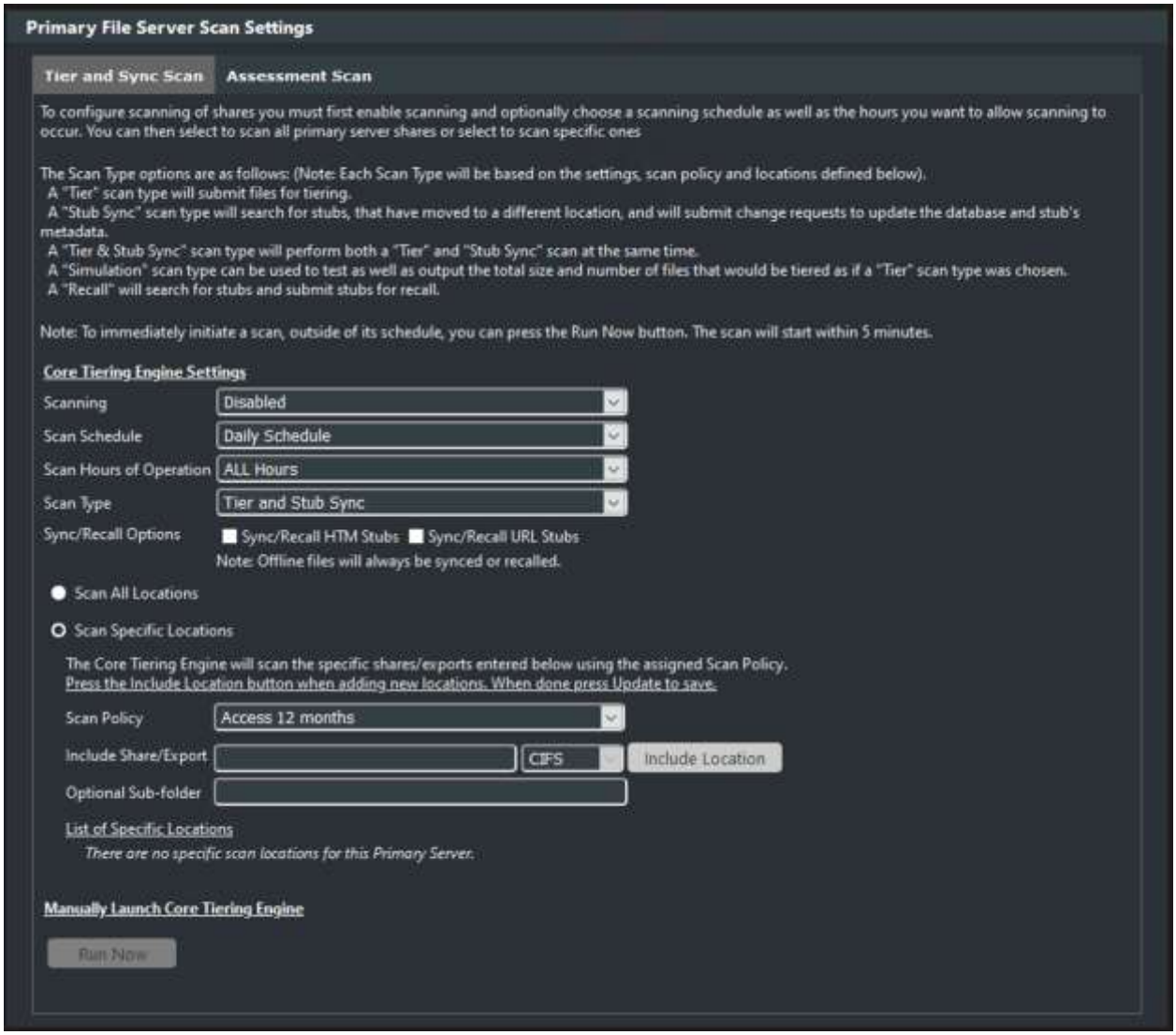
Configuring CTE

To configure one or more primary file server shares, perform the following steps:

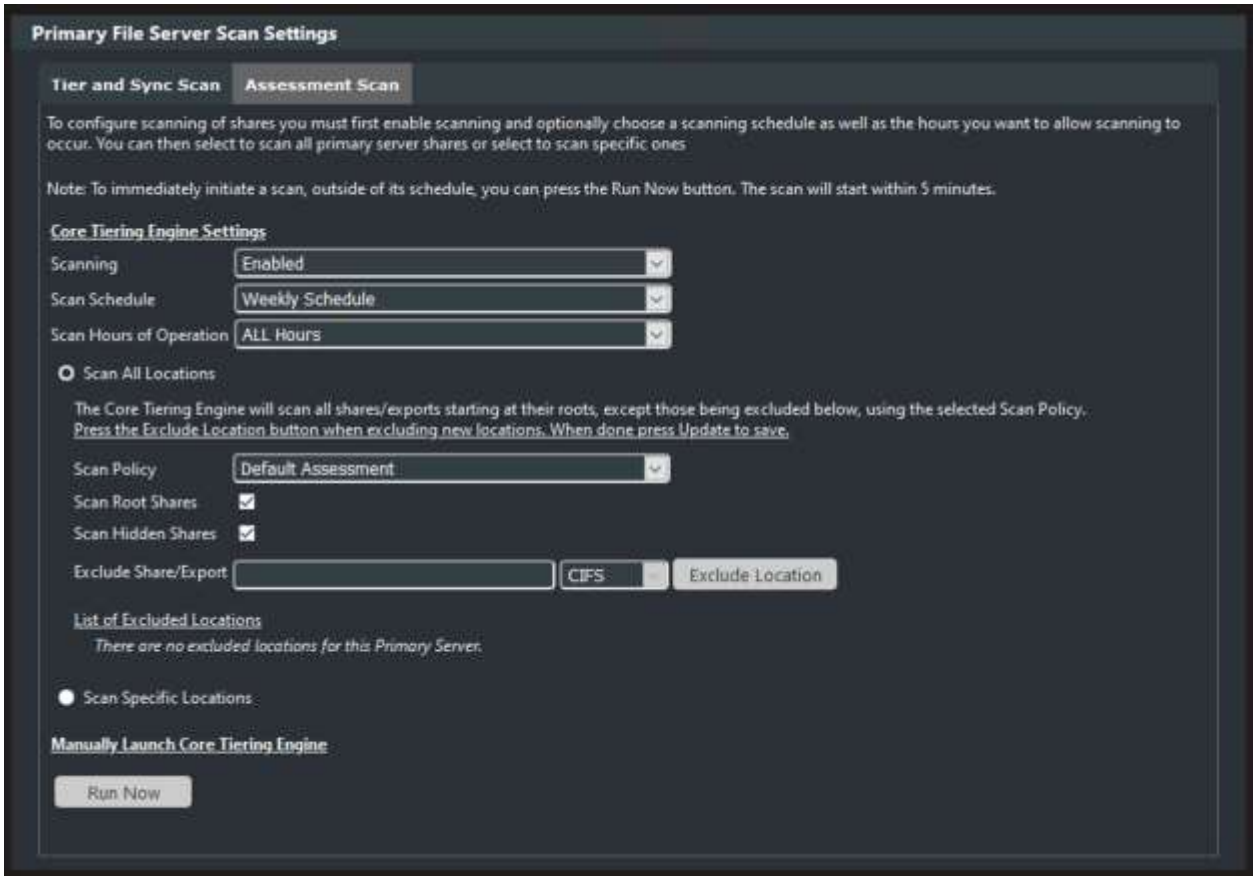
1. Under **Primary Storage** in the left-hand main menu, click **Primary File Servers**.

2. In the **Primary File Servers** dialog box, click **Edit CTE** for the primary server name that you want to edit.

3. The **Primary File Scan Settings** dialog box will be displayed.



4. Switch to the “Assessment” tab to configure assessment scans.



Notes

- Scanning must be Enabled to perform an assessment and to be able to change the Scan Type.
- The Default Assessment Scan Policy will be automatically selected. However, you can change it to use any scan policy.
- Scan All Locations will be automatically selected. However, you can change it to use Scan Specific Locations too.
- You can either set a Scan Schedule, to perform an assessment at a later time, or set it to "Not Scheduled" and simply press the "Run Now" button to assess immediately (within 5 minutes).
- Monitor the Core Tiering Engine assessment using the "Status – Primary Storage Status" page.
- When the assessment is complete then change the Scan Type and Scan Schedule.

The Core Tiering Engine (CTE) Settings

The DefendX Software Core Tiering Engine must be installed on the same server as the Task Server defined above.

To enable the CTE to scan the specified primary server, the CTE must be set to **enabled** and a Scan Policy and Scan Locations must be defined. The Scan Schedule is optional if you do not want CTE to scan based on a schedule.

CTE can be configured to scan all CIFS shares and/or all NFS exports that are found on the primary server by selecting the *Scan All Locations* radio button.

If you want CTE to scan specific locations then select that radio button, enter a Scan Location along with a policy and press the *Add* button.

Field	**Description**
Format of the Scan Location	"share name\path" when the location you want to scan is a CIFS share located on the primary server. The primary server name is not included with the scan location. The "\path" is optional and can be used to limit the scan to specific paths on the share.
Format of the Export Location	"export\path" when the location you want to scan is an NFS export. The primary server name is not included with the scan location. The "\path" is optional and can be used to limit the scan to specific paths on the export. For example, if a location of "/vol/vol2" is entered then the export "\vol\vol2" will be scanned. NFS export and path names are case sensitive.
NOTES: • Microsoft Services for NFS must be installed on the same server that the CTE engine is installed if you want to scan NFS exports located on EMC VNX/Unity or Generic NAS devices. It is not needed for NetApp devices. • Once you have *added* specific locations, a grid will appear displaying those	

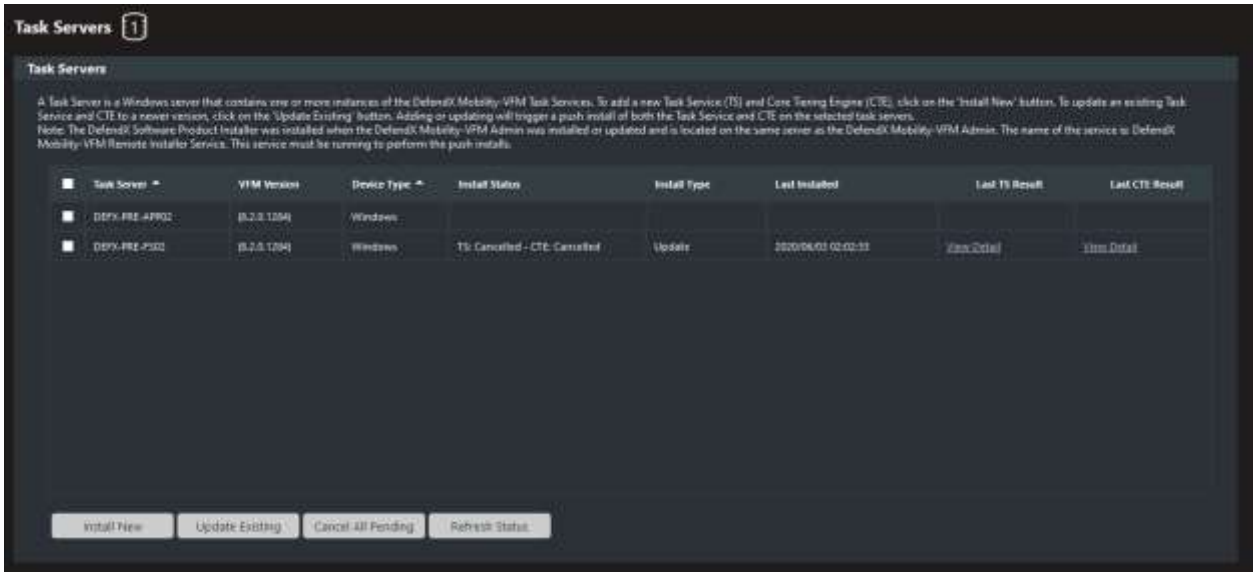
locations for which you will then have an option to remove them.

- Pressing the *Run Now* button to manually launch the CTE will trigger a scan within 5 minutes after pressing the button. You can view the *Primary File Servers Status* page to see its progress. The *Run Now* button will become disabled and will remain disabled until the CTE status becomes *Idle* as shown on the Primary File Servers Status page. This is to prevent multiple instances of the CTE from being executed.
- If you chose to enable the *Simulate Tiering* option, then the CTE will scan the locations but will not send tiering notifications to the DefendX Mobility VFM Admin web site. Instead, it will log the total number of files and the total size of the files that meet the criteria for tiering. The log file will be located in the CTE's installation folder.
- Tier and Stub Sync: Performs a tiering and stub sync scan at the same time.
- Stub Sync: Updates the database with the location of all stubs that have moved to new locations.
- Recall – Performs a mass recall of all stub files.

Task Servers

Use this page to push install new Task Services and Core Tiering Engines or to update one or more older versions of them

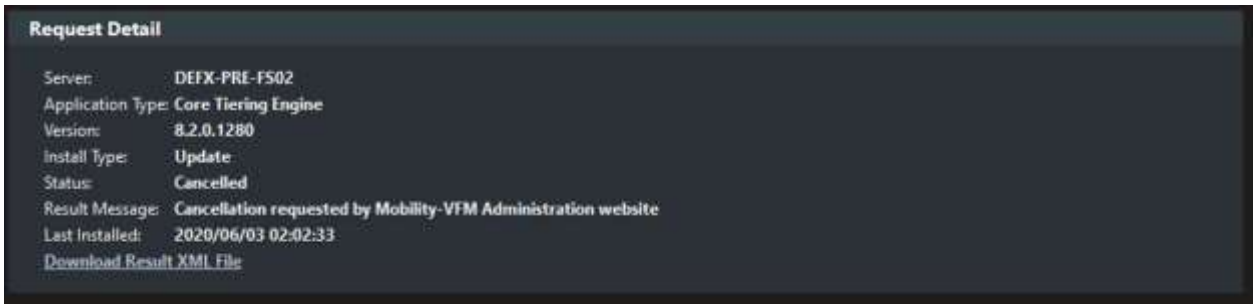
A list of existing Task Servers, where one or more Task Services are currently installed, will be displayed on this page and will include a checkbox in the first column to give you the capability of selecting multiple Task Servers to update at once. Simply select each Task Server and press the "Update Existing" button.



The Task Servers page provides the following details on Task Servers installed in the environment:

- **Task Server**: The name of the Windows server where the Task Services is installed.
- **Mobility Version**: The current version of the Task Service.
- **Device Type**: The type of Task Service installed, i.e., Windows, NetApp, VNX, Unity, Generic
- **Install Status**: The status of the push install that was last run.
- **Install Type**: Indicates whether it was a “New” install or an “Update”.
- **Last Installed**: The date of when the last push install was run.
- **Last TS Result**: The result of the Task Service’s last push install.
- **Last CTE Result**: The result of the Core Tiering Engine’s last push install.

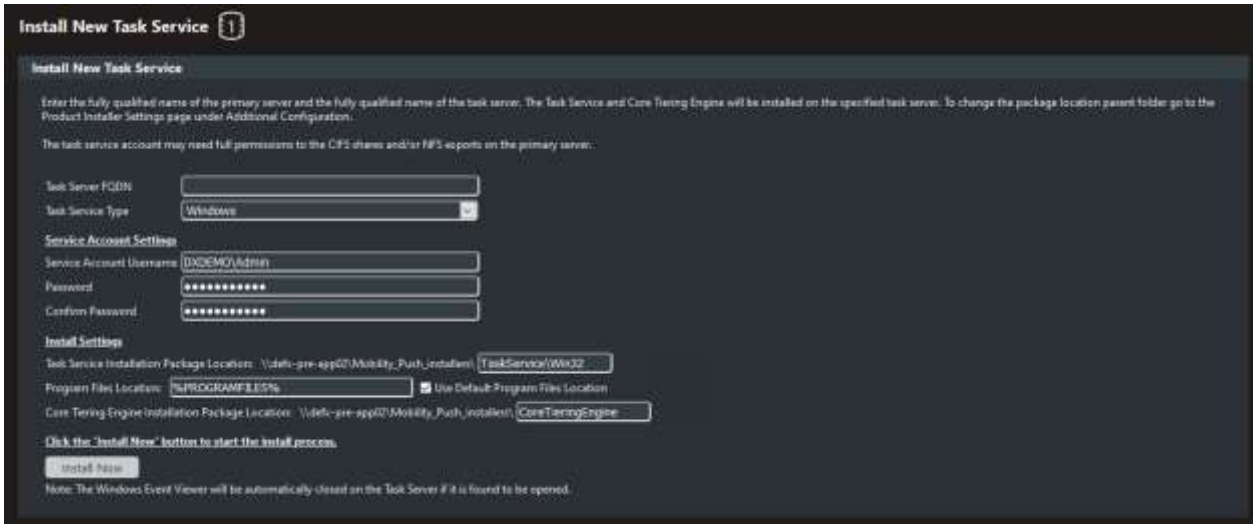
Clicking on “**View Detail**” for either the Last TS Result or the Last CTE Result will display additional information as seen below.



Clicking on the "**Download Result XML File**" will display the actual XML file created by the DefendX Mobility VFM Admin as well as messages and errors that were added to it by the product installer service. This is normally used to help with debugging issues.

Installing a New Task Server

If you want to install a Task Service and Core Tiering Engine on a new Task Service, then press the "Install New" button.



1. Add the information for the server fully qualified domain name.

2. Select the type of system this Task Service will be used to tier and recall files from. The options are Windows, EMC Unity, EMC VNX, Generic, or NetApp.

3. Add the credentials for the service account that will be running the Task Service

4. Optionally, change the location of the installation path for the Task Service and Core Tiering Engine.

Configuring Secondary Storage

A secondary Storage Section contains the location and connection settings used to store the files that have been tiered.

Configuring Storage Policies

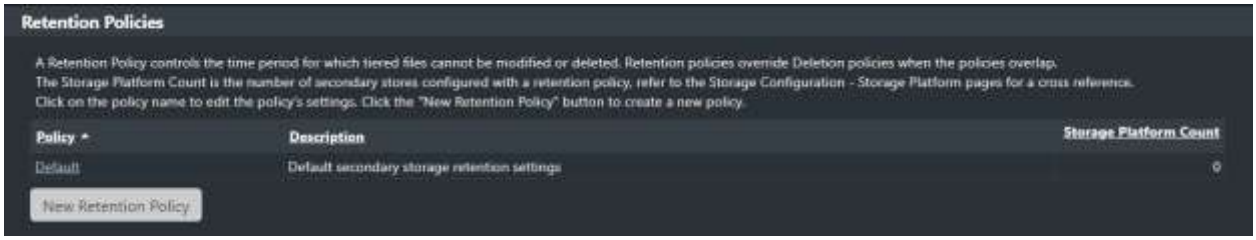
Storage Policies consist of Retention Policies and Deletion Policies. Retention policies control the time period for which secondary storage objects cannot be deleted. Deletion policies specify the time frame with which secondary storage objects can be deleted. If a retention and deletion policy overlap, then the retention policy will take precedence. When a retention policy expires then the secondary storage objects remain until a deletion policy removes them.

Retention Policies

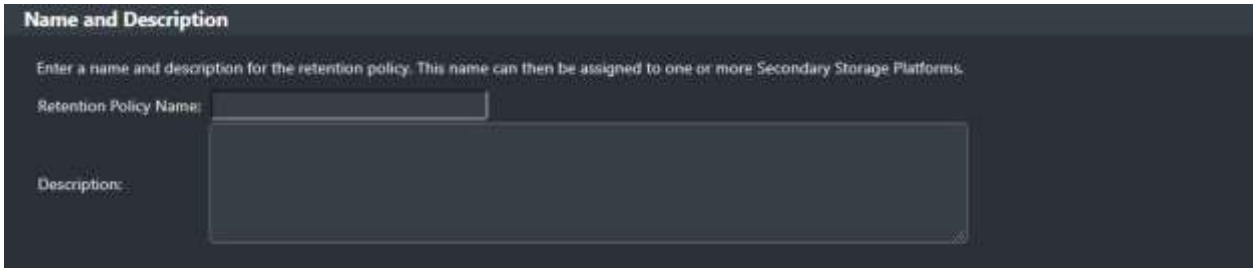
To configure a Retention Policy:

1. Under Secondary Storage in the left-hand main menu, click Storage Policies > Retention Policies.

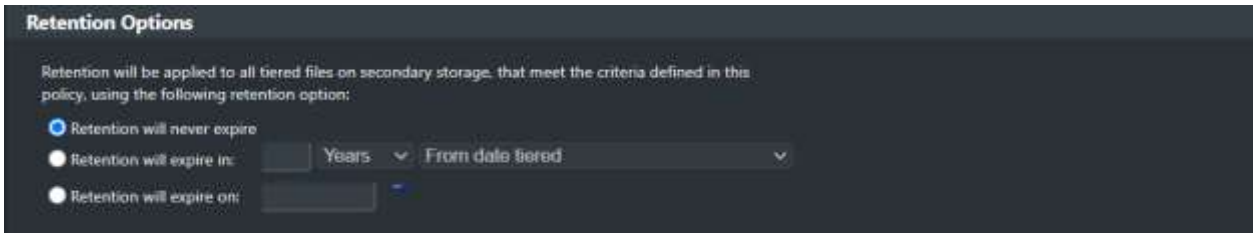
2. In the **Retention Policies** section, click a policy name to edit an existing policy or click **New Retention Policy** to configure a new policy.



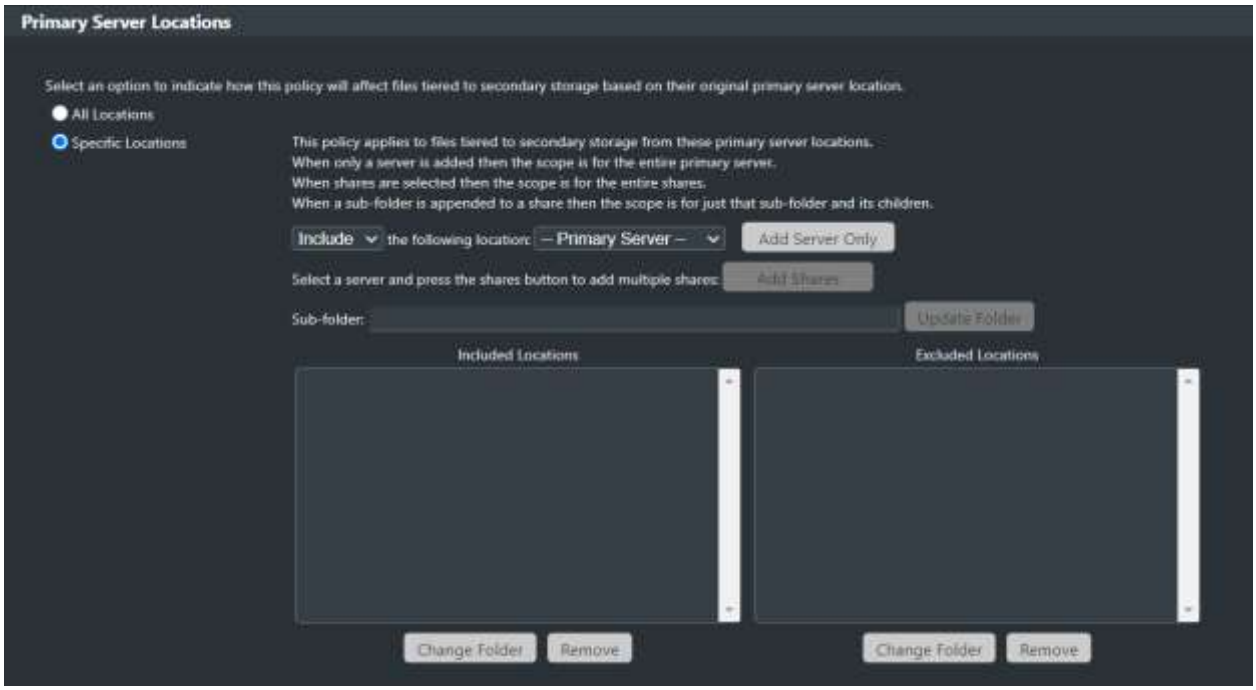
3. In the **Add New Retention Policy** section, specify a name and description for the Retention Policy.



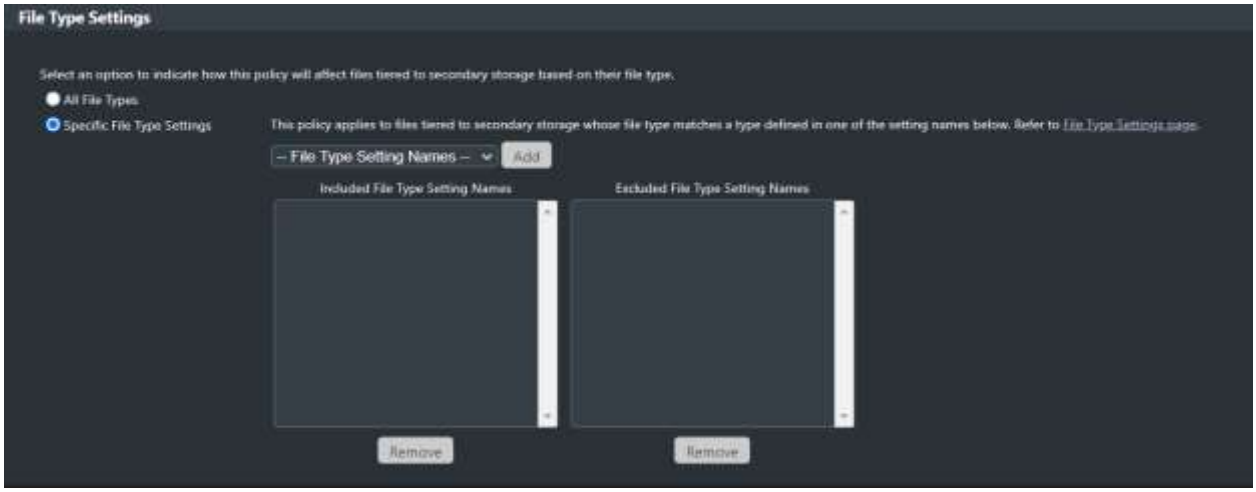
4. In the **Retention Options** section, set the expiration options for the retention policy.



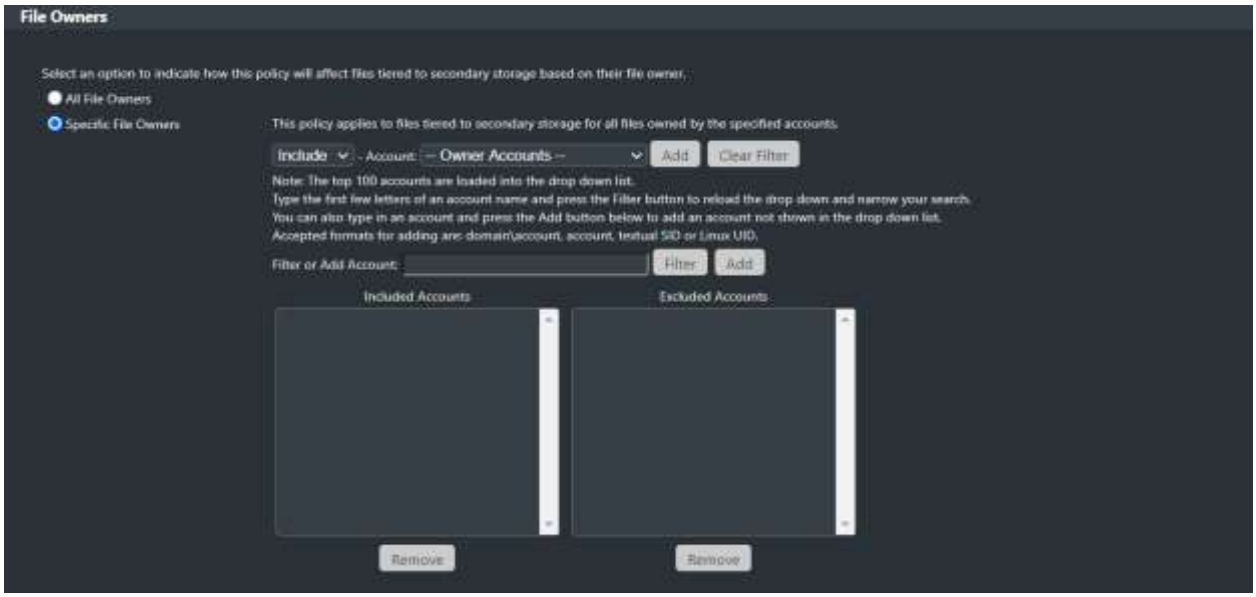
5. In the **Primary Server Locations** section, either apply the retention policy to All Locations or specify which primary servers the retention policy will be applied to.



6. In the **File Type Settings** section, indicate whether the retention policy should be applied to all file types or specific file types only.

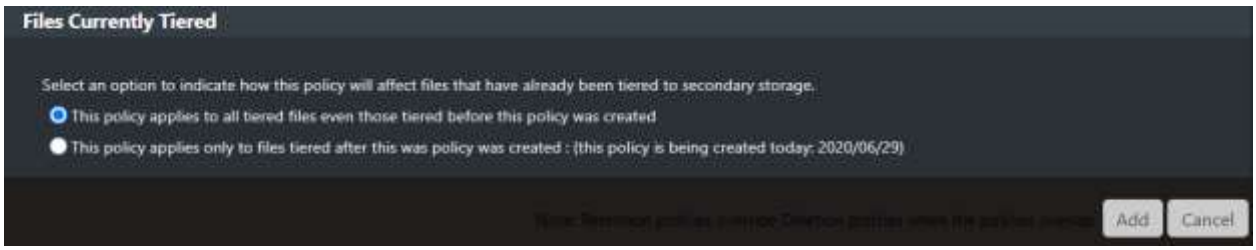


7. In the **File Owner** section, indicate whether the retention policy should be applied all file owners or specific file owners only.



8. In the **File Versions** section, indicate whether the retention policy should apply to the most recent version of the file, all previous versions, or both.

9. In the **Files Currently Tiered** section, indicate whether the retention policy should be applied to all tiered files or only files tiered since the retention policy was created. Click **Add**.



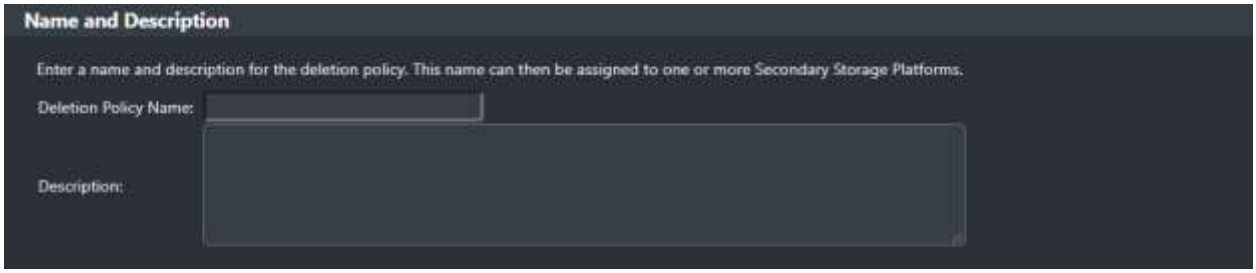
Deletion Policies

To configure a Deletion Policy:

1. Under Secondary Storage in the left-hand main menu, click Storage Policies > Deletion Policies.

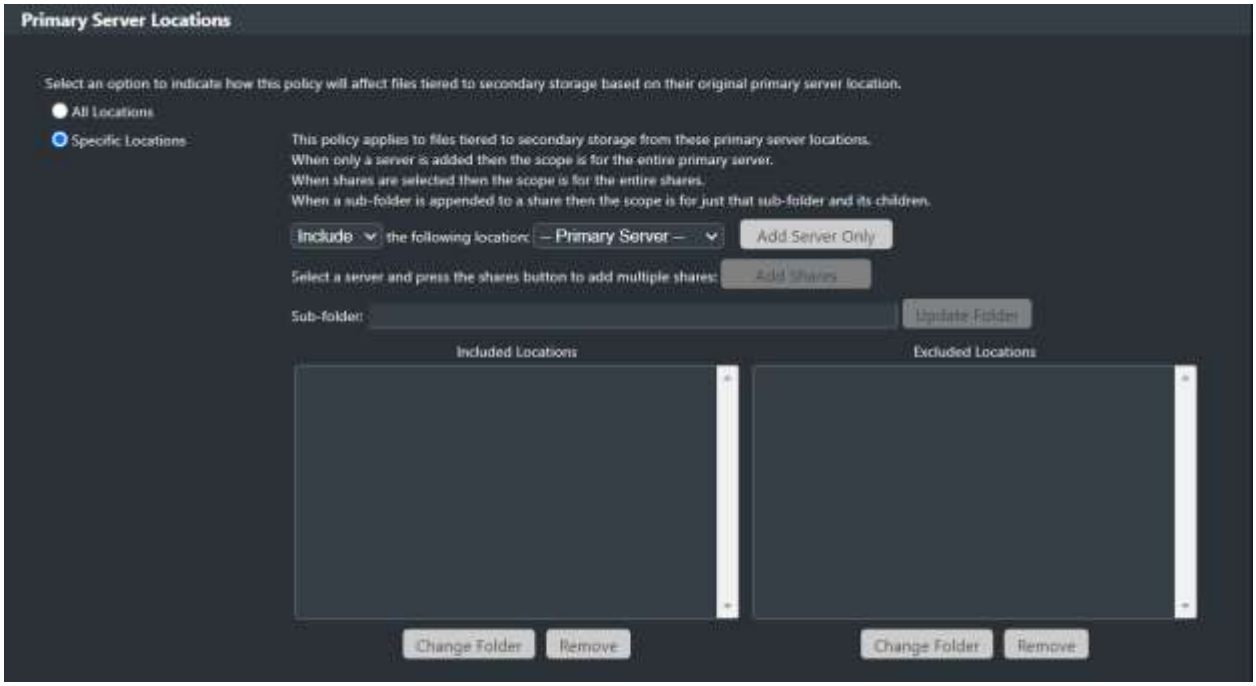
2. In the **Deletion Policies** section, click a policy name to edit an existing policy or click **Deletion Policy** to configure a new policy.

3. In the **Add New Deletion Policy** section, specify a name and description for the deletion policy.

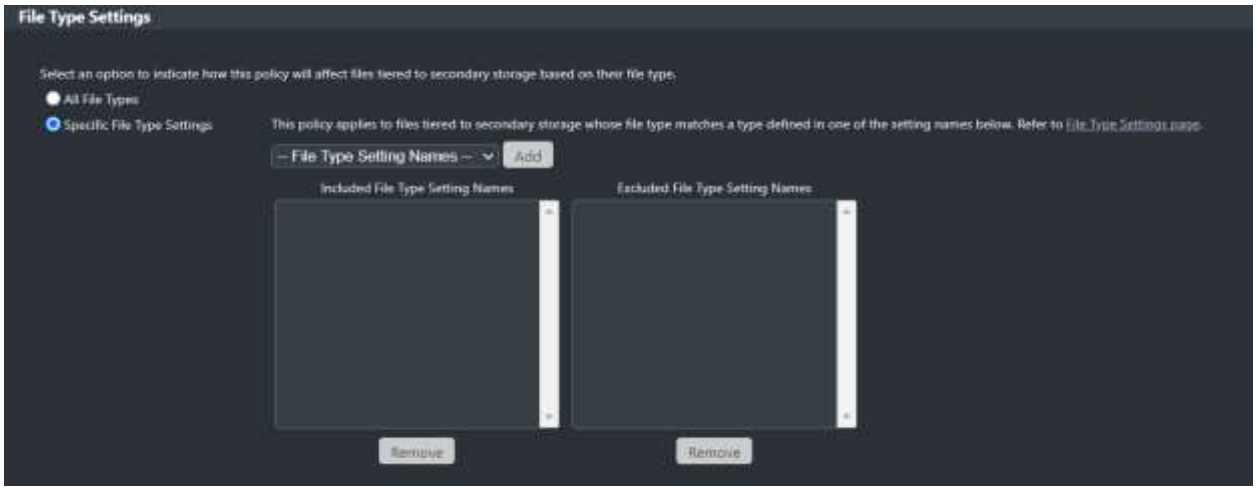


4. In the **Deletion Options** section, set the date or time frame by which the deletion policy will delete tiered files.

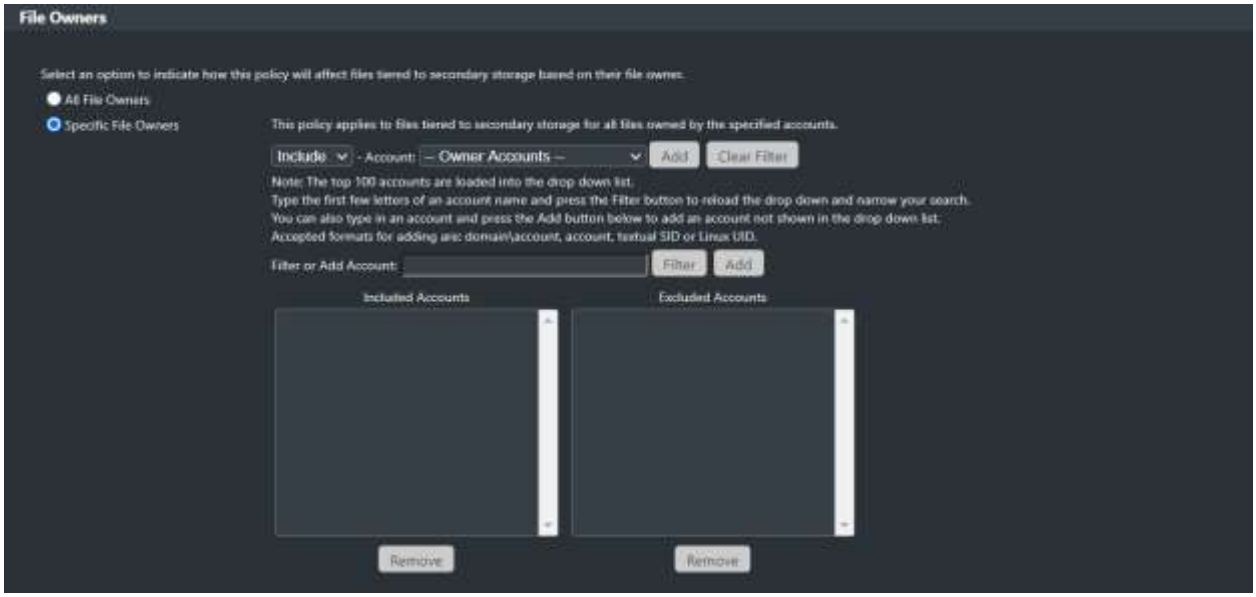
5. In the **Primary Server Locations** section, either apply the deletion policy to All Locations or specify which primary servers the deletion policy will be applied to.



6. In the **File Type Settings** section, indicate whether the deletion policy should be applied to all file types or specific file types only.

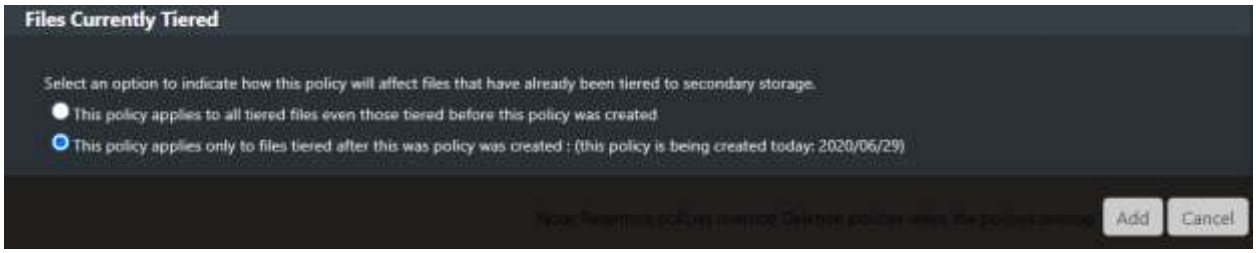


7. In the **File Owner** section, indicate whether the deletion policy should be applied all file owners or specific file owners only.



8. In the **File Versions** section, indicate whether the deletion policy should apply to the most recent version of the file, all previous versions, or both.

9. In the **Files Currently Tiered** section, indicate whether the deletion policy should be applied to all tiered files or only files tiered since the deletion policy was created. Click **Add**.

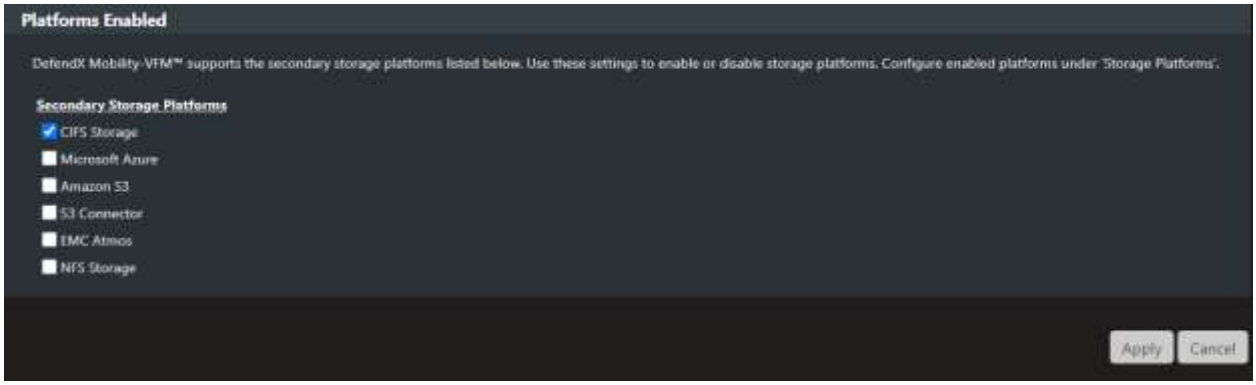


Storage Configuration

The Storage Configuration section allows users the ability to enable or disable Secondary storage platforms as well as the ability to create Storage Groups.

Platforms Enabled

The Platforms Enabled Section allows users to select which Secondary Storage Devices are available for configuration with DefendX Mobility VFM. To enable or disable a storage platform simply select the checkbox for the platform.



Storage Groups

Storage Groups are how DefendX Mobility VFM determines where a policy will use as a repository for tiered files. A Storage group can contain one or more storage devices or platforms. If there are multiple storage devices, DefendX Mobility VFM will write tiered files to all locations specified. Recall operations will be prioritized in the order specified in the "Secondary Storage Group Assignment" section.

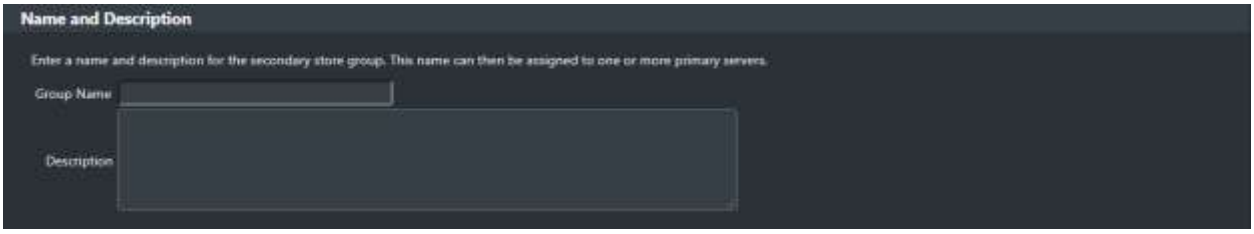
To add/edit secondary store group, perform the following steps:

1. Under Secondary Storage in the left-hand main menu, click Storage Configuration > Store Groups.

2. In the **Secondary Stores Groups** section, click **New Secondary Store Group** or click the name of an already existing secondary store group to edit these properties.

NOTE: New secondary storage groups being created will initially be assigned to the secondary storage type shown in the above drop-down control.

3. In the **Name and Description** section, provide a group name and description for the Secondary Storage Group.

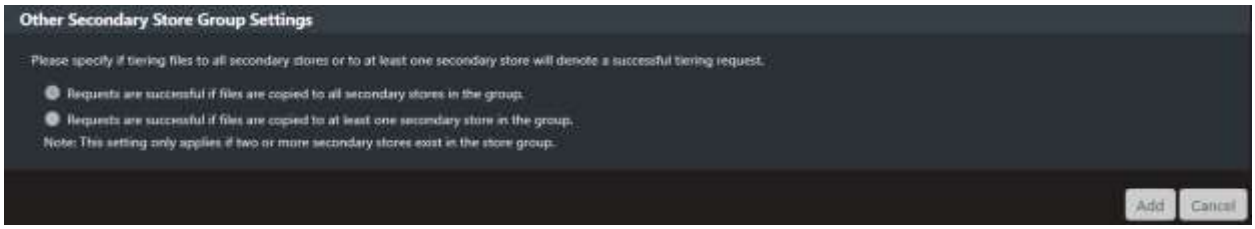


4. In the **Secondary Stores and Optional File Type Assignments** section, assign one or more secondary stores to a group.

Mobility Football-Suitcase feature

The "Football/Suitcase" feature allows files to be tiered to one location and the database and stubs are stamped with a different "Final" location. This scenario is used to temporarily tier files locally and then move the store to a different Final location.

1. In the **Other Secondary Store Group Settings** section, specify the criteria for a successful tiering request.



NOTES:

- An optional “File Types” name can be assigned separately to each of the secondary stores. Files that match those file types will be tiered to that secondary store. You can assign different file type names if you want to tier files of different types to different locations.
- If the *Requests are successful if files are copied to all secondary stores in the group* is selected, then only when the file has been successfully tiered to all the secondary stores will the file be stubbed.
- If the *Requests are successful if files are copied to at least one secondary store in the group* is selected, then the file will be stubbed if it has been tiered to at least one of the secondary stores.
- If you want to encrypt the contents on the secondary store, then choose an encryption settings name.

Storage Platforms

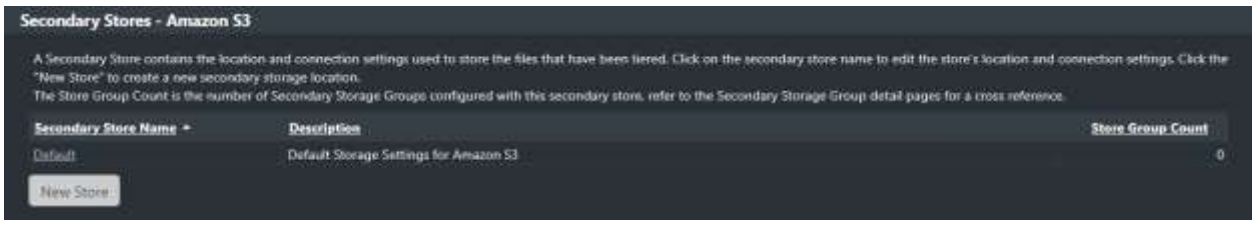
The Storage Platforms section contains all the configured Secondary Storage locations in the DefendX Mobility VFM Admin. There will be a menu item for each of the storage platforms that were enabled in the “Platforms Enabled” Section. The section below specifies how to configure specific storage platforms.

Secondary Storage – Common for all Platforms

Adding/Editing a Secondary Store

1. Under Secondary Storage in the left-hand main menu, click Secondary Storage > Storage Configuration > Storage Platforms > applicable platform.

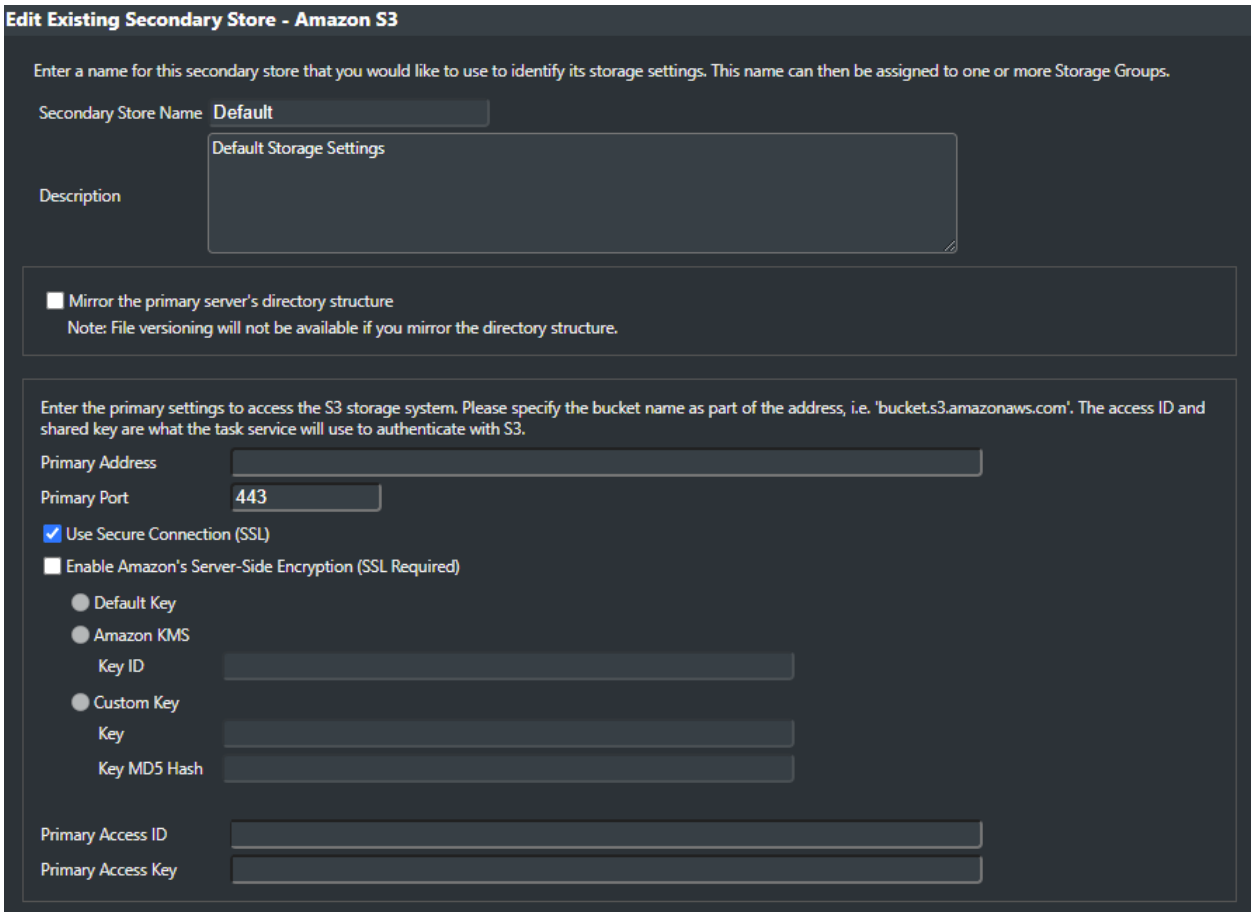
2. In the **Secondary Stores** section, click **New Store** or click the name of an already existing secondary store to edit these properties.



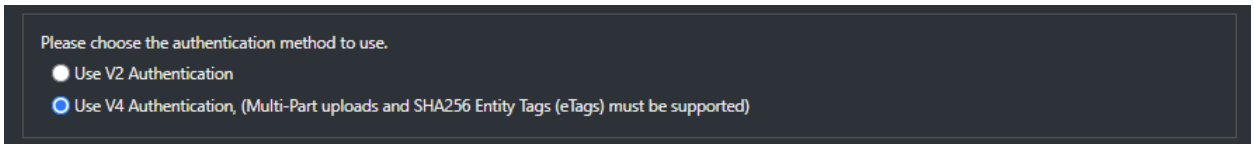
Secondary Storage – Cloud Platforms

This section allows for configuration of Cloud storage as targets for DefendX Mobility VFM.

1. In the **Add New or Edit Existing Secondary Store** dialog box enter the needed information. The name of the secondary store can be assigned to one or more primary servers to instruct the primary server where to place the tiered files.
2. All cloud platforms are very similar. The screenshot below corresponds with the Amazon S3 platform.



This portion is only applicable for S3 Connector platforms:



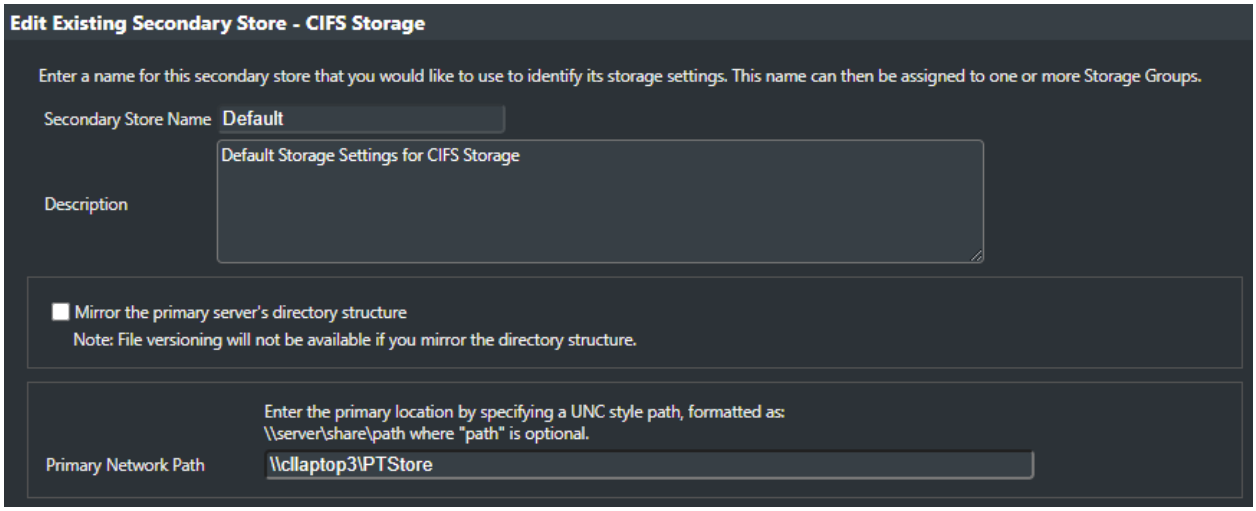
Field	Description
Primary Address	Enter the primary settings to access the storage system. Specify the bucket name as part of the address. Examples: • For Amazon: bucket.s3.amazonaws.com • For S3 Connector: bucket.s3.vendor.com • For Azure: blob.core.windows.net/bucket
Primary Port	Enter the port to communicate with the Storage's web service. This will usually be port 80 when not using SSL and port 443 when using SSL.
Use Secure Connection (SSL)	Check this option if web service is using https otherwise uncheck when using http for the connection.
Primary Access ID or Storage Account	Enter the Primary Storage Account name that will be used to gain access to the cloud storage.
Primary Access Key or Shared Key	Enter the Access Key that corresponds with the Primary Storage Account.
Authentication Method	Choose to authenticate with cloud storage using V2 or V4 authentication. This option is only applicable for the S3 Connector platform. Note: Amazon S3 platform will implicitly use V4 authentication.
Default Key or Amazon KMS Key ID	This is only applicable for Amazon S3 and is used in conjunction with Amazon's server-side encryption.

Custom Key and MD5 Hash	This is only applicable for Amazon S3 and is used in conjunction with Amazon's server-side encryption.
Mirror the primary server's directory structure option	Check this option if you want to create the same directory structure and file names on cloud storage that are found on the primary servers for files being tiered. If this option is used, then the file versioning feature will not be available. Uncheck this option if you want file versioning to be available. The directory structure and file names created will consist of GUIDs.

Secondary Storage – CIFS

This section allows for configuration of CIFS storage paths as targets for DefendX Mobility VFM.

1. In the **Add New or Edit Existing Secondary Store** dialog box enter the needed information. The name of the secondary store can be assigned to one or more primary servers to instruct the primary server where to place the tiered files.



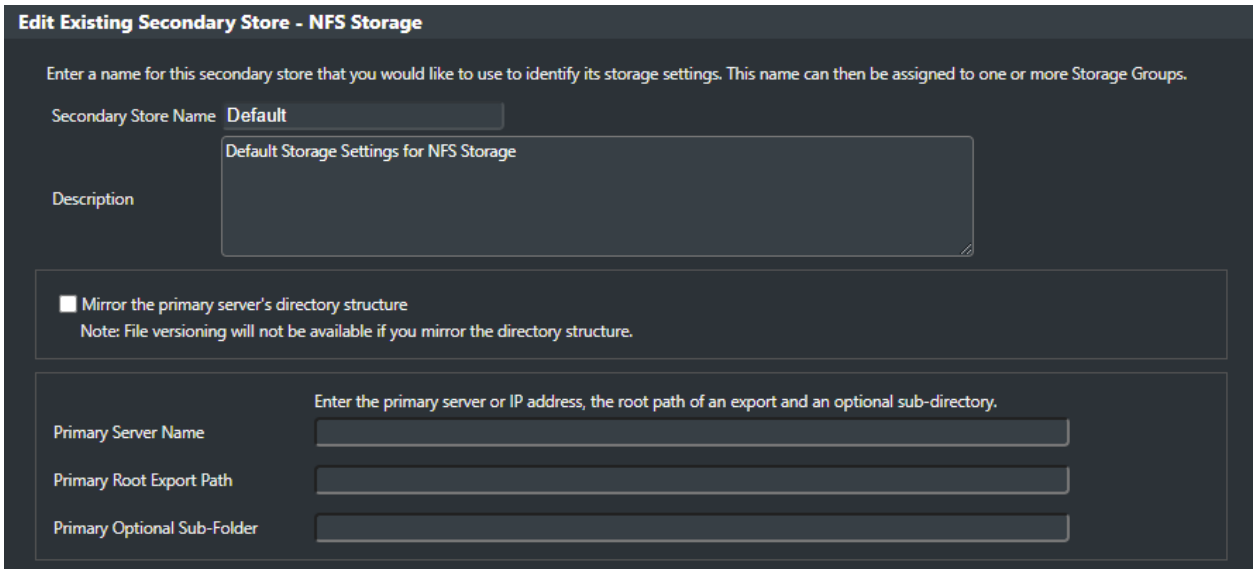
Field/Option	Description

Primary Network Path	Enter the UNC style path of a CIFS share that will be used to store the tiered files. The Primary Network Path must always contain a UNC path.
Mirror the primary server's directory structure option	Check this option if you want to create the same directory structure and file names created on the storage share that are found on the primary servers for files being tiered. If this option is used, then the file versioning feature will not be available. Uncheck this option if you want file versioning to be available. The directory structure and file names created will consist of GUIDs.
NOTE: The Task Services service account	Must be granted full permissions to the secondary store's share name and root share path as well as the primary server shares and directories it will be tiering files from.

Secondary Storage – NFS Storage

This section allows for configuration of NFS storage paths as targets for DefendX Mobility VFM

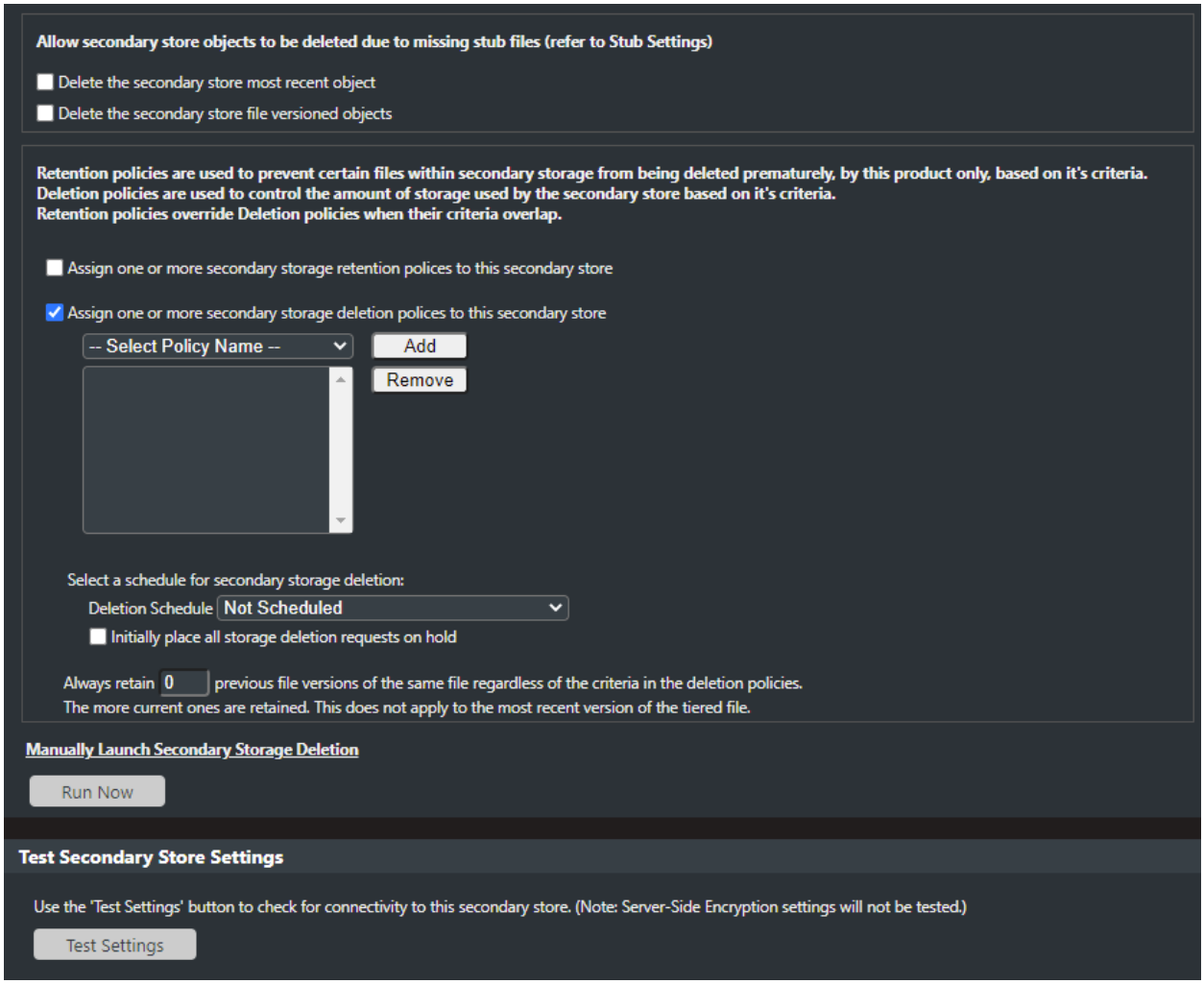
1. In the **Add New or Edit Existing Secondary Store** dialog box enter the needed information. The name of the secondary store can be assigned to one or more primary servers to instruct the primary server where to place the tiered files.



Field/Option	**Description**
Primary Server Name	Enter the primary server or IP address of the NFS Server.
Primary Root Export Path	Enter the root path of an export to be used to store the tiered files.
Primary Optional Sub-Folder	Optionally enter the path to a sub folder to be used on the NFS export to store the tiered files.
Mirror the primary server's directory structure option	Check this option if you want to create the same directory structure and file names created on the storage export that are found on the primary servers for files being tiered. If this option is used, then the file versioning feature will not be available. Uncheck this option if you want file versioning to be available. The directory structure and file names created will consist of GUIDs.
NOTE: The Task Services service account	Must be granted full permissions to the secondary store's export path as well as the primary server shares and directories it will be tiering files from.

Secondary Storage – Common for all Platforms

1. The remaining sections, shown by the screenshot below, are the same for all platforms except the Test Secondary Store Settings section which is only applicable to the cloud platforms.



2. When the “Delete the secondary store object(s) when the stub file no longer exists” is selected in the Stub Settings that correspond to a primary server and that primary server is also configured to tier to this platform then you’ll need to choose which objects in the store are to be deleted. Choose to either delete the older file versions or the current, (most recent), objects.
   NOTE: If this secondary store platform has “Mirror the primary server’s directory structure” checked then file versioned objects is not applicable due to mirroring not having file versions.
3. Optionally assign Retention and Deletion policies to the storage platform.

Domain Storage Configuration

A Domain, for example Active Directory, is an object store that can be traversed to collect user properties which can then be associated with the owners of tiered files. To add a new domain, click the "New Domain" button. To update, delete, or disable scanning for an existing domain, click the "Edit" button corresponding to that domain.

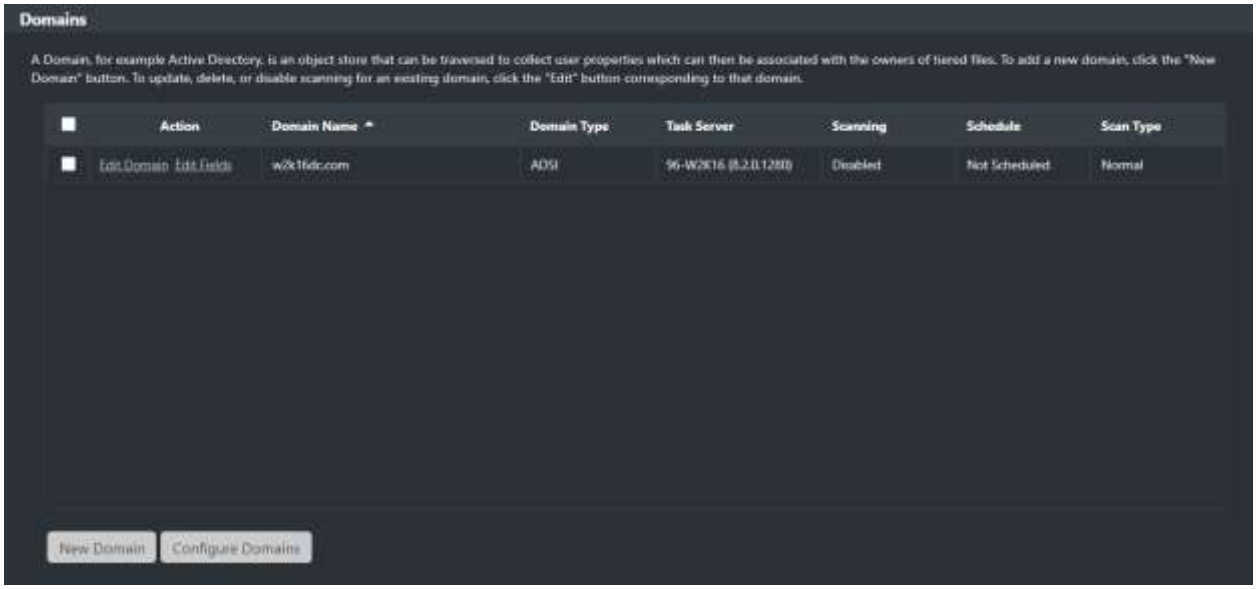
After installing the initial domain using the Domain Agent installer, you can edit or add additional domains using the Domain Storage - Domains pages. Use the “Edit Domain” link to edit the selected domain or use the “Edit Fields” link to edit the domain attributes that will be collected for the selected domain or use the “New Domain” button to add additional domains. You can also use the “Configure Domains” button to edit the multiple selected domains at once.

When a new domain agent service is installed, the domain entered during the domain agent service installation will be automatically added to the domains page within 60 seconds after the installation is complete. The “New Domain” button can then be used to add additional domains to an existing domain agent service.

There are three new pages to support the domain feature. “Domain Storage - Domains” page which displays the currently configured domains, “Status – Domain Storage Status” page which provides the status of the domain agent and the “Additional Configuration – Global Domain Attributes” page which allows for configuration of the domain attributes.

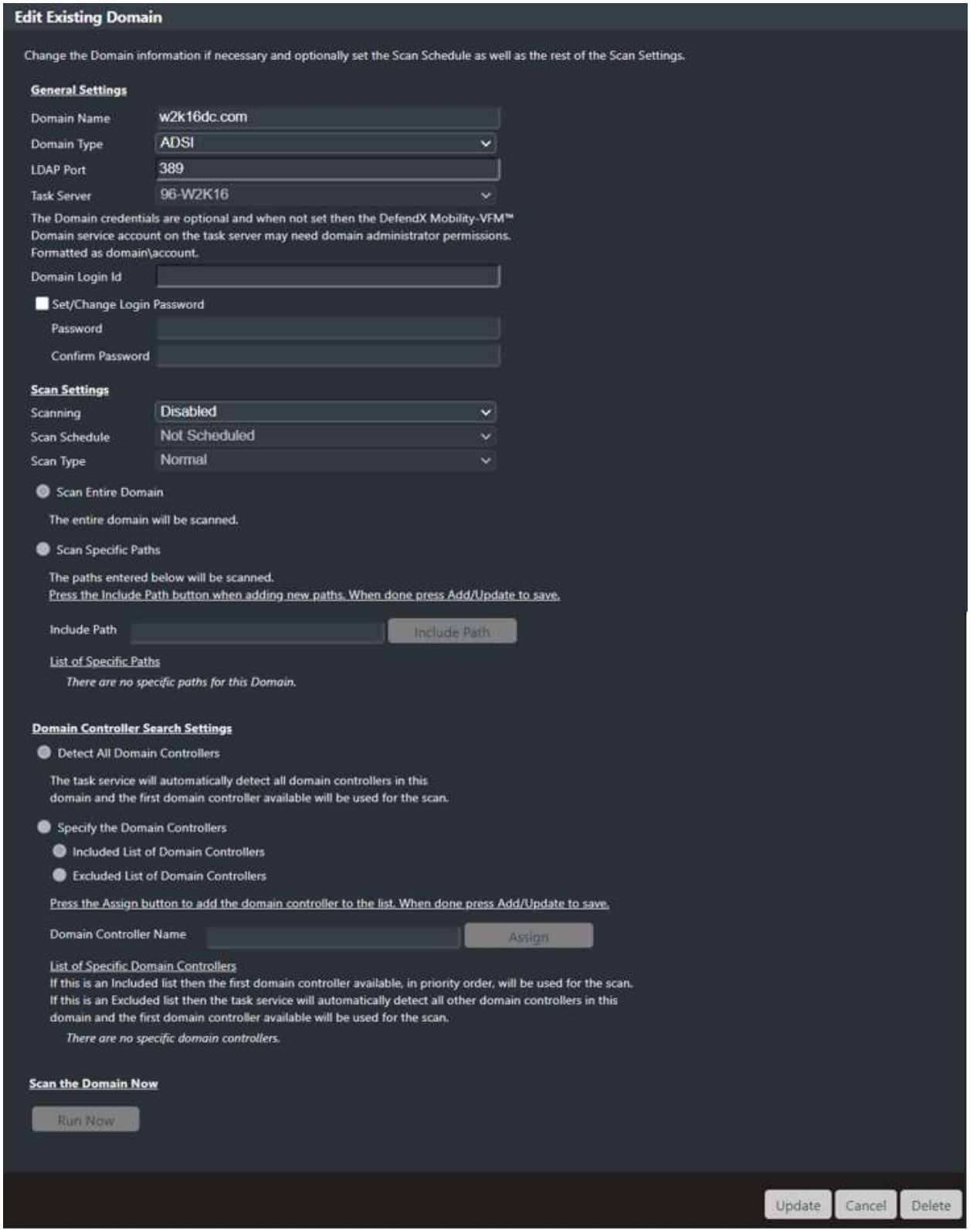
Domains

The Domains page Lists out all configured domains. It details the Domain Name, Type of directory structure, the Task Server that is configured to scan the domain, whether the scanning is enabled or disabled, the schedule that is associated with the scan of the domain, and the type of scan to be performed.



Edit Domain

To edit an existing domain, simply click on the link to edit the domain to display the Edit Domain Page. This page allows the user fo configure details on the domain as specified below:



Domain Name: The name of the domain to scan. This must match the root domain in your environment as display by the Active Directory Users and Computers application.

Domain Type: Currently "ADSI", Active Directory Services Interface, is the only domain type that is supported (i.e., only active directory domains can be scanned).

LDAP Port: Port 389 is the default port for ADSI. If your domain uses a different port, then enter it here.

Task Server: This is the name of the Windows server where the Domain Agent was installed to.

Domain Login Id: A login Id and password are optional. If the Domain Agent's service account does not have permissions to the domain then you can enter an account here which has permissions. This account will then be used to scan the domain.

Scanning: If you want the Domain Agent to scan this domain then you must enable it.

Scan Schedule: If you want the domain to be scanned on a schedule then choose a schedule. Schedules are defined under the "Scheduling Configuration – Schedule Settings" page.

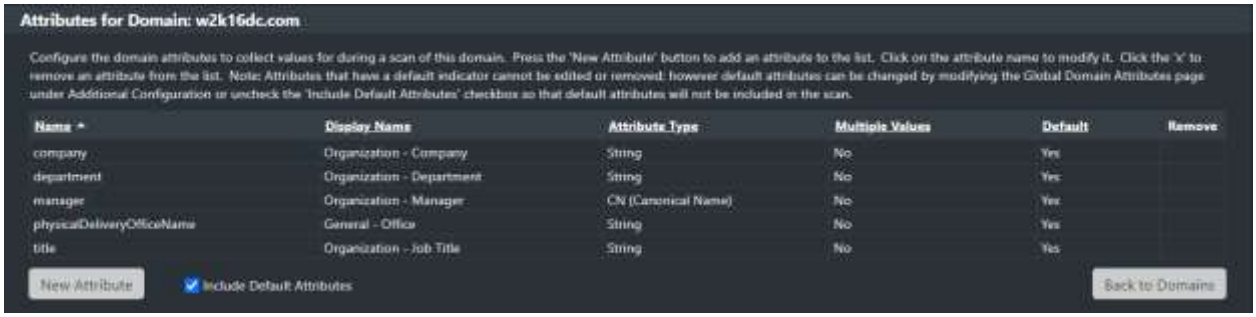
Scan Type: A scan type of "Normal" will collect domain attribute information for each user scanned and will store them in the Mobility stores database. A scan type of "Simulation" will collect information but will not store anything in the databases. This can be used to collect information of what will be collected.

Scan Entire Domain: When this is selected then all users in the domain, starting from the root, will have their attributes collected.

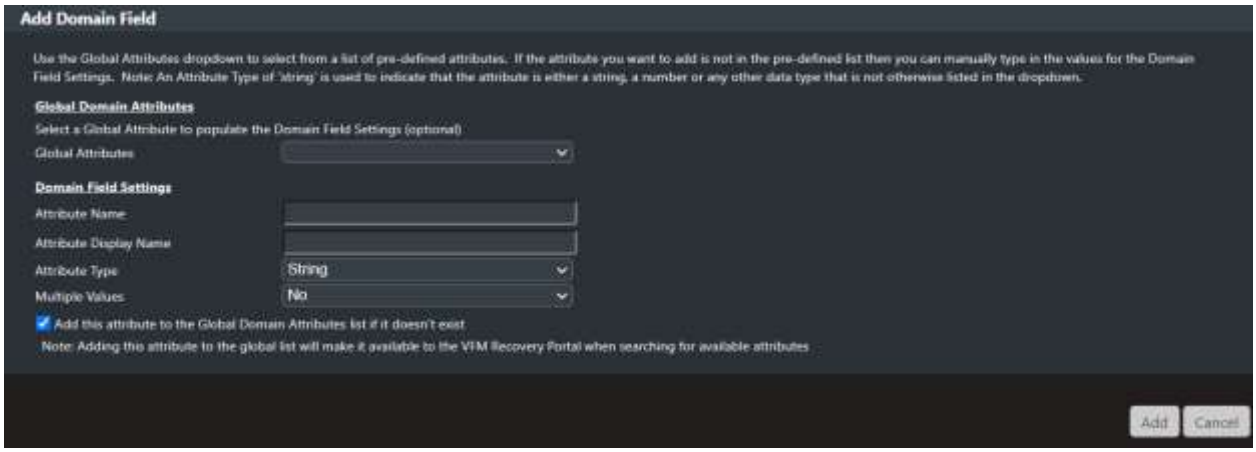
Edit Fields

The Edit Fields link allows the user to select which fields will be captured with every file that is tiered for the selected domain. DefendX Mobility VFM includes several fields by default, and

these can be augmented using this page.



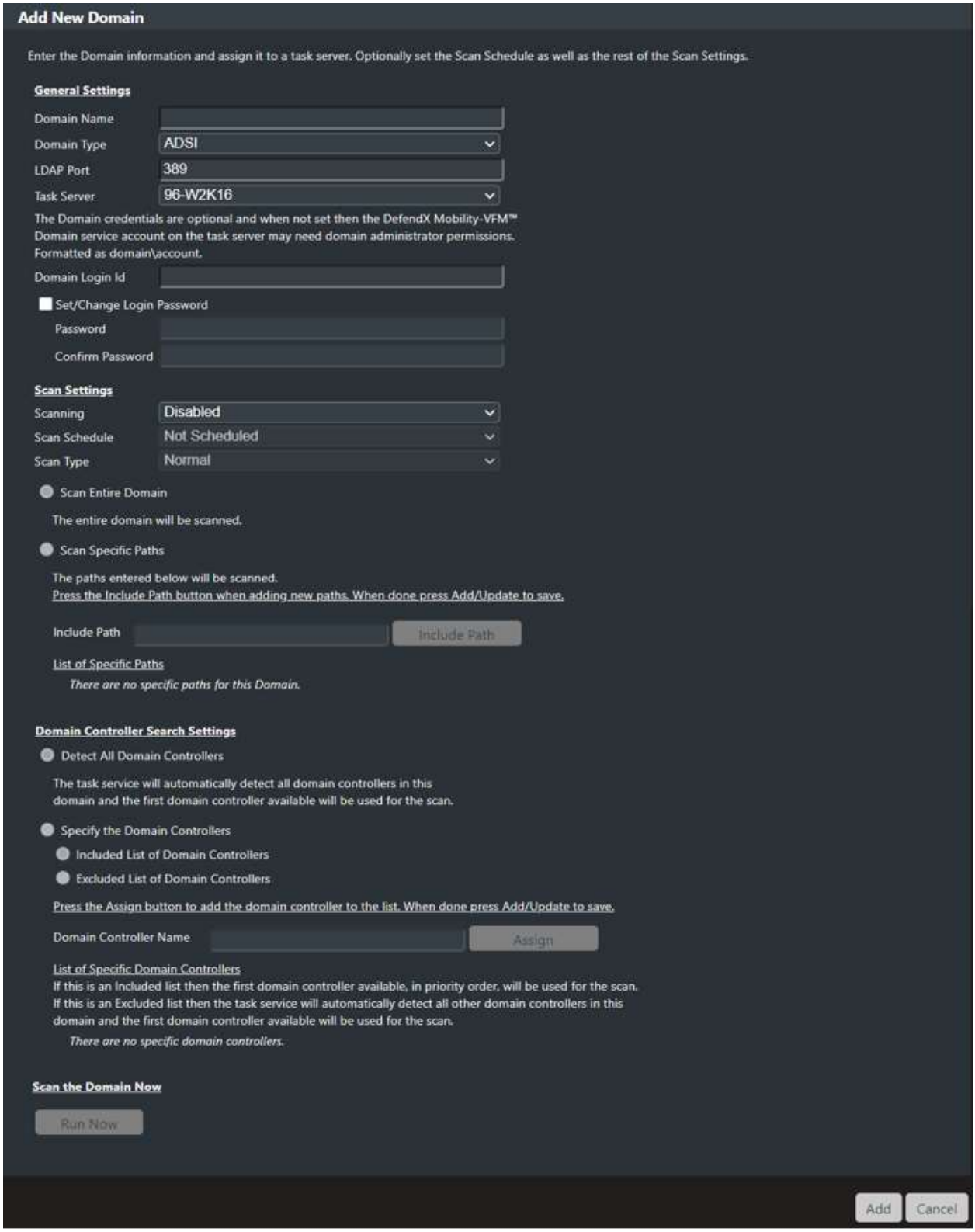
To add a new attribute to be captured for every file, click on the “New Attribute” button. This will bring up the Add Domain Field Screen. From the pull-down menu, select any of the pre-configured global attributes. This will populate the Attribute Name, Attribute Display name which is how it will be displayed in the DefendX Mobility VFM Admin pages, the Attribute type and if the attribute allows multiple values. These fields can also be entered manually and added to the list of Global domain attributes if the checkmark is selected at the bottom of the page.



Create new Domain

To scan a new domain that was not added in the original configuration of the Domain Agent, click on the configure domain button at the bottom of the list. This will bring up the “Add

New Domain” page where details for the domain can be specified as follows:



Domain Name: The name of the domain to scan. This must match the root domain in your environment as display by the Active Directory Users and Computers application.

Domain Type: Currently "ADSI", Active Directory Services Interface, is the only domain type that is supported (i.e., only active directory domains can be scanned).

LDAP Port: Port 389 is the default port for ADSI. If your domain uses a different port, then enter it here.

Task Server: This is the name of the Windows server where the Domain Agent was installed to.

Domain Login Id: A login Id and password are optional. If the Domain Agent's service account does not have permissions to the domain then you can enter an account here which has permissions. This account will then be used to scan the domain.

Scanning: If you want the Domain Agent to scan this domain then you must enable it.

Scan Schedule: If you want the domain to be scanned on a schedule then choose a schedule. Schedules are defined under the "Scheduling Configuration – Schedule Settings" page.

Scan Type: A scan type of "Normal" will collect domain attribute information for each user scanned and will store them in the Mobility stores database. A scan type of "Simulation" will collect information but will not store anything in the databases. This can be used to collect information of what will be collected.

Scan Entire Domain: When this is selected then all users in the domain, starting from the root, will have their attributes collected.

Configure Domains

To easily configure the schedule and type of scan for multiple domains, click on the "Configure Domains" after selecting one or more of the domains on the list. This button brings up the page where the scheduling details can be configured for the selected domains.

Scanning: Specifies if this domain will be scanned by the DefendX Mobility VFM Domain agent.

Scan Schedule: Allows the user to select when the domain scans will happen by selecting a schedule previously defined in the Schedule Configuration -> Schedule Settings section.

Scan Type: Allows the user to determine if this domain will be scanned or it will only run a simulation.

Schedule Configuration

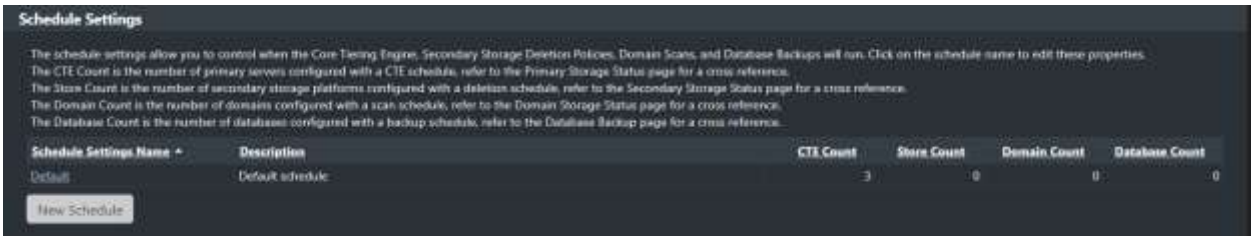
The Schedule Configuration section allows for building schedules for DefendX Mobility VFM components and policies to run at specific intervals and the creation of hours of operations that can be applied to scanning and tiering operations to limit the times that DefendX Mobility VFM components operate in the environment

Schedule Settings

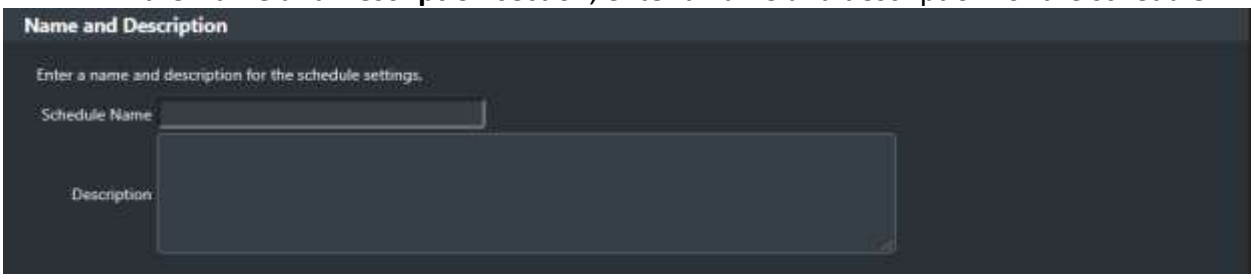
The **Schedule** settings allow you to control when the Core Tiering Engine, domain agent, database backup and Secondary Storage Deletion policies will run.

To configure Schedule settings, perform the following steps:

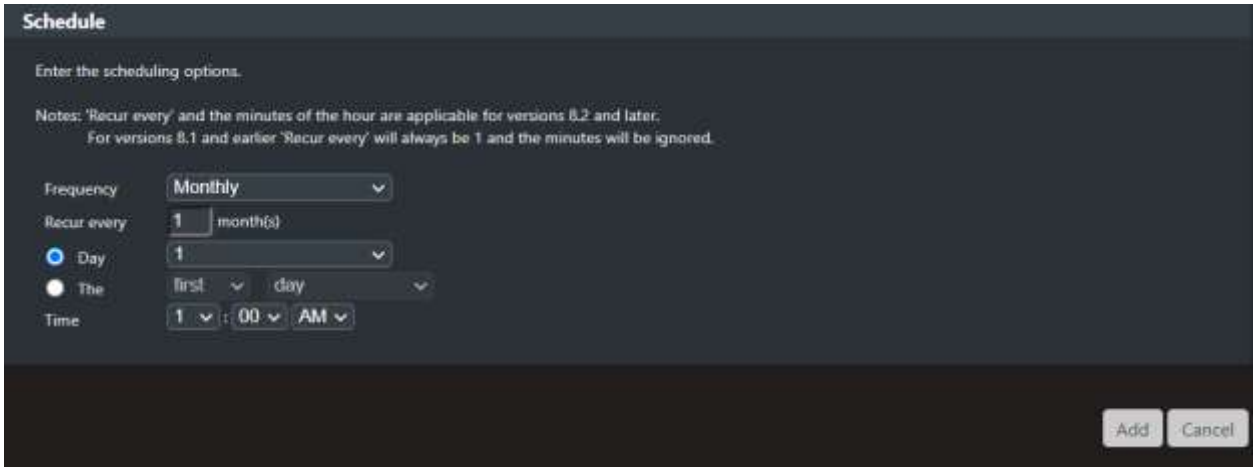
1. Click on a schedule name to edit its properties or click **New Schedule** to configure a new one.



2. In the **Name and Description** section, enter a name and description for the schedule.



3. In the **Schedule** section, provide the frequency, day, and time by which the schedule is to run and then click the **Add** button.

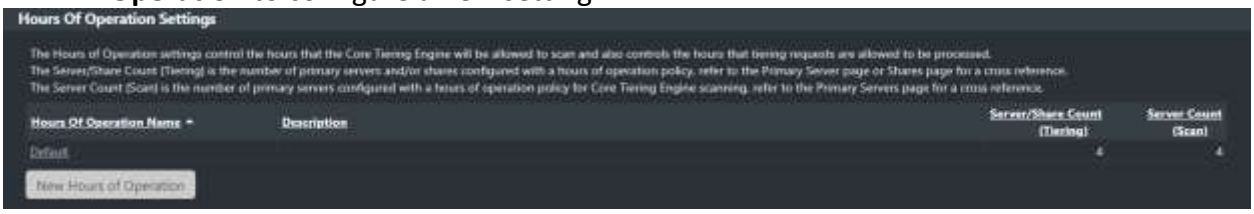


Hours of Operation Settings

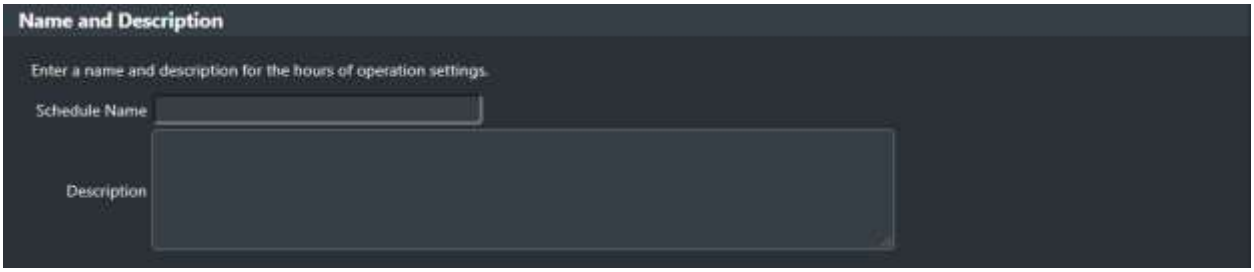
The Hours of Operation settings control the hours during which the Core Tiering Engine is allowed to scan, and tiering requests are able to be processed.

To configure Hours of Operation settings, perform the following steps:

1. Click an Hours of Operation name to edit existing settings or click **New Hours of Operation** to configure a new setting.



2. In the **Name and Description** section, provide a schedule name and description for the Hours of Operation schedule. The name can then be assigned to one or more primary servers.



3. In the **Hours of Operation** section, select the days and times by which the schedule will be defined. Hours can either be selected manually or by choosing one of the Include All, Working Hours, Exclude All, or Non-Working Hours presets.

Database Configuration

The Database Configuration section allows users to change the DefendX Mobility VFM Database configuration for both the databases that are used in the product. The Configuration Database contains all the application configuration settings such as passwords, store locations, shares, etc. The Stores Database maintains a record of every file that has been tiered in the environment. This section also allows for DefendX Mobility VFM controlled backups and restores of the database components.

Configuration Database Server Settings

This section shows the database settings that will store all configuration information.

The database settings were provided when DefendX Mobility VFM was installed. If you change the name of the database server or the name of the database here, then you must also do the same within SQL server.

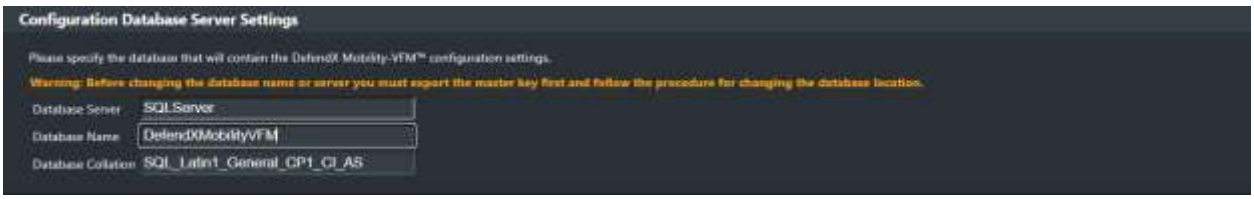
The database credentials were created automatically when DefendX Mobility VFM was installed. If you change the name or password of the SQL account here, then you must also do the same within SQL server.

NOTE: The password will be encrypted for security purposes.

To configure DefendX Mobility VFM database settings, perform the following steps:

1. Under Database Configuration in the left-hand main menu, click Database Config Settings. The Configuration Database Settings dialog is displayed.

2. On the **Configuration Database Server Settings** section, enter the name of the server and the name of the database.



NOTE: Please refer to the *Database Appendix*. The appendix has details on moving the database to another server if you choose to change the name of the database server.

To configure database security settings, perform the following steps:

1. Under Database Configuration in the left-hand main menu, click Database Config Settings. The Configuration Database Security Settings section is displayed.

2. The **Configuration Database Security Settings** section specifies how the website establishes a connection with SQL Server. The website can use either Windows integrated security or a SQL Server account. If a SQL Server account is chosen, the account name and password need to be specified. If Windows security is chosen, then the ODDMAdmin pool identity configured in IIS will be used to access SQL.

3. Apply any additional database connection settings.

4. Click the **Apply** button and then click **OK** to finish.

NOTE: If the Set/Change Password option is not checked, the password that is stored in the database is not changed.

Configuring Stores Database Server Settings

This section shows the configuration of the database that will store the objects that have been tiered.

The database settings were provided when DefendX Mobility VFM was installed. If you change the name of the database server or the name of the database here, then you must also do the same within SQL server.

The database credentials were created automatically when DefendX Mobility VFM was installed. If you change the name or password of the SQL account here, then you must also do the same within SQL server.

To configure stores database settings, perform the following steps:

1. Under Database Configuration in the left-hand main menu, click Database Stores Settings. The Stores Database Settings dialog is displayed.

2. On the **Stores Database Server Settings** section**,** enter the name of the server and the name of the database.

NOTE: Please refer to the *Database Appendix*. The appendix has details on moving the database to another server if you choose to change the name of the database server.

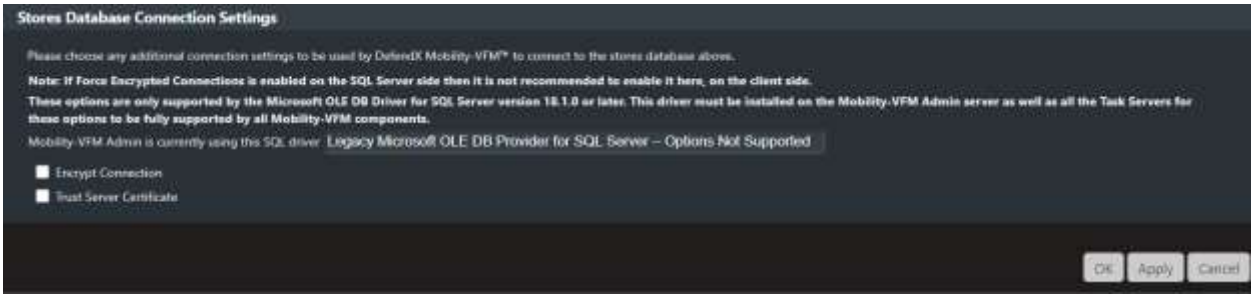
To configure stores database security settings, perform the following steps:

1. Under Database Configuration in the left-hand main menu, click Database Stores Settings. The Stores Database Security Settings section is displayed.

2. Specify the type of security to be used to connect to the stores database. The website can use either Windows-integrated security or a SQL Server account. If a SQL Server account is chosen, the account name and password need to be specified. If Windows

security is chosen, then the ODDMAdmin pool identity configured in ISS will be used to access SQL.

3. Apply any additional database connection settings.



4. Click the **Apply** button and then click **OK** to finish.

NOTE: If the Set/Change Password option is not checked, the password that is stored in the database is not changed.

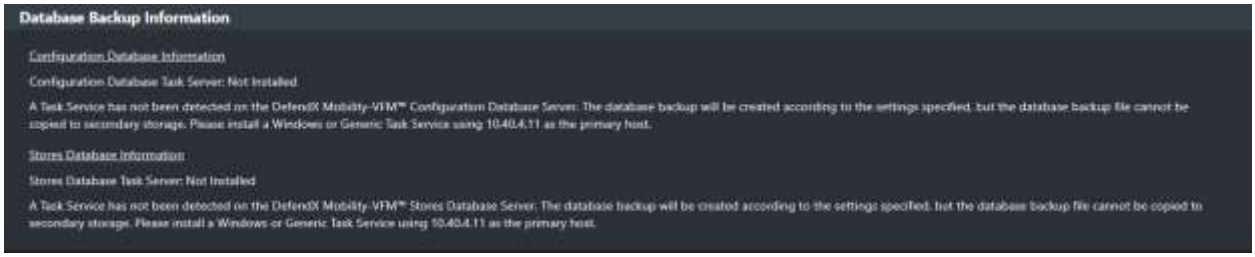
Configuring Database Backup

To configure database Backup settings, perform the following steps:

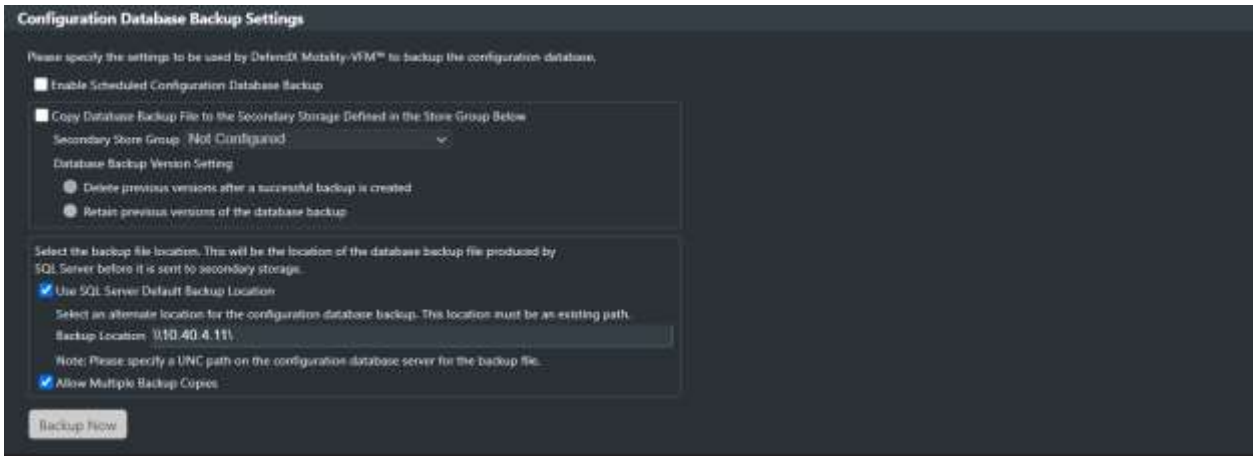
Note: A Task Service is required to be installed on the same server as the database server.

1. Under **Database Configuration** in the left-hand main menu, click **Database Backup**.

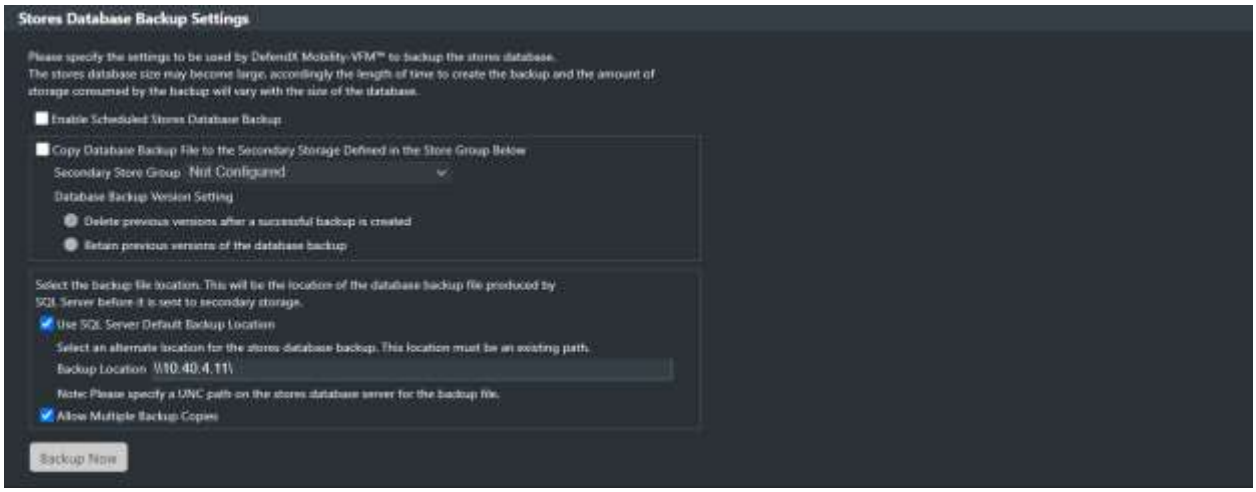
2. The **Database Backup Information** section displays information on configuration database and stores database.



3. In the **Configuration Database Backup Settings** section, specify the settings to be used by DefendX Mobility VFM to backup the configuration database.



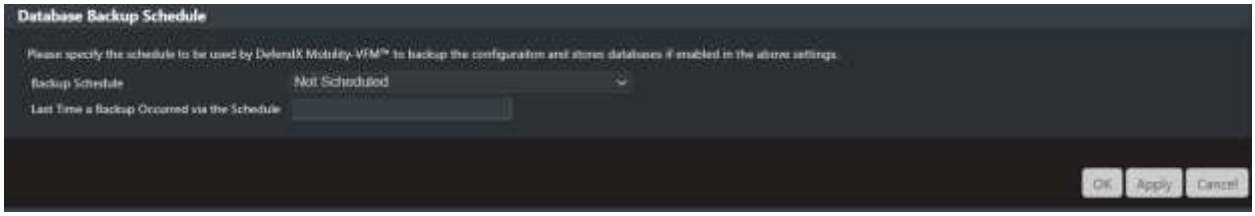
4. In the **Stores Database Backup Settings** section specify the settings to be used by DefendX Mobility VFM to backup the configuration database.



NOTES:

- When the *Copy Database Backup File to the Secondary Storage Defined in the Store Group* option is checked, the database will first be backed up to the *Backup Location* on the Windows server; therefore, a backup location must be selected. The database will then be tiered to the secondary stores defined in the storage group. After a successful tier, the previous databases in each of the secondary stores will be removed if the *Delete previous versions* is selected otherwise multiple backup copies will be kept on each of the secondary stores.
- Database backups can be very large in size which should be taken into consideration in choosing the correct options for your environment.
- When *Allow Multiple Backup Copies* is checked for the *Backup Location* then multiple copies of the database will be kept in that location. DefendX Mobility VFM does not maintain these copies so it is up to the administrator to delete the copies which are no longer wanted.

4. In the **Database Backup Schedule** section, specify the date to be used by DefendX Mobility VFM to backup the configuration and stores databases if enabled in the above settings.



Recovering Database

1. Under **Database Configuration** in the left-hand main menu, click **Database Recovery**.

2. The **Database Recovery** section displays information on the configuration database and stores database.

3. To recover a database that has been tiered to a secondary store, perform the following steps:

NOTE:

A Task Service is required to be installed on the same server as the database server.

a. Supply the UNC path to recover the database backup files to.
b. Press the appropriate *Recover* button for the database you want to recover.
c. Use SQL Server Management Studio to manually restore the database, from the UNC path, after it has been recovered from the secondary store.

4. To recover a database that has been backed up to the *Backup Location* defined in *Database Backup* page, perform the following step,

Simply use SQL Server Management Studio to manually restore the database from the Backup Location.

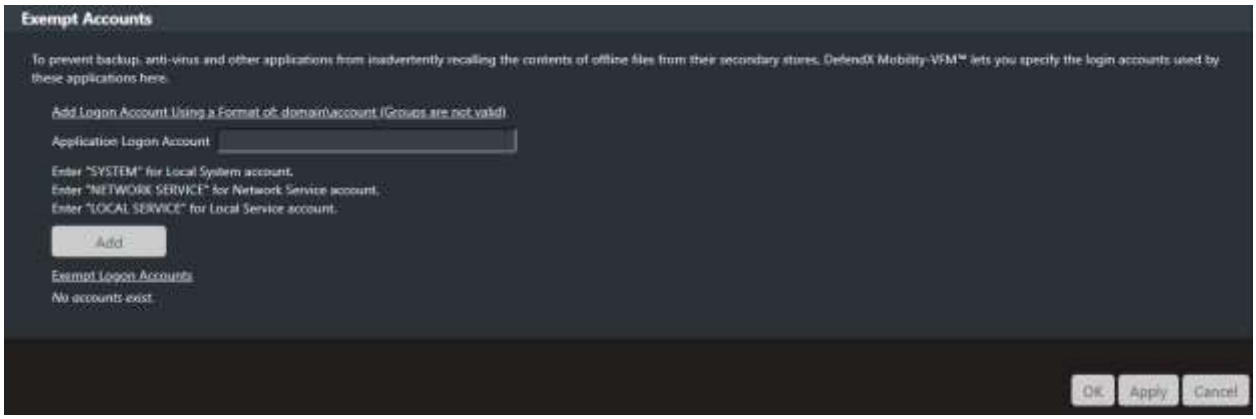
Account and Process Configuration

The account and process configuration section allows for specification of service accounts and/or processes that will be ignored by DefendX Mobility VFM if they request a file recall. These configurations are often used to prevent other applications such as backup from potentially recalling files that have been archived.

Exempt Accounts

Use the **Exempt Accounts** section to define the Windows accounts that are exempt from being able to auto-recall files from secondary storage. This is used to prevent applications that backup files on the primary servers or scan for viruses from recalling all files stubbed with the offline file attribute from secondary storage. Instead, the backup applications will backup the stub file without recalling its contents, and the anti-virus applications will scan the stub file instead of recalling its contents.

To add an exemption account, simply type in the name of the application's service login account and press the Add button. These accounts are global, i.e., used by all Task Services.



Note: For UNIX, type in the UID of the user for the Application Login Account.

Exempt Processes

Use the **Exempt Process** section to define the Windows processes that are exempt from being able to auto-recall files from secondary storage. This is used to prevent applications that backup files on the primary servers or scan for viruses from recalling all files stubbed with the

offline file attribute from secondary storage. Instead, the requesting process will receive the stub file without recalling its contents.

Note: The Exempt Processes are only applicable for the Task Services for Windows. Processes that are entered here will affect all Windows Primary servers. Each primary server can set its own exempt processes, using the MainConfig.xml file, which will override these.

To add an exemption process, simply type in the name of the process to be excluded. The process name can be found by launching the Task Manager and use the Name column value from the details tab to locate the process name.

Additional Configuration

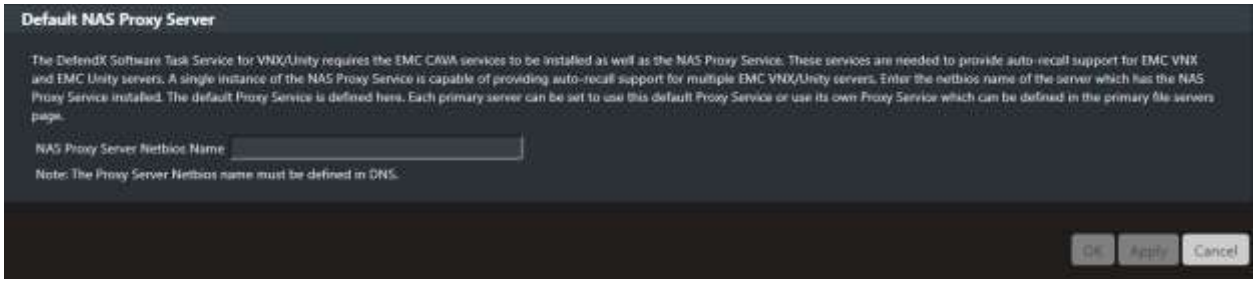
The Additional Configuration section allows for configuration of settings not associated with other sections on the DefendX Mobility VFM platform.

Default Download Location

When the DefendX Mobility VFM File Intranet, Recovery Portal or Access Portal Websites are used, the user is presented with a choice of options. One of the options is to recall or recover a tiered file to the download location. The default download location is defined at the DefendX Mobility VFM File Download UNC outlined. Each primary server can be set to use this default location or use its own location which can be defined in the primary file server page.

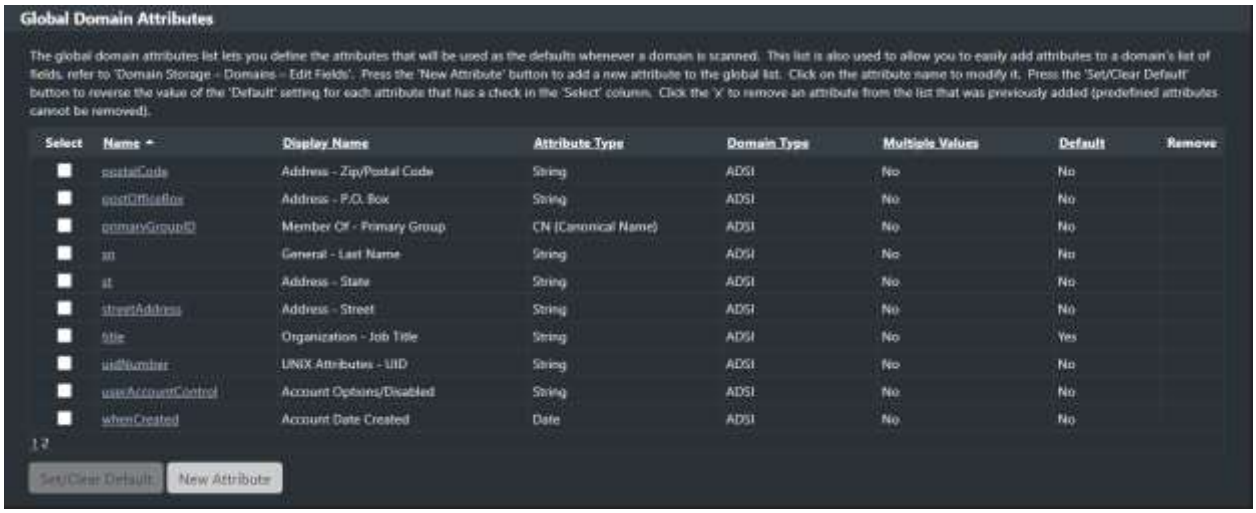
Default NAS Proxy Server

The Task Service for VNX requires the EMC CAVA services to be installed as well as the Proxy Service. These services are needed to provide auto-recall support for EMC VNX servers version 7.1.74.5 and later. A single instance of Proxy Service is capable of providing auto-recall support for multiple EMC VNX servers. Enter the NetBIOS name of the server which has the Proxy Service installed. Each VNX primary server can be set to use this default server or use its own proxy server which can be defined in the primary file server page.



Global Domain Attributes

The global domain attributes list lets you define the attributes that will be used as the defaults whenever a domain is scanned. This list is also used to allow you to easily add attributes to a domain's list of fields, refer to 'Domain Storage – Domains – Edit Fields'. Press the 'New Attribute' button to add a new attribute to the global list. Click on the attribute name to modify it. Press the 'Set/Clear Default' button to reverse the value of the 'Default' setting for each attribute that has a check in the 'Select' column. Click the 'x' to remove an attribute from the list that was previously added (predefined attributes cannot be removed).



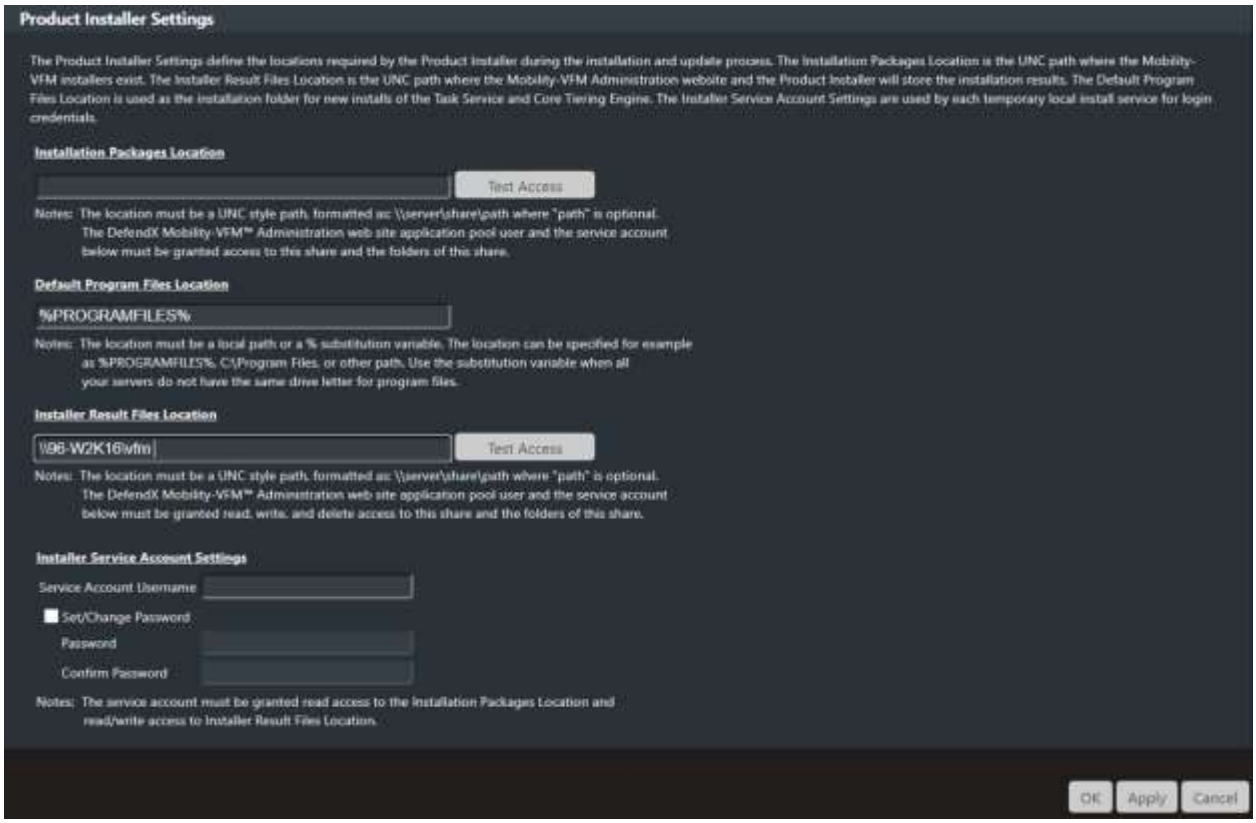
To Create a new attribute, click on the "New Attribute" button and specify the Attribute Name. The name of the attribute must match exactly with one that is defined for the Domain Type, for example ADSI (Active Directory). Define the Attribute Display name which is how it will be displayed in the DefendX Mobility VFM Admin pages. Select the Attribute type. An Attribute Type of 'string' is used to indicate that the attribute is either a string, a number or any other data type that is not otherwise listed in the dropdown. Specify if the attribute contains multiple values and whether it will be added to the default Domain Scan.

Product Installer Settings

The Product Installer feature of DefendX Mobility VFM allows for the ability to remotely install or upgrade Task Servers and Core Tiering engines in the environment. There are two new pages to support the product install feature. "**Primary Storage – Task Servers**" page that allows the actual push of the installers to the new locations and the "**Additional Configuration – Product Installer Settings**" page that configures the requirements for the push installer.

Note: After installing the DefendX Mobility VFM Admin you must fill in the missing information on the "Additional Configuration – Product Installer Settings" page required for push installs.

The Product Installer Settings Page contains the locations, default paths, and accounts to be used for the installation or upgrade process.



Installation Packages Location: This is the first share name, UNC Path, required for push installs. Refer to the "Additional Requirements To Support Push Installs" above for further explanation.

Default Program Files Location: This is the default parent location on each Task Server to install the Task Services and Core Tiering Engine.

Note: "Defend Software\Mobility\Task Service\<type>" will automatically be appended to this path when a Task Service is installed and "Defend Software\Mobility\Core Tiering Engine" will automatically be appended to this path when a core tiering engine is installed. Therefore, do not include them in this location. If you want to use a parent location of "\Program Files (x86)" on all of your servers on the drive that the OS is installed upon then use "%PROGRAMFILES86%" as the location.

Installer Results Files Location: This is the second share name, UNC Path, required for push installs. Refer to the "Additional Requirements To Support Push Installs" above for further explanation.

Installer Service Account Settings: This account will be used by the product installer service when temporarily installing a local service on each of the servers where a push install will occur. This account can be the same as the account used by the product installer's service. This account must be an administrator on each of the servers where a push install will occur.

Note: Additional Requirements to Support Push Installs.

- A share name is required which will allow access to the location of VFM's installation packages. This share name and its directories must give the VFM™ Administration web site application pool user as well as the product installer's service login account read access.
- Another share name is required which will allow the DefendX Mobility VFM Admin to create XML files for which the product installer service will also monitor. The XML files will define all the necessary settings for push installations. The XML file will also be updated by the product installer service to change the status of the push install as well as to include any messages or errors from the install. This share name and its directories must give the VFM™ Administration web site application pool user as well as the product installer's service login account read, write and delete access.

Notification Configuration

The Notification Configuration section is used to configure outbound mail settings and to select or modify which events will trigger email warnings in DefendX Mobility VFM.

Note: If the “Mail Settings” section has not been configured then the tree menu item will be displayed in orange.

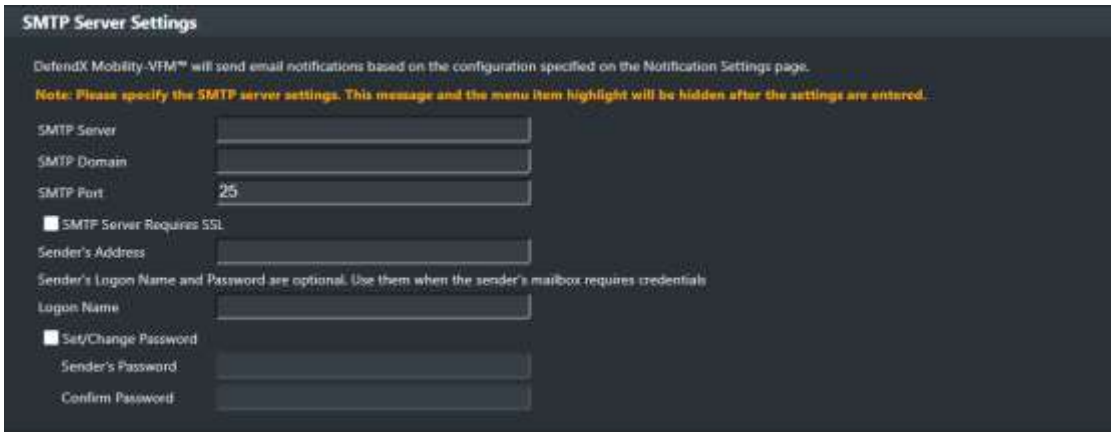
Mail Settings

DefendX Mobility VFM can send out notifications to end users when their requests have been successfully completed. If you want the DefendX Mobility VFM web application to send email notifications and alerts, then you need to provide the SMTP settings here.

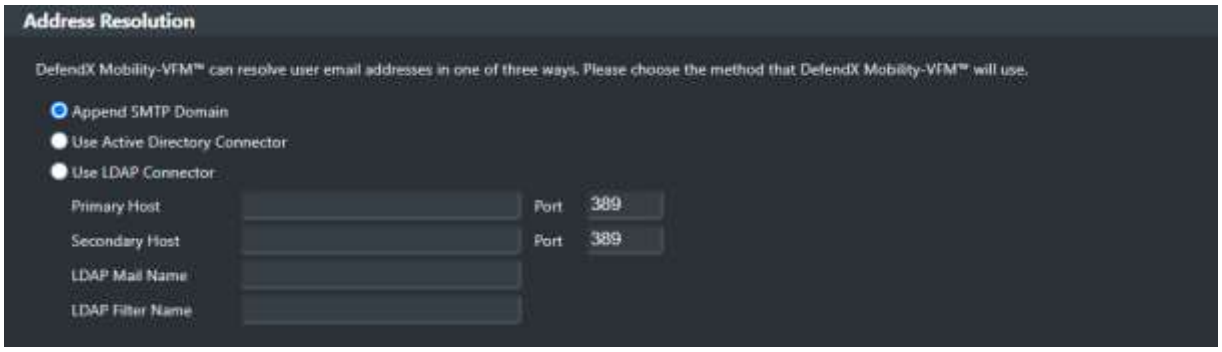
To configure the mail settings, perform the following steps:

1. Under **Notification Configuration** in the left-hand main menu, click **Mail Settings**. The **SMTP Server Settings** section is displayed.

2. Add in the SMTP server name, SMTP domain, and sender’s address. Enter the SMTP sender’s password only if the SMTP server uses secure authentication.



3. In the **Address Resolution** section, select the option to append the SMTP domain, use the Active Directory connector, or use the LDAP connector.



The table below will help you configure the mail settings:

Field	**Description**
Append SMTP Domain	The user's email address will be determined by concatenating the user's login account name with the name of the SMTP DNS Domain specified above in the SMTP Server Settings.
Use Active Directory	The user's email address will be determined by looking up the user's account in active directory and extracting their primary email address.
Use LDAP	The user's email address will be determined by looking up the user in another LDAP database other than active directory. A search will be done based on the values returned by the *LDAP Filter Name* attribute against the user's account. If a match is found, then the user's email address will be extracted from the value of *LDAP Mail Name* attribute.
Primary Host	This is the name or IP address of your active directory or LDAP server that will be used first for searching.
Primary Port	This is the LDAP port number, usually 389.
Secondary Host	This is the name or IP address of your active directory or LDAP server that will be used second for searching. This is optional.
Secondary Port	This is the LDAP port number, usually 389.

LDAP Mail Name	Refer to *Use LDAP*. This is the name of the attribute used to store user email addresses, for example, mail.
LDAP Filter Name	Refer to *Use LDAP*. This is the name of the attribute used to store usernames, for example, uid.

NOTES:

- If you want the DefendX Mobility VFM web app to send email notifications back to the users who sent a tier or recall request, then you must provide a mechanism for the web app to determine the user's email address.
- The Primary Host and Port are required for the "Use Active Directory" or "Use LDAP Connector" options.
- The Secondary Host and Port are optional for the "Use Active Directory" or "Use LDAP Connector" options. If the user's email address was not found using the primary server, then the secondary server will be searched.
- The LDAP Mail Name and Filter Name are required for the "Use LDAP Connector" option.

4. In the **Mail format** section, select either **HTML** or **Plain Text** mail format.

5. Test Email Settings

Notification Settings

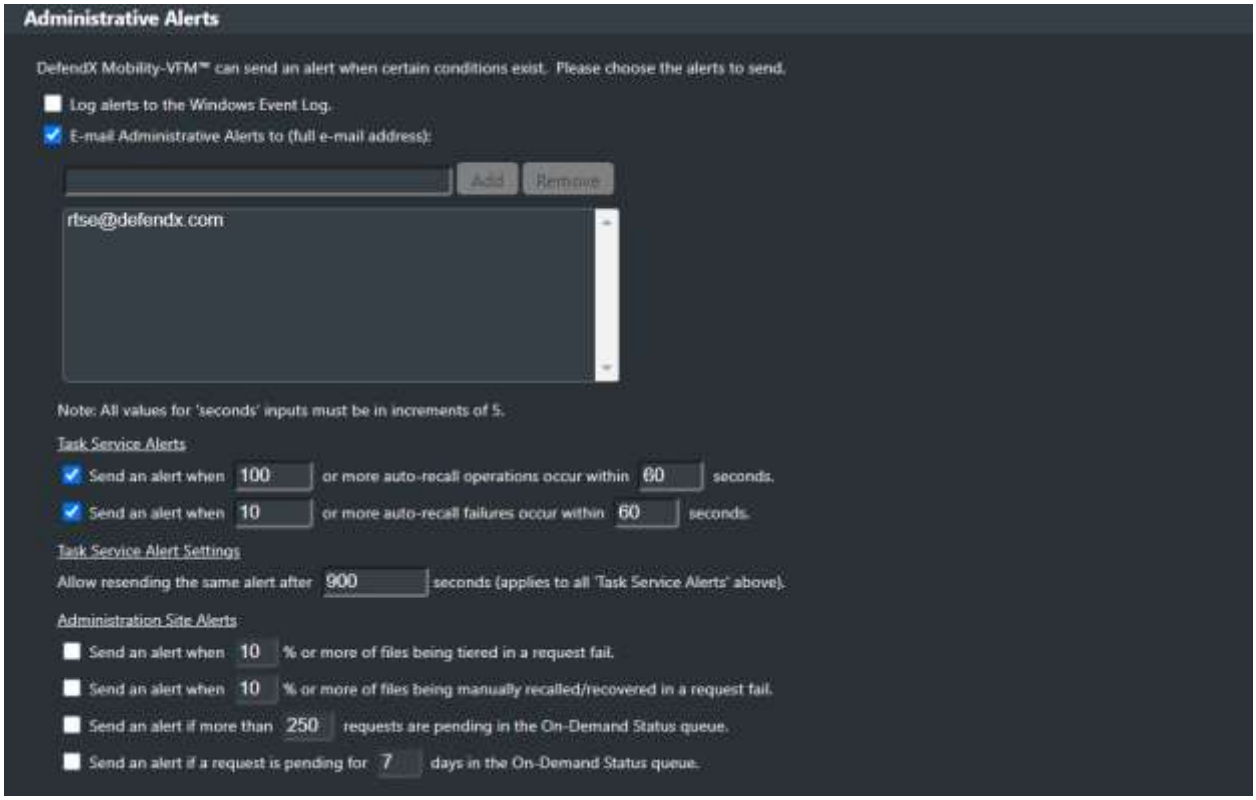
User notifications are emails sent to the user making the data movement request. DefendX Mobility VFM can email an acknowledgment to users to notify them that their request has been successfully received. It also emails the results of the request to the user and provides the option to email the results to other recipients.

Configuring Administrative Alerts

The DefendX Mobility VFM web app can send email notifications to a list of recipients, such as administrators, whenever one or more alerts are generated. An entry to the application event log can also be created. Administrative Alerts assist the administrator with troubleshooting data movement requests. Alerts are based on events that are triggered when a request fails or when a request is pending for a period of time. Alerts can be emailed to a list of those people by specifying the users or a distribution list.

To configure the administrative alerts, perform the following steps:

1. Under Notification Configuration in the left-hand main menu, click Notification Settings. The Administrative Alerts section is displayed.

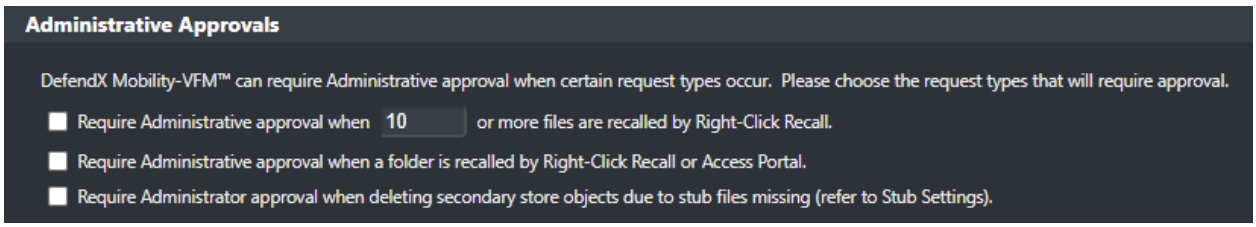


2. Select the type of alert you want to send.

3. Select one or more options determining when you want to have an alert sent.

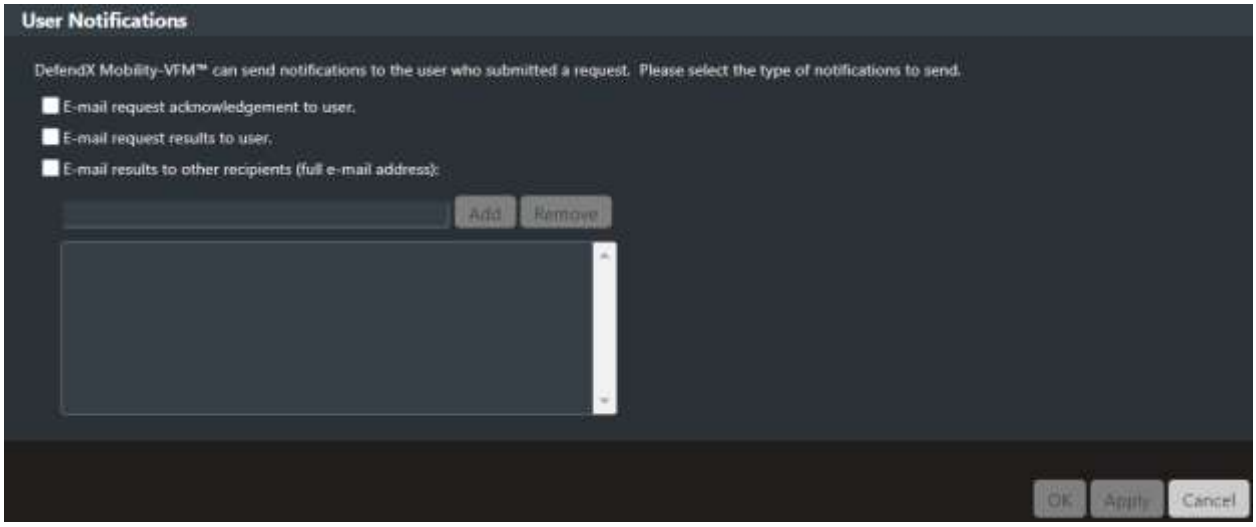
4. Click **Apply** and then click **OK** to finish.

DefendX Mobility VFM can require Administrative approval when certain request types occur. The purpose of the Administrative approval is to provide a safety mechanism for certain events that could either delete or recall large amounts of data. To configure Administrative approvals, choose the request types that will require approval.



To configure the user notifications, perform the following steps:

1. Under **Notification Configuration** in the left-hand main menu, click **Notification Settings**. The **User Notifications** section is displayed.



2. Select the type of notifications you want to send and then specify to whom you want to send the notification(s).

3. To send notifications to other recipients, you need to add a username or a distribution list that exists within Active Directory so that other recipients can receive the data movement results.

4. Click **Apply** and then click **OK** to finish.

License and Assessment information

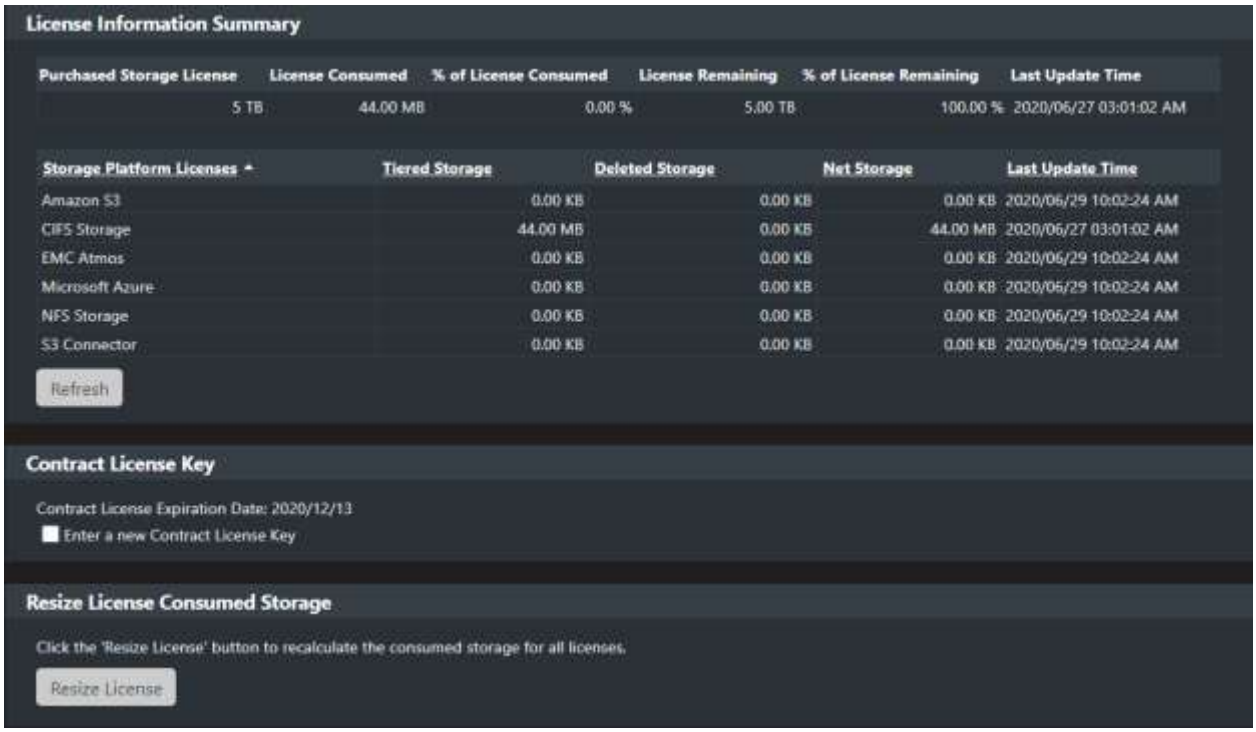
The License and Assessment Information section provides a view of the consumption of DefendX Mobility VFM licensing and perform license maintenance operations. It also allows for transmittal of license information to DefendX Software and management of file system assessments.

License Information Summary

The license Information Summary page presents a view of the current license consumption of the system. The License Information summary provides a table that outlines the purchased license capacity, the total license consumption, the percentage of the consumption, the remaining licensing and the percentage of the total licensed capacity, and the timestamp of the last update.

The view also provides capacity information for all secondary store platforms around the capacity that has been tiered, deleted, and the net storage in that platform. Net storage is defined as the tiered storage minus the deleted storage and can be used as a gauge on how much storage is on any specific platform at the time of the licensing query.

Note: the platform totals are for all storage locations on each particular platform. For example, if a user has three buckets in Amazon S3 storage, each with 2TB of capacity tiered, the total will be 6TB.



The Contrack License Key section updates the capacity-based key for the product. A new license key will be issued if you increase your license capacity for your DefendX Mobility VFM product. Updating your license key is very straightforward. Select the checkmark labeled “Enter a new Contract License Key.” This will enable a text field where the license key can be pasted. Once pasted press the update button.

DefendX Mobility VFM calculates licensing consumption every night. The Resize License Consumed Storage section recalculates the licensing to give a more current update. Click the 'Resize License' button to recalculate the consumed storage for all licenses.

License Information File Generator

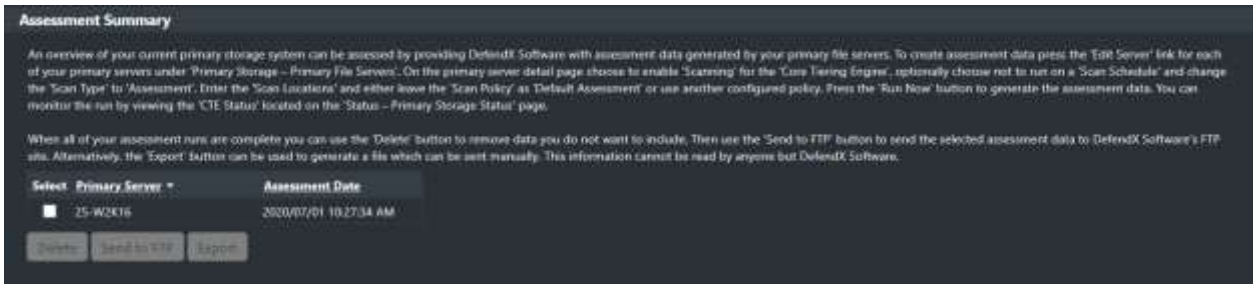
DefendX Software collects license capacity statistics from our products. This information is typically sent to our servers automatically. For some customers this may not be possible. In order to facilitate licensing compliance checks, the License Information File Generator can be used. Clicking the “Generate and Download” button will create a secure, encrypted file that contains the license information about the installation. This information cannot be read by anyone but DefendX Software.

Assessment Information Summary

When all your primary file servers have been assessed then use this page to select the servers you want to include in the assessment report. The assessment report will be generated by DefendX Software and therefore the data can either be FTPed to DefendX Software's FTP site or it can be exported and sent using another mechanism such as email.

Only the most recent assessment data for each server will be displayed on this page. Therefore, you can perform another assessment for one or more of the listed servers if you find the Scan Policy needs to be changed or the Scan Locations need to change.

Note: All data is encrypted when either FTP or Export is selected.



Delete: If you want to remove unwanted assessments then Select each Primary Server and press the Delete button.

Send to FTP: Select the Primary Servers you want to include in the assessment report and press the Send to FTP button to encrypt and send the data to DefendX Software's FTP site.

Export: Select the Primary Servers you want to include in the assessment report and press the Export button to encrypt and save the data to a file. You can send the data file to DefendX Software via email or some other mechanism.

Database Appendix

DefendXMobilityVFM: This is the configuration database; it holds configuration data as well as queued and completed request data.

DefendXMobilityVFMStores: This is the stores database; it holds all tiered file data.

Moving VFM Databases from one SQL Server to Another

Step 1: VFM Task Services:

- Stop all VFM Task Services.

Step 2: VFM Administration:

- View the "Database Configuration – Database Config Settings" page and note the name of the SQL Login Account. By default, it will be "oddm_web_svc". If it is a different name, then substitute that name for "oddm_web_svc" in all sections below.

Step 3: Old SQL Server:

- Open SQL Management Studio on the old SQL Server and backup both existing VFM databases.

Step 4: New SQL Server:

- Open SQL Management Studio on the new SQL Server, right click on "Databases" and choose "Restore Database". Do this for both VFM databases.
- When the restores are complete, expand "Security – Users" for each VFM database and delete the "oddm_web_svc" user, (The SID is wrong and therefore this account needs to be deleted and readded). Do this for both VFM databases.
- Re-dd the "oddm_web_svc" account to SQL Server.
    - Select "New Login" under "Security-Logins".
    - General Section:
        - Choose SQL authentication and enter "oddm_web_svc" for the Login Name.
    - Server Roles:

        - Check Public.
    - User Mappings:
        - Check both VFM databases.
        - For each VFM database check: db_backupoperator, db_datareader, db_datawriter, public.
- Grant the “oddm_web_svc” permissions to execute stored procedures.
    - Highlight the DefendXMobilityVFM database and press the “New Query” button.
    - Copy the contents of the “odagrant.sql” script to the query window and press Execute. The odagrant.sql file can be found on the Windows server where the VFM Administration component was installed. The default location is: “C:\Program Files\DefendX Software\Mobility-VFM\DBScripts”.
    - Highlight the DefendXMobilityVFMStores database and press the “New Query” button.
    - Copy the contents of the “odagrantstores.sql” script to the query window and press Execute.
- Add the VFM Task Service account to SQL Server.
    - Select “New Login” under “Security-Logins”.
    - General Section:
        - Choose Windows authentication and enter “domain\account” that the VFM Task Service uses.
    - Server Roles:
        - Check Public.
    - User Mappings:
        - Check both VFM databases.
        - For each VFM database check: db_backupoperator, db_datareader, db_datawriter, public.
- Grant the VFM Task Service account permissions to execute stored procedures.
    - Highlight the DefendXMobilityVFM database and press the “New Query” button.
    - Copy the contents of the “odagrant.sql” script to the query window.
    - Replace “oddm_web_svc” with “[domain\account]”, (surround the account with square brackets as shown).
    - Press Execute.
    - Highlight the DefendXMobilityVFMStores database and press the “New Query” button.
    - Copy the contents of the “odagrantstores.sql” script to the query window.
    - Replace “oddm_web_svc” with “[domain\account]”, (surround the account with square brackets as shown).
    - Press Execute.

Step 5: VFM Administration – Verify Database Connectivity:

- Select the “Database Configuration – Database Config Settings” page.

    - Enter the name of the new database server.
    - Optionally enter user “oddm_web_svc” and its password. The default is “OddmS3rv1ceAcct”.
    - Press the Apply button.
- Select the “Database Configuration – Database Stores Settings” page and perform the same steps as above.
- Select the “Home” page to verify that the database settings are correct. There should be no errors displayed.

Step 6: VFM Task Services:

- Start all VFM Task Services.

Step 7: VFM Administration – Verify Task Services:

- Select the “Primary File Server Status” page and view the status of each Task Service. Each should show as “Idle” after about 5 minutes.

Step 8: Task Services - Verify Database Connectivity:

- Use VFM Right-Click to tier a sample file. Verify that the file was tiered by viewing the “Status – On-Demand Status – Completed Requests” page.

Windows Cluster Server Appendix

Configuring VFM to Operate in a Windows Cluster Server Environment

Note: VFM currently supports a two-node cluster; however, if your environment has more than two nodes then you must choose two nodes to use with VFM.

Step 1: Installing the Task Service for Windows on the cluster server nodes.

- Install a VFM Task Service for Windows on each of the Cluster server nodes.
- In the DefendX Mobility VFM Administration web site wait for each of the Task Servers to display on the Primary Servers page.
- Decide whether or not you want to allow tiering of files located on each of the Task Servers' local shares. The answer to this is usually no since these shares are not part of the cluster resources.
- Select the Primary Servers page and click on each of the primary server names that correspond to the cluster nodes.
    - If you do NOT want to allow tiering on the local nodes, then set "Tiering" to "Disabled".

Step 2: Configuring the VFM Task Services for Windows for use with the Windows Cluster.

- On the Primary Servers page, click on the "New Primary Server" button.
- Check the checkbox: "The Primary Server name represents a File Server in the Cluster".
- Enter the FQDN name of the cluster in the "Primary Server" field.
- Select one of the Windows Task Servers installed on the cluster server nodes, from the drop down, to be used as the initial "Task Server". It will process tiering requests issued from any of the clustered shares. It is recommended to use the server which currently has control of the quorum.
- Select the other Windows Task Server installed on the other cluster server node, from the drop down, to be used as the "Failover Task Server".
- Select the rest of your configuration options.

Step 3: Enabling Auto-Recall for the Cluster

- If the Task Service will be stubbing files located on the clustered resources as active stubs, i.e., setting the offline file attribute then:

- Select the Primary Servers page and click on each of the primary server names that correspond to the cluster nodes and the cluster server.
- Check the checkbox to “Enable the file filter for offline events”. (Do this for both nodes of the cluster as well as the cluster server).
- For auto-recall to function properly, both cluster nodes and the Cluster server must be configured to use the same exact secondary store group, otherwise auto-recall may fail trying to retrieve a replicated file on the secondary storage device.

Controlling User Access to the DefendX Mobility VFM Administration Website Appendix

Step 1: Open Internet Information Services (IIS) Manager.

- Expand the Default website and select “VFMAdmin”.

Step 2: Ensure that Windows Authentication is turned on for the Administration site

- Double click on Authentication and ensure Windows Authentication is enabled and all other authentication methods are set to disabled.
- This will allow the Task Services, the Access and Recovery Portal and the FileIntranet sites access to the Administration site.

Step 3: Enabling SSL on the Administration Web Site

- Double click on SSL Settings and check the “Require SSL” checkbox.
- NOTE: During installation of the other Mobility components, you may be prompted to supply the name of the administration web site. Use “https” instead of “http” when SSL has been enabled here. Also, include the port number when not using port 80. If the components have already been installed, then refer to Step 9 below.

Step 4: Allowing Authorization to specific users and groups to access the DefendX Mobility VFM Administration site.

- Go to the VFM Administration component installation folder, by default it is installed here: “C:\Program Files\DefendX Software\Mobility-VFM\Web”
- Open the “Web.config” file in a text editor.
- To allow specific users place the following xml directly underneath this tag: <authentication mode="Windows"/>.
- Note: Separate each user account with a comma.

```
<authorization>
<allow users="domainname\user1,domainname\user2,domainname\user3" />
<deny users="*" />
</authorization>
```

- To allow specific groups place the following xml directly underneath this tag: <authentication mode="Windows"/>.

```
<authorization>
<allow roles="domainname\group1,domainname\group2,
domainname\group3" />
<deny users="*" />
</authorization>
```

- Note: To allow both users and groups then combine <allow users>, <allow roles> and <deny users> into a single <authorization> section.

Step 5: VFM Task Service Accounts need to be Authorized when authorization to specific users and groups was configured above.

- The login accounts for each Task Service must be entered in the list of “allow users”, otherwise the Task Service will not be able to communicate with the DefendX Mobility VFM Admin site.

Step 6: VFM Access and Recovery Portals and the VFM FileIntranet sites need to be Authorized when authorization to specific users and groups was configured above.

- If one of the components is installed on the same host as the DefendX Mobility VFM Admin site, then add **“NT AUTHORITY\NETWORK SERVICE”** to the list of “allow users”.
- If one of the components is installed on a different host than the DefendX Mobility VFM Admin site, then add **“Domain\Host$”** to the list of “allow users”, where Domain is the name of the domain that the host is in, and Host$ is the NetBIOS name of the host followed by the dollar symbol.

Step 7: VFM Administration Web Site Prompt for Credentials when authorization to specific users and groups was configured above.

- When a user is logged on as one of the accounts in the “allow users” list, they should not be prompted for credentials when accessing the DefendX Mobility VFM Admin site because Windows Authentication will automatically allow them access. This is usually the case when using Microsoft Edge or Internet Explorer. Other browsers may still prompt for credentials unless specific NTLM settings are applied to the browser as described below.
- When a user is logged on with an account that is not in the list, then they will be prompted for credentials

Step 8: Enabling NTLM Authentication on Firefox.

- Firefox may always prompt for credentials even when logged on as an account in the “allow users” list; however, the following options can be set to try and avoid the prompt.
- Type “about:config” in Firefox’s address bar and then click OK.
- In the search/filter type: “network.automatic-ntlmauth.trusted-uris”
- Double click the one item in the list and enter this into the dialog box (replacing servername with the name of your web server): http://servername/VFMAdmin
- Note: If SSL was configured for the administration web site then use “https” instead of “http”.

Step 9: SSL Configuration for DefendX Mobility VFM Components.

- When SSL is enabled on the administration web site then the following components must be configured to use “https” instead of “http” to be able to access to the DefendX Mobility VFM Admin site.

    - The format of the URL should be either:
    - http://WebServer:80/VFMAdmin/ODDMService.asmx
    - (A port must be specified unless using port 80 which is the default port and is optional).
    - https://WebServer:443/VFMAdmin/ODDMService.asmx
    - (A port must be specified unless using port 80 or 443 which are the default ports for http/https and is optional).
- For each VFM Task Service
    - Go to its installation directory, default is: "C:\Program Files\DefendX Software\Mobility-VFM\Task Service\<platform>".
    - Edit the MainConfig.xml file.
    - Change the <URL> value to use https and include the port number when different than port 443.
    - Save the file and restart the Task Service.
- For the VFM Access and Recovery Portals and the VFM FileIntranet sites
    - Go to their installation directory, default is: "C:\Program Files\DefendX Software\Mobility-VFM\<component>".
    - Edit the Web.Config file.
    - Change "http" to "https" and include the port number when different than port 443 for each line found, i.e., there may be multiple lines in each web.config file that contains the "ODDMService.asmx" URL.
- For Right-Click Data Movement (RCDM)
    - Open the registry by running "regedt32".
    - "HKEY_LOCAL_MACHINE\SOFTWARE\DefendX Software\ DefendX Mobility-VFM Right-Click Tiering\Data".
    - Change the value for "OddmUrl" to use "https" and include the port number when different than port 443.
    - For this new setting to take effect you must close all Windows Explorers and Control Panel windows and then obtain a new Windows Explorer window. If the change still does not take effect, then logoff and back on to your workstation.
- For Event-Driven Data Movement (EDDM)
    - Go to its installation directory, default is: "C:\Program Files\DefendX Software\Mobility-VFM\EDDM".
    - Edit the cseda.inf file.
    - Change the value for "OddmUrl=" to use "https" and include the port number when different than port 443.
    - Save the file.

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#DFX1211EF