DefendX Software

DefendX Software Mobility ™ Administration Web Site

User Manual
Version 7.5

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™. The latest addition to the DefendX Software® product portfolio, DefendX Software Mobility 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 Software Mobility 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 Software Mobility 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 Software Mobility 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 web admin's server to your local intranet sites. If this option is disabled then the admin site's left-hand main menu will not be able to expand.

DefendX Software Mobility Administration Site Configuration

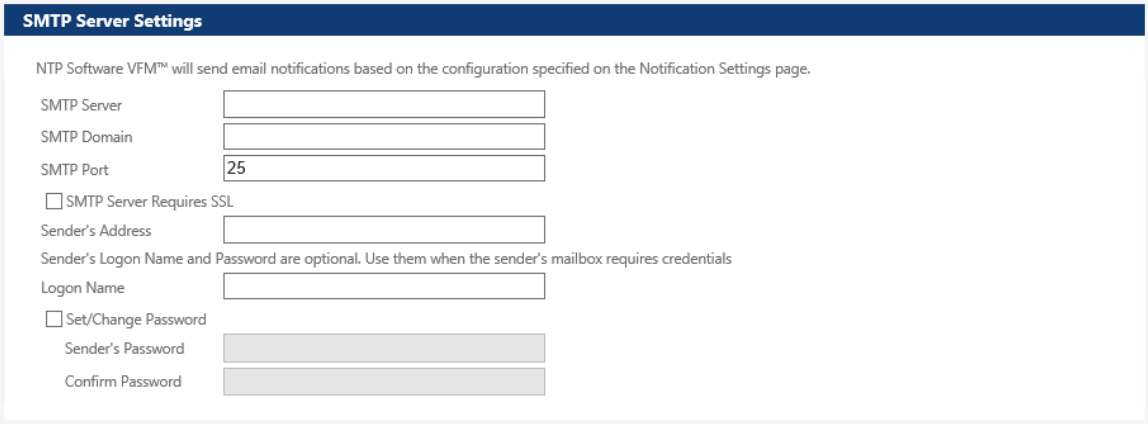
Configuring Mail Settings

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

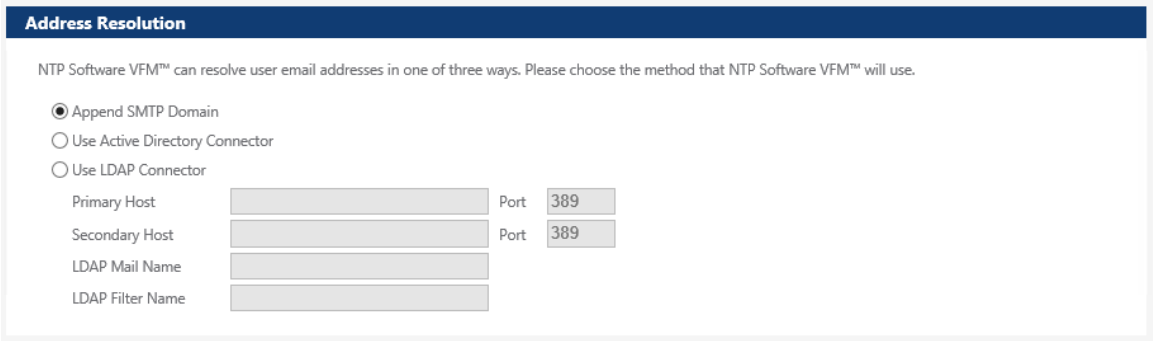
To configure the mail settings, perform the following steps:

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.



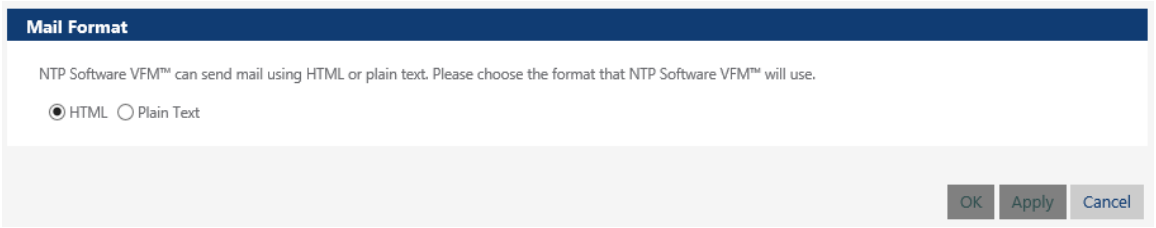
The table below will help you configure the mail settings:

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 user names, for example, uid.

NOTES:

- If you want the DefendX Software Mobility 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.

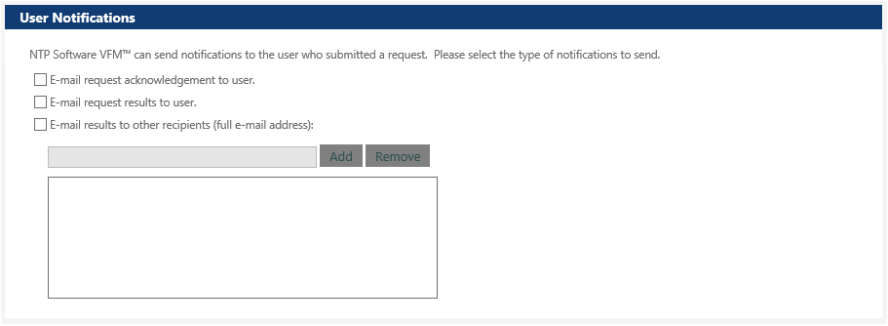


Configuring User Notifications

User notifications are emails sent to the user making the data movement request. DefendX Software Mobility 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.

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.

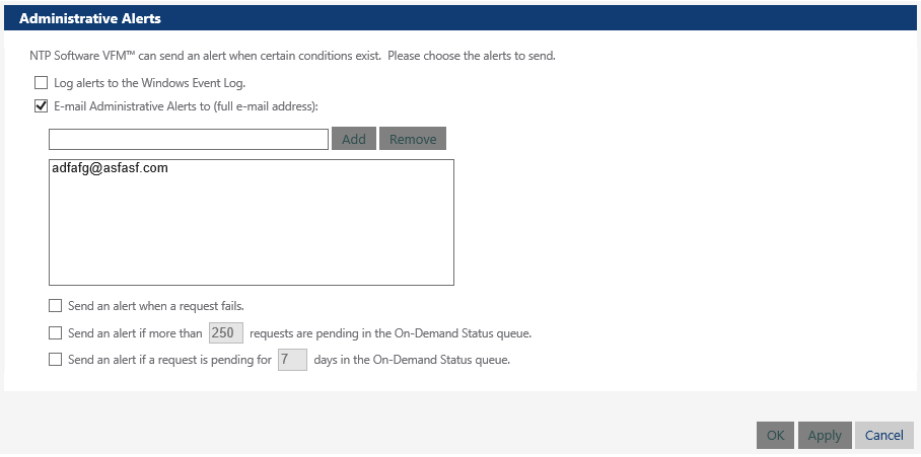
4. Click **Apply** and then click **OK** to finish.

Configuring Administrative Alerts

The DefendX Software Mobility 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.

Configuring Database Server Settings

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

The database settings were provided when DefendX Software Mobility 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.

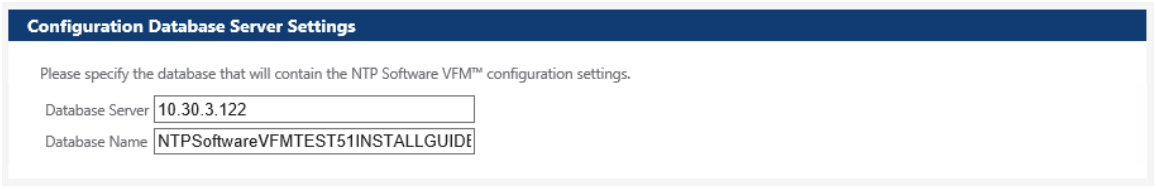
The database credentials were created automatically when DefendX Software Mobility was installed. If you change the name or password of the SQL account here, then you must also do the same within SQL server.

NOTE: The password will be encrypted for security purposes.

To configure DefendX Software Mobility 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.



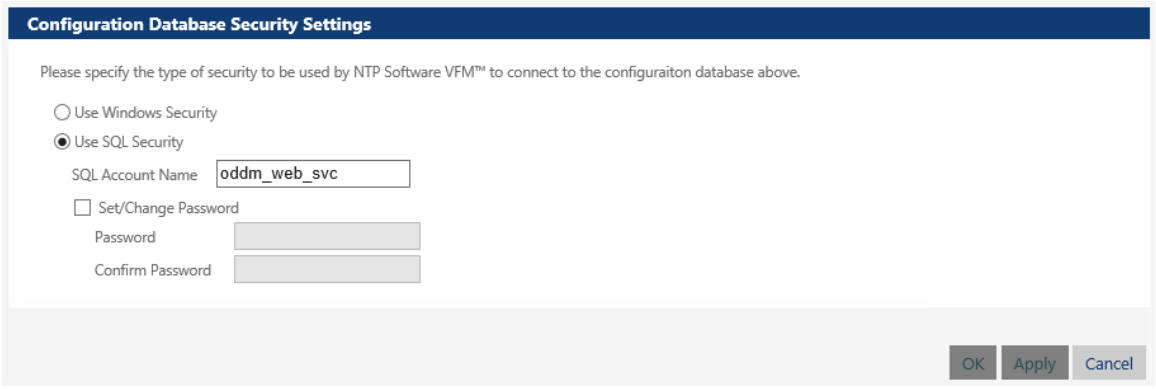
NOTE: Please refer to the *Database Appendix*. The appendix has details on moving the database to another server if you choose to change the name of the database server.

Configuring Database Security Settings

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. 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.

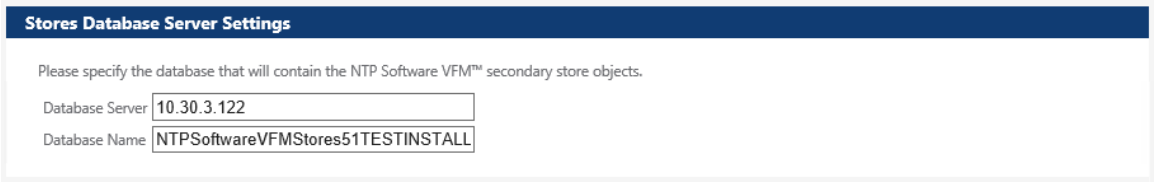
The database settings were provided when DefendX Software Mobility was installed. If you change the name of the database server or the name of the database here, then you must also do the same within SQL server.

The database credentials were created automatically when DefendX Software Mobility 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.



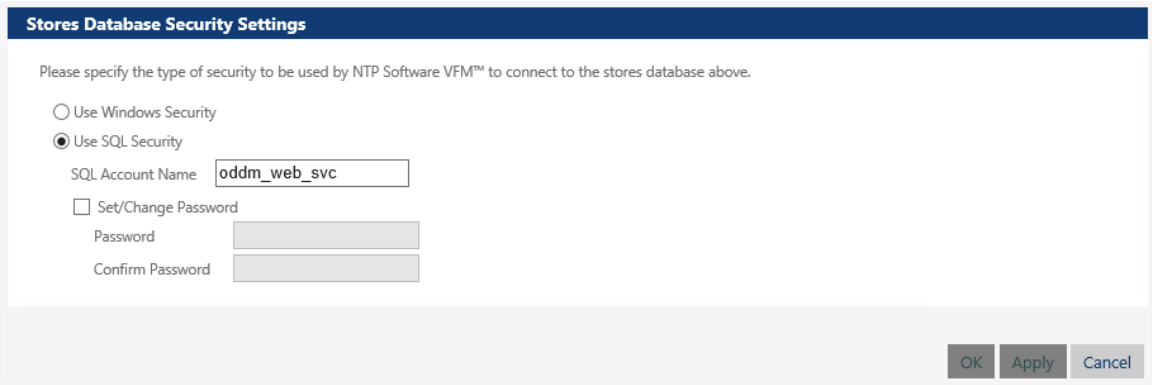
> **NOTE:** Please refer to the *Database Appendix*. The appendix has details on moving the database to another server if you choose to change the name of the database server.

Configuring Stores Database Security Settings

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

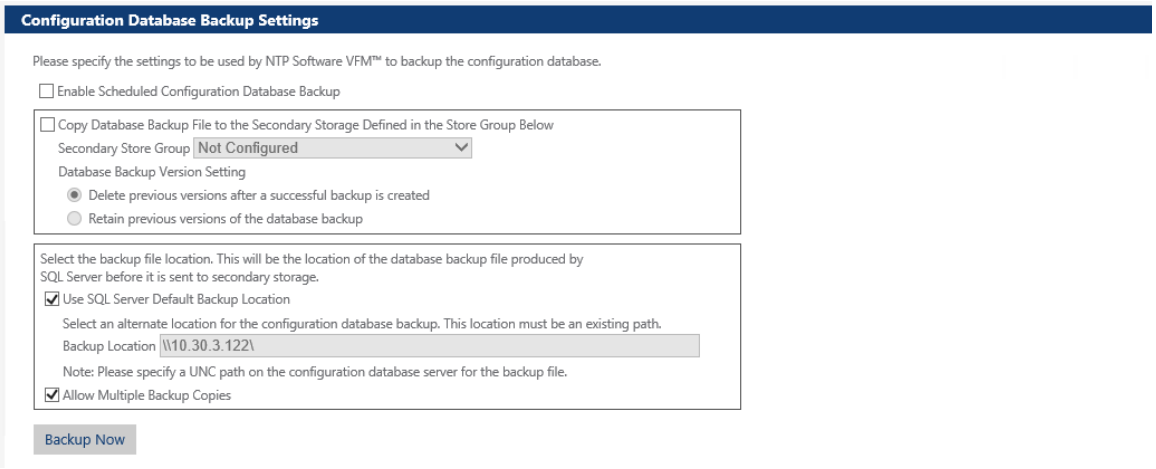
> **NOTE**: If the Set/Change Password option is not checked, the password that is stored in the database is not changed.

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



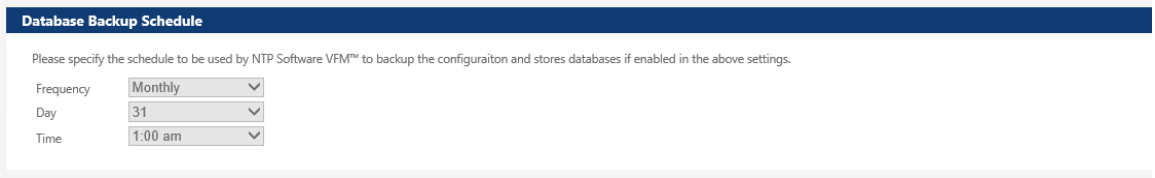
NOTES:

1. 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.

2. Database backups can be very large in size which should be taken into consideration in choosing the correct options for your environment.

3. When *Allow Multiple Backup Copies* is checked for the *Backup Location* then multiple copies of the database will be kept in that location. DefendX Software Mobility 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 Software Mobility to backup the configuration and stores databases if enabled in the above settings.



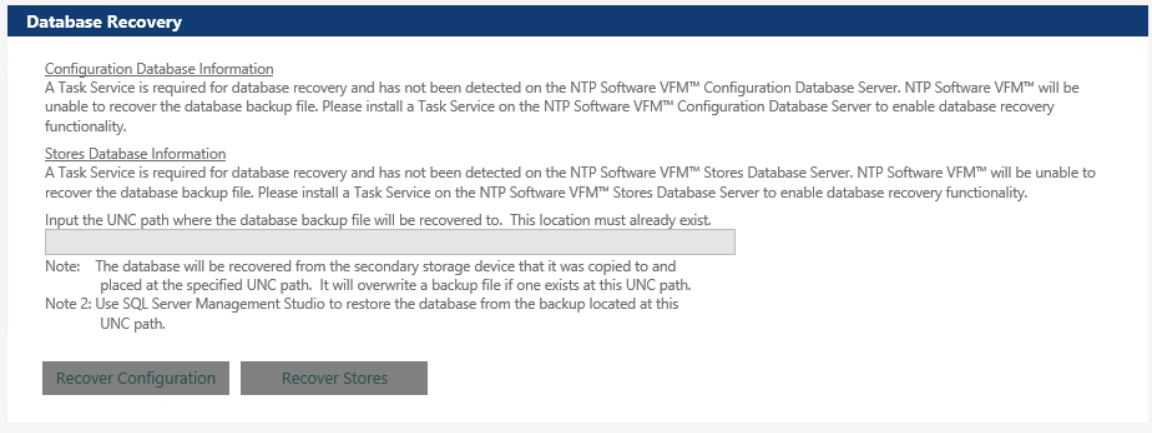
Recovering Database

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.



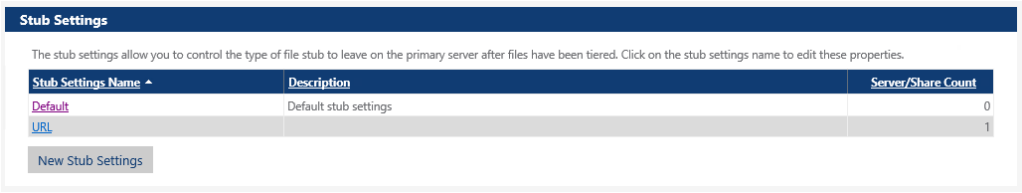
Configuring Stub and Schedule Settings

The stub and schedule settings allow you to control how files will be stubbed after being tiered as well as the times allotted for tiering.

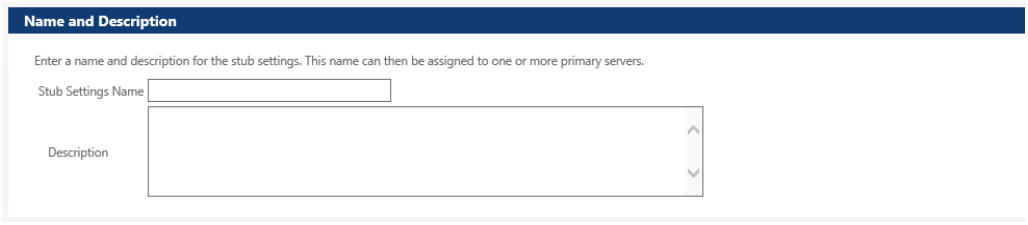
To configure Stub and Schedule settings, perform the following steps:

1. Under **Tiering Configuration** in the left-hand main menu, click **Stub and Schedule Settings**.

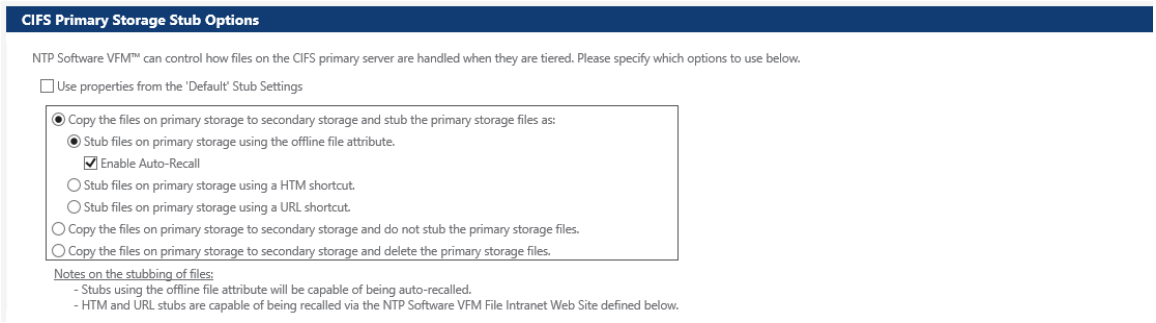
2. In the **Stub and Schedule Settings** section, click **New Stub and Schedule Settings** or click the name of an already existing stub and schedule settings name to edit these properties.



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

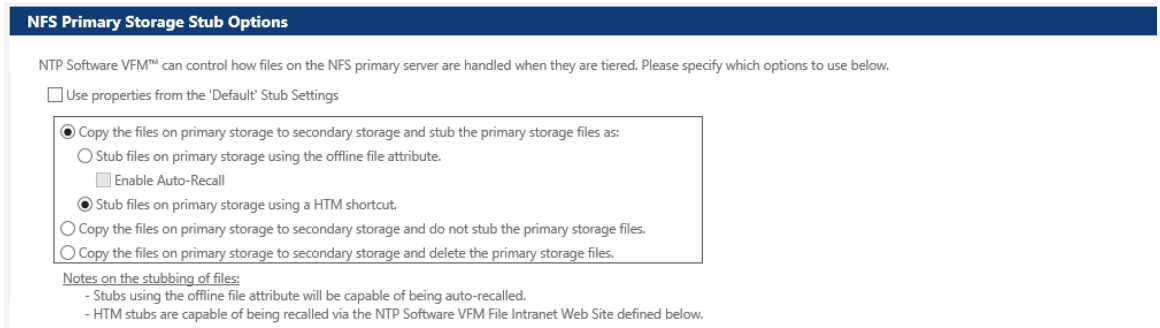


4. In the **CIFS Primary Storage Stub Options** section, specify the options through which you want DefendX Software Mobility to handle files located on primary servers CIFS shares when they are tiered.



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

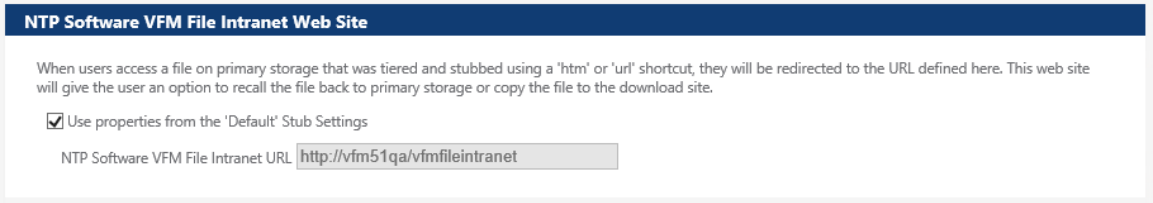
> **NOTE:** Microsoft Services for NFS must be installed on the task servers if you want to tier files from NFS exports.



6. In the **DefendX Software Mobility 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>/MobilityFileIntranet". Note: The DefendX Software Mobility File Intranet must be installed on <server>.

7. In the DefendX Software Mobility File Download UNC section, enter the UNC path that will be used as a temporary location to store recovered files. The format is:\\server\share\path where "\path" is optional. The DefendX Software Mobility Access and Recovery portals offer users a choice when recovering files. If the user chooses to recover the files to the download site then those files will be temporarily stored in the UNC specified here.

8. In the **File Intranet Web Site** section, either use properties from the default settings or provide a URL to use for the Mobility File Intranet.

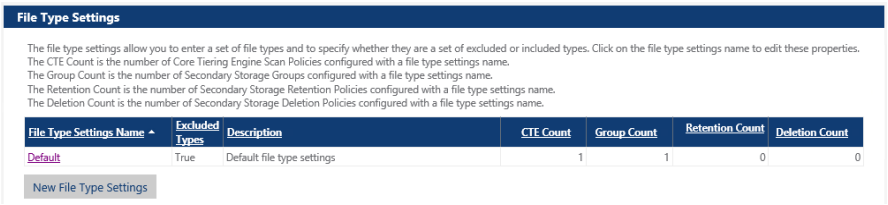


Configuring File Type Settings

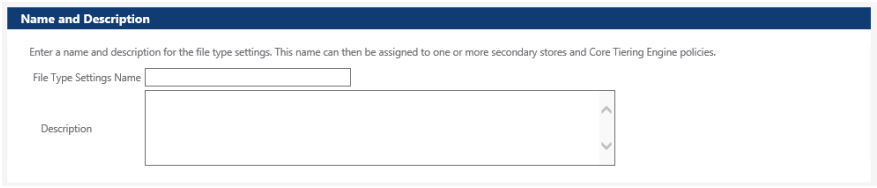
The file type settings allow you to enter a set of file types and to specify whether they are a set of excluded or included types.

To configure File Type settings, perform the following steps:

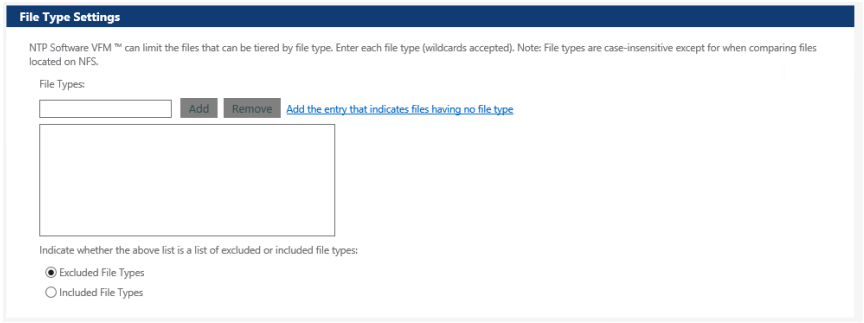
1. Under **Tiering Configuration** in the left-hand main menu, click **File TypeSettings**.
2. In the **File type Settings** section, click **New File Type Settings** or click the name of an already existing File Type Settings name to edit these properties.



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.



4. In the **File Type Settings** section, enter one or more file types by which DefendX Software Mobility can limit the files that can be tiered.
5. Indicate whether the listed file types are a list of excluded or included file types.

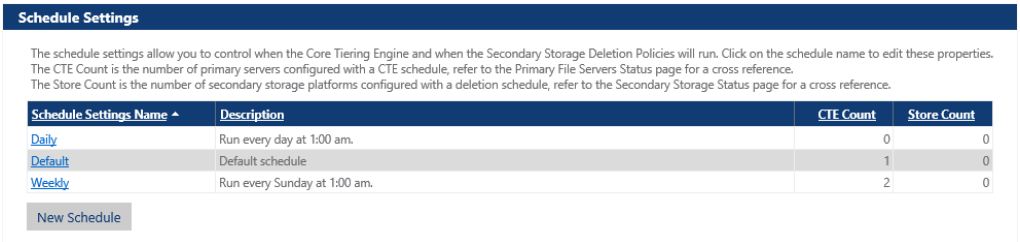


Schedule Settings

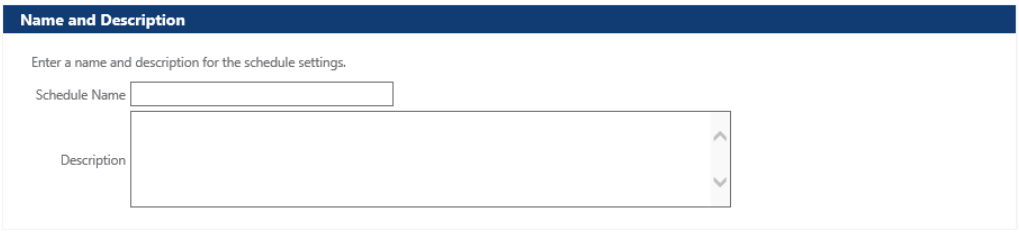
The **Schedule** settings allow you to control when the Core Tiering Engine and Secondary Storage Deletion policies will run.

To configure Schedule settings, perform the following steps:

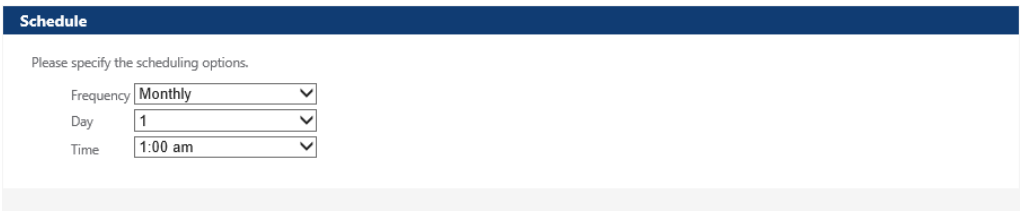
1. Click on a schedule name to edit its properties or click **New Schedule** to configure a new one.



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.

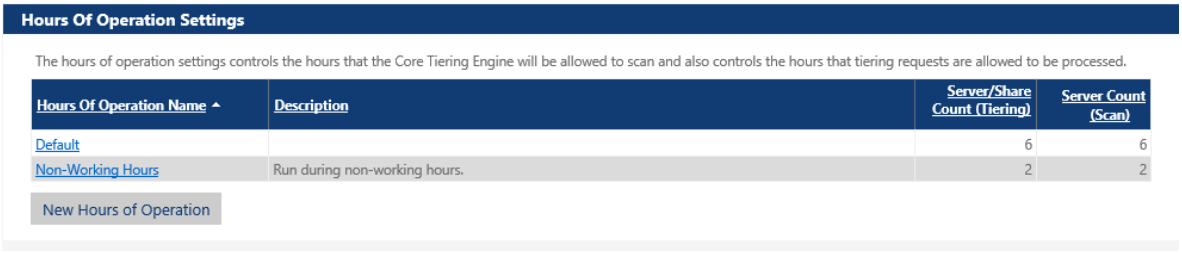


Hours of Operation Settings

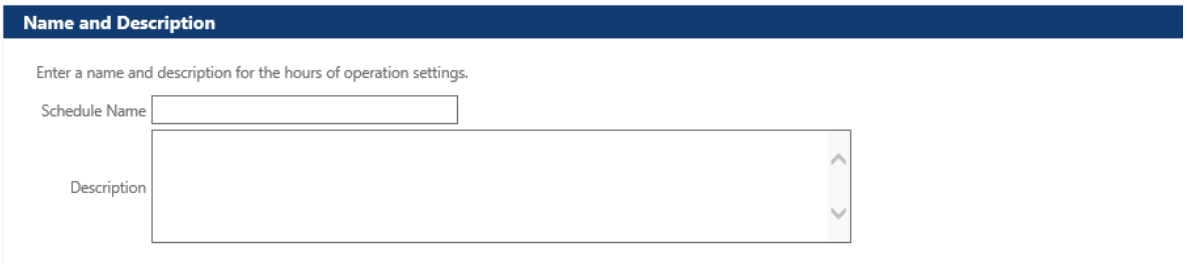
The Hours of Operation settings control the hours during which the Core Tiering Engine is allowed to scan and tiering requests are able to be processed.

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

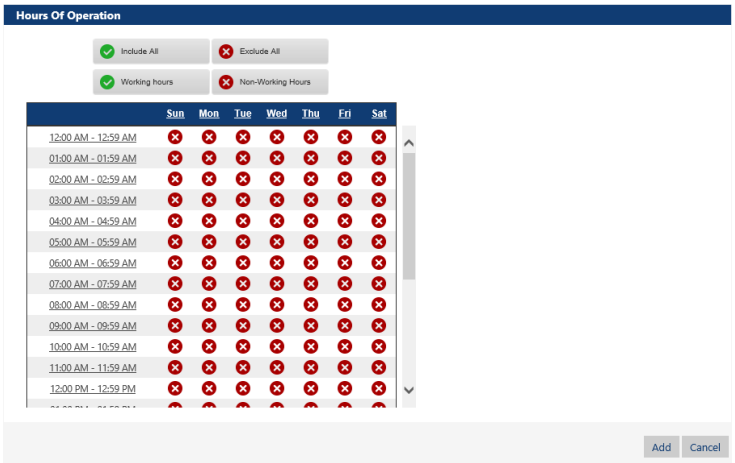
1. Click an Hours of Operation name to edit existing settings or click **New Hours of Operation** to configure a new setting.



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.



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.



Core Tiering Engine in Brief

The Core Tiering Engine works in conjunction with DefendX Software Mobility 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 Software Mobility Administration 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 Software Mobility (Administration web site). The corresponding Task Services will process the tier requests that have been submitted to DefendX Software Mobility as would occur in any standard DefendX Software Mobility deployment.

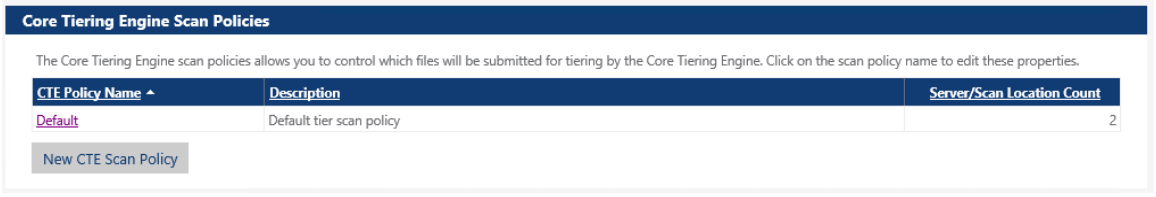
NOTE: The Core Tiering Engine must be installed on the Windows server for which the DefendX Software Mobility Task Service controls the tiering of the primary server's files. To assign a Core Tiering Engine schedule and policy, click on the *Edit Server link for* the primary server on the primary servers 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.

Configuring Core Tiering Engine Scan Policies

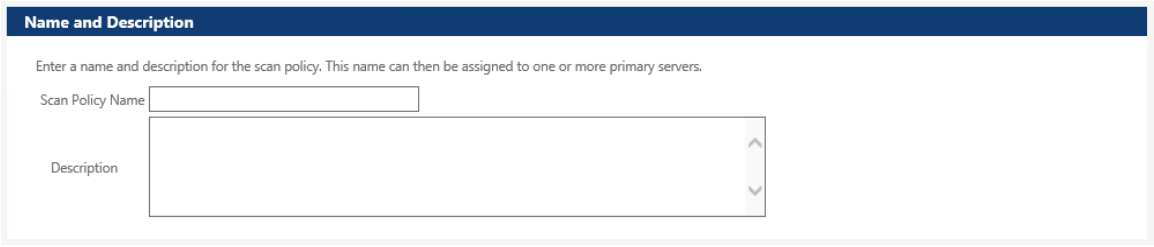
The **Core Tiering Engine Scan Policies** allows you to control which files will be submitted for tiering by the Core Tiering Engine.

To configure 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.

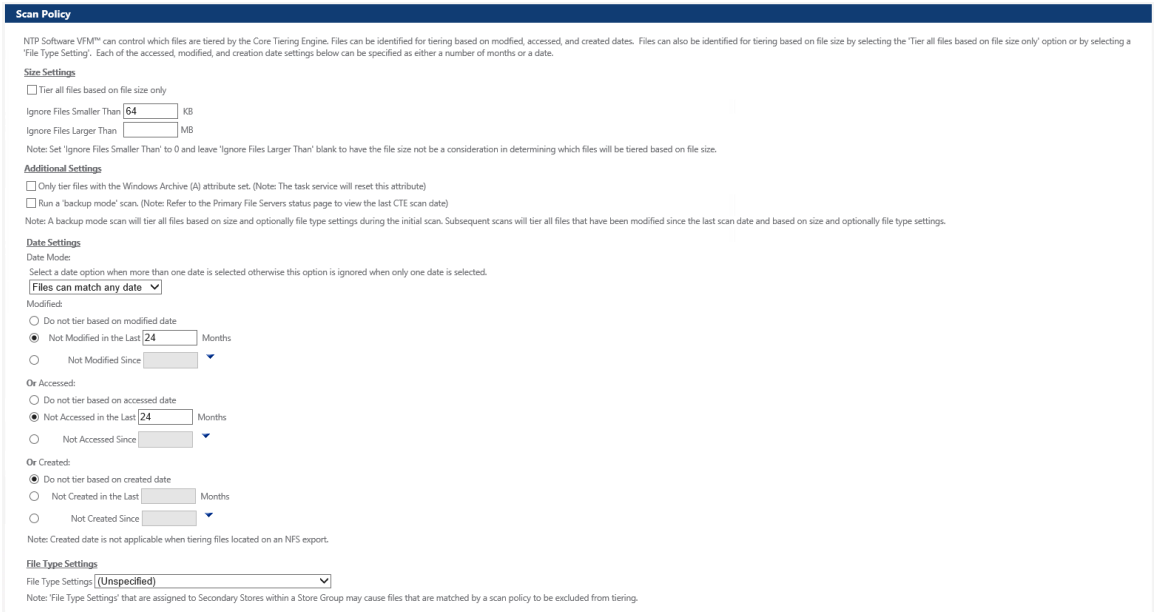


3. In the **Name and Description** section, enter a name and description for the Scan Policy. The name can then be assigned to one or more primary servers.



4. In the **Scan Policy** section, specify the criteria by which DefendX Software Mobility 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 Software Mobility 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.



NOTES:

- The date creation option will be ignored when the CTE scans files located on NFS exports.
- If multiple dates are selected then a file that meets one of the date's criteria will be tiered if it also meets the file size criteria and file type criteria.

Configuring Secondary Storage

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

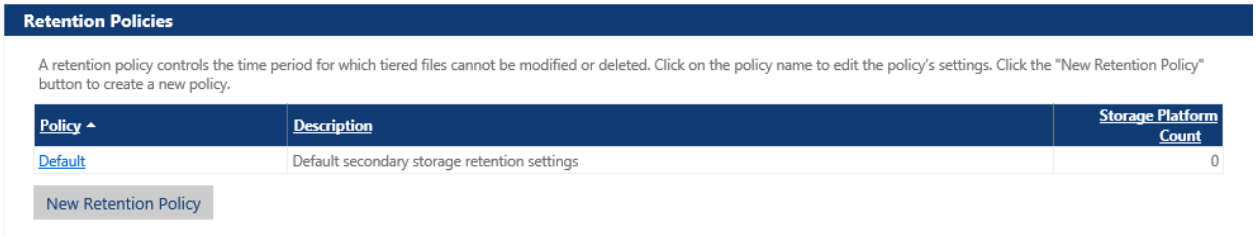
Configuring Storage Policies

Storage Policies consist of Retention Policies and Deletion Policies. Retention policies control the time period for which tiered files cannot be modified or deleted. Deletion policies specify the time frame with which tiered files will be held before they are deleted.

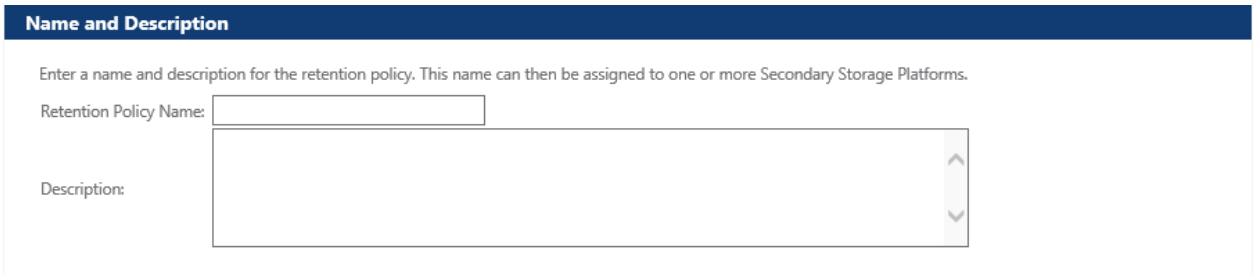
To configure a Retention Policy:

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

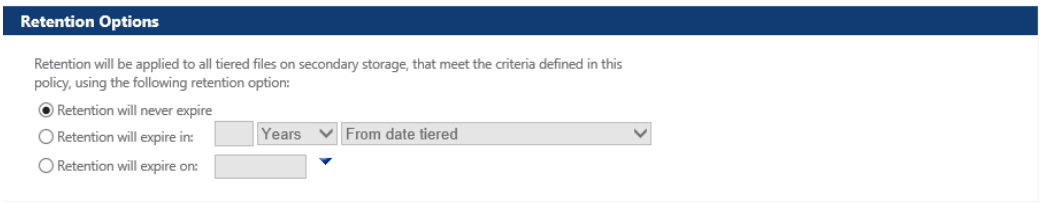
2. In the **Retention Policies** section, click a policy name to edit an existing policy or click **New Retention Policy** to configure a new policy.



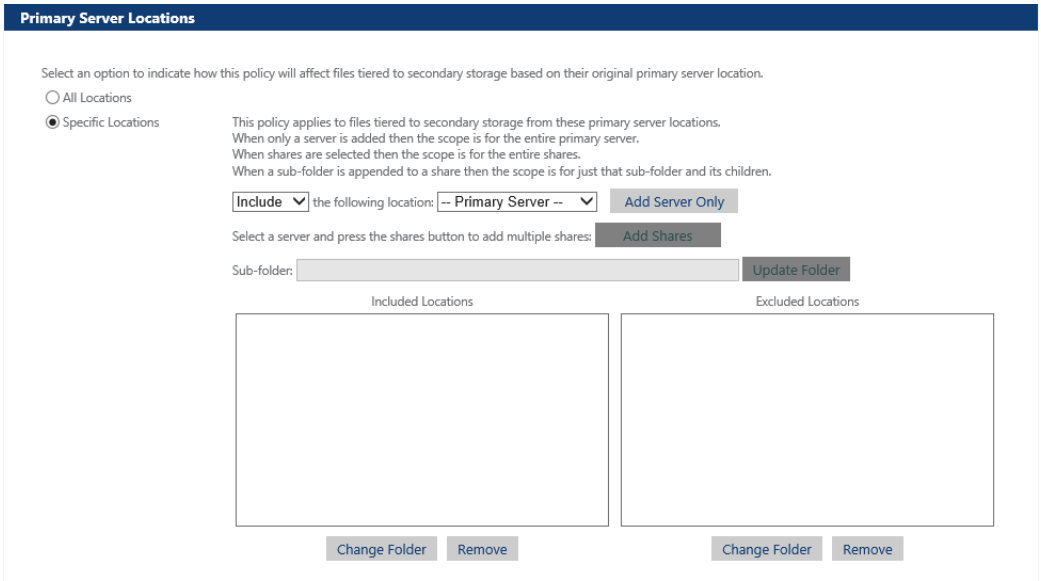
3. In the **Add New Retention Policy** section, specify a name and description for the Retention Policy.



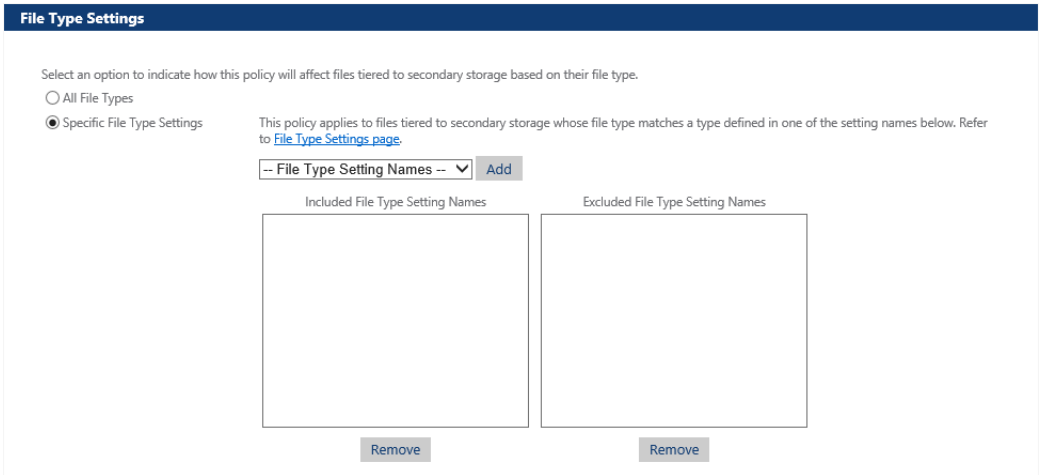
4. In the **Retention Options** section, set the expiration options for the retention policy.



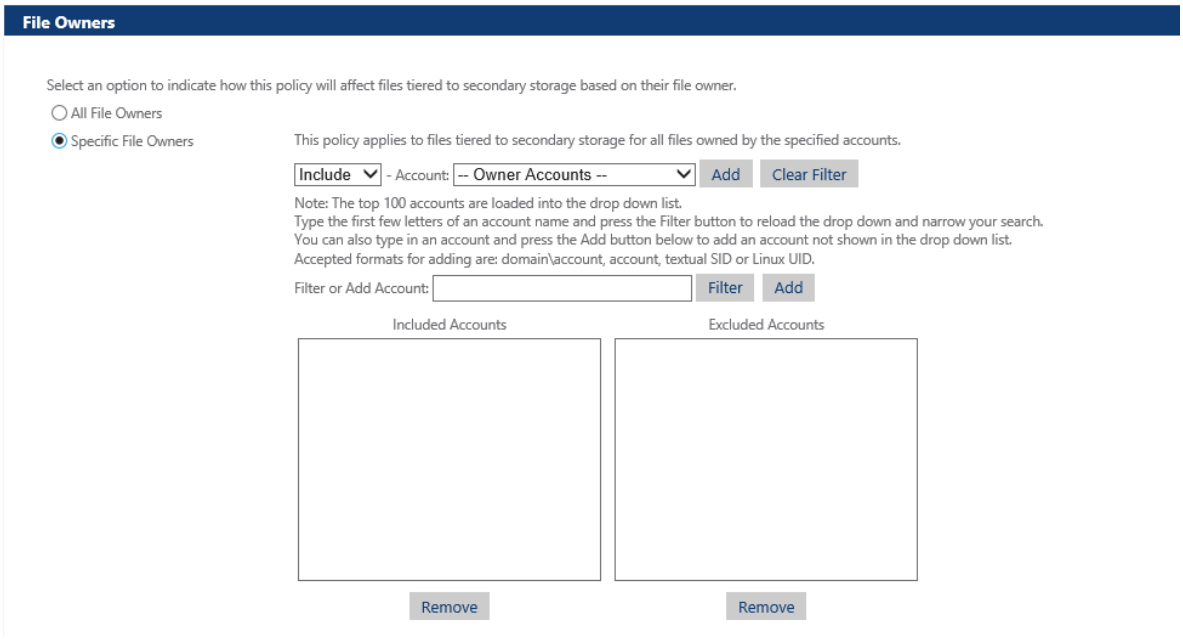
5. In the **Primary Server Locations** section, either apply the retention policy to All Locations or specify which origin servers the retention policy will be applied to.



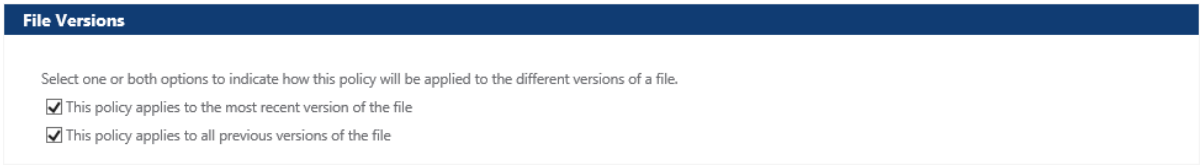
6. In the **File Type Settings** section, indicate whether the retention policy should be applied to all file types or specific file types only.



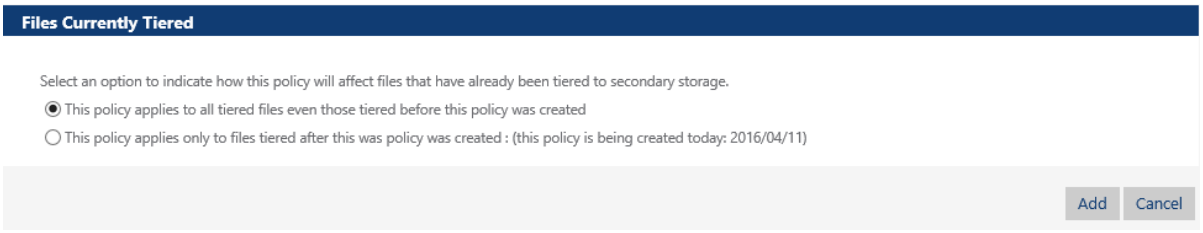
7. In the **File Owner** section, indicate whether the retention policy should be applied all file owners or specific file owners only.



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.



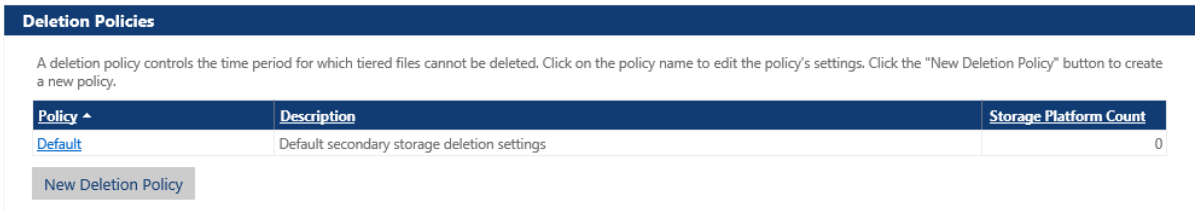
9. In the **Files Currently Tiered** section, indicate whether the retention policy should be applied to all tiered filed or only files tiered since the retention policy was created. Click **Add**.



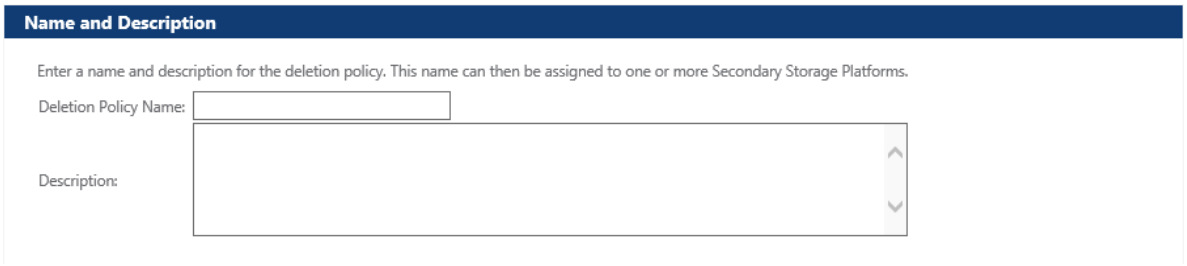
To configure a Deletion Policy:

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

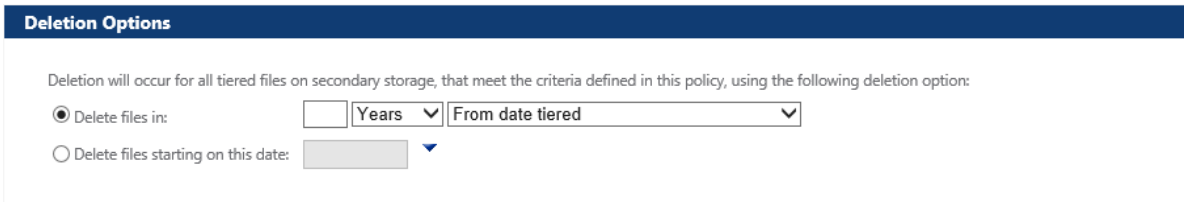
2. In the **Deletion Policies** section, click a policy name to edit an existing policy or click **Deletion Retention Policy** to configure a new policy.



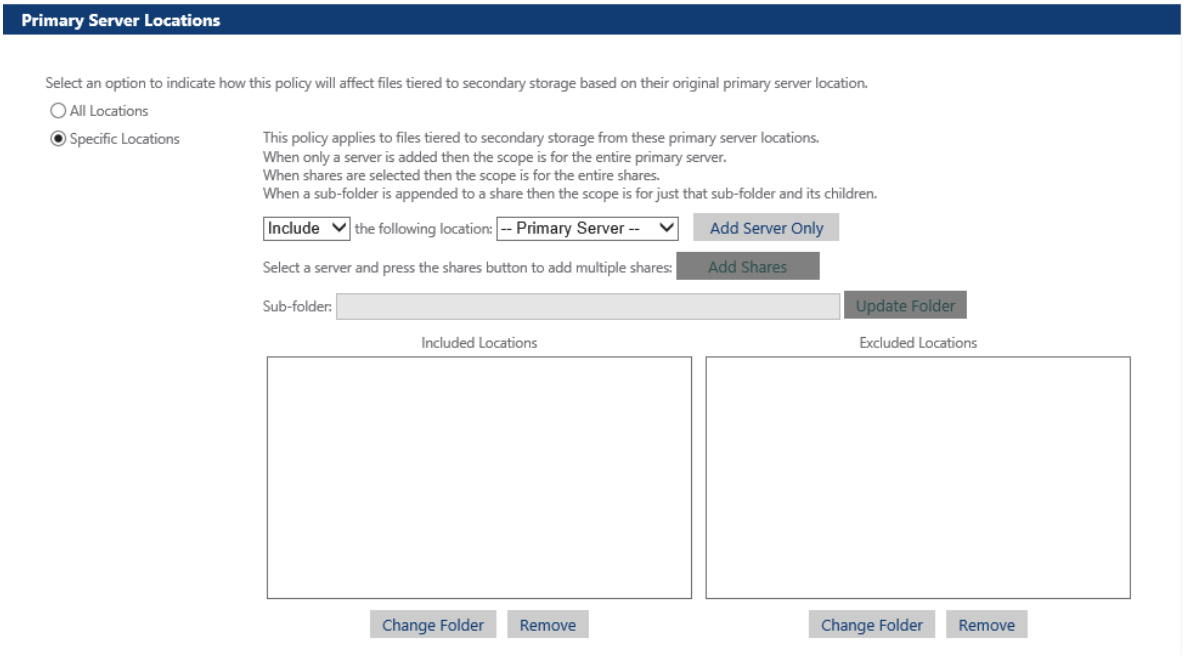
3. In the **Add New Deletion Policy** section, specify a name and description for the deletion policy.



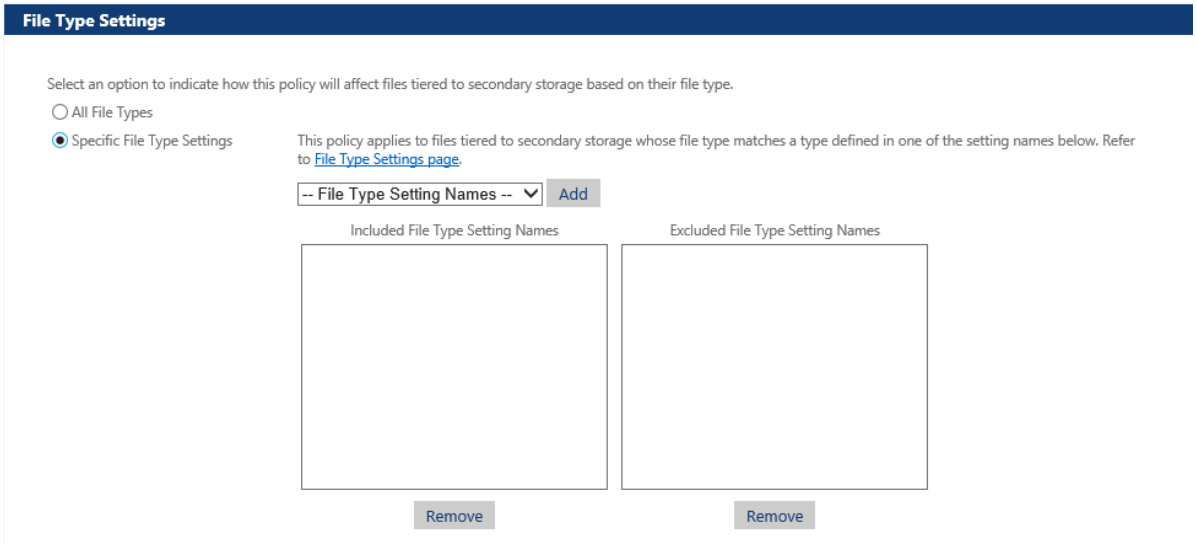
4. In the **Deletion Options** section, set the date or time frame by which the deletion policy will delete tiered files.



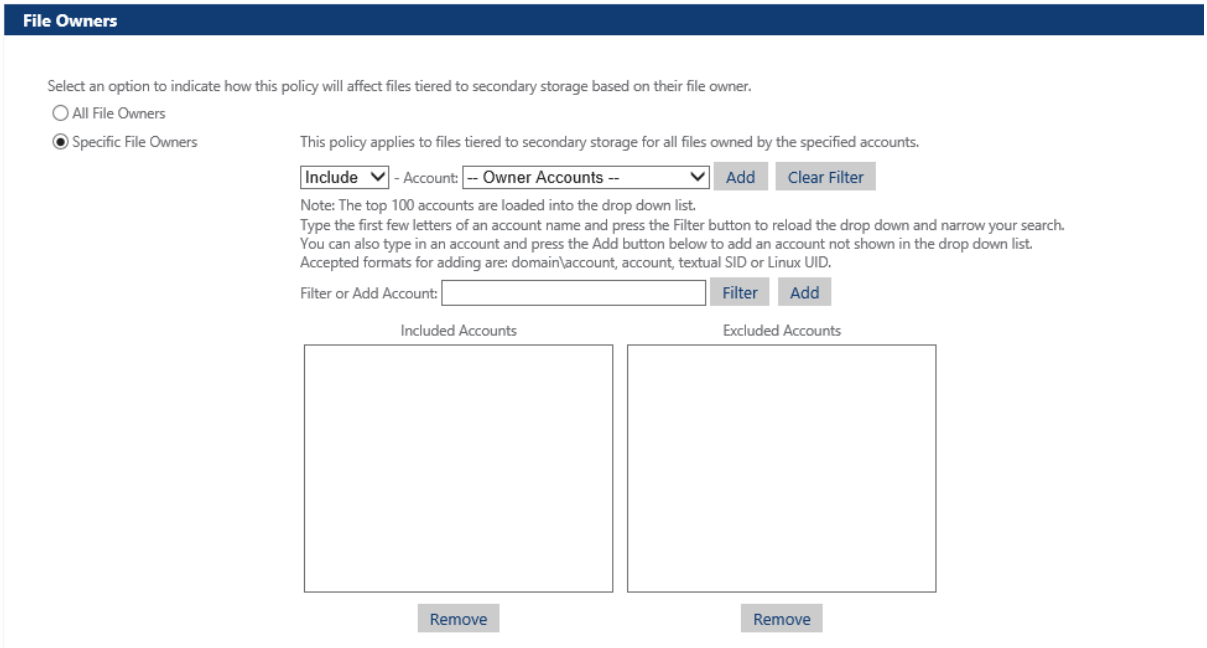
5. In the **Primary Server Locations** section, either apply the retention policy to All Locations or specify which origin servers the retention policy will be applied to.



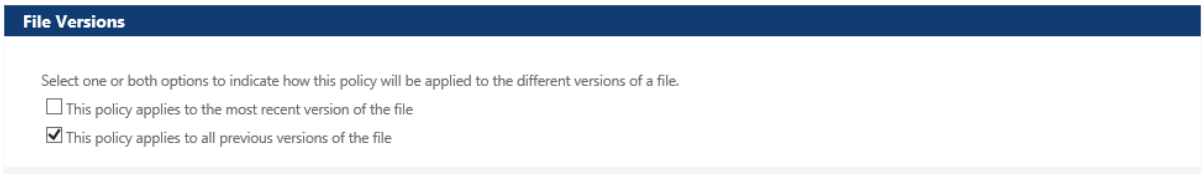
6. In the **File Type Settings** section, indicate whether the retention policy should be applied to all file types or specific file types only.



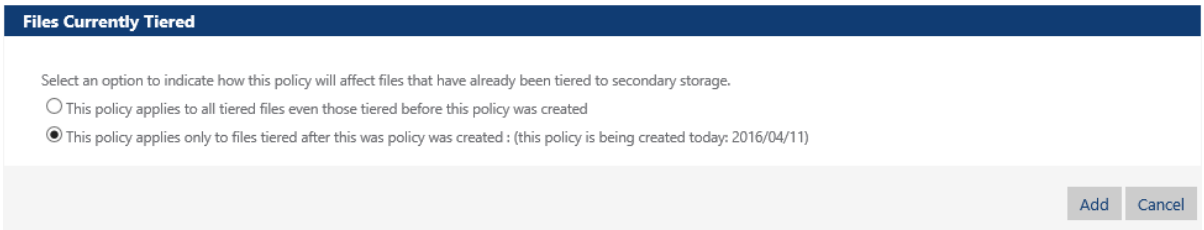
7. In the **File Owner** section, indicate whether the retention policy should be applied all file owners or specific file owners only.



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 filed or only files tiered since the retention policy was created. Click **Add**.

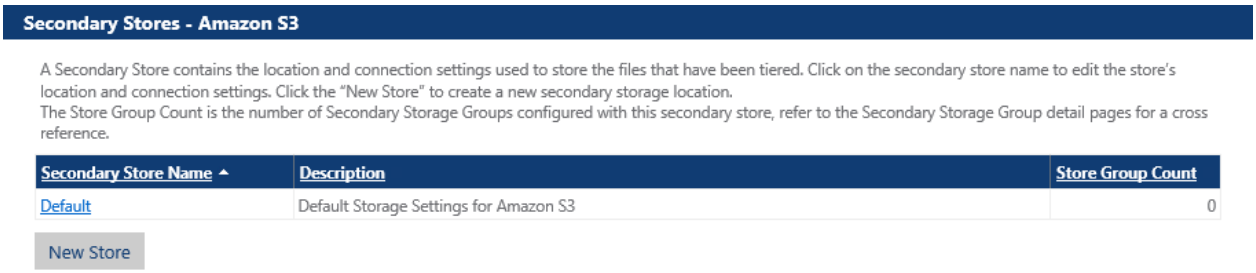


Secondary Storage – Amazon S3

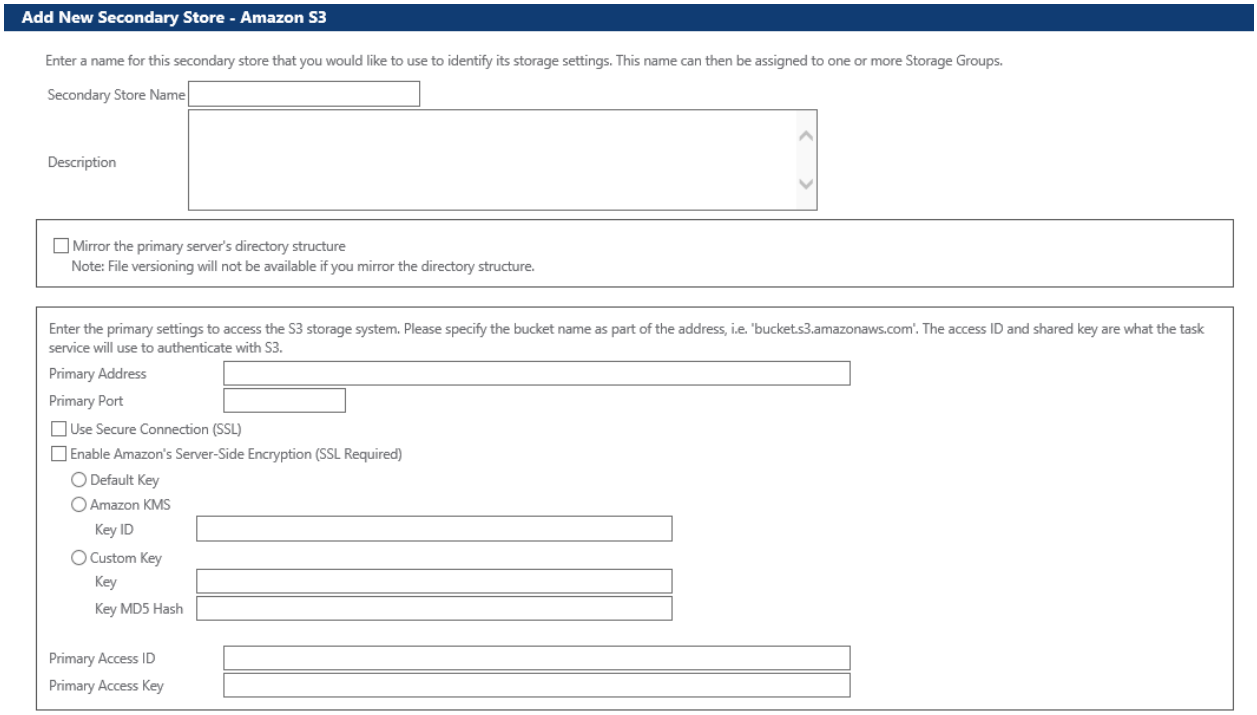
Adding/Editing a AmazonS3 Secondary Store

1. Under **Secondary Storage** in the left-hand main menu, click **Secondary Storage > Storage Platforms > AmazonS3 Storage**.

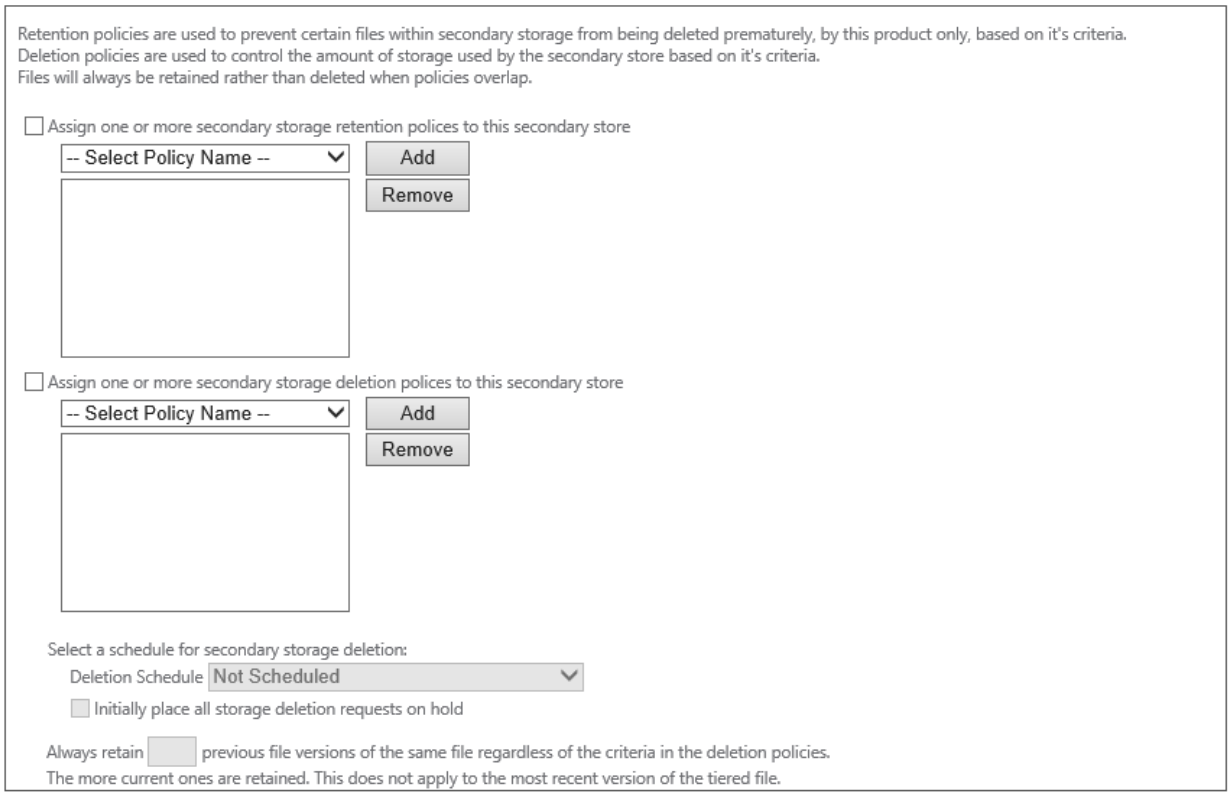
2. In the **Secondary Stores AmazonS3 Storage** section, click **New Store** or click the name of an already existing secondary store to edit these properties.



3. In the **Add New Secondary Store – AmazonS3 Storage** 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.



4. At the bottom of the **Add New Secondary Store – AmazonS3 Storage** dialog box, retention and deletion policies can be added to the secondary store.



Field/Option	Description
Primary Address	Enter the primary settings to access the S3 storage system. Please specify the bucket name as part of the address, i.e. 'bucket.s3.amazonaws.com'.

Primary Port	Enter the port that will be used for communication with the AmazonS3 bucket. I.e, 80, or 443 for SSL

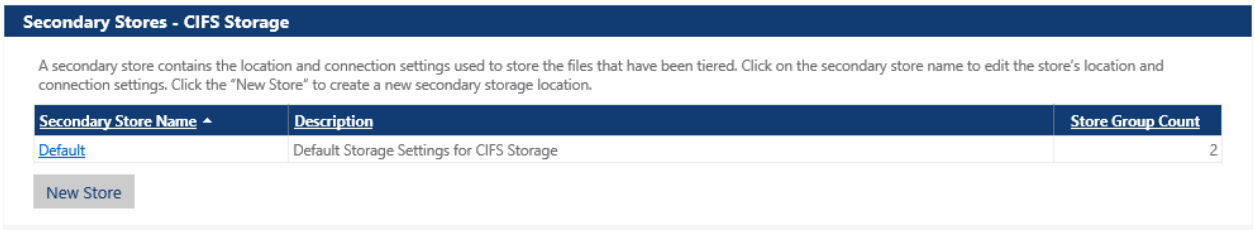
NOTE: The Task Services service account must be granted full permissions to the secondary store UNC paths as well as the primary server shares and directories it will be tiering files from.

Secondary Storage – CIFS

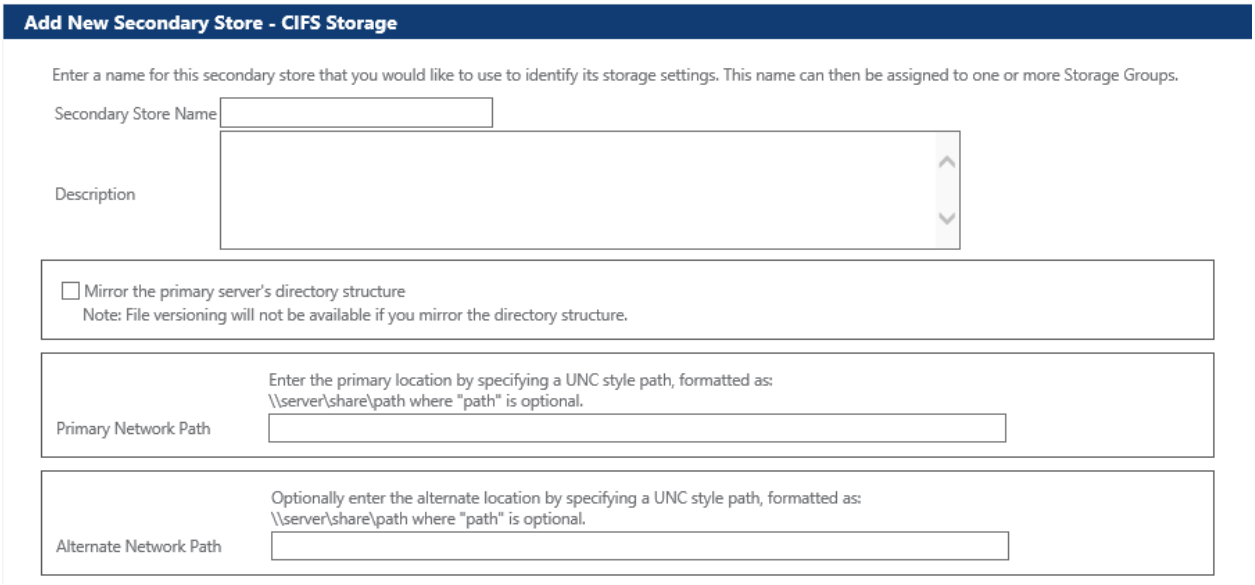
Adding/Editing a CIFS Secondary Store

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

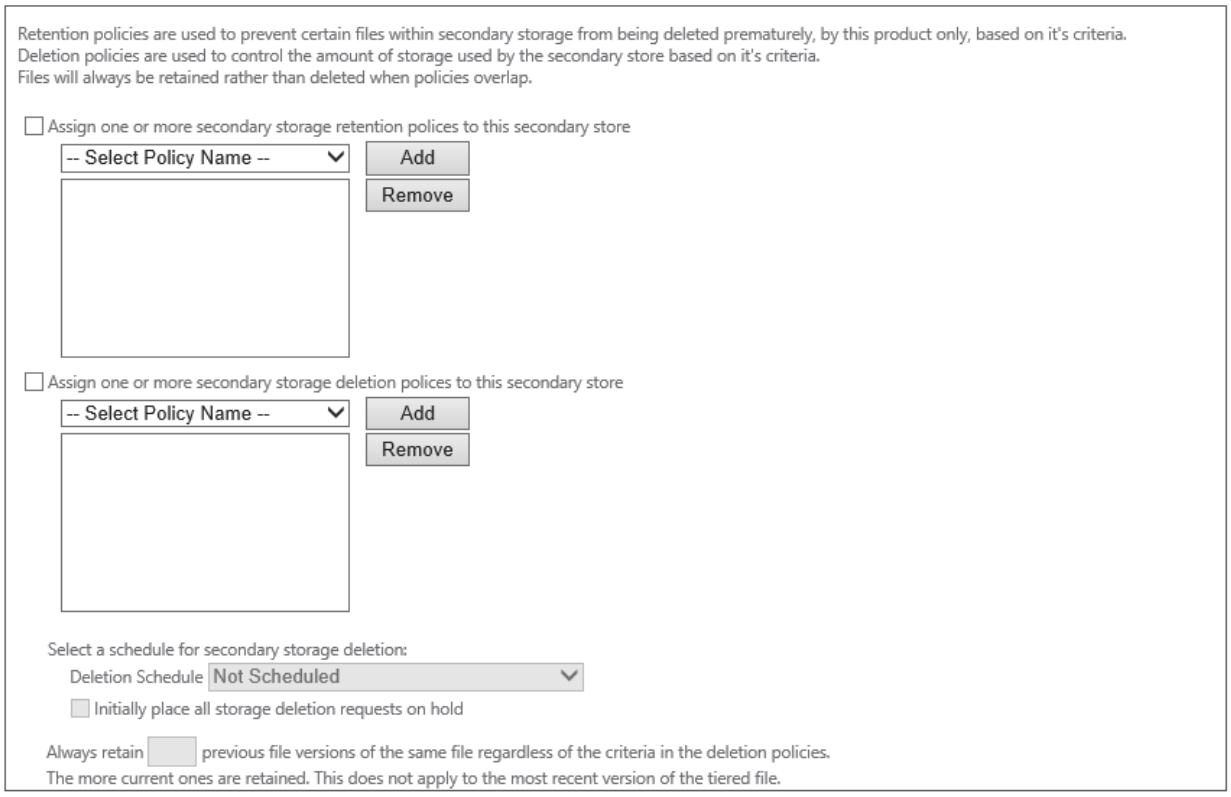
2. In the **Secondary Stores CIFS Storage** section, click **New Store** or click the name of an already existing secondary store to edit these properties.



3. In the **Add New Secondary Store – CIFS Storage** 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.



4. At the bottom of the **Add New Secondary Store – CIFS Storage** dialog box, retention and deletion policies can be added to the secondary store.



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. DefendX Software Mobility will attempt to tier files to the UNC path first.
Alternate Network Path	Enter an optional UNC style path of a CIFS share that will be used to store the tiered files as an alternate whenever the Primary Network Path is not available. DefendX Software Mobility will only attempt to tier files to the Alternate UNC path if it cannot tier to the primary 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 CIFS 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 on the CIFS share will consist of GUIDs.

NOTE: The Task Services service account must be granted full permissions to the secondary store UNC paths as well as the primary server shares and directories it will be tiering files from.

Secondary Store – EMC Atmos

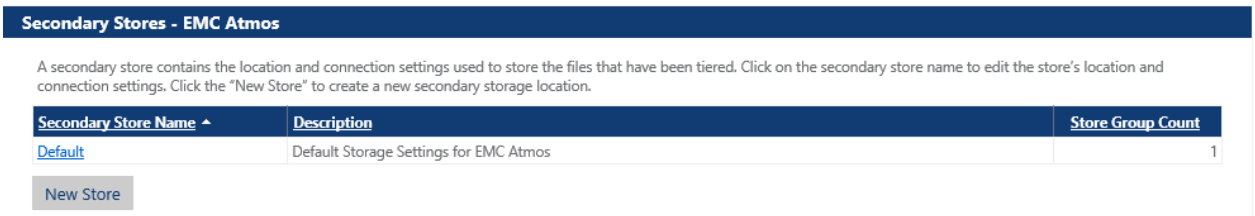
Configuring EMC Atmos for use with DefendX Software Mobility:

1. Log on to the EMC Administration console using the "SysAdmin" account.
   i. Create the Tenant(s) that will be used in conjunction with DefendX Software Mobility.
   ii. Ensure Web Service is enabled on each node. iii. Enable/Disable SSL for Web Service Connections. iv. Refer to the EMC Atmos Storage System documentation for a complete description on configuring the storage system.

2. Log on to the EMC Administration console using the Tenant credentials.
   i. Create the Sub Tenant(s) that will be used in conjunction with DefendX Software Mobility.
   ii. For each sub tenant create a UID and Shared Secret key that will be used in conjunction with DefendX Software Mobility.
   iii. Refer to the EMC Atmos Storage System documentation for a complete description on configuring Tenants and Sub tenants.

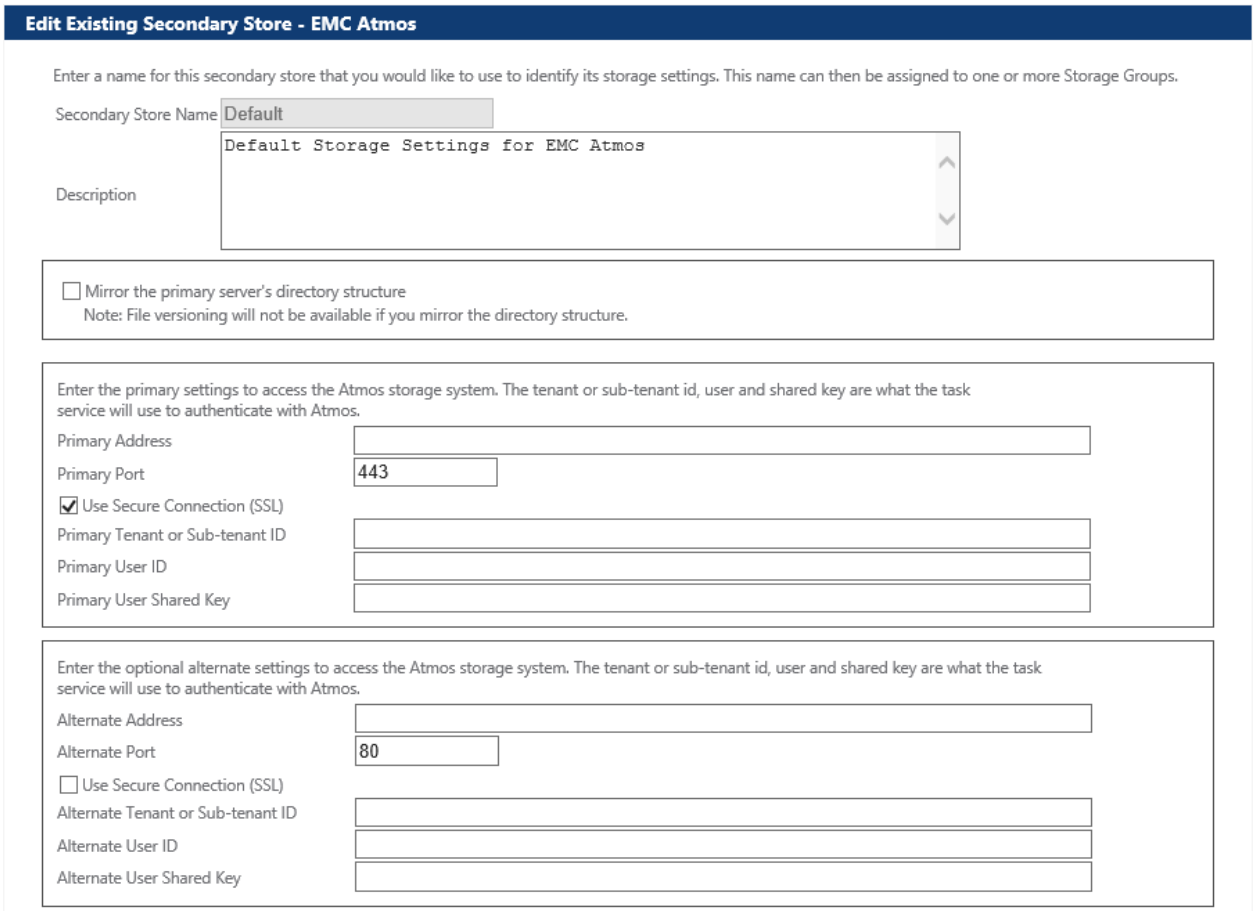
Adding / Editing an EMC Atmos Secondary Store:

1. Under **Secondary Storage** in the left-hand main menu, click **Secondary Storage** > **Storage Platforms** >**EMC Atmos**.



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

3. In the **Edit Existing Secondary Store – EMC Atmos** dialog box edit 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.



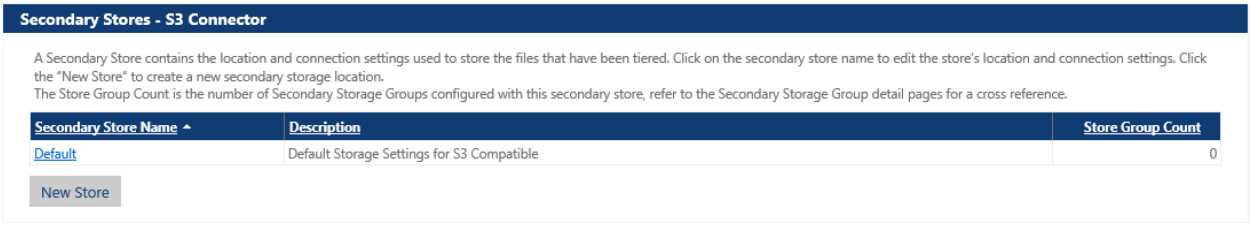
Field	Description
Address	Enter the fully qualified name of the EMC Atmos Storage System. An IP address can also be entered but will be limited to that one storage node.
Port	Enter the port to communicate with the EMC Atmos Storage System's web service. This will usually be port 80 when not using SSL 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.
Tenant or Subtenant ID	Enter the ID of either a tenant or subtenant. This can be found in the EMC Atmos Administration console dashboard when logged in as a tenant or sub tenant.
User ID	Enter the UID name that will be used in conjunction with DefendX Software Mobility. This can be found in the Atmos Administration console dashboard when logged in as a tenant or sub tenant. Use one of the UID names listed in the UID List that was setup to use with Mobility.
User Shared Key	Enter the Shared Secret key that corresponds with the User Id (UID). Click the *View* link on the Atmos Administration console next to the UID and enter that value.

Secondary Storage –Hitachi HCP

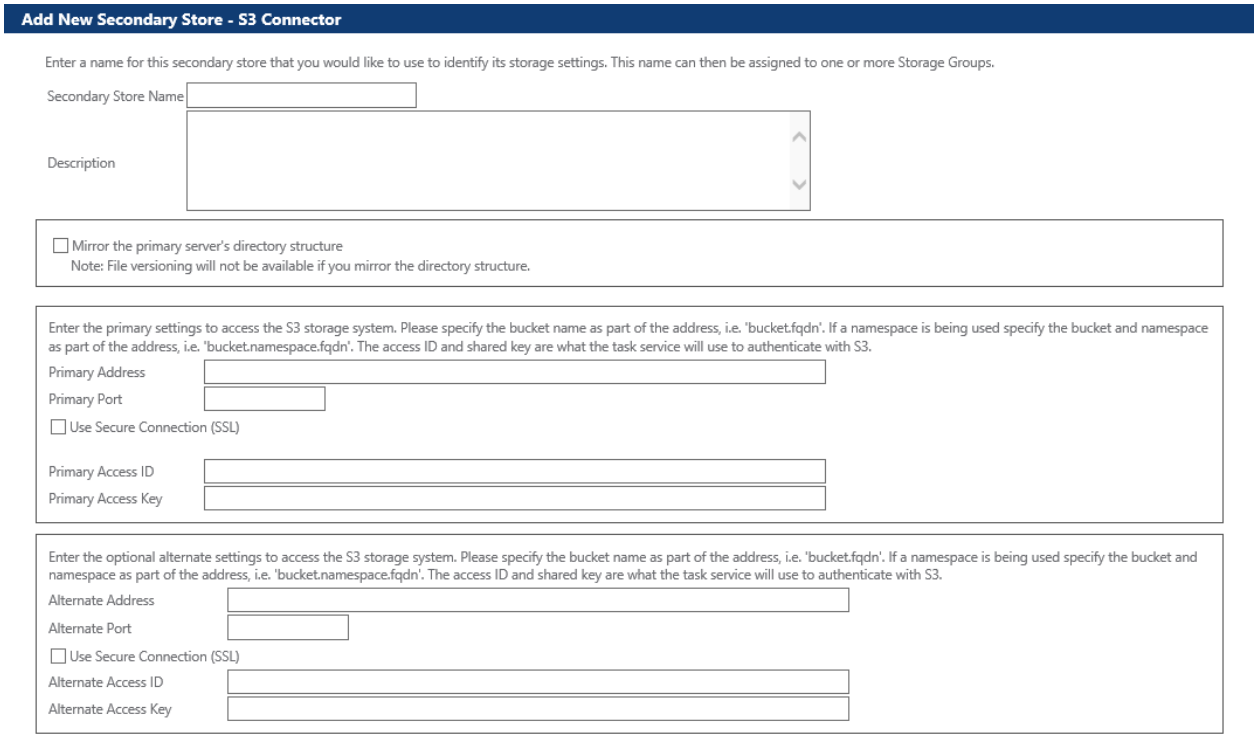
Adding/Editing Hitachi HCP Secondary Store

1. Under **Secondary Storage** in the left-hand main menu, click **Secondary Storage > Storage Platforms > S3 Connector**.

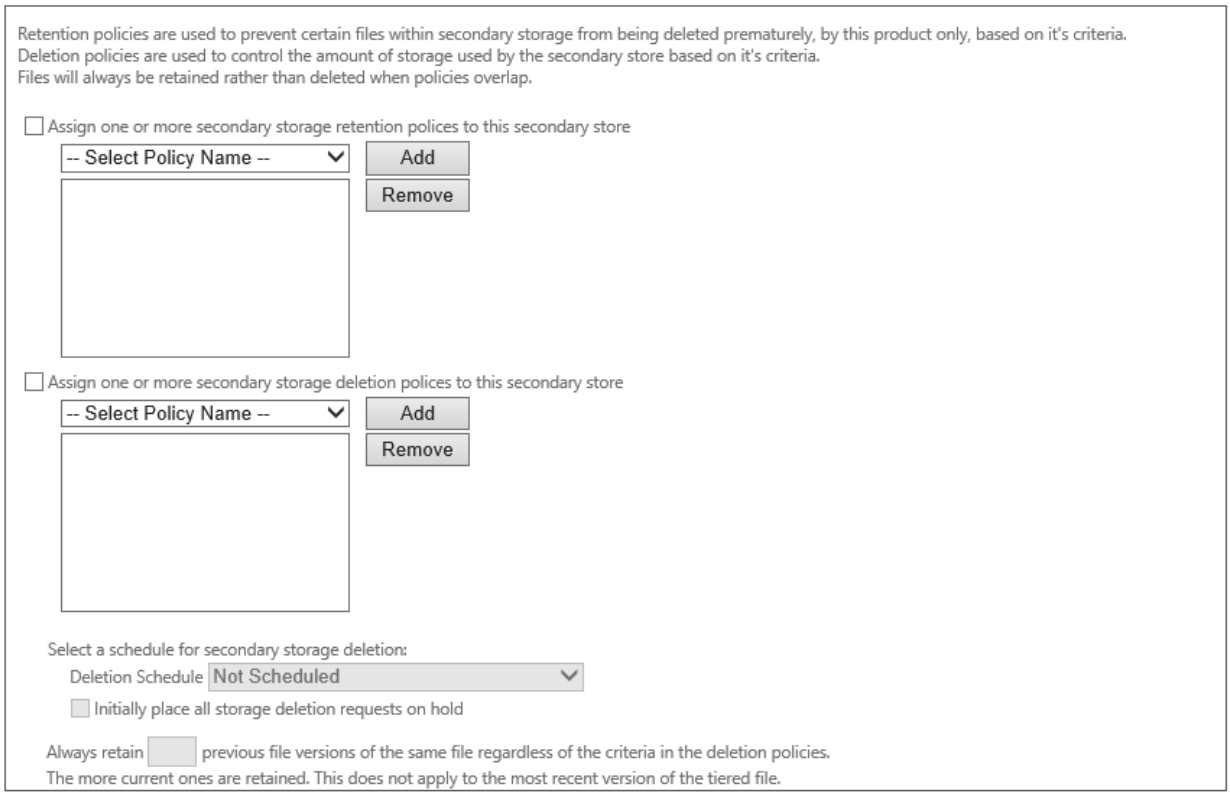
2. In the **Secondary Stores S3 Connector** section, click **New Store** or click the name of an already existing secondary store to edit these properties.



3. In the **Add New Secondary Store – S3 Connector Storage** 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.



4. At the bottom of the **Add New Secondary Store – S3 Connector** dialog box, retention and deletion policies can be added to the secondary store.



Field/Option	**Description**
Primary Address	Enter the primary settings to access the S3 storage system. Please specify the bucket name as part of the address, i.e. 'bucket.fqdn.com'.

Primary Port	Enter the port that will be used for communication with the AmazonS3 bucket. I.e, 80, or 443 for SSL

NOTE: The Task Services service account must be granted full permissions to the secondary store UNC paths as well as the primary server shares and directories it will be tiering files from.

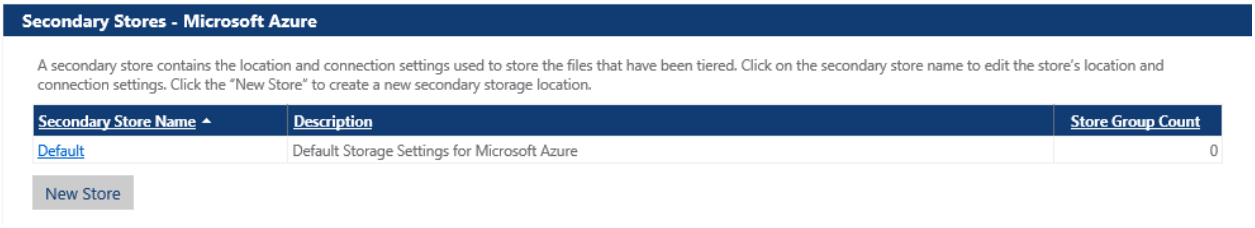
Secondary Store – Microsoft Azure

Configuring Microsoft Azure for use with DefendX Software Mobility:

1. Log on to the Azure Portal using the Microsoft Account associated with your Microsoft Azure subscription.
2. Create a Storage Account. The Storage Account and associated Access Key will be used in conjunction with DefendX Software Mobility.

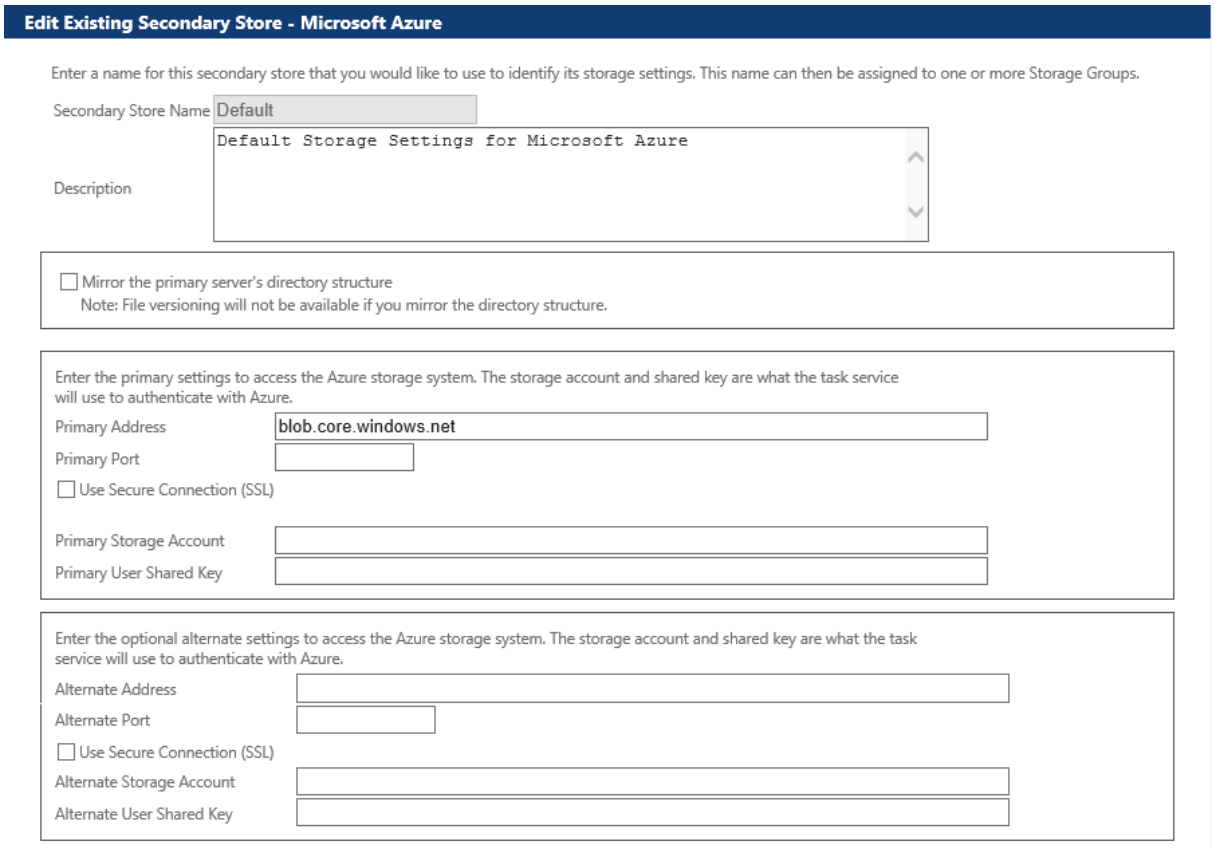
Adding / Editing a Microsoft Azure Secondary Store:

1. Under **Secondary Storage** in the left-hand main menu, click **Secondary Storage** > **Storage Platforms** > **Microsoft Azure**.



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

3. In the **Edit Existing Secondary Store – Microsoft Azure** dialog box edit 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.



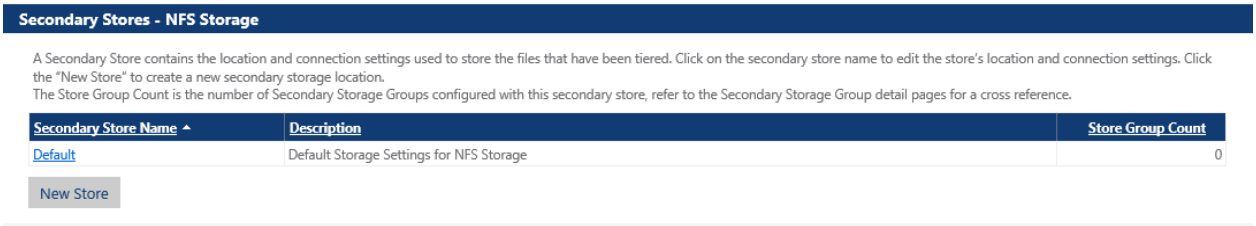
Field	Description
Primary Address	Enter the fully qualified name for the Azure Storage.
Primary Port	Enter the port to communicate with the Azure Storage's web service. This will usually be port 80 when not using SSL and port 443 when using SSL.
Use Secure Connection (SSL)	Check this option if web service is using https otherwise uncheck when using http for the connection.
Primary Storage Account	Enter the Primary Storage Account name that will be used in conjunction with DefendX Software Mobility. This can be found in the storage section of the Azure Portal when logged in.
Access Key	Enter the Access Key that corresponds with the Primary Storage Account.

Secondary Storage – NFS Storage

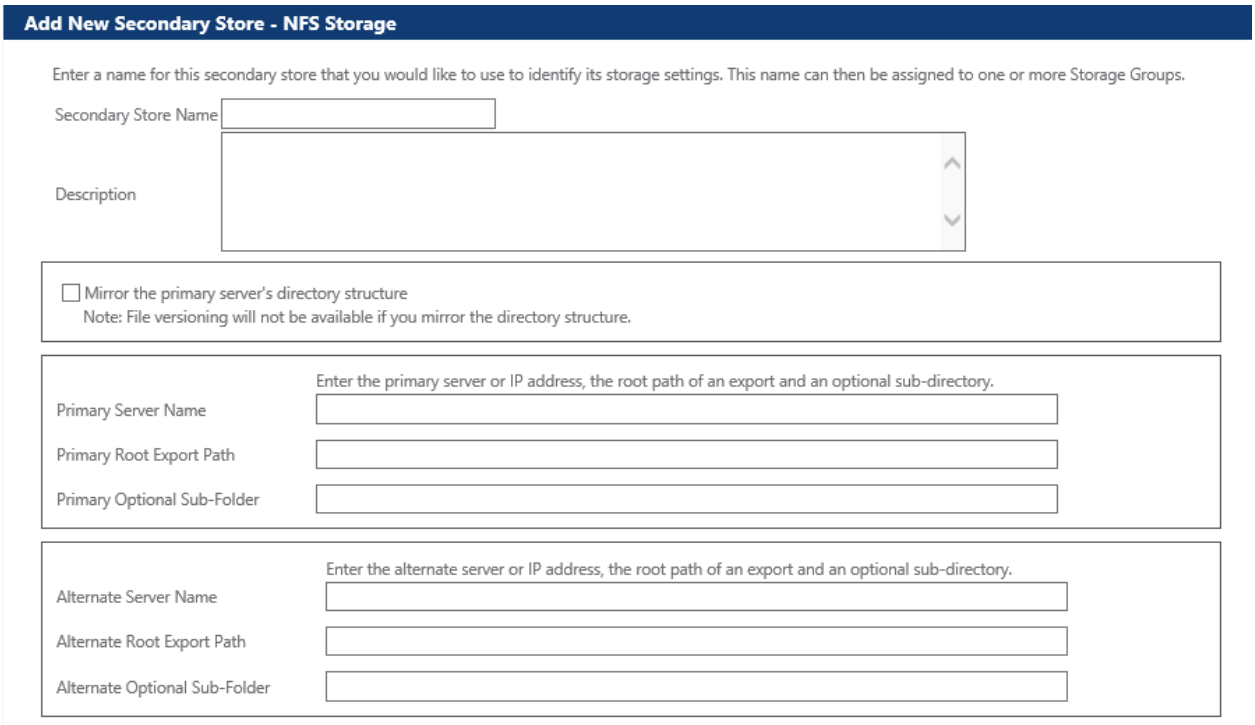
Adding/Editing an NFS Secondary Store

1. Under **Secondary Storage** in the left-hand main menu, click **Secondary Storage > Storage Platforms > NFS Storage**

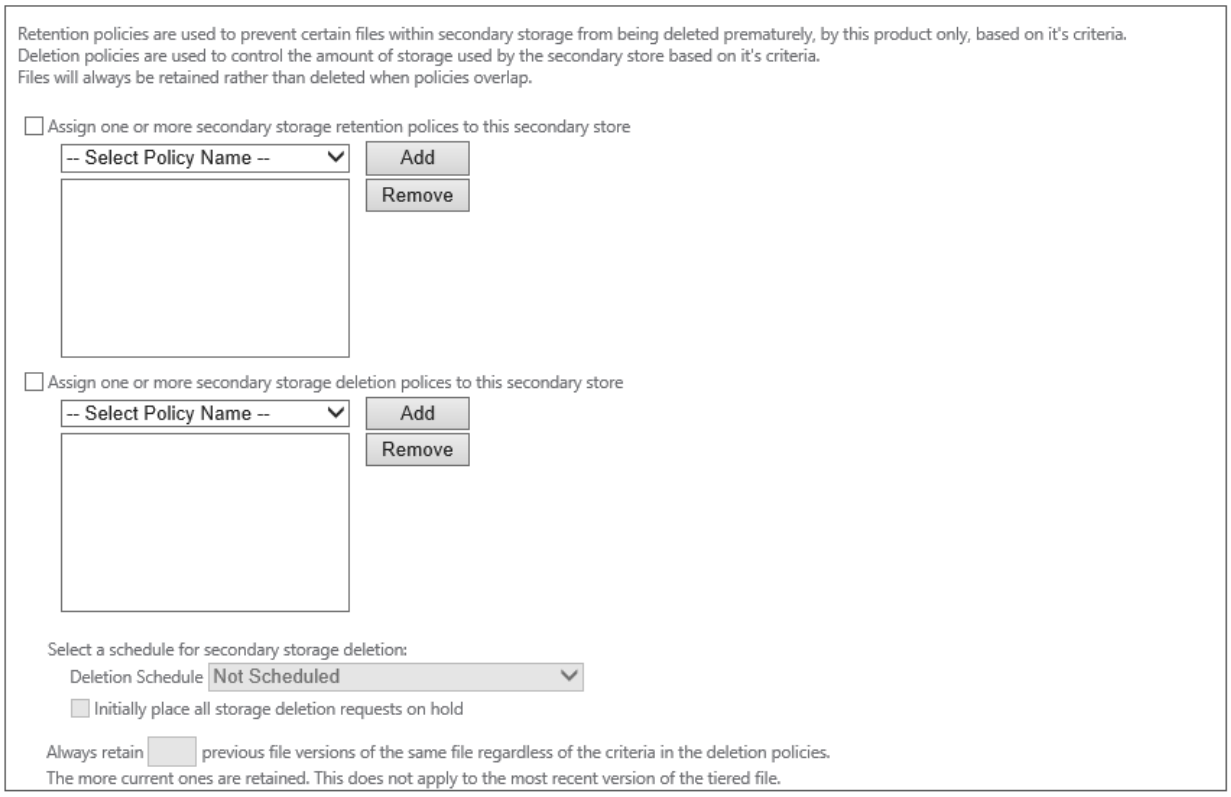
2. In the **Secondary Stores NFS Storage** section, click **New Store** or click the name of an already existing secondary store to edit these properties.



3. In the **Add New Secondary Store – NFS Storage** 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.



4. At the bottom of the **Add New Secondary Store – NFS Storage** dialog box, retention and deletion policies can be added to the secondary store.



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 for storage.

Primary Optional Sub-Folder	Optionally enter the path to a sub folder to be used on the NFS export.

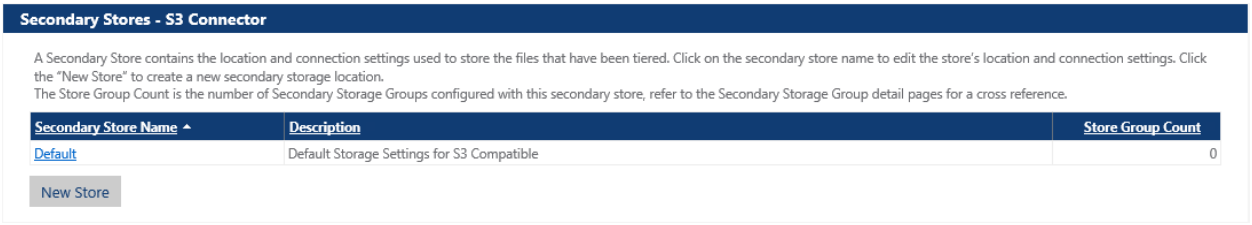
NOTE: The Task Services service account must be granted full permissions to the secondary store UNC paths as well as the primary server shares and directories it will be tiering files from.

Secondary Storage –S3 Connector

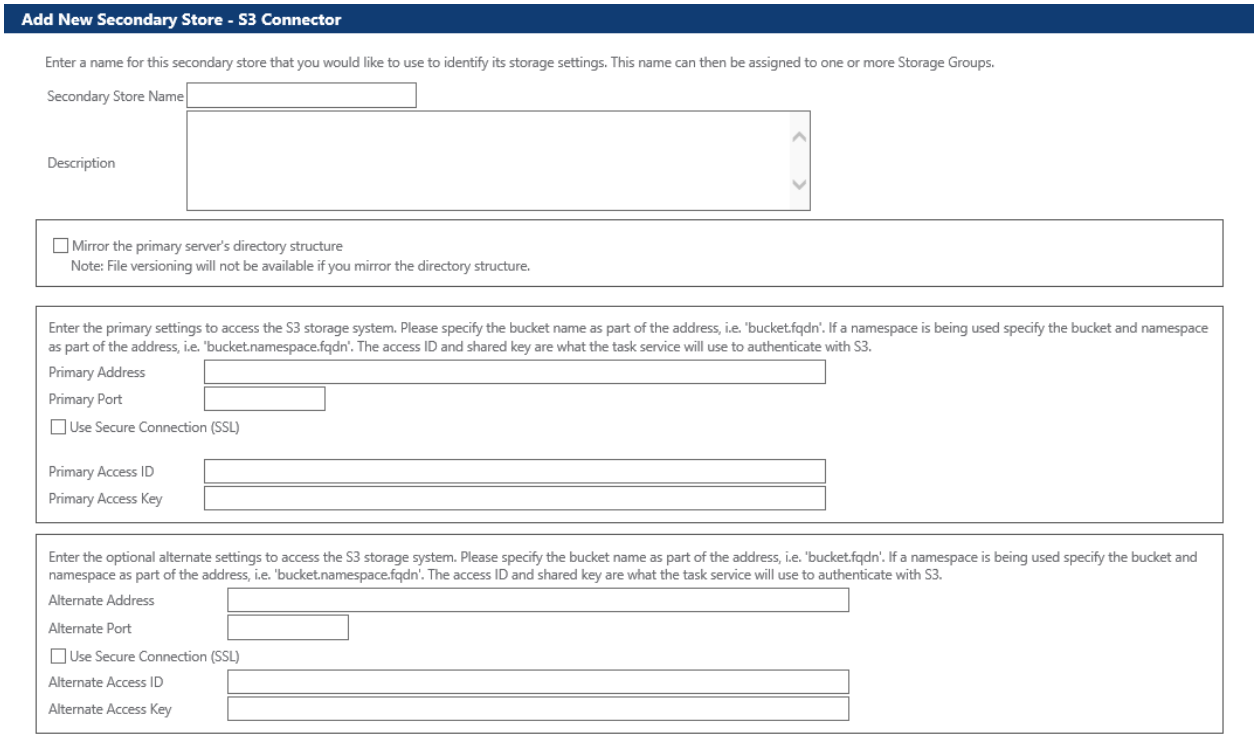
Adding/Editing an S3 Connector Secondary Store

1. Under **Secondary Storage** in the left-hand main menu, click **Secondary Storage > Storage Platforms > S3 Connector**.

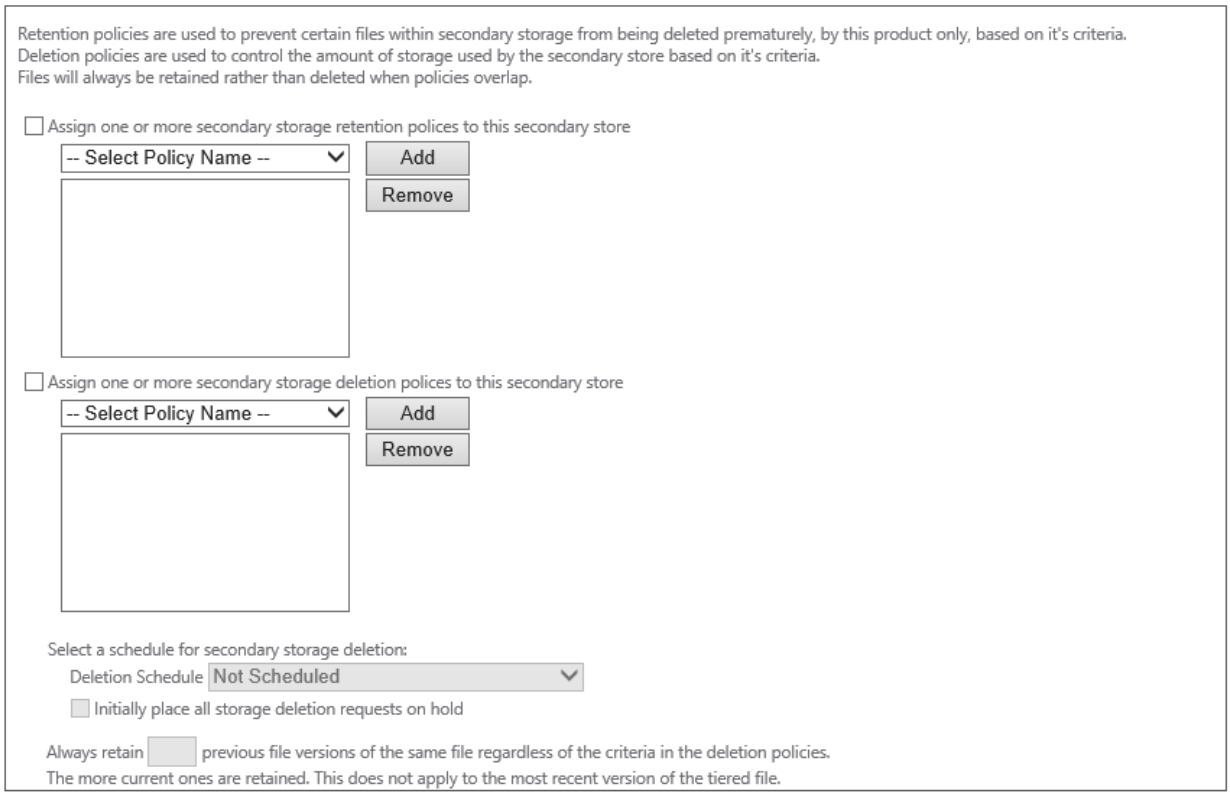
2. In the **Secondary Stores S3 Connector** section, click **New Store** or click the name of an already existing secondary store to edit these properties.



3. In the **Add New Secondary Store – S3 Connector Storage** 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.



4. At the bottom of the **Add New Secondary Store – S3 Connector** dialog box, retention and deletion policies can be added to the secondary store.



Field/Option	**Description**
Primary Address	Enter the primary settings to access the S3 storage system. Please specify the bucket name as part of the address, i.e. 'bucket.fqdn.com'.

Primary Port	Enter the port that will be used for communication with the AmazonS3 bucket. I.e, 80, or 443 for SSL

NOTE: The Task Services service account must be granted full permissions to the secondary store UNC paths as well as the primary server shares and directories it will be tiering files from.

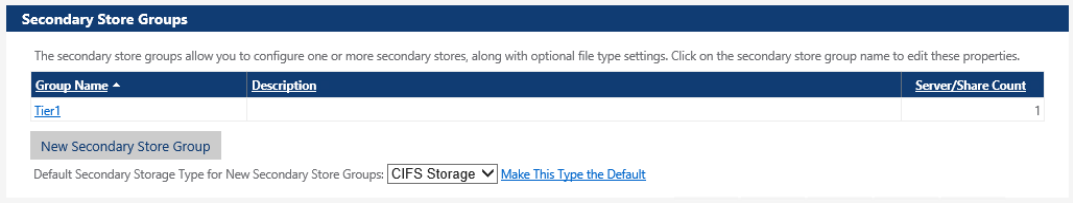
Adding/Editing Secondary Store Groups

One or more secondary store names can be assigned to a group. Files will be tiered to each of the secondary stores assigned to the group.

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

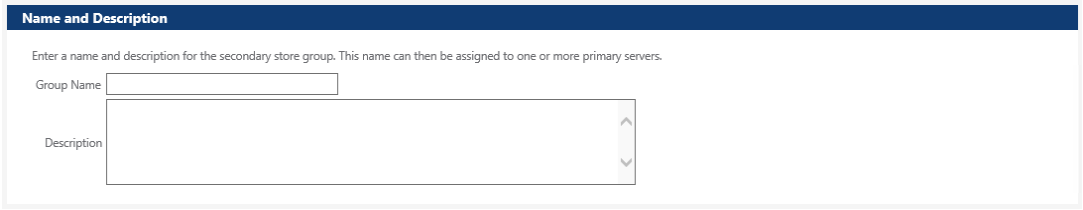
1. Under **Secondary Storage** in the left-hand main menu, click **Storage Configuration** > **Store Groups**.

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.

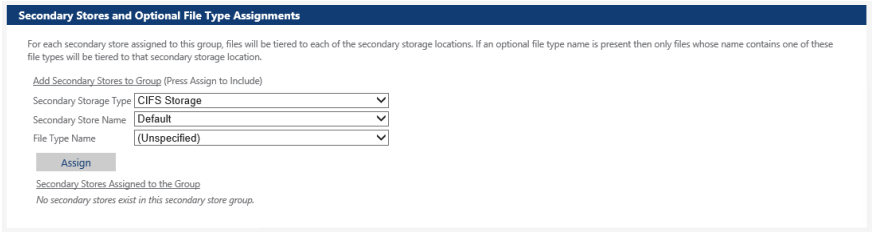


NOTE: New secondary storage groups being created will initially be assigned to the secondary storage type shown in the above drop down control.

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

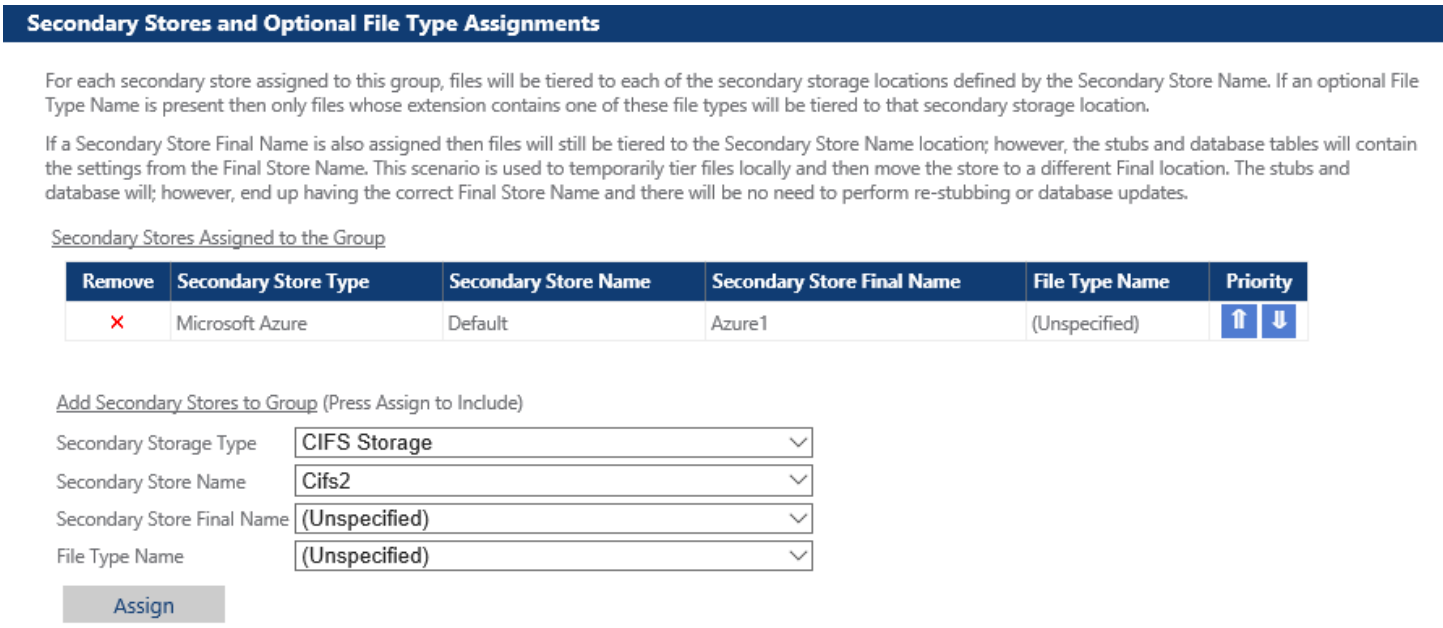


4. In the **Secondary Stores and Optional File Type Assignments** section, assign one or more secondary stores to a group.

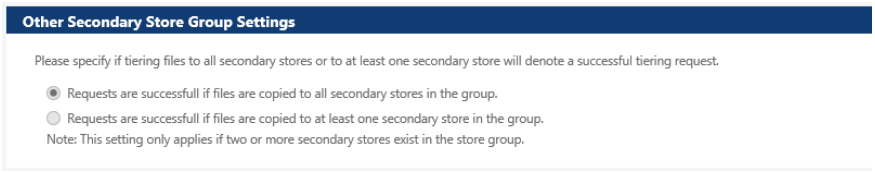


Mobility Football-Suitcase feature

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.



5. 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 types 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 of 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.

Configuring Primary Storage

Adding a New Primary Server

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 by the web 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:

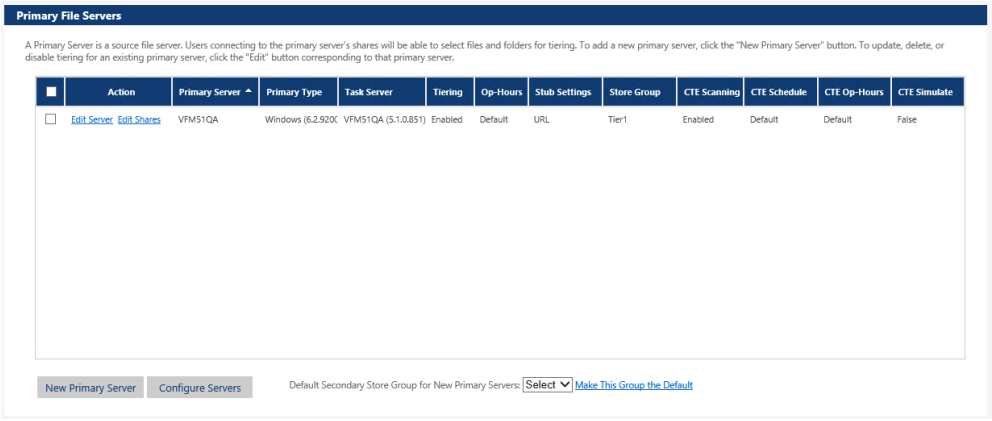
- The task service installer for a NAS or generic server will prompt for the initial NAS or generic host name. This host name will automatically be added to the primary servers, as described above.

- If you want the same task service to control more than one of the same type of NAS or generic server, then use the **New Primary Server** button.

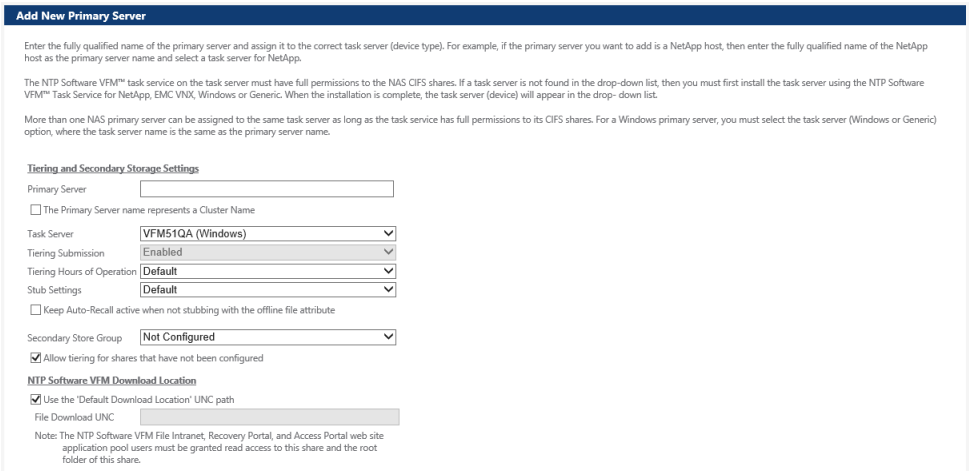
To add a new primary server, perform the following steps:

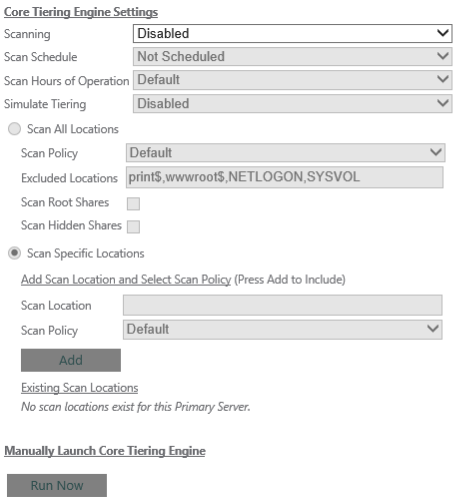
1. Under **Primary Storage** in the left-hand main menu, click **Primary File Servers**.

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 and the CTE settings 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 Software Mobility 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.
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.

Stub and Schedule Settings	Select the name of a stub and schedule setting that will be used for stubbing files on the primary server after the file has been tiered.
Keep Auto-Recall active when not stubbing with the offline file attribute NOTE: This setting is not present for primary servers using the Task Service for Generic task server.	If checked then the Auto-Recall connector will always be loaded and active even when files are being stubbed as HTM or URL file types instead of using the offline file attribute. This setting is useful when some files were previously being stubbed and set with the offline file attribute, but that is no longer the setting now. This allows for these previous files to be auto-recalled.

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.
Allow tiering for shares that have not been configured.	If checked then all of 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.

Use the Default Download Location UNC Path	If checked then all file download requests initiated from the Access Portal, Recovery Portal or MobilityFileIntranet 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 MobilityFileIntranet 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.

- **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 following applies to Task Services for Generic ONLY;**

  The optional Linux Settings are for future use and should be left unset.

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	"sharename\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.
- 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 Software Mobility 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.

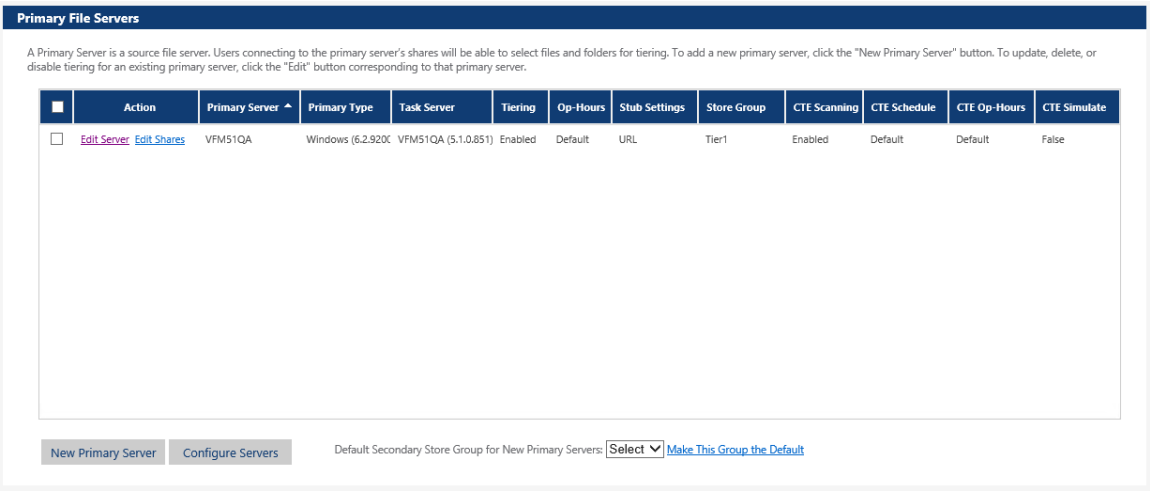
4. Click the **Add** button to add the new primary server.

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 **Edit Server** next to the 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:

1. Uninstall the DefendX Software Mobility Task Service first.
2. Click the Delete button in the **Edit Existing Primary Server** dialog box.

Configuring Primary Server Shares

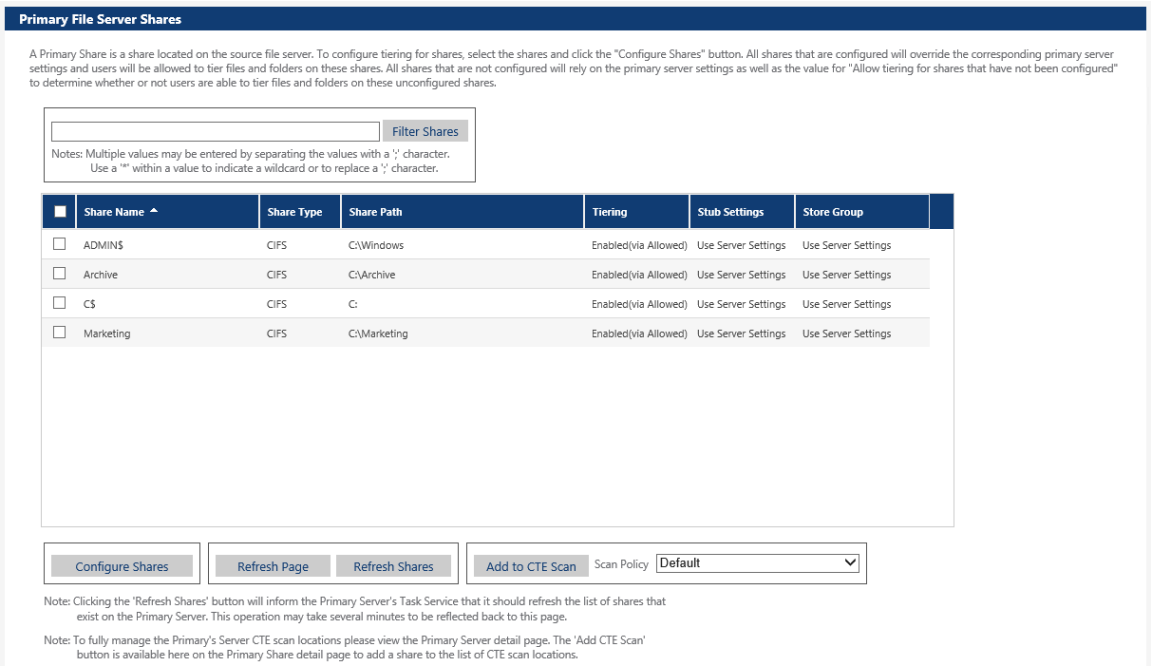
One or more shares and exports for a primary server can be configured with separate tiering options, stub and schedule settings and secondary storage group than the settings defined for the primary server itself.

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. .

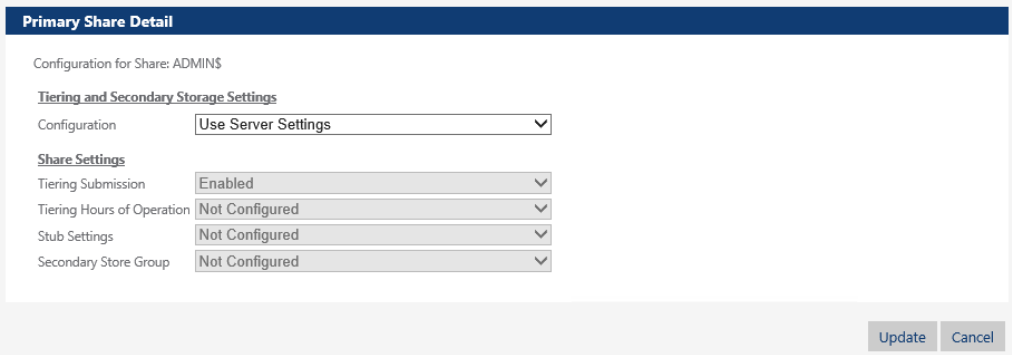


Field	Description
Filter Shares text box and button	Used to display share names using a wild card. This is useful when there are thousands of shares defined on the primary server.
Share Name column	Displays the name of the CIFS share or NFS export.

Share Type column	Indicates if the sharename 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 of 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.



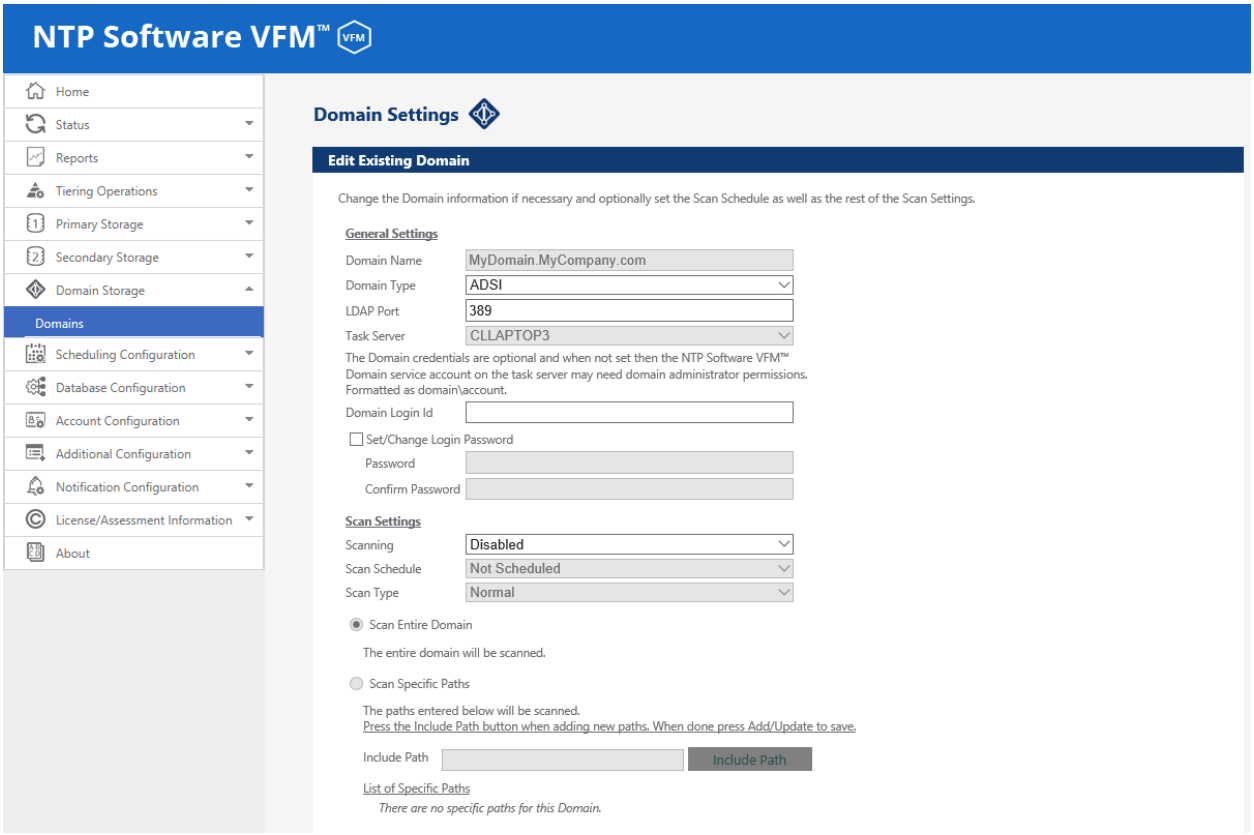
The tabular form outlined below displays the Configuration Options;

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.

Domain Configuration

There are three new pages to support the domain feature. "**Domain Storage - Domains**" page, "**Status – Domain Storage Status**" page and the "**Additional Configuration – Global Domain Attributes**" page.

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.



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.

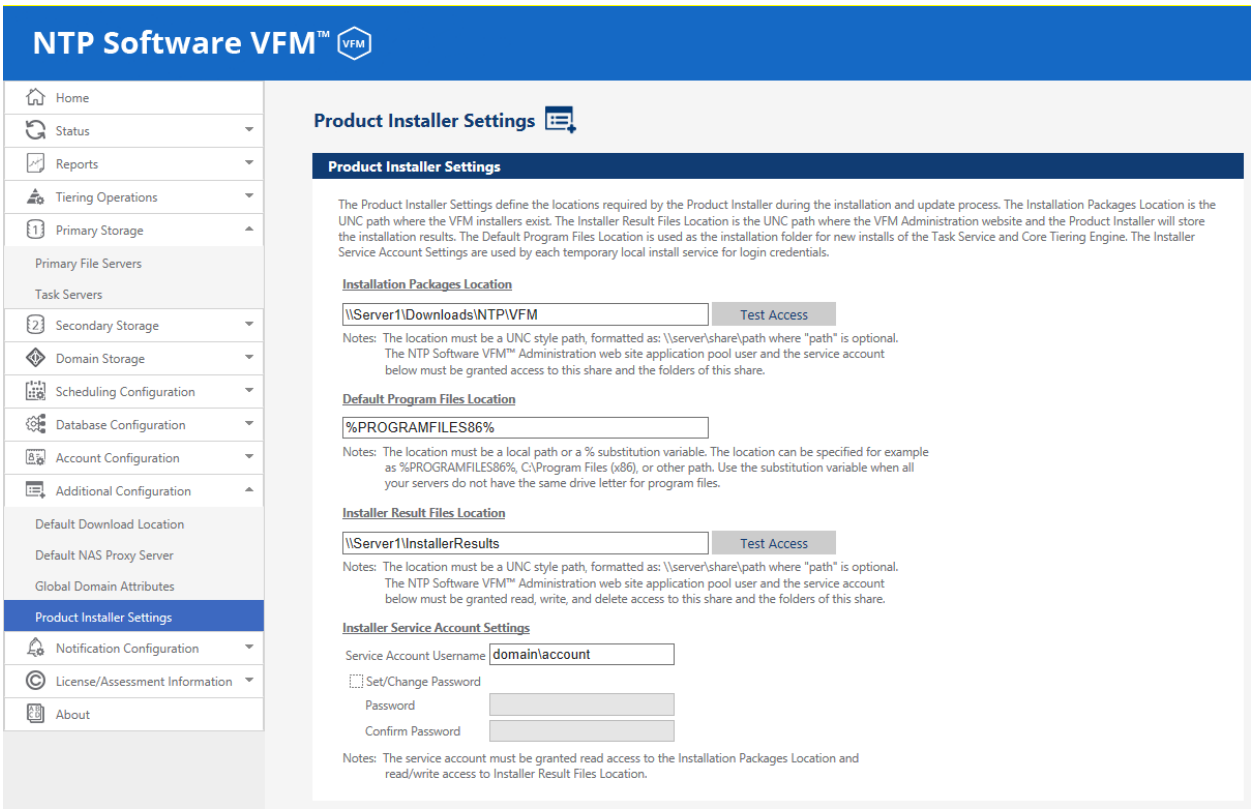
Scan Entire Domain: When this is selected then all users in the domain, starting from the root, will have their attributes collected.

Product Installer

There are two new pages to support the product install feature. "**Primary Storage – Task Servers**" page and the "**Additional Configuration – Product Installer Settings**" page.

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

Additional Configuration – Product Installer Settings Page



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 to. Note: “DefendXSoftware\Mobility\Task Service\<type>” will automatically be appended to this path when a task service is installed and “DefendXSoftware\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.

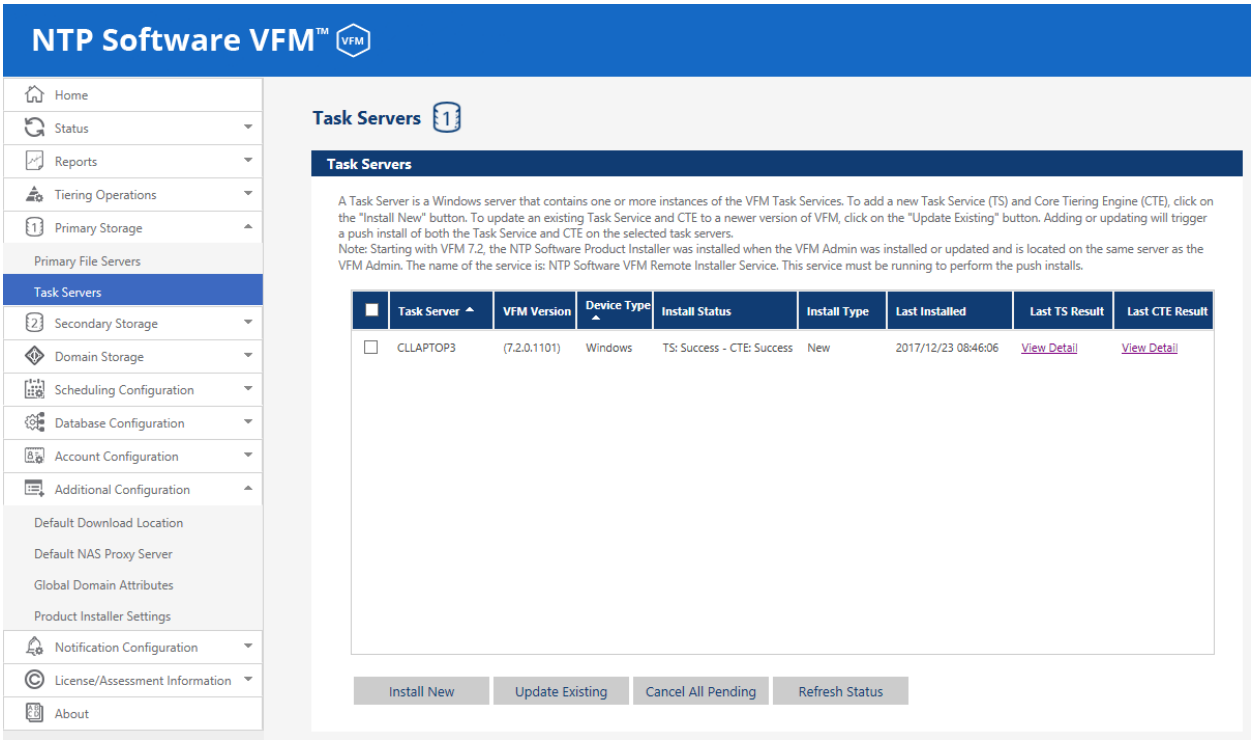
Installer Service Account Settings: This account will be used by the product installer service when temporarily installing a local service on each of the servers where a push install will occur. This account can be the same as the account used by the product installer’s service. This account must be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

Primary Storage – Task Servers Page

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.

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



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.

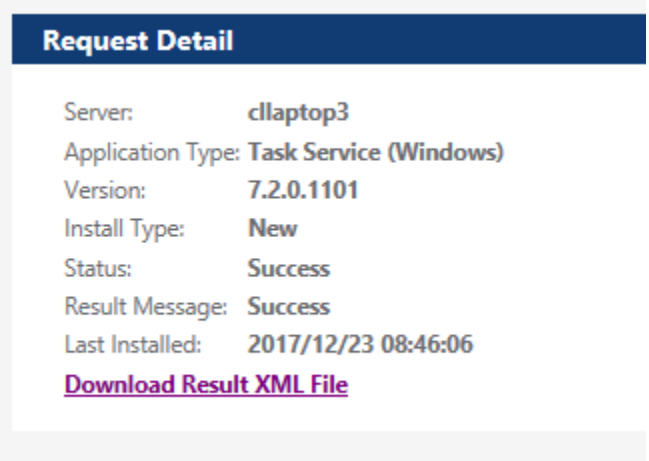
Install Type: Indicates whether it was a “New” install or an “Update”.

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.

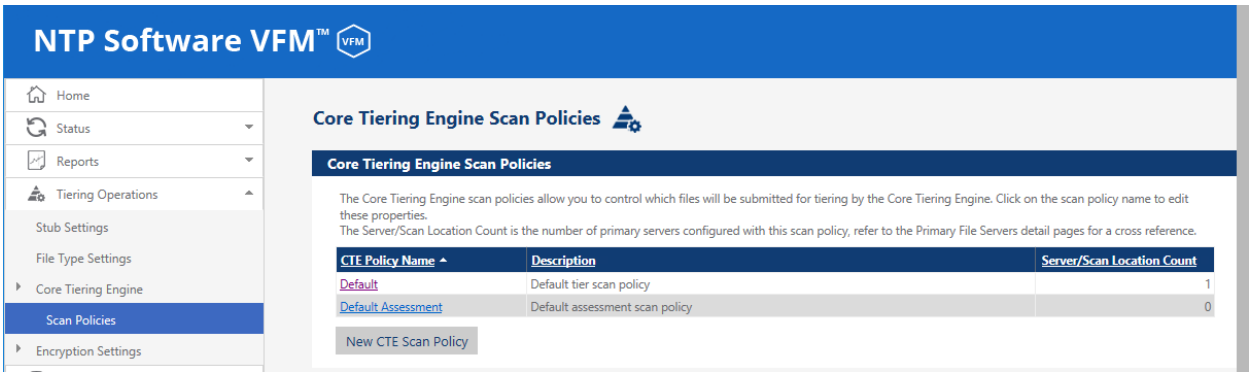
Clicking on "**View Detail**" for either the Last TS Result or the Last CTE Result will display additional information as seen below.



Clicking on the "**Download Result XML File**" will display the actual XML file created by the Mobility 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.

Assessment

Tiering Operations – Core Tiering Engine – Scan Policies Page

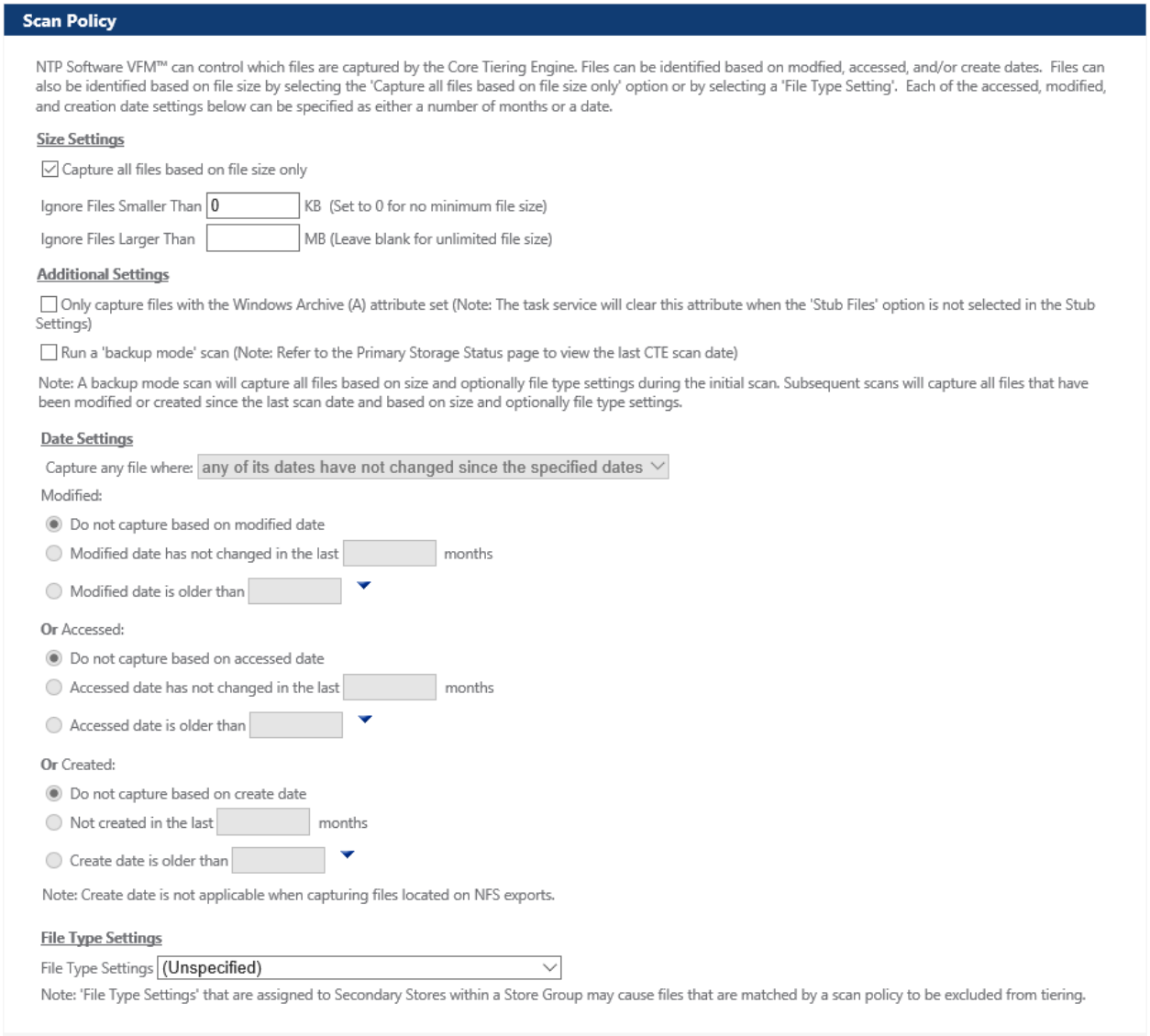


Default Assessment: A new default assessment policy will be created during the upgrade and is assigned as the default Core Tiering Engine policy when the primary server is set to a scan type of assessment.

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

Tiering Operations – Core Tiering Engine – Scan Policies – Default Assessment

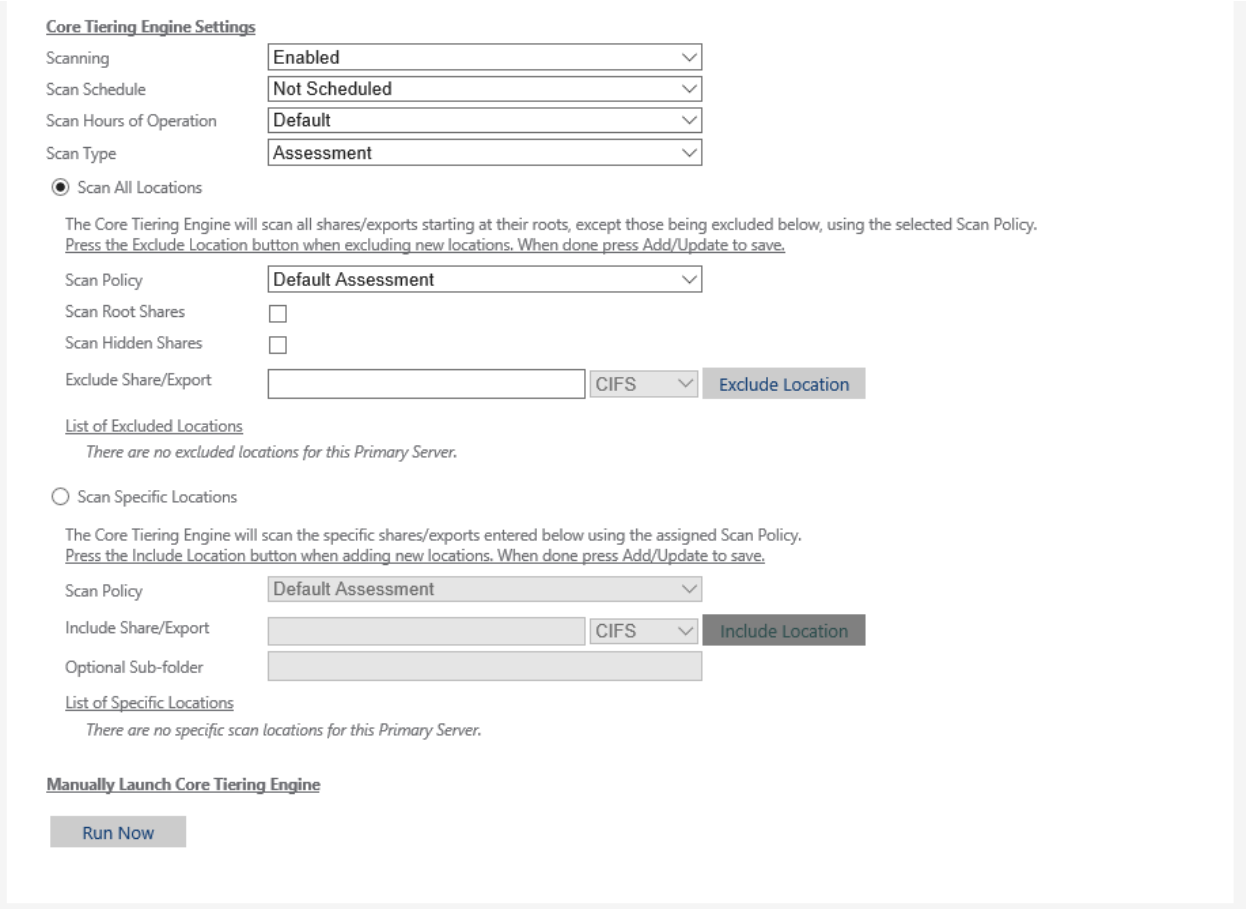
By default, the Default Assessment policy will scan all files based on file size only. Since the file size setting is set to zero, all files will be used in the assessment. However, this policy can be modified to assess files based on date and/or file types as well.



Primary Storage – Primary File Servers – Edit Server Page

Use the Edit Server page to set the Scan Type to “Assessment” under the Core Tiering Engine Settings.

- 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.

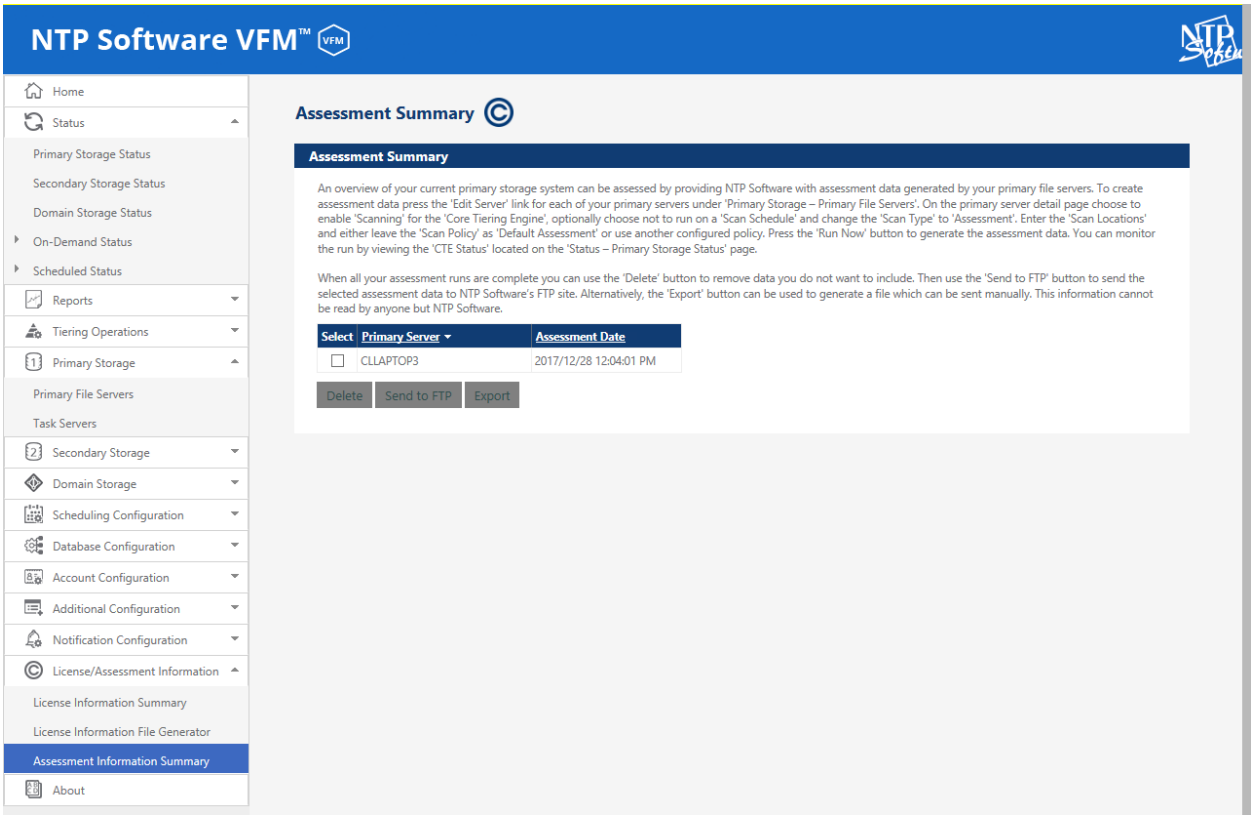


License/Assessment – Assessment Information Summary Page

When all of 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.

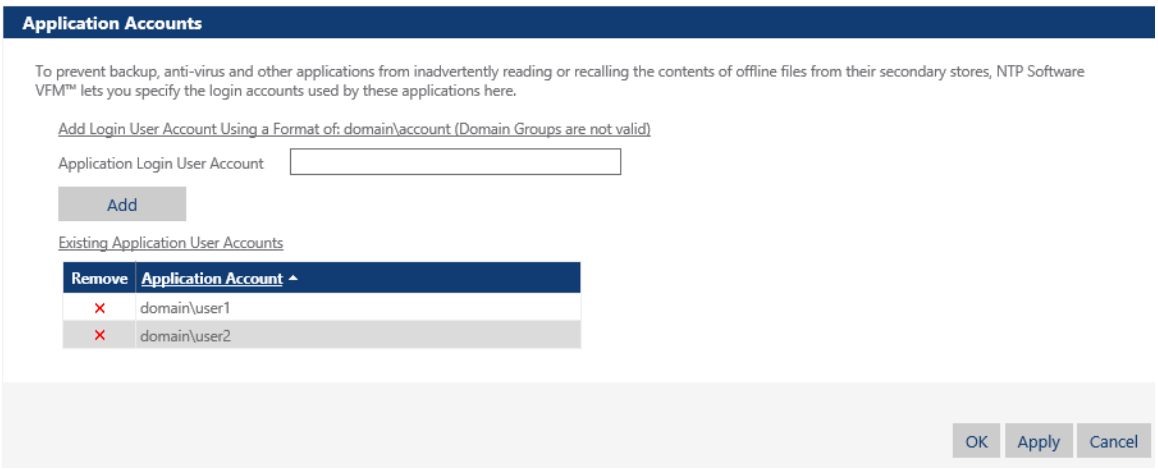
Send to FTP: Select the Primary Servers you want to include in the assessment report and press the Send to FTP button to encrypt and send the data to DefendX Software's FTP site.

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..

Account Configuration

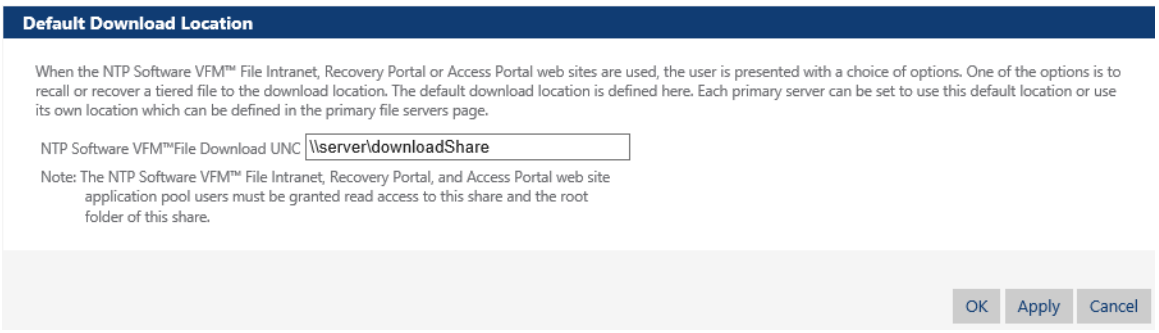
Use the **Application Accounts** section to define the Windows accounts that are exempt from being able to auto-recall files from secondary storage. This is used to prevent applications that backup files on the primary servers or scan for viruses from recalling all files stubbed with the offline file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

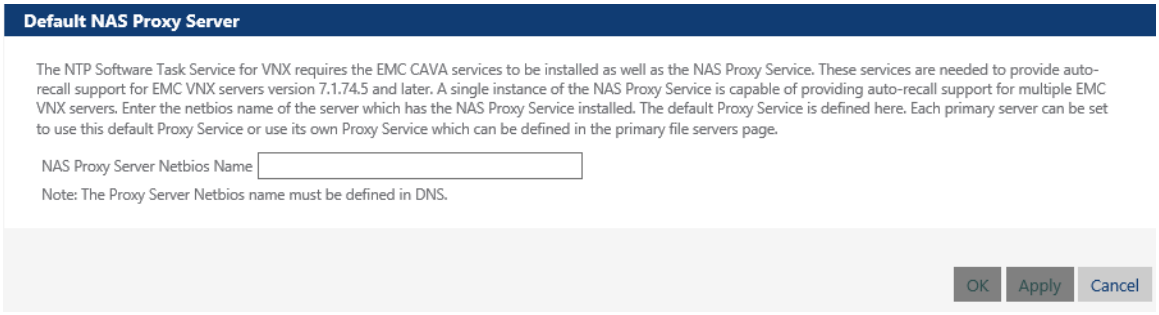


Additional Configuration

When the DefendX Software Mobility 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 Software Mobility 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.



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.

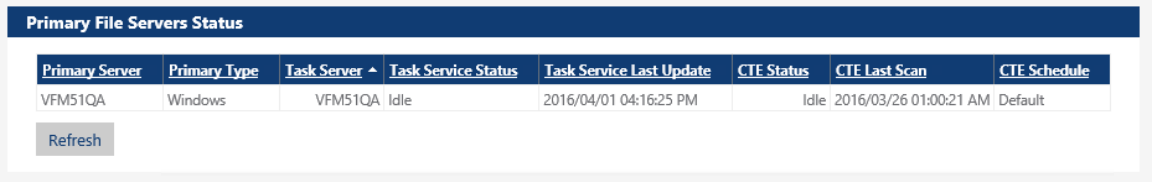


Mobility Status Pages

Viewing Primary File Server Status

This page displays the status of your DefendX Software Mobility 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). If it is executing, it will show the request ID that is currently 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 or not 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.

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.
- **"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.

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

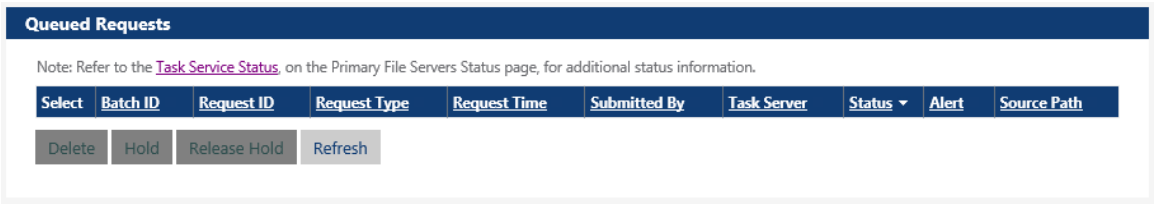
Viewing Queued Requests (On-Demand)

This page displays all the pending requests that have been submitted by the Right-Click Data Movement (RCDM) application or the Event-Driven Data Movement (EDDM) application. 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.

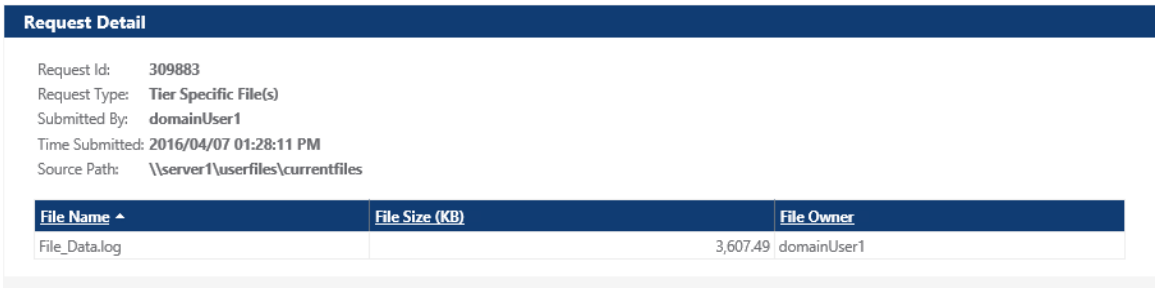
To view queued requests, perform the following steps:

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.

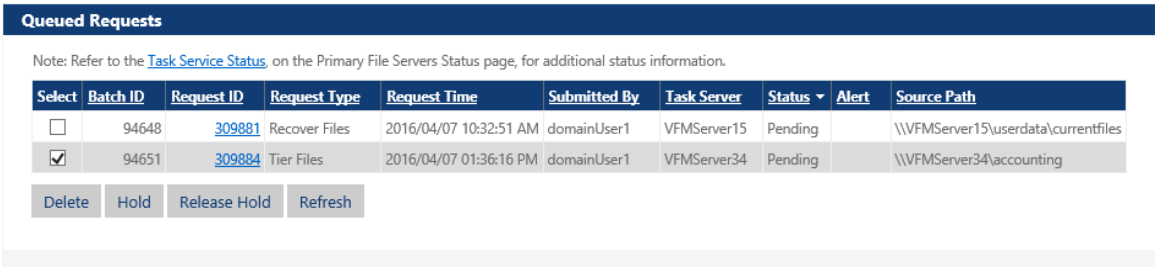


NOTES:

- 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.

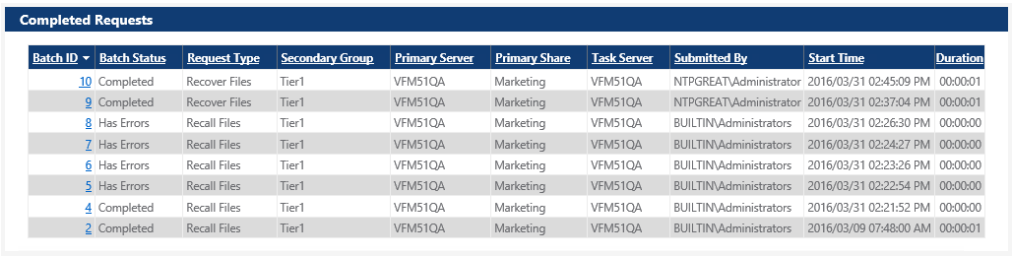


Viewing Completed Requests (On-Demand)

This page displays all of 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.



Completed Requests

Batch ID	Batch Status	Request Type	Secondary Group	Primary Server	Primary Share	Task Server	Submitted By	Start Time	Duration
10	Completed	Recover Files	Tier1	VFM51QA	Marketing	VFM51QA	NTPGREAT\Administrator	2016/03/31 02:45:09 PM	00:00:01
9	Completed	Recover Files	Tier1	VFM51QA	Marketing	VFM51QA	NTPGREAT\Administrator	2016/03/31 02:37:04 PM	00:00:01
8	Has Errors	Recall Files	Tier1	VFM51QA	Marketing	VFM51QA	BUILTIN\Administrators	2016/03/31 02:26:30 PM	00:00:00
7	Has Errors	Recall Files	Tier1	VFM51QA	Marketing	VFM51QA	BUILTIN\Administrators	2016/03/31 02:24:27 PM	00:00:00
6	Has Errors	Recall Files	Tier1	VFM51QA	Marketing	VFM51QA	BUILTIN\Administrators	2016/03/31 02:23:26 PM	00:00:00
5	Has Errors	Recall Files	Tier1	VFM51QA	Marketing	VFM51QA	BUILTIN\Administrators	2016/03/31 02:22:54 PM	00:00:00
4	Completed	Recall Files	Tier1	VFM51QA	Marketing	VFM51QA	BUILTIN\Administrators	2016/03/31 02:21:52 PM	00:00:00
2	Completed	Recall Files	Tier1	VFM51QA	Marketing	VFM51QA	BUILTIN\Administrators	2016/03/09 07:48:00 AM	00:00:01

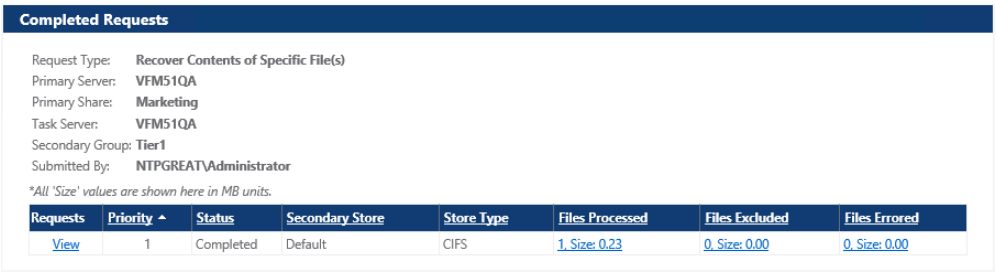
2. To view the details of the batch, click the link for the Batch ID. This will show the details of the batch.

Completed Requests

Batch Id: **10**
Request Type: **Recover Stubs Of Specific File(s)**
Number of Requests: **1**
Submitted By: **NTPGREAT\Administrator**
Time Submitted: **2016/03/31 02:45:05 PM**
Time Started: **2016/03/31 02:45:09 PM**
Duration: **00:00:01**
Folder Counts: **Processed: 1, Excluded: 0, Errored: 0**
Files Processed: **1, Total Size: 0.82 MB**
Files Excluded: **0, Total Size: 0.00 MB**
Files Access Denied: **0, Total Size: 0.00 MB**
Files In-Use: **0, Total Size: 0.00 MB**
Files Errored: **0, Total Size: 0.00 MB**

Request ID	Request Status	Task Server	Start Time	Duration	Source Path
10	Completed	VFM51QA	2016/03/31 02:45:09 PM	00:00:01	\\VFM51QA\Marketing

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.



Completed Requests

Request Type: **Recover Contents of Specific File(s)**
Primary Server: **VFM51QA**
Primary Share: **Marketing**
Task Server: **VFM51QA**
Secondary Group: **Tier1**
Submitted By: **NTPGREAT\Administrator**

**All 'Size' values are shown here in MB units.*

Requests	Priority	Status	Secondary Store	Store Type	Files Processed	Files Excluded	Files Errored
View	1	Completed	Default	CIFS	1, Size: 0.23	0, Size: 0.00	0, Size: 0.00

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

NOTES:

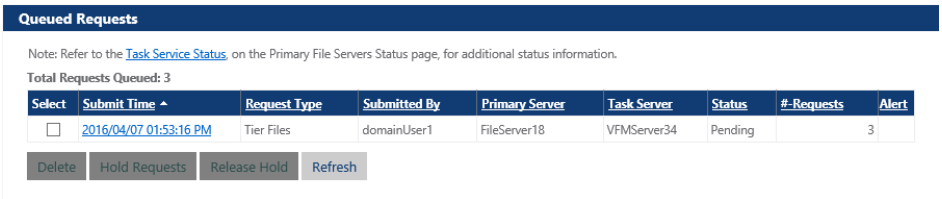
- If the request type was to tier or recall specific files, then those file names and sizes will appear.
- If the request type was to tier or recall a folder, then the file grid will not appear.

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.

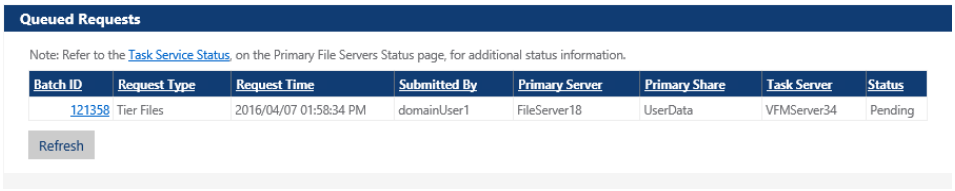
Viewing Queued Requests (CTE)

This page displays the requests that have been submitted by a Core Tiering Engine (CTE) scan. The requests are sorted by the date and time the Core Tiering Engine was executed. You can drill into and view additional information. To view queued requests, perform the following steps:

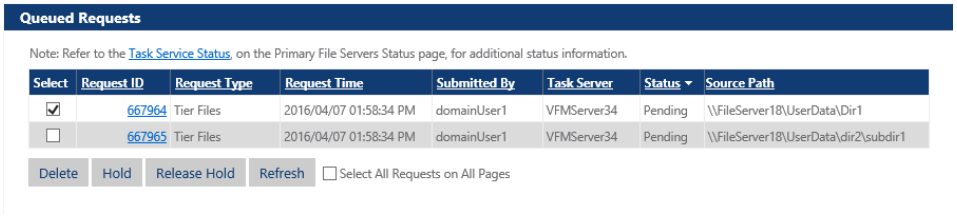
1. Under **Status** in the left-hand main menu, click **Core Tiering Engine Status**>**Queued Requests**. The **Queued Scans** page is displayed.



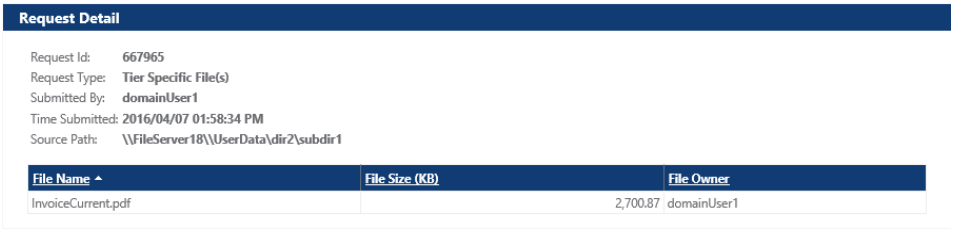
2. To view the details of the request, click the link for the Request Time. This will show the details of the request and the current status. The Core Tiering Engine divides a scan into multiple batches. Each batch contains multiple requests and each request contains multiple files that will be tiered. 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 RequestID.

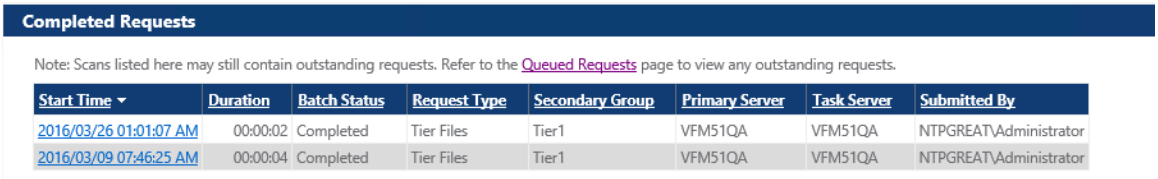


Viewing Completed Requests (CTE)

This page displays all of 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 **Core Tiering Engine Status**>**Completed Requests**. The **Completed Requests** page is displayed. The requests are sorted by the date and time the Core Tiering Engine was executed.

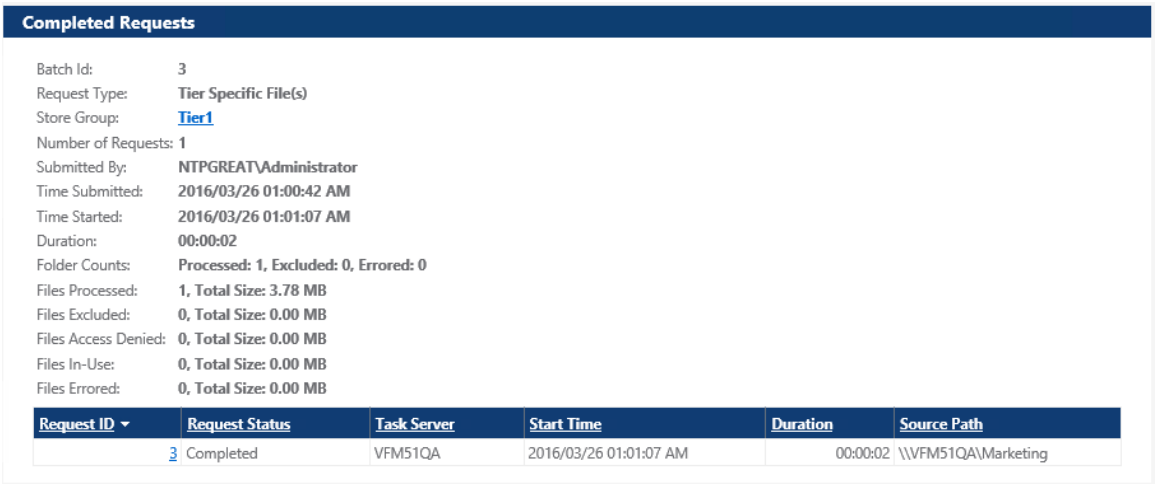


2. The Core Tiering Engine divides a scan into multiple batches. Each batch contains multiple requests and each request contains the results of files that were tiered. By drilling into a

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.

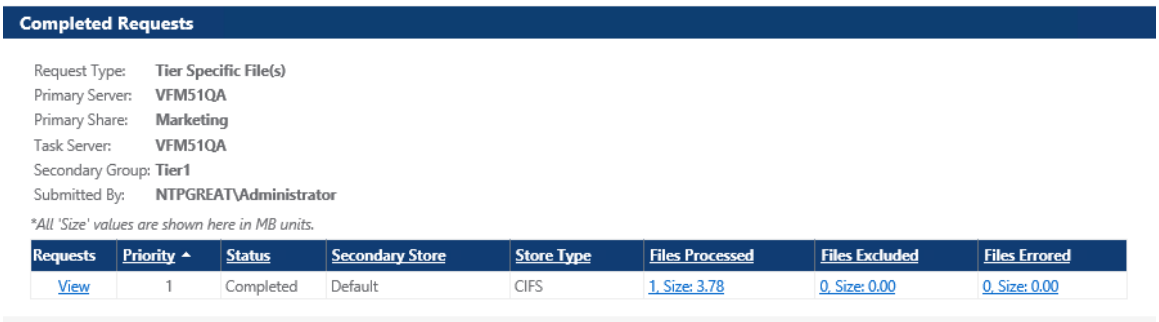
3. To view the details of the request, click the link for the Start Time. This will show the status for each batch.

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

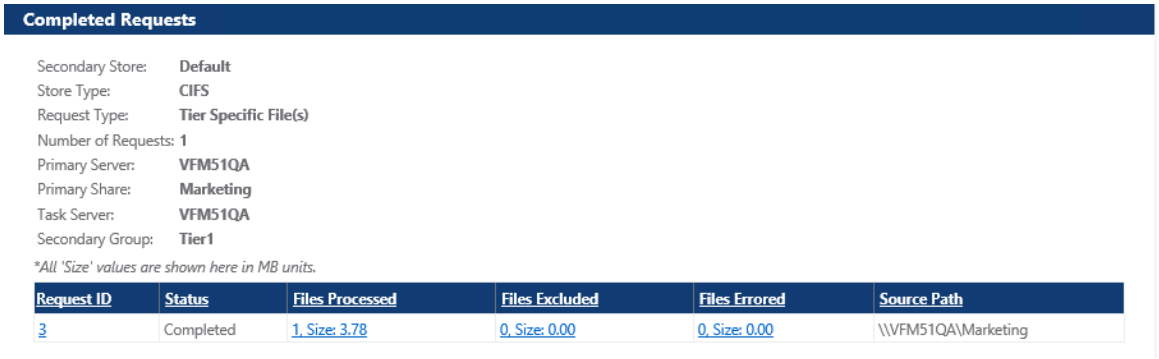


5. To view the results of the files being tiered to each of the secondary stores defined in the storage group, click on the Store Group link.

> **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.



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



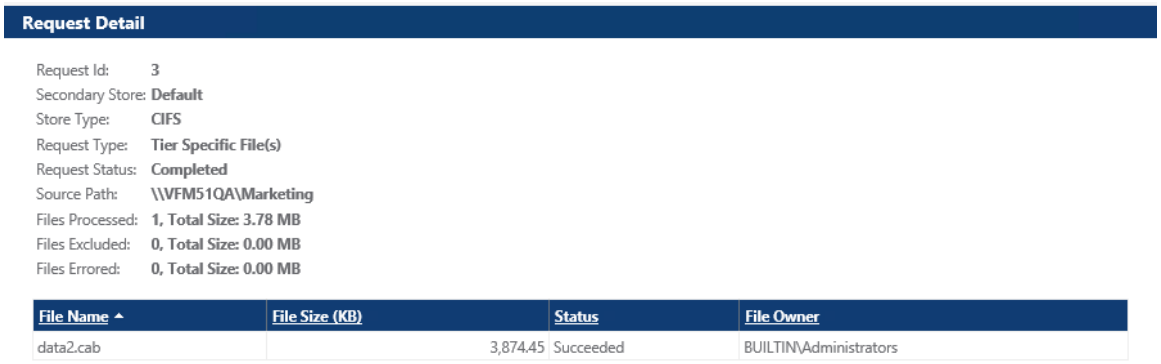
Completed Requests

Secondary Store: **Default**
Store Type: **CIFS**
Request Type: **Tier Specific File(s)**
Number of Requests: **1**
Primary Server: **VFM51QA**
Primary Share: **Marketing**
Task Server: **VFM51QA**
Secondary Group: **Tier1**

**All 'Size' values are shown here in MB units.*

Request ID	Status	Files Processed	Files Excluded	Files Errored	Source Path
3	Completed	1, Size: 3.78	0, Size: 0.00	0, Size: 0.00	\\VFM51QA\Marketing

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



Request Detail

Request Id: **3**
Secondary Store: **Default**
Store Type: **CIFS**
Request Type: **Tier Specific File(s)**
Request Status: **Completed**
Source Path: **\\VFM51QA\Marketing**
Files Processed: **1, Total Size: 3.78 MB**
Files Excluded: **0, Total Size: 0.00 MB**
Files Errored: **0, Total Size: 0.00 MB**

File Name ▲	File Size (KB)	Status	File Owner
data2.cab	3,874.45	Succeeded	BUILTIN\Administrators

8. 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 or not the file was stubbed or a warning or error occurred.

Completed Requests

Batch Id: 3
Request Type: Tier Specific File(s)
Store Group: Tier1
Number of Requests: 1
Submitted By: NTPGREAT\Administrator
Time Submitted: 2016/03/26 01:00:42 AM
Time Started: 2016/03/26 01:01:07 AM
Duration: 00:00:02
Folder Counts: Processed: 1, Excluded: 0, Errored: 0
Files Processed: 1, Total Size: 3.78 MB
Files Excluded: 0, Total Size: 0.00 MB
Files Access Denied: 0, Total Size: 0.00 MB
Files In-Use: 0, Total Size: 0.00 MB
Files Errored: 0, Total Size: 0.00 MB

Request ID	Request Status	Task Server	Start Time	Duration	Source Path
3	Completed	VFM51QA	2016/03/26 01:01:07 AM	00:00:02	\\VFM51QA\Marketing

Request Detail

Request Id: 3
Request Type: Tier Specific File(s)
Request Status: Completed
Submitted By: NTPGREAT\Administrator
Time Submitted: 2016/03/26 01:00:42 AM
Time Started: 2016/03/26 01:01:07 AM
Duration: 00:00:02
Source Path: \\VFM51QA\Marketing
Folder Counts: Processed: 1, Excluded: 0, Errored: 0
Files Processed: 1, Total Size: 3.78 MB
Files Excluded: 0, Total Size: 0.00 MB
Files Access Denied: 0, Total Size: 0.00 MB
Files In-Use: 0, Total Size: 0.00 MB
Files Errored: 0, Total Size: 0.00 MB

File Name	File Size (KB)	Status	File Owner
data2.cab	3,874.45	File Tiered, (URL Stub)	BUILTIN\Administrators

DefendX Software Mobility Reports

Viewing Tiering Summary

This page displays the total number of tier requests processed and storage savings by all primary servers for the past 7 days and the past 6 months.

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

To view the data movement summary, click **Home** in the left-hand main menu. The **Tiering Summary** page is displayed.

The top section shows the total number of requests that have been made by end users. There are 6 charts on the screen divided into 2 rows; the top row shows what happened in the last 7 days, and the bottom row shows what happened in the last 6 months.

The tiering requests, files tiered, and storage usage savings shown in the top charts represent what the user has done during the last week.

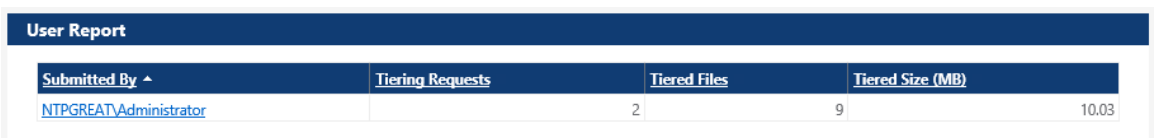
Similarly, the bottom charts show what happened on a monthly basis, with the number of tiering requests, number of files tiered, and storage usage savings the user has achieved during the last 6 months.

Viewing Requests By User

This page displays the number of tier and recall 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 user name. 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.

Viewing Requests By Primary Server

This page displays the number of tier and recall 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.

Database Appendix

Appendix Name	Database Appendix
Default Names for Mobility Databases	DefendXSoftwareMobility: This is the configuration database, it holds configuration data as well as queued and completed request data. DefendXSoftwareMobilityStores: This is the stores database; it holds all tiered file data.
Steps to move the location of the configuration database	• Using Microsoft SQL Server Management Studio on the current database server; Backup the configuration database to a file. • Using Microsoft SQL Server Management Studio on the new database server; 1. Create the database on the new server. It is recommended to use a collation of: "SQL_Latin1_General_CP1_CI_AS" 2. Restore the configuration database to the new server. 3. Remove the "oddm_web_svc" user from the "Security" item under the configuration database, it is no longer valid. Remove the schema, if prompted to do so.

	4. Create a new “Login” under the main “Security” item, using a login name of: “oddm_web_svc” a. Set it to use SQL Server authentication. b. Set the default database to the name of the configuration database, default is: “DefendXSoftwareMobility”. c. Set the default language to “English”. d. Server Roles can be left as all unchecked. e. User Mapping: Assign “db_backupoperator”, “db_datareader”, “db_datawriter” and “public” to the configuration database. 5. NOTE: The “oddm_web_svc” user should now be a “User” in the “Security” item under the configuration database too. This occurred during step 4b. Select the “oddm_web_svc” user in the “Security” item under the configuration database and choose “Properties”. b. On the “Securables” tab, “Add” the three stored procedures and grant “Execute” permissions to each. The three stored procedures are: I. dbo.BackupDatabase II. dbo.DeleteAgedRequests III. dbo.DeleteRequest 6. Open the DefendX Software Mobility Administration web site and update the database settings for the configuration database. Be sure to update the password field too. a. The database move is now complete

Steps to move the location of the stores database	• Using Microsoft SQL Server Management Studio on the current database server Backup the stores database to a file. • Using Microsoft SQL Server Management Studio on the new database server 1. Create the database on the new server. It is recommended to use a collation of: "SQL_Latin1_General_CP1_CI_AS" 2. Restore the stores database to the new server. 3. Remove the "oddm_web_svc" user from the "Security" item under the stores database, it is no longer valid. Remove the schema too if prompted to do so. 4. If the new stores database server is the same as the configuration database server then skip step 5 and go to step 6. 5. Create a new "Login" under the main "Security" item, using a login name of: "oddm_web_svc" a. Set it to use SQL Server authentication. b. Set the default database to the name of the stores database, default is: "DefendXSoftwareMobilityStores". c. Set the default language to "English". d. Server Roles can be left as all unchecked. e. User Mapping: Assign "db_backupoperator", "db_datareader", "db_datawriter" and "public" to the stores database. f. Go to Step 7.

	6. If step 5 was performed then skip this step and go to step 7, otherwise the "oddm_web_svc" login must be added to the "Security – User" item under the stores database as a new user: a. User name: "oddm_web_svc". b. Login name: "oddm_web_svc" (select it from the browse menu). c. Assign database roles of: "db_backupoperator", "db_datareader", "db_datawriter".

	7. Create a new “Login” under the main “Security” item, using a login name of: “domain\account” where this account is the same as the service account used by the DefendX Software Mobility Task Services. If the task services use different accounts then Steps 7 and 8 must be performed for each account. a. Set it to use Windows authentication. b. Set the default database to the name of the stores database, default is: “DefendXSoftwareMobilityStores”. c. Set the default language to “English”. d. Server Roles can be left as all unchecked. e. User Mapping: Assign “db_backupoperator”, “db_datareader”, “db_datawriter”, “db_owner” and “public” to the stores database. 8. NOTE: The “domain\account” user should now be a “User” in the “Security” item under the stores database too. This occurred during step 7b. a. Select the “domain\account” user in the “Security” item under the stores database and choose “Properties”. b. On the “Securables” tab, “Add” the stored procedure and grant “Execute” permissions to it. The stored procedure is: i. dbo.spNextFileId 9. Open the DefendX Software Mobility Administration web site and update the database settings for the stores database. Be sure to update the password field too. 10. The database move is now complete.

Windows Cluster Appendix

Appendix Name	**Windows Cluster Appendix**
Installing the Task Service for Windows on the cluster server nodes	1. Install a Task Service for Windows on each of the 2. Cluster server nodes.

	In the DefendX Software Mobility Administration web site wait for each of the task servers to display on the Primary Servers page. 3. Decide whether or not you want to allow tiering of files located on each of the task servers local shares. Local shares are not part of the clustered shares. a. If you want to allow tiering upon local shares then click on the “edit” selection for each of these servers on the Primary Server page and select your configuration options. b. If you do NOT want to allow tiering upon the local shares then click on the “edit” selection for each of these servers on the Primary Server page and set “Tiering” to “Disabled”.
Configuring the Task Services for Windows for use with the cluster	1. On the Primary Servers page, click on the “New 2. Primary Server” button. Enter the name of the cluster in the “Primary Server” field. 3. Check the checkbox for “The Primary Server name represents a cluster name” 4. 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. 5. 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”. 6. Select the rest of your configuration options.
Enabling Auto-Recall for the cluster when the cluster is configured to stub files using the offline file attribute	If both of these bullet items are true, then perform this step. Otherwise, there is nothing more to do and you are done. □ □ The cluster will be stubbing files using the offline file attribute.

	▯ The cluster server nodes are either disabled or will be stubbing files using a different stubbing option, i.e. not using the offline file attribute. a. Auto-Recall must be kept enabled on each of the cluster server nodes so that auto-recall of files located on the cluster will function. To allow this do: i. On the Primary Servers page, “edit” each of the cluster server nodes and check the checkbox for “Keep Auto-Recall active when not stubbing with the offline file attribute. ii. Note: There is no need to check the checkbox for “Keep Auto-Recall active when not stubbing with the offline file attribute” on the cluster. It will have no effect.
Additional configuration when in an environment whose tiered files are being replicated and the source files are stubbed using the offline file attribute	For auto-recall to function properly, in this type of environment, both of the Windows server nodes and the Cluster node must be configured to use the same exact secondary store name, otherwise auto-recall may fail trying to retrieve a replicated file on the secondary storage device.

Controlling User Access to the DefendX Software Mobility Administration Website Appendix

Appendix Name	**Controlling User Access to the DefendX Software Mobility Administration Website.**

To make sure that Windows Authentication is turned on for the Admin site.	• Open IIS Manager. • Expand the Default website and select the "MobilityAdmin" virtual directory. Note: The virtual directory name may be "ODDMAdmin" if the admin was upgraded from an earlier version. • Double click on Authentication and ensure Windows Authentication is enabled and all other authentication methods are set to disabled.
Enabling SSL on the Administration Web Site	• Open IIS Manager. • Expand the Default website and click on the "MobilityAdmin" virtual directory. Note: The virtual directory name may be "ODDMAdmin" if the admin was upgraded from an earlier version. • 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 the SSL section below.
Allowing Authorization to specific users and groups to access the DefendX Software Mobility Administration site	Go to the Admin site installation folder, by default it is installed here: "C:\Program Files (x86)\DefendXSoftware\Mobility\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"/>. 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"/>. Separate each group account with a comma. When allowing both users and groups, simply insert the "<allow roles" line under the "<allow users" line in the xml above. **<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.**
DefendX Software Mobility Task Service Accounts need to be Authorized	• When authorization to specific users and groups was configured above, then: 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 admin site. • When authorization to specific users and groups was not configured, then: o The administration web site's authentication must be enabled for Windows Authentication and/or Anonymous. This will allow the task services access to the admin site.

DefendX Software Mobility Access and Recovery Portals and the MobilityFileIntranet sites need to be Authorized	▯ When authorization to specific users and groups was configured above, then: o If the portal is installed on the same host as the admin site then add **"NT AUTHORITY\NETWORK SERVICE"** to the list of "allow users". o If the portal is installed on a different host than the 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. ▯ When authorization to specific users and groups was not configured, then: o The administration web site's authentication must be enabled for Windows Authentication and/or Anonymous. This will allow the portal access to the admin site.
DefendX Software Mobility Administration Web Site Prompt for Credentials	▯ When authorization to specific users and groups was configured above, then: ▯ 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 admin site, because Windows Authentication will automatically allow them access. This is usually the case when using 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. ▯ When authorization to specific users and groups was not configured, then: o If the administration web site's authentication has Anonymous enabled then users will not be prompted for credentials. o If the administration web site's authentication has Windows Authentication enabled then users may or may not be prompted for credentials.

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/MobilityAdmin Notes: ○ If the name of the administration web site is “ODDMAdmin” then use it instead of “MobilityAdmin”. ○ If SSL was configured for the administration web site then use “https” instead of “http”.
SSL Configuration for DefendX Software Mobility 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 admin site. The format of the URL should be either: http://WebServer:80/MobilityAdmin/ODDMService.asmx (A port must be specified unless using port 80 which is the default port and is optional). https://WebServer:443/MobilityAdmin/ODDMService.asmx (A port must be specified unless using port 80 which is the default port and is optional). **For each Task Service** • Go to their installation directory, default is: “C:\Program Files (x86)\DefendXSoftware\Mobility\Task Service\<platform>” • Edit the MainConfig.xml file • Change the <URL> value to use https and include the port number if different than port 80. • Save the file and restart the task service.

	For the Access and Recovery Portals and the MobilityFileIntranet sites • Go to their installation directory, default is: “C:\Program Files (x86)\DefendXSoftware\Mobility\<appname>” • Edit the Web.Config file • Change “http” to “https” and include the port number if different than port 80 for each line found, there may be multiple lines, that contains the “ODDMService.asmx” text. **For Right-Click Data Movement (RCDM)** • Open the registry by running “regedt32” • “HKEY_LOCAL_MACHINE\SOFTWARE\DefendXSoftware\Right-Click Tiering\Data” • Change the value for “OddmUrl” to use “https” and include the port number if different than port 80 • 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. **For Event-Driven Data Movement (EDDM)** • Go to its installation directory, default is: “C:\Program Files (x86)\DefendXSoftware\Mobility\EDDM” • Edit the cseda.inf file • Change the value for “OddmUrl=” to use “https” and include the port number if different than port 80 □ 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