opentext™ | File Dynamics

Data Owner Client

Version 24.1

Legal Notices

Condrey Corporation makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Condrey Corporation reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Condrey Corporation makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Condrey Corporation reserves the right to make changes to any and all parts of the software at any time, without obligation to notify any person or entity of such revisions or changes. See the Software EULA for full license and warranty information with regard to the Software.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export, or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. Condrey Corporation assumes no responsibility for your failure to obtain any necessary export approvals.

Copyright © 2024 Condrey Corporation. All Rights Reserved.

No part of this publication may be reproduced, photocopied, or transmitted in any fashion with out the express written consent of the publisher.

Condrey Corporation
122 North Laurens St.
Greenville, SC 29601
U.S.A.

http://condrey.co

Third Party Systems

The software is designed to run in an environment containing third party elements meeting certain prerequisites. These may include operating systems, directory services, databases, and other components or technologies. See the accompanying prerequisites list for details.

The software may require a minimum version of these elements in order to function. Further, these elements may require appropriate configuration and resources such as computing, memory, storage, or bandwidth in order for the software to be able to perform in a way that meets the customer requirements. The download, installation, performance, upgrade, backup, troubleshooting, and management of these elements is the responsibility of the customer using the third party vendor's documentation and guidance.

Third party systems emulating any these elements must fully adhere to and support the appropriate APIs, standards, and protocols in order for the software to function. Support of the software in conjunction with such emulating third party elements is determined on a case-by-case basis and may change at any time.

Contents

Data Owner Client ... ***1***

Version 24.1 ... *1*

Legal Notices ... ***3***

Third Party Systems ... ***5***

Contents ... ***7***

About This Guide ... ***1***

Audience ... *1*

1 - Introduction ... ***3***

1.1 - About the Data Owner Client ... *3*

1.2 - Data Owners ... *3*

1 - Web Client ... ***4***

1.3 - Accessing the Data Owner Service ... *4*

1.4 - Security Notifications and Actions ... *5*

1.4.1 - Viewing Security Policies ... *5*

1.4.2 - Viewing Notifications ... *6*

1.4.3 - Generating Detail Reports ... *7*

1.4.4 - Disabling a Policy ... *9*

1.4.5 - Enabling a Policy ... *10*

1.5 - Workload Actions ... *12*

1.5.1 - Running Workload Jobs ... *12*

1.5.2 - Copy ... *12*

1.5.3 - Move ... *16*

1.5.4 - Delete ... *18*

1.5.5 - Set Owner ... *20*

1.5.6 - Managing Workload Jobs ... *22*

1 - Desktop Client ... ***24***

1.6 - Installing the Data Owner Client ... *24*

1.7 - Security Notifications and Actions ... *26*

1.7.1 - Viewing Security Policies 26
1.7.2 - Viewing Notifications 27
1.7.3 - Generating Detail Reports 29
1.7.4 - Disabling a Policy 31
1.7.5 - Enabling a Policy 32
1.8 - Workload Actions 33
1.8.1 - Running Workload Jobs 34
1.8.2 - Copy 35
1.8.3 - Move 40
1.8.4 - Delete 43
1.8.5 - Set Owner 43
1.8.6 - Managing Workload Jobs 44

About This Guide

This guide is written to provide Data Owners the conceptual and procedural information for using the File Dynamics 24.1 Data Owner Client. This includes:

- Notifications of security changes to high-value target paths
- Manage Security Policies and view security change reports
- Performing remediation via Workload policies

Audience

This guide is intended for designated File Dynamics Data Owners.

1 - Introduction

This chapter provides an introduction to the role of Data Owner in a File Dynamics deployment and how to perform tasks using the Data Owner Client.

1.1 - About the Data Owner Client

The Data Owner Client is the administrative tool used by designated Data Owners to perform specific types of data management actions. These actions include:

- Reporting on security changes to high-value target paths.
- Importing and initiating remediation actions via File Dynamics Workload policies.

The Data Owner Client is delivered as both a Windows desktop application and a web service accessible from a modern desktop browser.

1.2 - Data Owners

Network administrators assign individuals as Data Owners when they create the following types of File Dynamics policies:

- Security Notification policies
- Security Lockdown policies
- Security Fencing policies
- Workload policies

In addition to direct assignments through these policies, members of the File Dynamics Admins group have permissions to perform the tasks that Data Owners can perform.

You would normally assign Data Owners based on a user's association with a folder or share that an administrator classifies as a high-value target. For example, if the Human Resources network share were classified as a high-value target, and the administrator created a Security Notification policy to monitor folder permissions on that share, it would make sense to assign a member of the HR Department as a Data Owner for the policy.

Making a user who is associated with a high-value target the Data Owner also makes sense because that user, based on his or her role, is typically familiar with the documents that need to be secured or moved. Using the Human Resources network share again as an example, the Data Owner could view security reports of associated file shares and review changes to permissions.

1 - Web Client

The Data Owner Web Client is web application that may be accessed by assigned Data Owners via a modern web browser. Select the desktop client the following applies to you as a Data Owner or systems administrator:

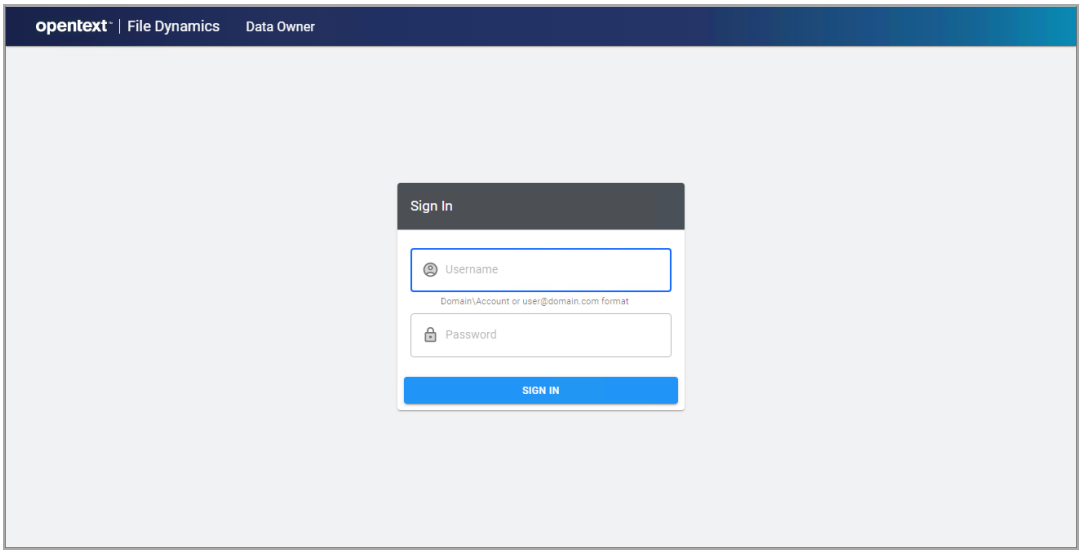
- You require or prefer web based access over installing a desktop client.
- You require access to the Data Owner functions from a system other than Windows

See the following for details on using the Data Owner Web Client:

1.3 - Accessing the Data Owner Service

To access the Data Owner web service:

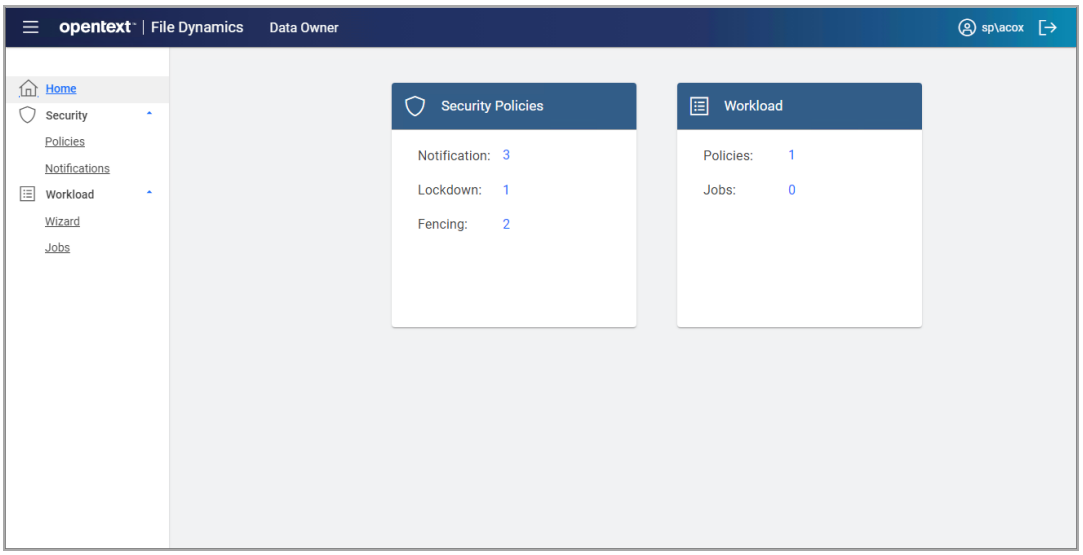
1. In a web browser, go to the Data Owner web service URL provided by your administrator. For example, https://dataowner.sp.cctec.org:3079.



2. Enter your Active Directory username and password. The username may be entered using *Domain\Account* or User Principal Name (UPN) format.

   For example, `SP\acox` or `acox@sp.cctec.org`.

3. Click **Sign In** to authenticate.



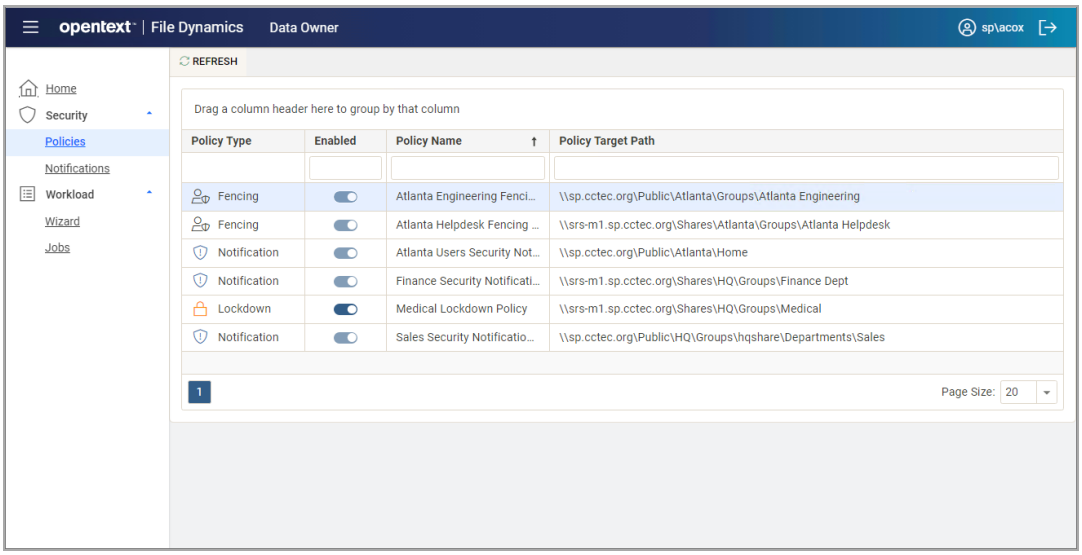
4. After initial login, the Home page will appear showing basic counts for Security Policies and Workload jobs.
5. Proceed to manage either *Security Notifications and Actions (page 5)* or *Workload Actions (page 12)*.
6. To sign out, click the sign out link in the header.

1.4 - Security Notifications and Actions

The *Security* region of the Data Owner Client provides the means of getting notifications when access permissions for specified target paths have changed, viewing reports, and when authorized to do so, disabling and enabling a policy.

1.4.1 - Viewing Security Policies

1. Click *Security* > *Policies* to view a list of Security policies to which you have been assigned as a Data Owner.



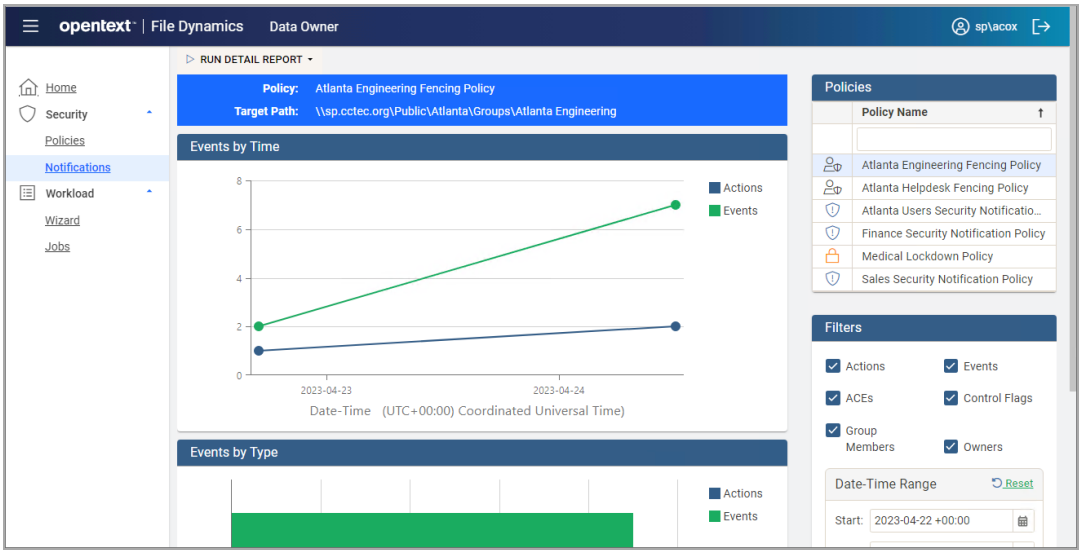
2. Click each listing individually to see if you have been authorized to enable or disable a policy.

   In the graphic above, Amanda Cox is authorized to disable the Medical Lockdown policy.

1.4.2 - Viewing Notifications

Notifications in the Data Owner Client display graphically security-specific events and resulting actions according to the filters you specify. Events take place in the network file system, actions are what File Dynamics did as a result.

1. Click *Security* > *Notifications* to access the Security Notifications page.



2. From the *Policies* list, select the policy for which you want to see graphical information and reported in the Detail Report.

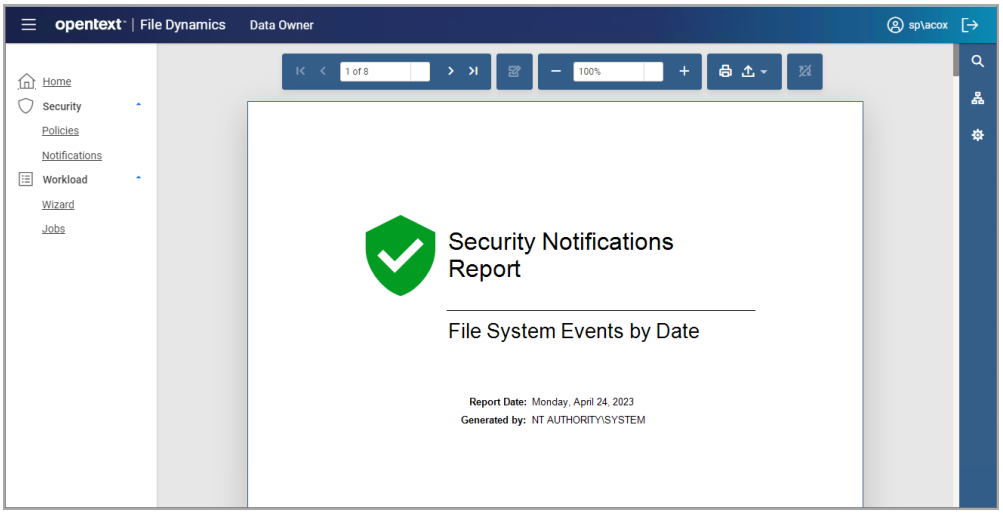
   If the policies are not displayed, you can click *Reload Policies* and select the security policy types to display.

3. From the *Filters* region, specify the options you want displayed in the graphs and reported in the Detail Report.

4. In the same region, specify the date range you want displayed in the graphs and reported in the Detail Report.

5. From the *Run Detail Report* drop-down menu, choose one of the following options:

   - **File System Events:** Generates a preview report of file system events that have taken place within the parameters you have specified in the right-hand portion of the Security Notifications page.
   - **Group Membership Events:** Generates a preview report of group membership events that have taken place within the parameters you have specified in the right-hand portion of the Security Notifications page.



6. From the report dialog box, export or email the report in the format you want.

1.4.3 - Generating Detail Reports

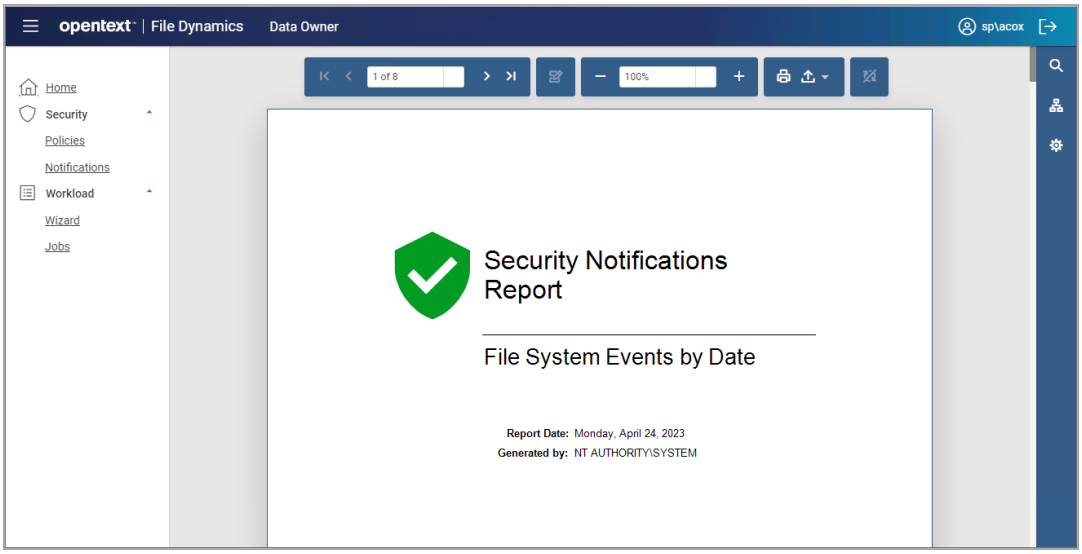
The Data Owner Client notifies the Data Owner of security changes for target paths through generated reports. The Data Owner Client generates the following reports.

File System Events Reports

File System Events reports detail the changes in permissions that have taken place within the designated target path.

1. Click *Security > Notifications* to access the Security Notifications page.
2. In the *Filters* region of the page, specify if you want the report to include Events, Actions, or both by selecting the appropriate check boxes.
3. From the *Run Detail Report* drop-down menu, select *File System Events*.

   The report is generated in preview mode where it can be printed or saved into a variety of formats.

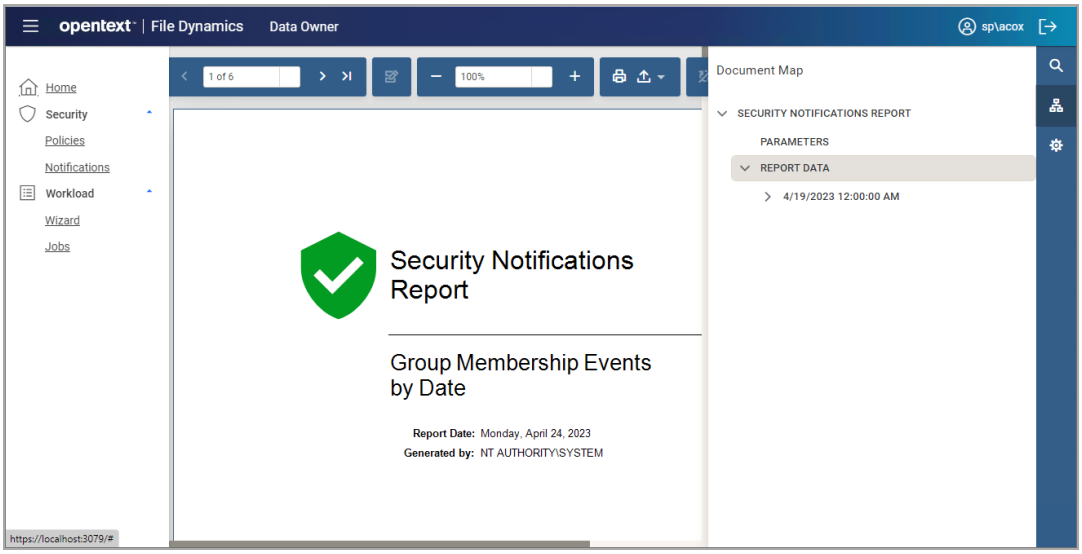


Group Membership Events Reports

Group Membership Events reports detail the changes in group memberships that have taken place for groups that have access to the designated target path.

1. Click *Security > Notifications* to access the Security Notifications page.
2. In the *Filters* region of the page, specify if you want the report to include Events, Actions, or both by selecting the appropriate check boxes.
3. From the *Run Detail Report* drop-down menu, select *Group Membership Events*.

The report is generated in preview mode where it can be printed or saved into a variety of formats.



1.4.4 - Disabling a Policy

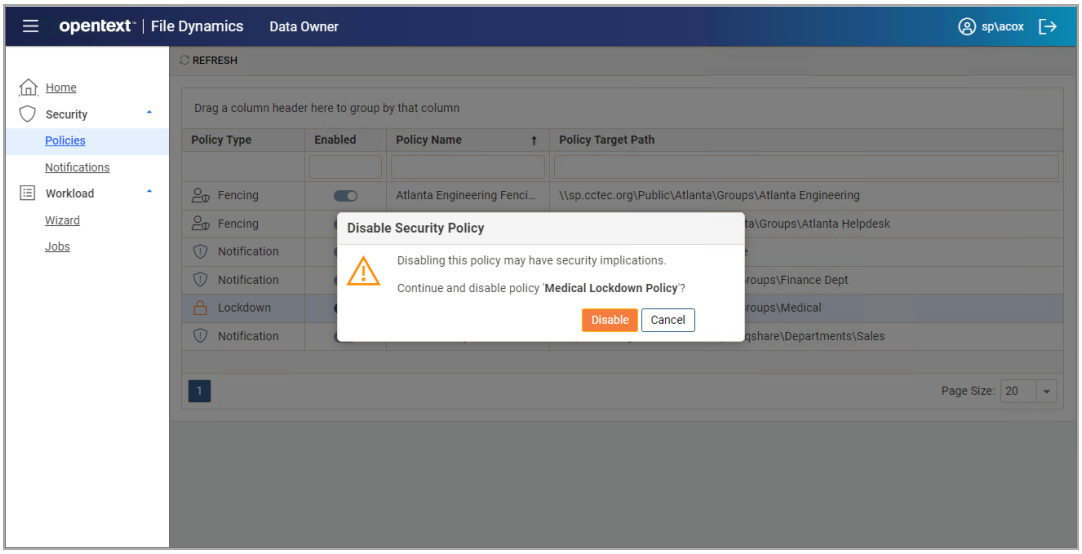
Data Owners authorized to disable a policy will normally do so when access permissions to a high-value target need to be temporarily overridden or modified.

Disabling a policy stops all scheduled security scans until it is enabled.

A Data Owner that has been authorized to disable a policy is also authorized to enable a policy.

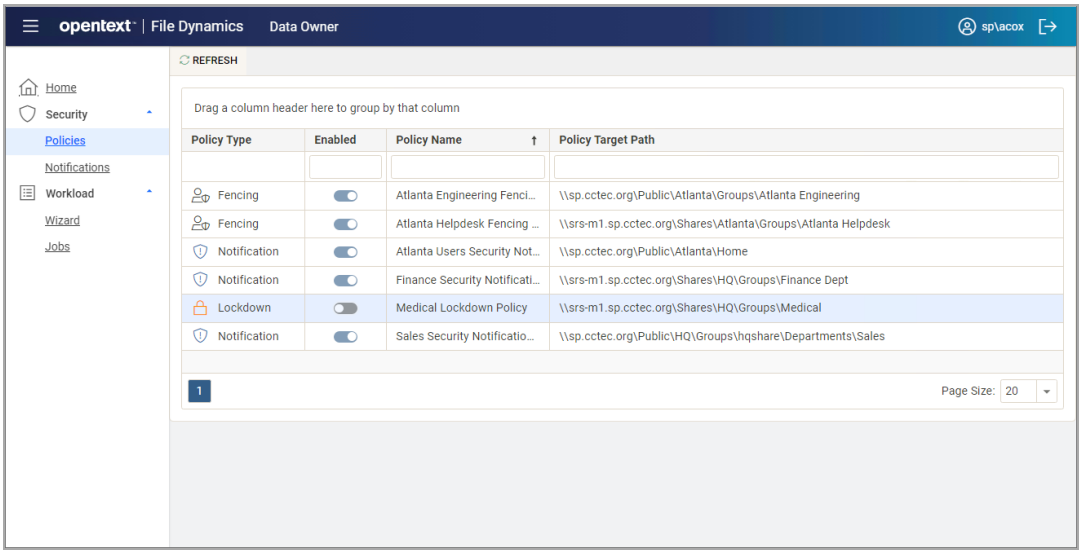
1. From the list of security policies, click toggle button of the enabled policy you wish to disable.

The following dialog box appears:



2. Click *Disable*.

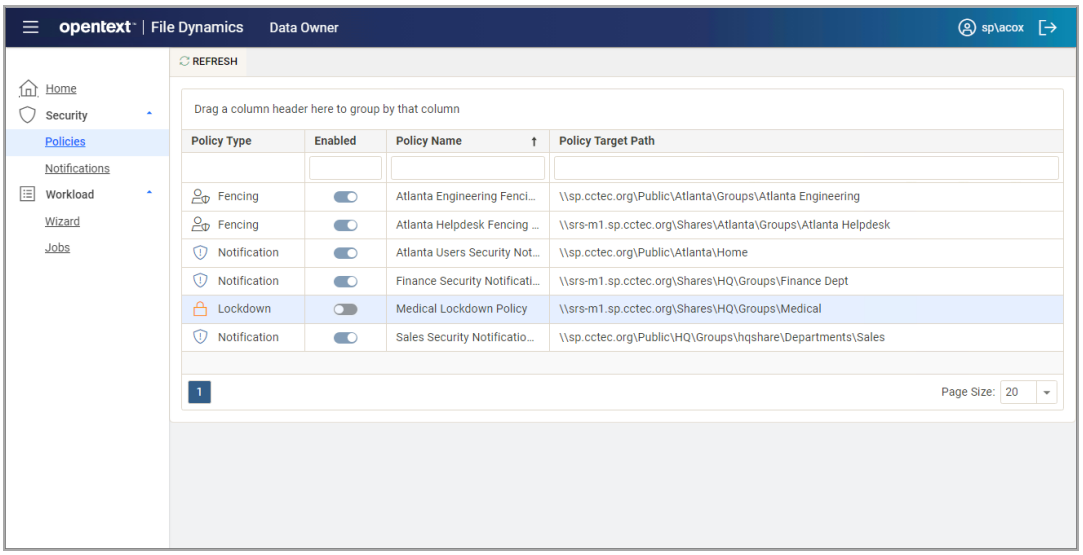
   The policy is displayed as disabled.



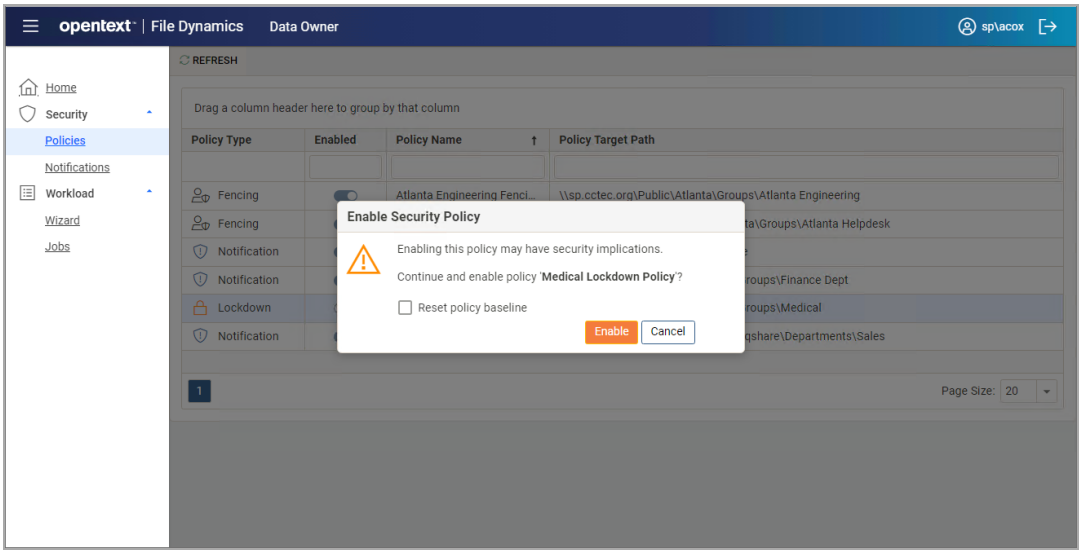
1.4.5 - Enabling a Policy

Once the IT department has concluded its need for disabling the policy, an authorized Data Owner can enable the policy using the Data Owner Client.

1. From the list of security policies, click toggle button of the disabled policy you wish to enable.



The following dialog box appears:



2. Do one of the following:

   - If you want to keep the original baseline permissions for the target path before the policy was disabled, click *Enable*.
   - If you want establish the new permissions specified in the policy for the target path, select the *Reset* policy baseline check box and click *Enable*.

     This option removes previous security scans from the database and initiates a new security scan that will serve as the baseline.

1.5 - Workload Actions

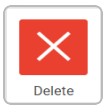
Workload policies in File Dynamics provide the ability to handle work processes initiated from other applications. For example, reports generated in OpenText OpenText File Reporter that specify the location of sensitive files can be imported into the Data Owner Client where a designated Data Owner can remediate the location of these sensitive files. This approach empowers organizations to provide automated network file system security remediation approved by a gatekeeper familiar with the files.

1.5.1 - Running Workload Jobs

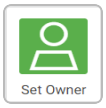
1. Click *Workload* > *Wizard*.
2. Click the desired operation to start the associated wizard:

Copy (page 12): copy one or more paths to a desginated target path

Move (page 16): move one or more paths to a desginated target path



Delete (page 18): delete one or more paths

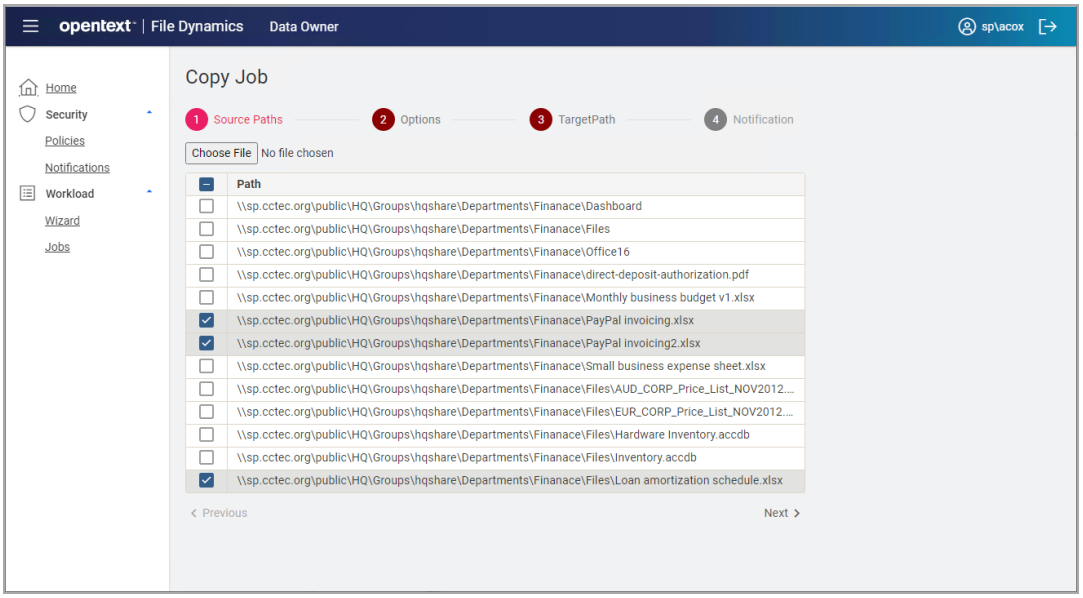


Set Owner (page 20): set the owner for one or more paths

1.5.2 - Copy

This option copies selected entries to a designated target path.

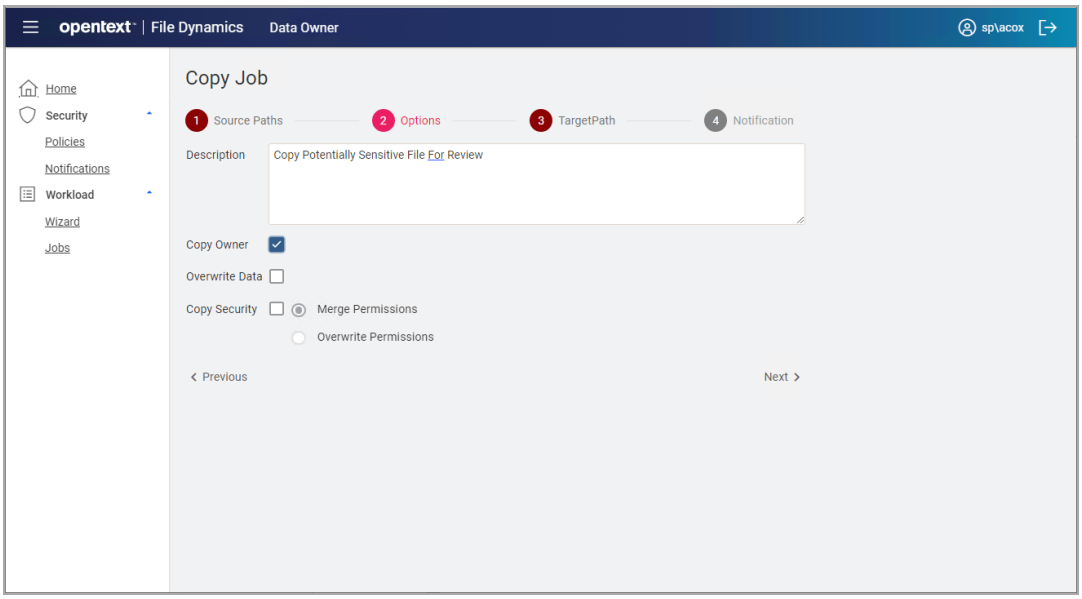
1. From the Data Owner web client, select *Workload* > *Wizard* > *Copy*.



2. Click *Choose File* and select a paths import file.

> **NOTE:** Currently, only a plain-text file with a list of UNC paths, one per line, is supported. CSV file support will be added in a future update.

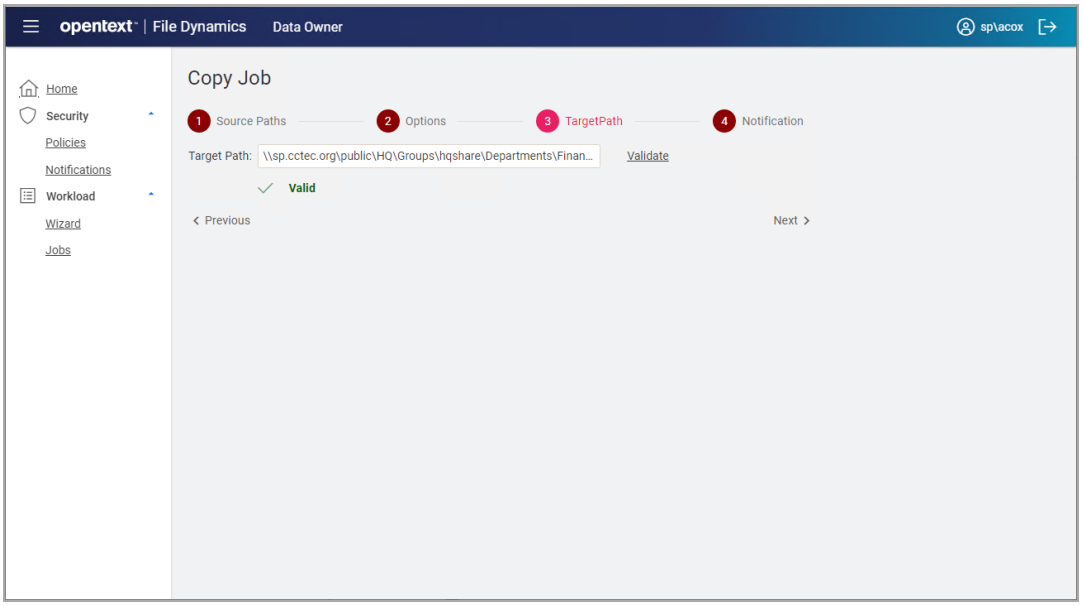
3. Select one or more source paths from the list that you wish to copy.
4. Click *Next*.



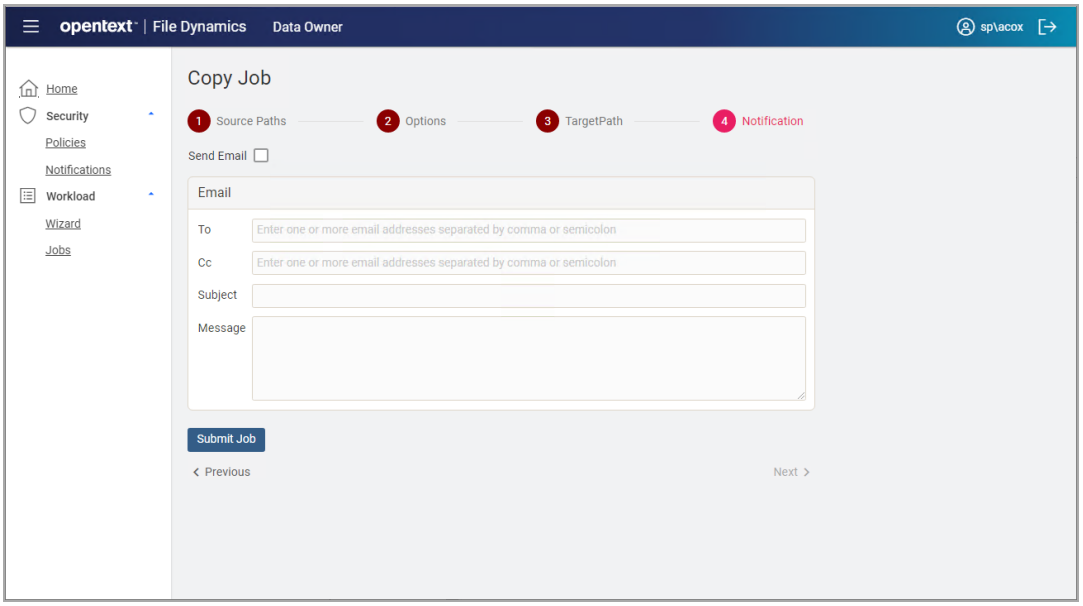
5. In the *Options* panel, specify any of the applicable options.

    - **Description**: enter a description for this job. This is a required field.
    - **Copy Owner**: Selecting this check box maintains the ownership information of the copied files. If this is not selected, the Proxy Rights group becomes the owner.
    - **Overwrite Data**: When there is a naming conflict between files, this option allows you to overwrite the existing file with the one being copied.
    - **Copy Security**: Selecting this check box maintains the security settings for the copied files. If this is not selected, the copied files inherit the security of the network file system location to where they are copied.
    - **Merge Permissions**: Merges permissions from the source to the target if the target contains permissions that are not present in the source. This applies to all folders and files in the source folder structure.
    - **Overwrite Permissions**: Overwrites permissions in the target with those found in the source. This applies to all folders and files in the target folder structure.

6. Click *Next*.



7. In the *Target Path*, enter a valid UNC path where the files will be copied.
8. (Optional) Click **Validate** to validate the entered target path. Note that changing focus from the *Target Path* field will also auto-validate this path.
9. Click *Next*.



10. (Optional) If you want an email notification sent to someone once the files have been copied, check the check box for **Send Email** and then specify the recipients and the

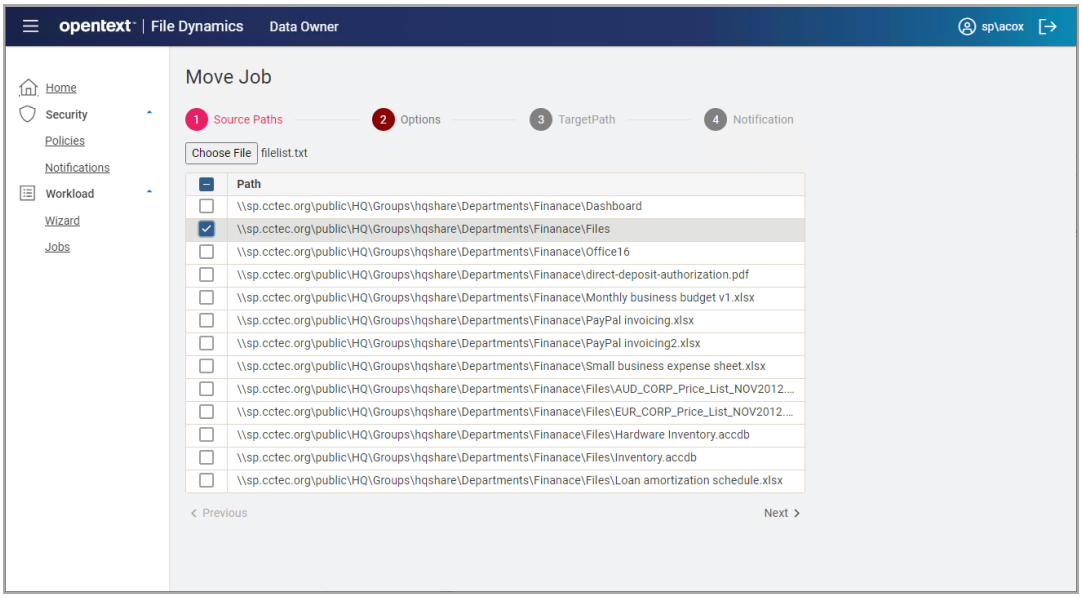
email message in the fields provided.

11. Click *Submit Job*.

1.5.3 - Move

This option moves selected entries to a designated target path.

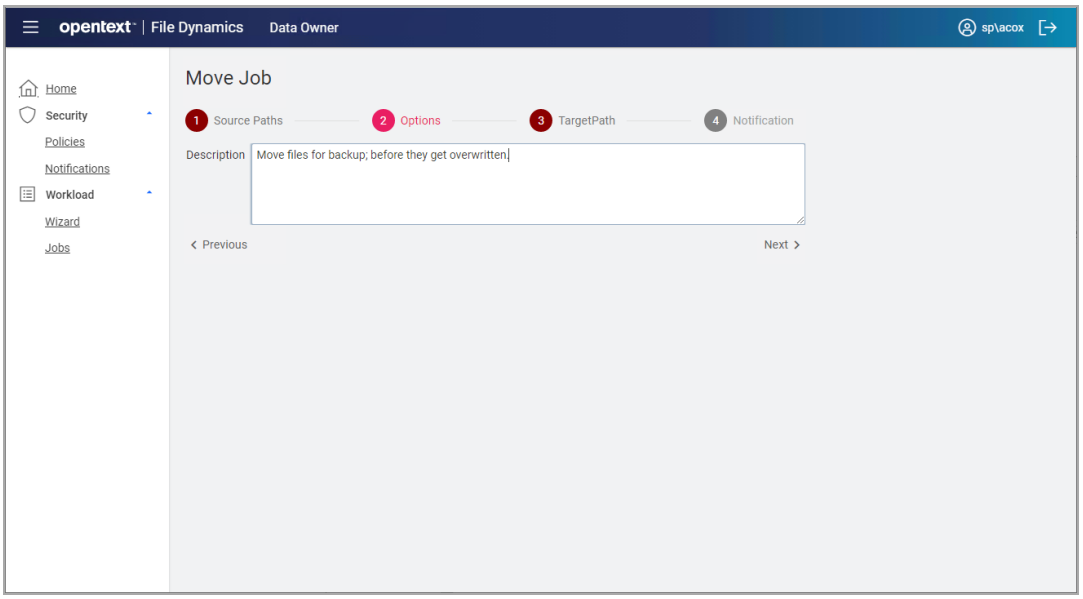
1. From the Data Owner web client, select *Workload* > *Wizard* > *Move*.



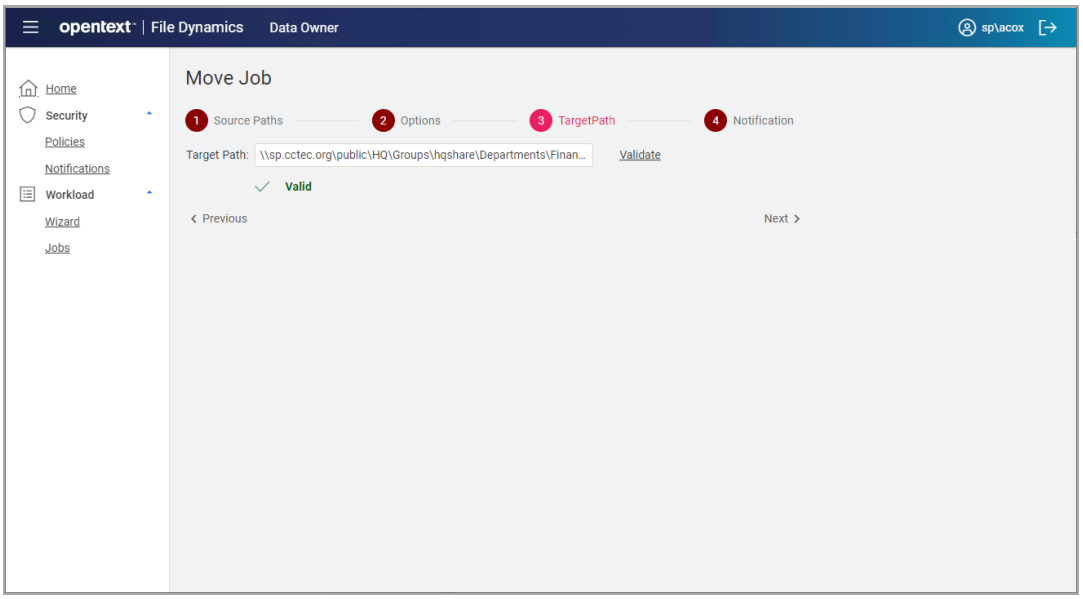
2. Click *Choose File* and select a paths import file.

> **NOTE:** Currently, only a plain-text file with a list of UNC paths, one per line, is supported. CSV file support will be added in a future update.

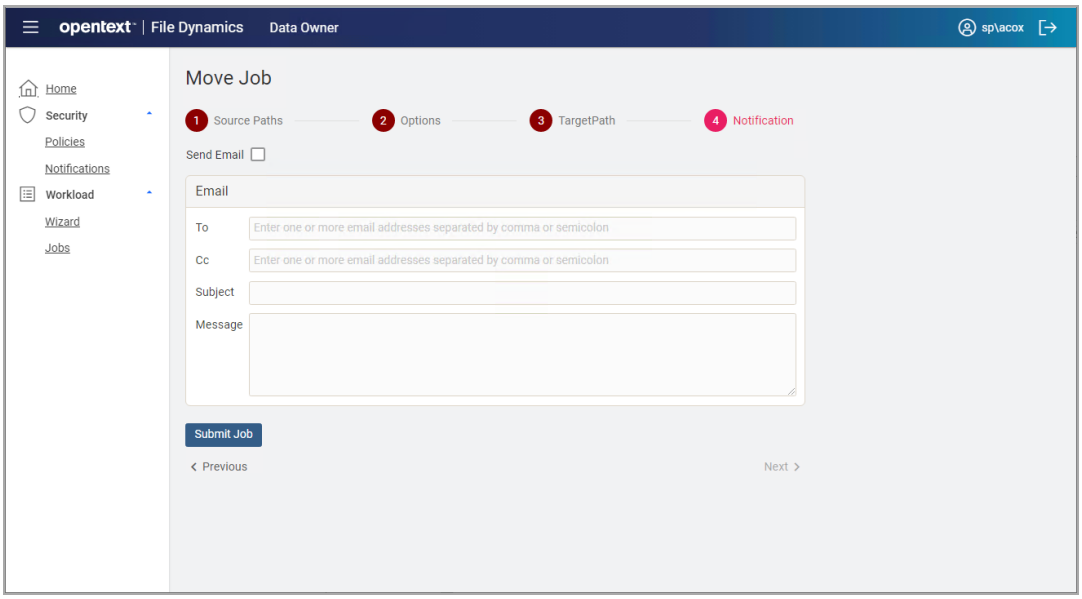
3. Select one or more source paths from the list that you wish to move.
4. Click *Next*.



5. In the *Options* panel, specify any of the applicable options.
    - **Description**: enter a description for this job. This is a required field.
6. Click *Next*.



7. In the *Target Path*, enter a valid UNC path where the files will be copied.
8. (Optional) Click **Validate** to validate the entered target path. Note that changing focus from the *Target Path* field will also auto-validate this path.

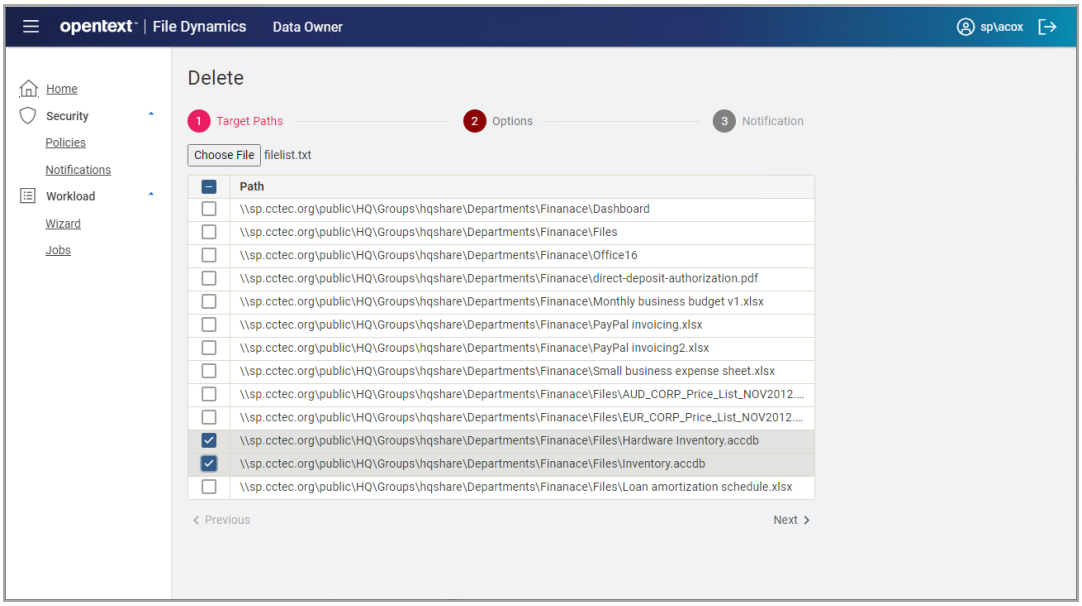


9. (Optional) If you want an email notification sent to someone once the files have been moved, check the check box for **Send Email** and then specify the recipients and the email message in the fields provided.
10. Click *Submit Job*.

1.5.4 - Delete

This option deletes selected file and folder entries.

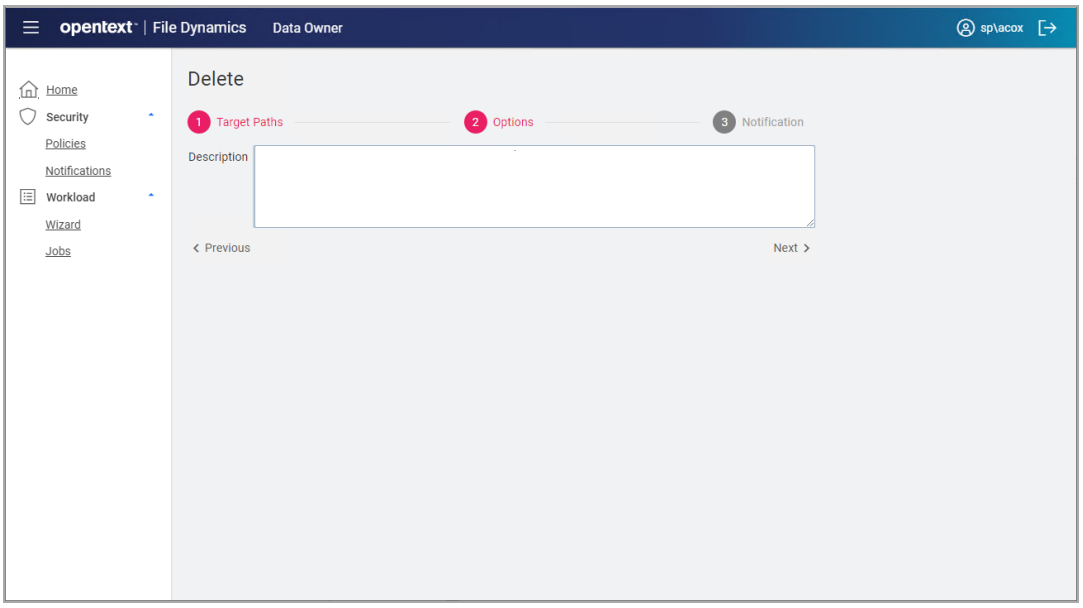
1. From the Data Owner web client, select *Workload* > *Wizard* > *Delete*.



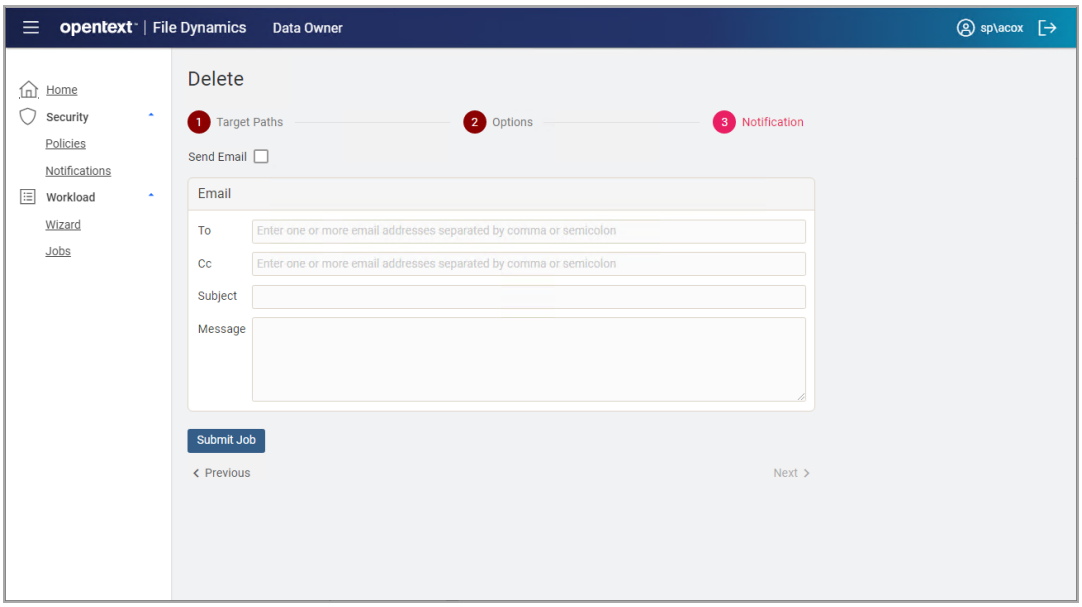
2. Click *Choose File* and select a paths import file.

> **NOTE:** Currently, only a plain-text file with a list of UNC paths, one per line, is supported. CSV file support will be added in a future update.

3. Select one or more source paths from the list that you wish to delete.
4. Click *Next*.



5. In the *Options* panel, specify any of the applicable options.
    - **Description**: enter a description for this job. This is a required field.
6. Click *Next*.

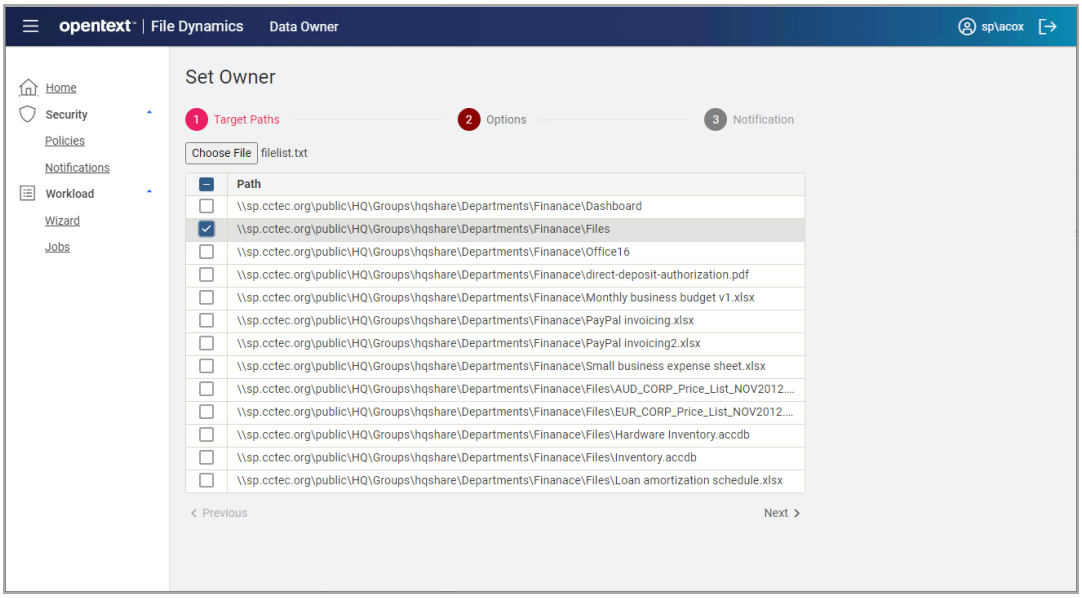


7. (Optional) If you want an email notification sent to someone once the files have been deleted, check the check box for **Send Email** and then specify the recipients and the email message in the fields provided.
8. Click *Submit Job*.

1.5.5 - Set Owner

This option sets the owner for selected file and folder entries.

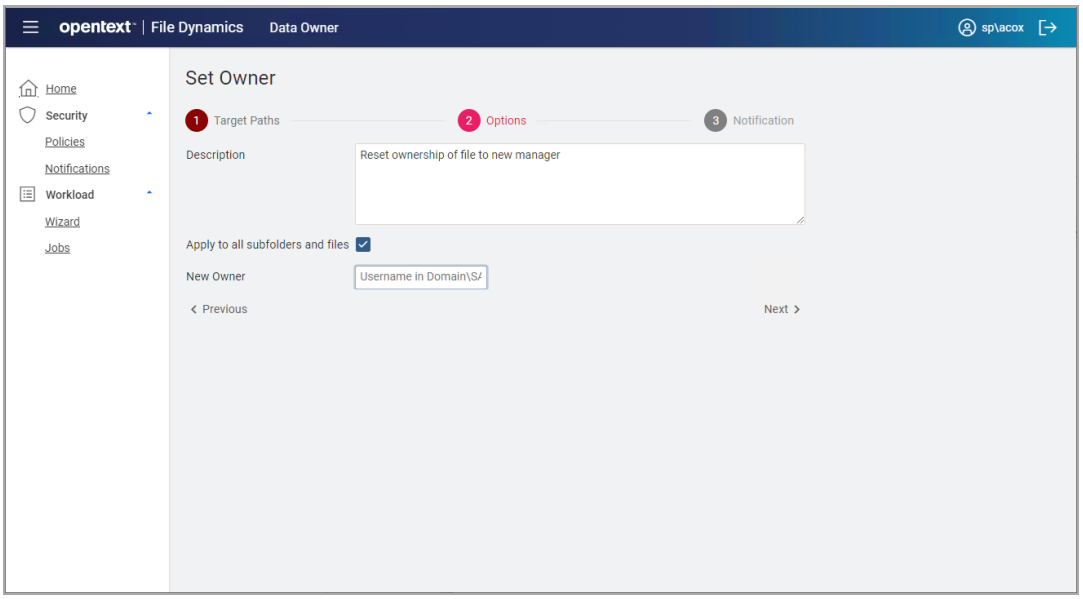
1. From the Data Owner web client, select *Workload* > *Wizard* > *Set Owner*.



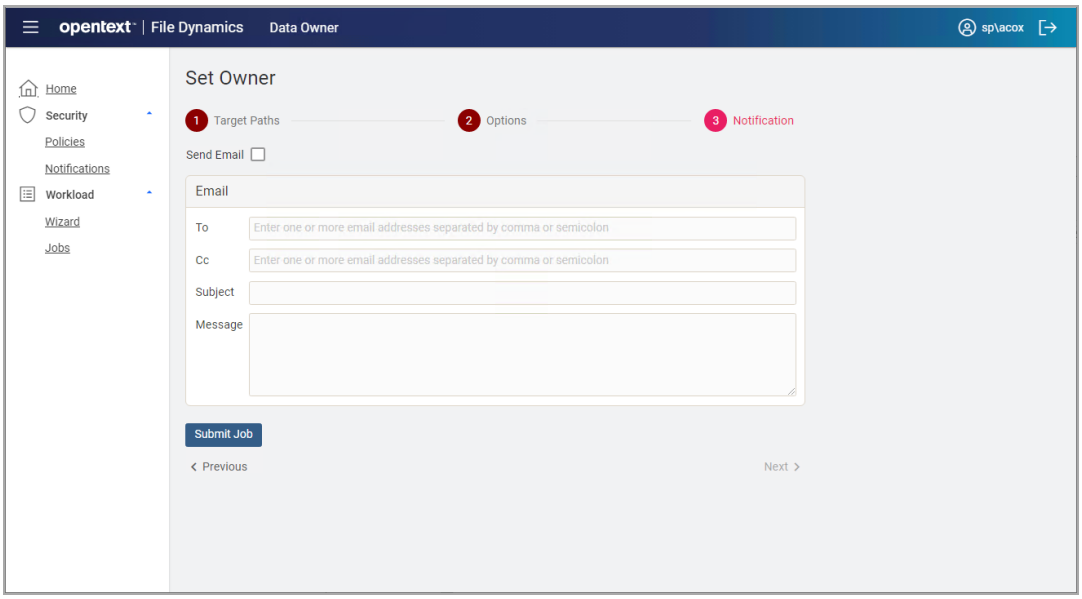
2. Click *Choose File* and select a paths import file.

> **NOTE:** Currently, only a plain-text file with a list of UNC paths, one per line, is supported. CSV file support will be added in a future update.

3. Select one or more source paths from the list for which you wish to modify the owner.
4. Click *Next*.



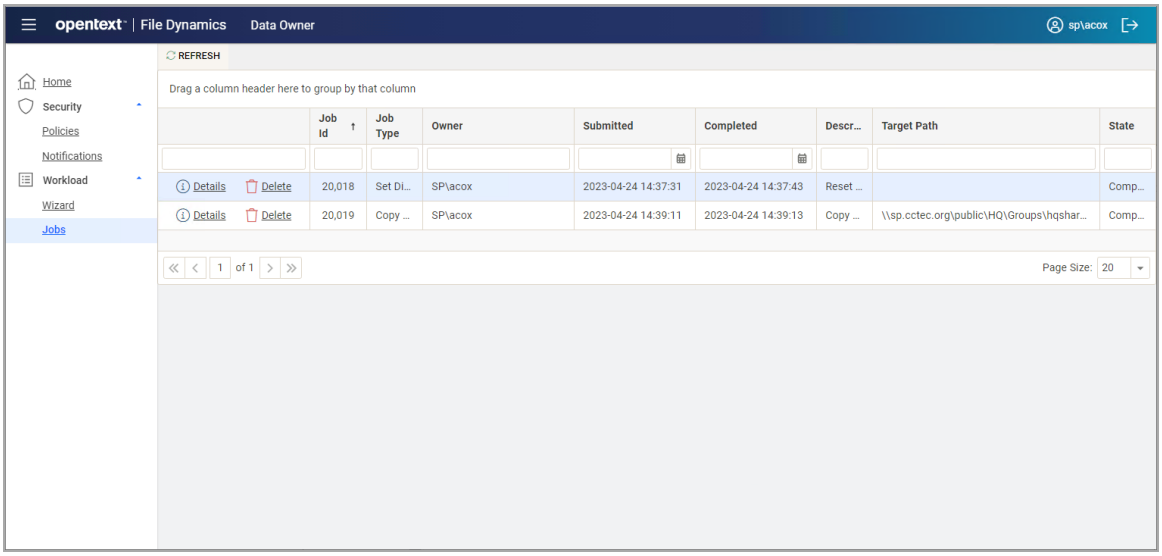
5. In the *Options* panel, specify any of the applicable options.
   - **Description**: enter a description for this job. This is a required field.
   - **Apply to all subfolder and files**: Select this check box to applpy the specified owner to all subfolders and files of each path.
   - **New Owner**: Enter the new owner using Domain\Account format such as `BUILTIN\Administrators` or `SP\acox` or by using a valid Security Identifier (SID) such as `S-1-5-32-544`.
6. Click *Next*.



7. (Optional) If you want an email notification sent to someone once the file and folder owners have been updated, check the check box for **Send Email** and then specify the recipients and the email message in the fields provided.
8. Click *Submit Job*.

1.5.6 - Managing Workload Jobs

From the Data Owner web client, select *Workload* > *Jobs* to bring up the list of Workload jobs.



Click the following links for a job to perform actions on that job:

- **Details**: displays a detail form for the job
- **Abort**: aborts a currently running job
- **Delete**: deletes the associated job

If you're a member of the File Dynamics Admins group, you will see the jobs for all users. If you are a regular user, you will see only the jobs that you have submitted.

1 - Desktop Client

The Data Owner Desktop Client is a Windows application that you can install and run on a Windows desktop or server. Select the desktop client if any of the following apply to you as a Data Owner:

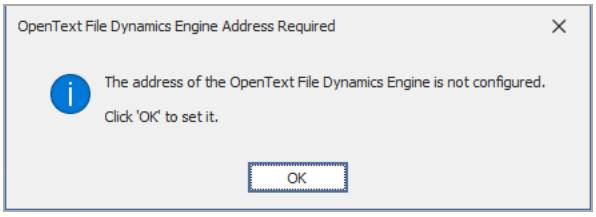
- You need to generate Security Policy reports containing several thousand pages or more in a single report.
- You need advanced filtering and copy options for Workload injection jobs.

See the following for details on installing and using the Data Owner Desktop Client:

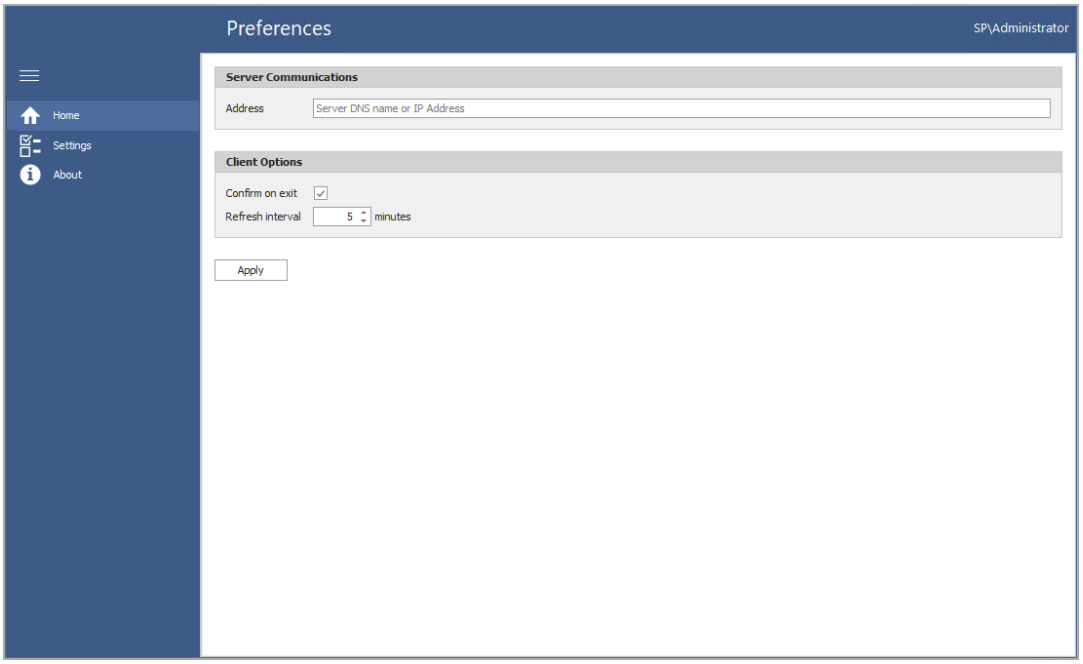
1.6 - Installing the Data Owner Client

The Data Owner Client can be installed on any platform where .NET 7.0 can run.

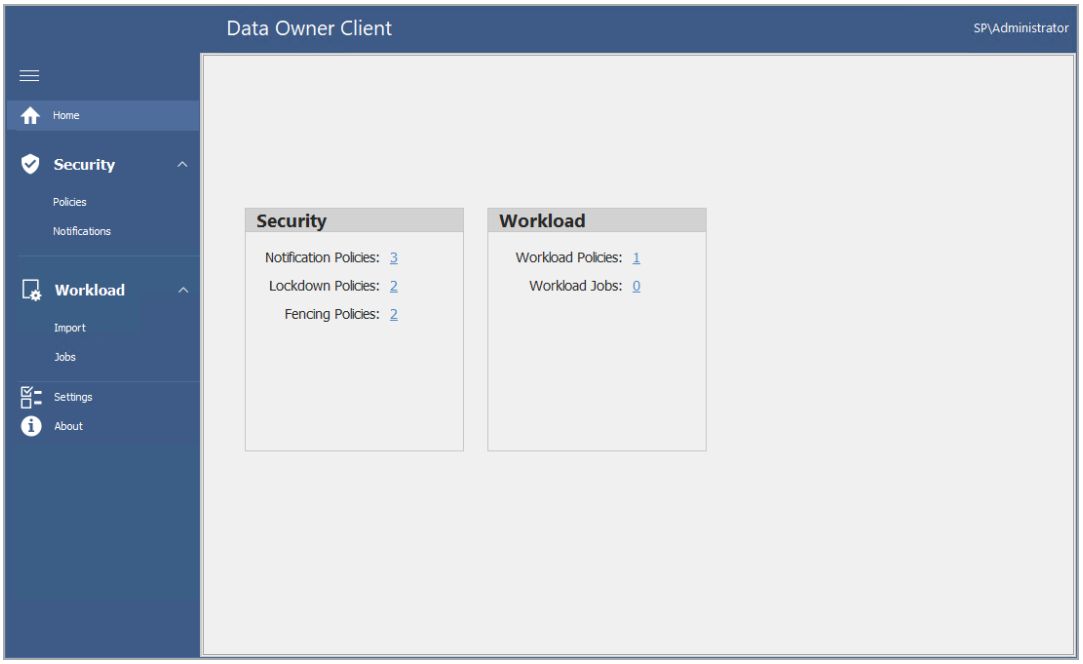
1. On the Windows server or workstation where you will run the Data Owner Client, copy to a directory the `FileDynamics-24.1.iso`.
2. Mount the `FileDynamics-24.1.iso` file.
3. At the root of the `FileDynamics-24.1.iso` image, double-click `FileDynamics-DataOwnerClient-24.1-xx.exe`.
4. Agree to the licensing terms and conditions and click *Install*.
5. When notified that the setup was successful, click *Run Data Owner Client*.
   The following notification appears:



6. Click *OK*.
   The following dialog box appears:

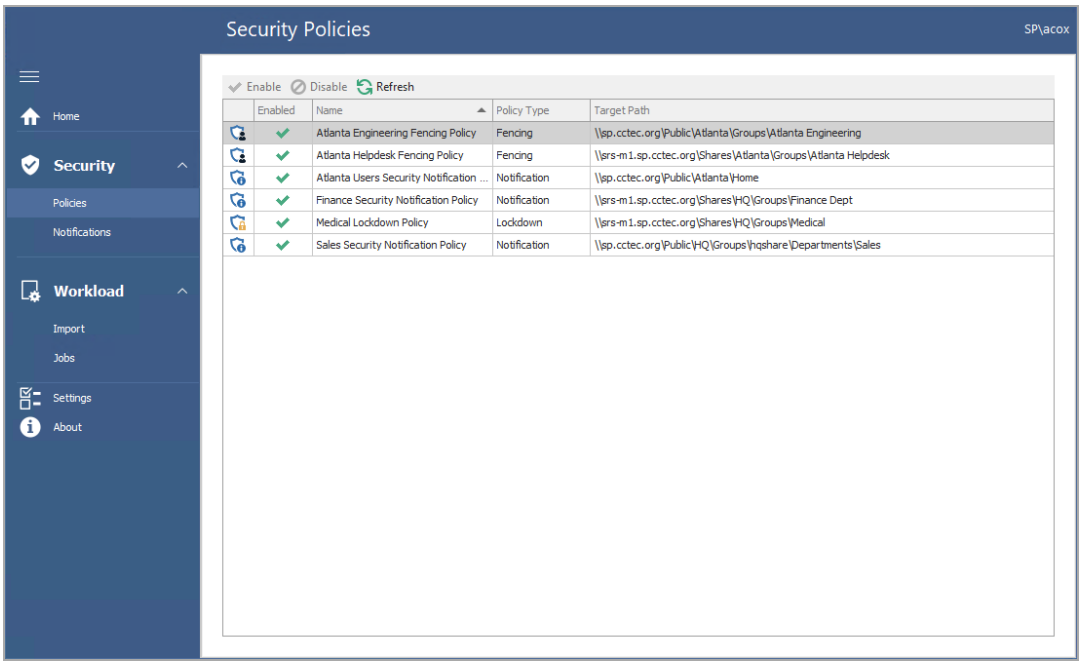


7. In the *Address* field, specify the DNS name or IP address of the server hosting the File Dynamics Engine.
   The following interface appears, indicating that the Data Owner Client is configured.



In the example above, Amanda Cox was specified previously as a Data Owner for Security and Workload policies, and each policy has been run at least once (resulting in a stored scan). If a user has not yet been specified for as a Data Owner in a policy, or has, but the policies have not yet been run, the right pane will be empty.

The numbers associated with each listed policy specify the number of policies of that type of which the logged in user is a Data Owner. For example, Amanda Cox is the Data Owner of one Security Notification policy. Clicking a number brings up details about the policies.



In the example above, Amanda Cox can view the Security policies for which she is a Data Owner.

The numbers associated with jobs specify the number of jobs that have been run. Clicking the number brings up details of all of the jobs.

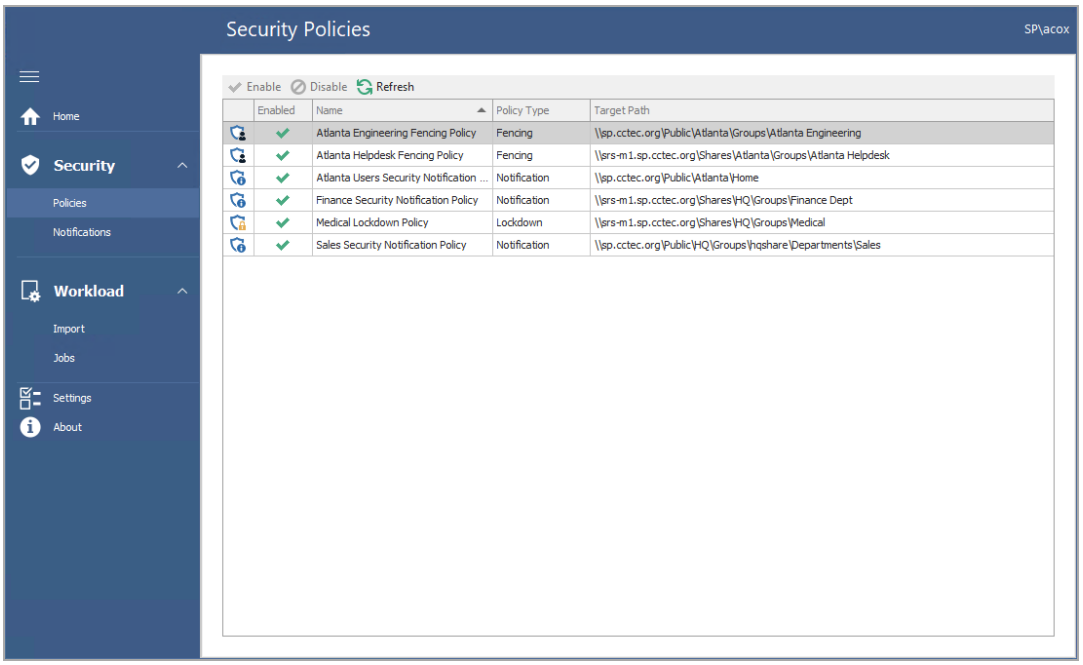
In the example above, each of the saved jobs are listed. You can get additional details about a job by double-clicking a listing from the job list.

1.7 - Security Notifications and Actions

The *Security* region of the Data Owner Client provides the means of getting notifications when access permissions for specified target paths have changed, viewing reports, and when authorized to do so, disabling and enabling a policy.

1.7.1 - Viewing Security Policies

1. Click *Security* > *Policies* to view a list of Security policies to which you have been assigned as a Data Owner.



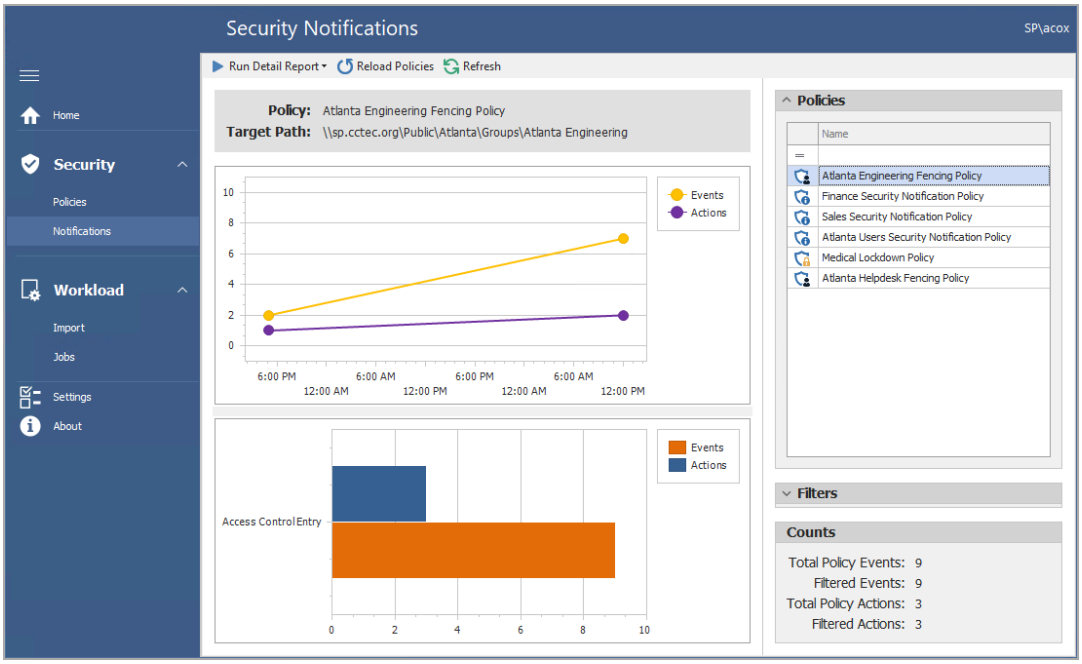
2. Click each listing individually to see if you have been authorized to enable or disable a policy.

   In the graphic above, Amanda Cox is authorized to disable the Medical Lockdown policy.

1.7.2 - Viewing Notifications

Notifications in the Data Owner Client display graphically security-specific events and resulting actions according to the filters you specify. Events take place in the network file system, actions are what File Dynamics did as a result.

1. Click *Security* > *Notifications* to access the Security Notifications page.

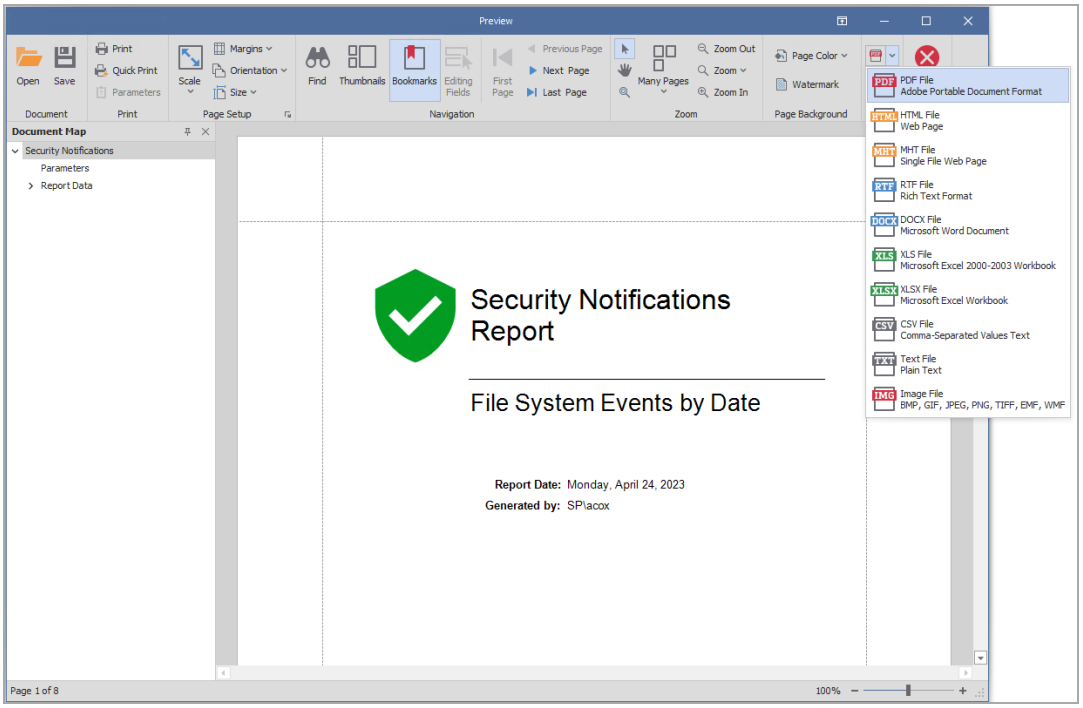


2. From the *Policies* list, select the policy for which you want to see graphical information and reported in the Detail Report.

   If the policies are not displayed, you can click *Reload Policies* and select the security policy types to display.

3. From the *Filters* region, specify the options you want displayed in the graphs and reported in the Detail Report.
4. In the same region, specify the date range you want displayed in the graphs and reported in the Detail Report.
5. From the *Run Detail Report* drop-down menu, choose one of the following options:
   - **File System Events:** Generates a preview report of file system events that have taken place within the parameters you have specified in the right-hand portion of the Security Notifications page.
   - **Group Membership Events:** Generates a preview report of group membership events that have taken place within the parameters you have specified in the right-hand portion of the Security Notifications page.

6. From the report dialog box, export or email the report in the format you want.



1.7.3 - Generating Detail Reports

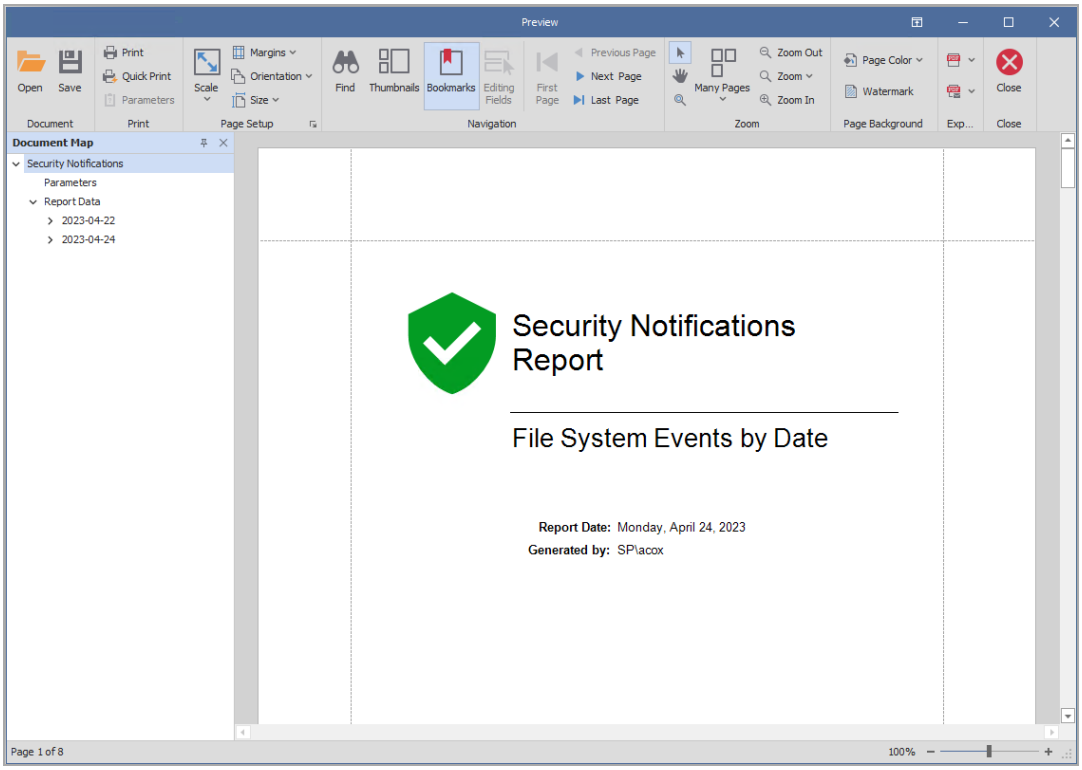
The Data Owner Client notifies the Data Owner of security changes for target paths through generated reports. The Data Owner Client generates the following reports.

File System Events Reports

File System Events reports detail the changes in permissions that have taken place within the designated target path.

1. Click *Security* > *Notifications* to access the Security Notifications page.
2. In the *Filters* region of the page, specify if you want the report to include Events, Actions, or both by selecting the appropriate check boxes.
3. From the *Run Detail Report* drop-down menu, select *File System Events*.

The report is generated in preview mode where it can be printed or saved into a variety of formats.

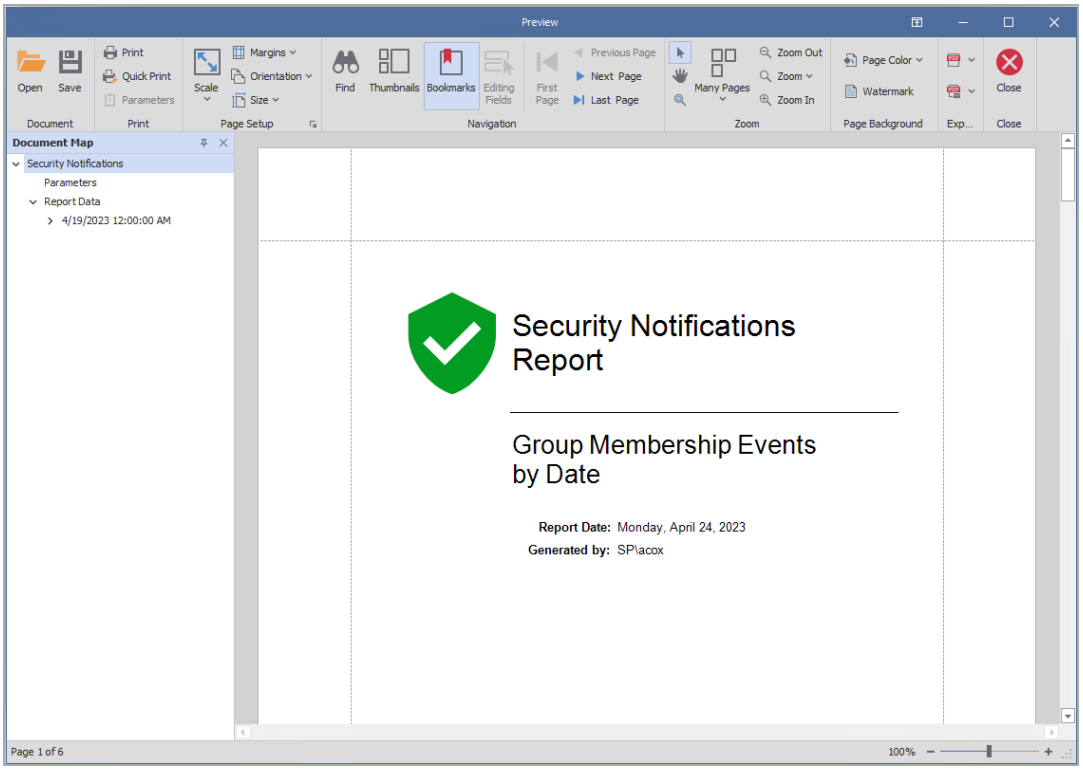


Group Membership Events Reports

Group Membership Events reports detail the changes in group memberships that have taken place for groups that have access to the designated target path.

1. Click *Security > Notifications* to access the Security Notifications page.
2. In the *Filters* region of the page, specify if you want the report to include Events, Actions, or both by selecting the appropriate check boxes.
3. From the *Run Detail Report* drop-down menu, select *Group Membership Events*.

The report is generated in preview mode where it can be printed or saved into a variety of formats.



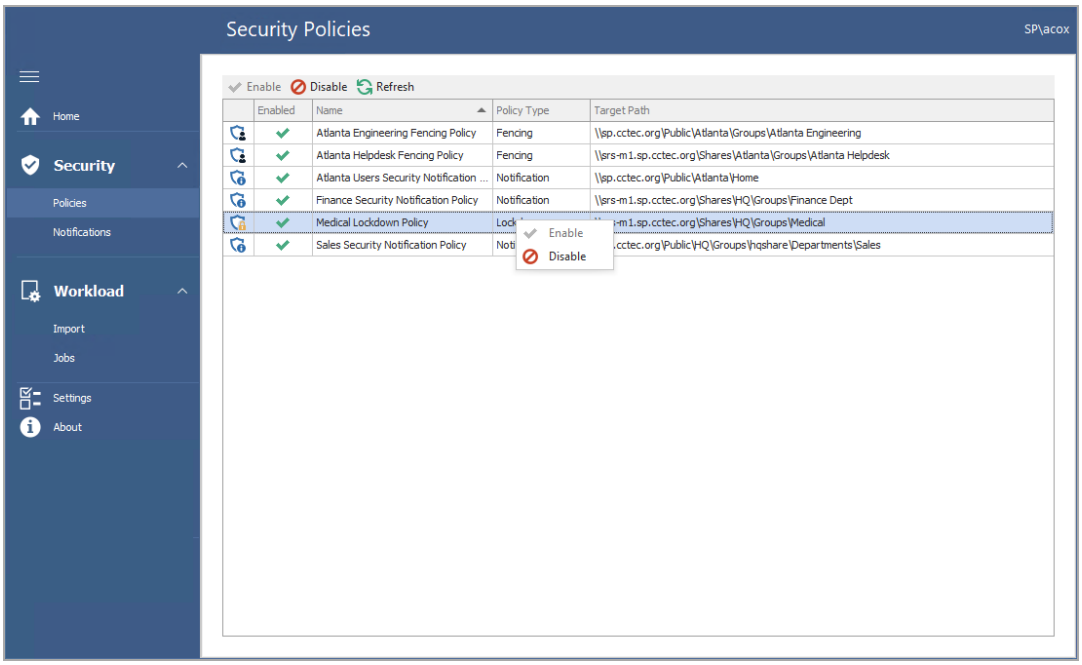
1.7.4 - Disabling a Policy

Data Owners authorized to disable a policy will normally do so when access permissions to a high-value target need to be temporarily overridden or modified.

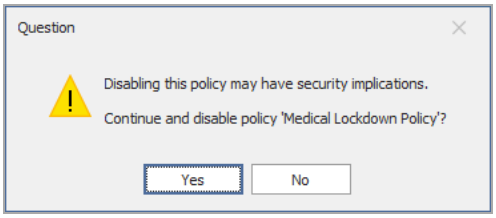
Disabling a policy stops all scheduled security scans until it is enabled.

A Data Owner that has been authorized to disable a policy is also authorized to enable a policy.

1. From the list of security policies, select the policy you want to disable, right-click and select *Disable*.



The following dialog box appears:



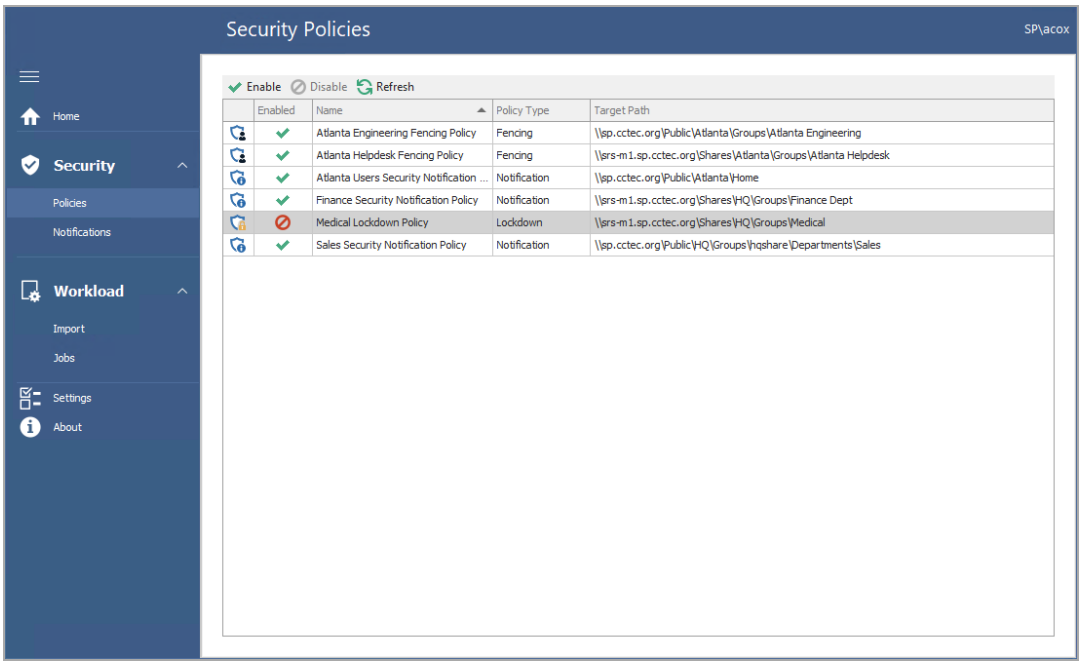
2. Click *Yes*.

   The policy is displayed as disabled.

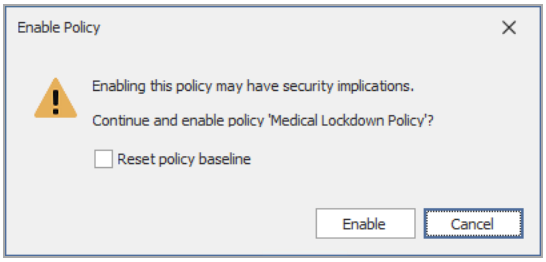
1.7.5 - Enabling a Policy

Once the IT department has concluded its need for disabling the policy, an authorized Data Owner can enable the policy using the Data Owner Client.

1. From the list of security policies, select the policy you want to enable, right-click and select *Enable*.



The following dialog box appears:



2. Do one of the following:
    - If you want to keep the original baseline permissions for the target path before the policy was disabled, click *Enable*.
    - If you want establish the new permissions specified in the policy for the target path, select the *Reset* policy baseline check box and click *Enable*.

      This option removes previous security scans from the database and initiates a new security scan that will serve as the baseline.

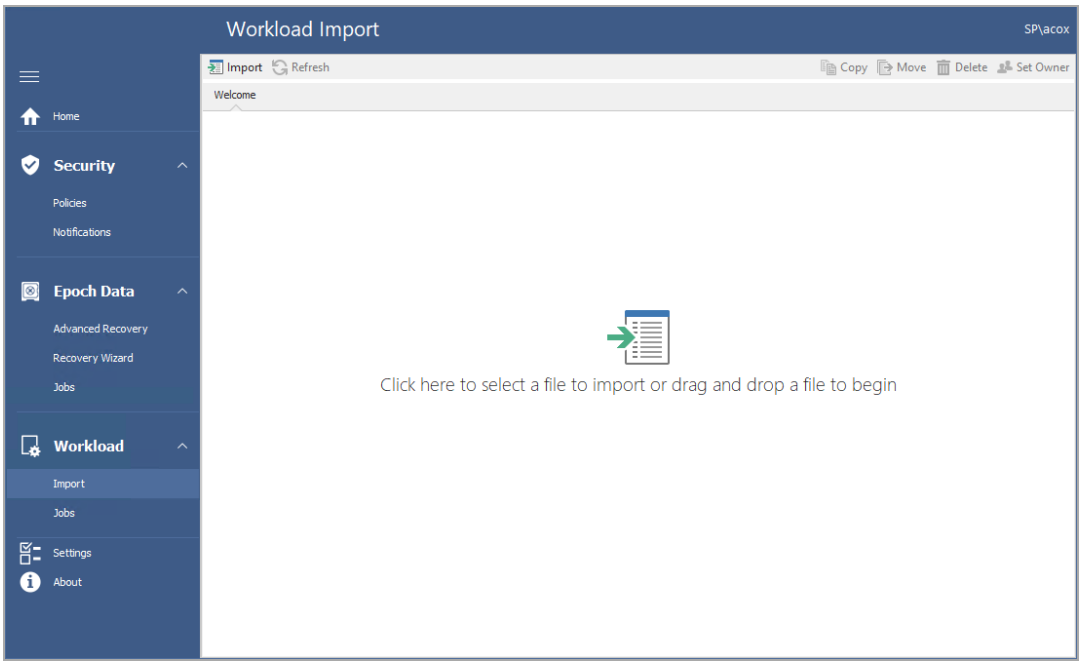
1.8 - Workload Actions

Workload policies in File Dynamics provide the ability to handle work processes initiated from other applications. For example, reports generated in OpenText OpenText File Reporter that specify the location of sensitive files can be imported into the Data Owner Client where a designated Data Owner can remediate the location of these sensitive files. This approach empowers organizations to provide automated network file system security remediation approved by a gatekeeper familiar with the files.

Imported files can be in either CSV or TXT format.

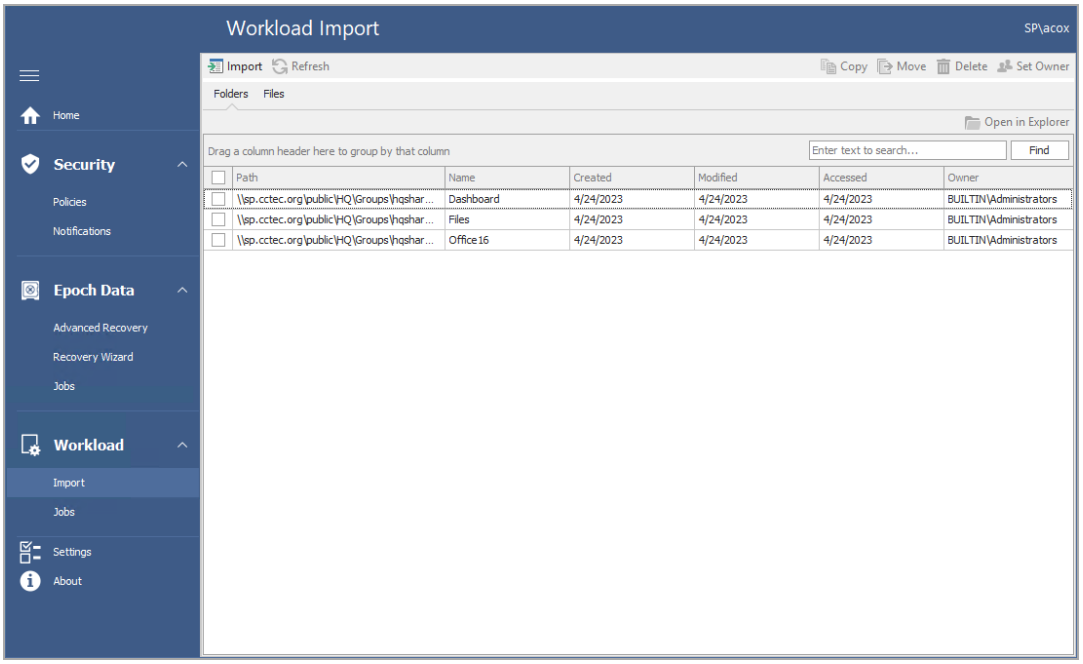
1.8.1 - Running Workload Jobs

1. Click *Workload* > *Import*.



2. Do one of the following:
    - On the Import page, drag the file you want to import.
    - Click the Import page, browse and then select the file you want to import.

The Import dialog box appears with the contents of the imported file.



3. Select each of the entries you want by clicking its corresponding check box and select whether to *Copy*, *Move*, *Delete*, or *Set Owner*.

   See the following sections for details on each of these operations.

1.8.2 - Copy

This option copies the files specified in each of the entries you select. The option simply duplicates the files and places the duplicate versions in a location selected by the Data Owner.

1. In the *Description* field, specify the purpose of the copy operation and click *Next*.
2. In the *Copy Options* region, specify any of the applicable options.

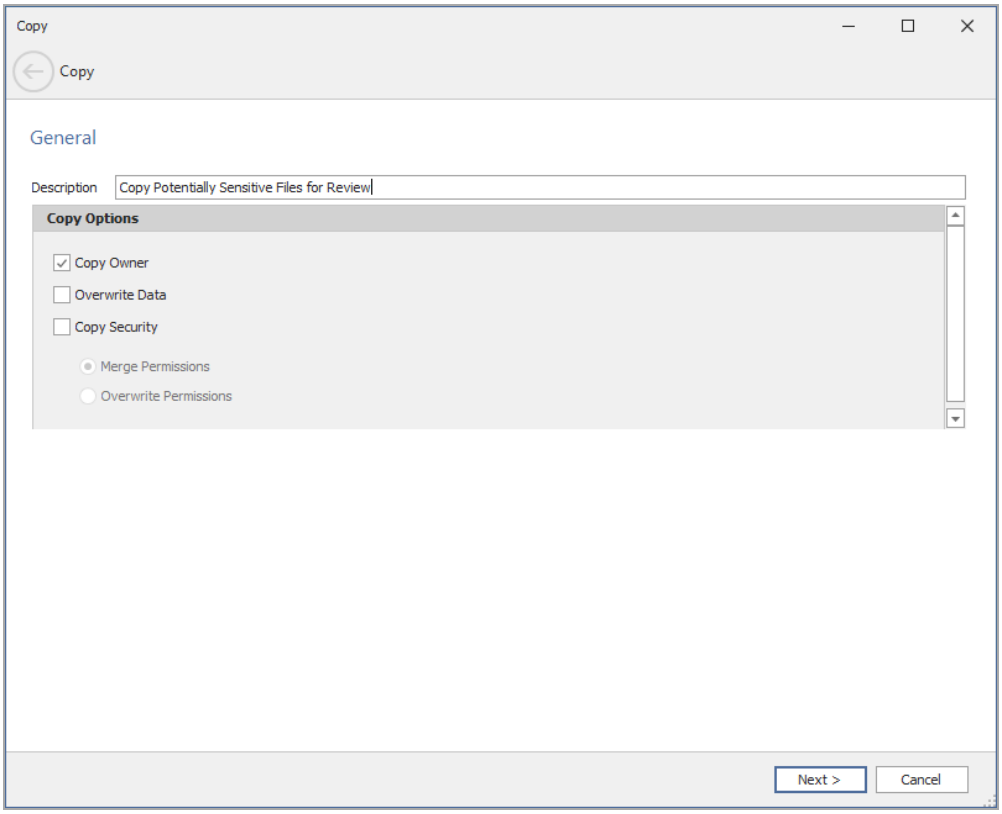
   Copy Owner: Selecting this check box maintains the ownership information of the copied files. If this is not selected, the Proxy Rights group becomes the owner.

   Overwrite Data: When there is a naming conflict between files, this option allows you to overwrite the existing file with the one being copied.

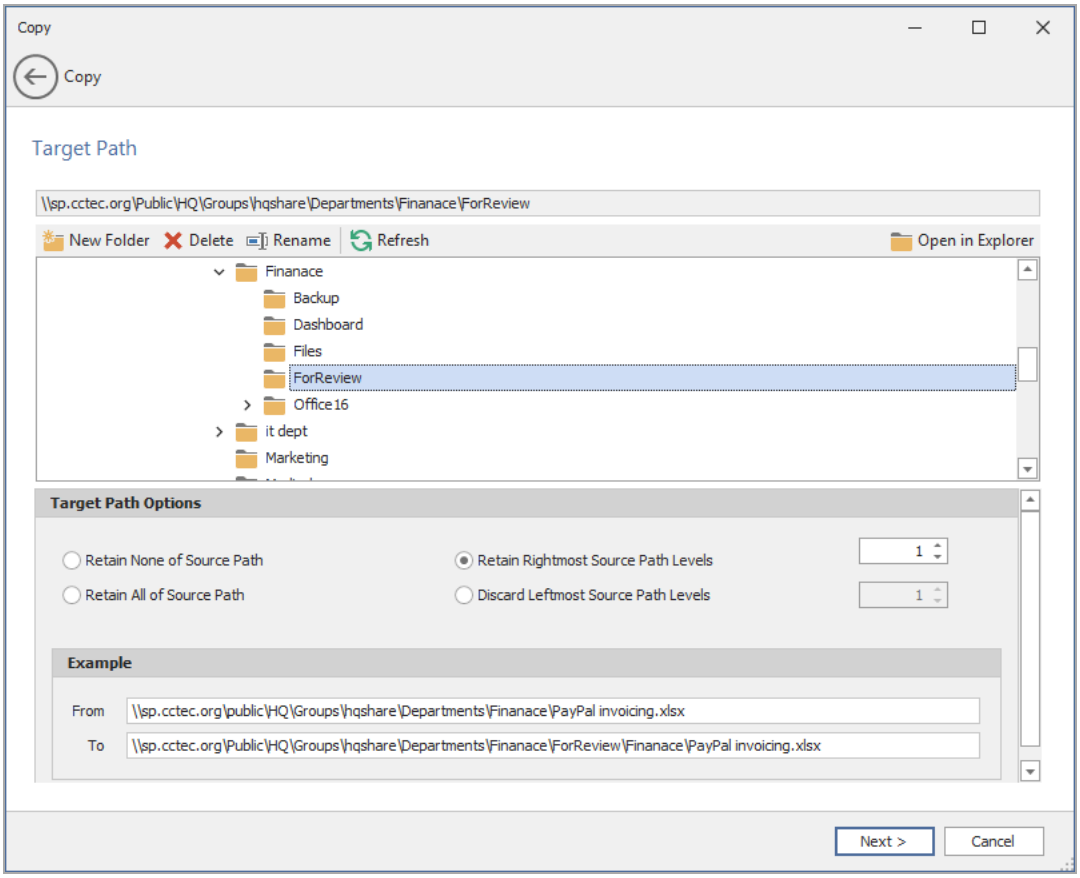
   Copy Security: Selecting this check box maintains the security settings for the copied files. If this is not selected, the copied files inherit the security of the network file system location to where they are copied.

   - **Merge Permissions:** Merges permissions from the source to the target if the target contains permissions that are not present in the source. This applies to all folders and files in the source folder structure.

- **Overwrite Permissions:** Overwrites permissions in the target with those found in the source. This applies to all folders and files in the target folder structure.



3. Click *Next*.



4. In the upper pane, browse to specify the location where the files will be copied.
5. In the *Target Path Options* region, select one of the following:
   - **Retain None of Source Path:** Copies files to the specified location without creating any subdirectories to store the copied files.

     For example, if you were copying files from the following location:

     `\\sp.cctec.org\Public\HQ\HQSHARE\Finance\Data`

     to

     `\\sp.cctec.org\Public\HQ\HQSHARE\Finance\Data\Gnance`

     The copied files would be located in the `Gnance` folder where other files might be located.

   - **Retain Rightmost Source Path Levels:** This option copies the files to a location according to the number of levels you specify.

     For example, if you were copying files from the following location:

     `\\sp.cctec.org\Public\HQ\HQSHARE\Finance\Data`

to

```
\\sp.cctec.org\Public\HQ\HQSHARE\Finance\Data\Gnance
```

and you select *Retain Rightmost Source Path Levels* and specify *1*,

the files would be copied to a new folder one level deeper in the path. The name of the new folder comes from the folder name one level higher in the current file path. So the files would be copied to:

```
\\sp.cctec.org\Public\HQ\HQSHARE\Finance\Data\Gnance\Data
```

- **Retain All of Source Path:** This option copies the files to a subdirectory in the specified folder using a duplicate path where the files are stored.

  For example, if you were copying files from the following location:

  ```
  \\sp.cctec.org\Public\HQ\HQSHARE\Finance\Data
  ```

  to

  ```
  \\sp.cctec.org\Public\HQ\HQSHARE\Finance\Data\Gnance
  ```

  the files would be copied to:

  ```
  \\sp.cctec.org\Public\HQ\HQSHARE\Finance\Data\Gnance\sp.cctec.org\Public\HQ\HQSHARE\Finance\Data\
  ```

- **Discard Leftmost Source Path Levels:** This option copies files to a subdirectory in the specified folder, based on the path where the files are stored, and the specified levels in the leftmost portion of the file path that you discard.

  For example, if you were copying files from the following location:

  ```
  \\sp.cctec.org\Public\HQ\HQSHARE\Finance\Data
  ```

  to

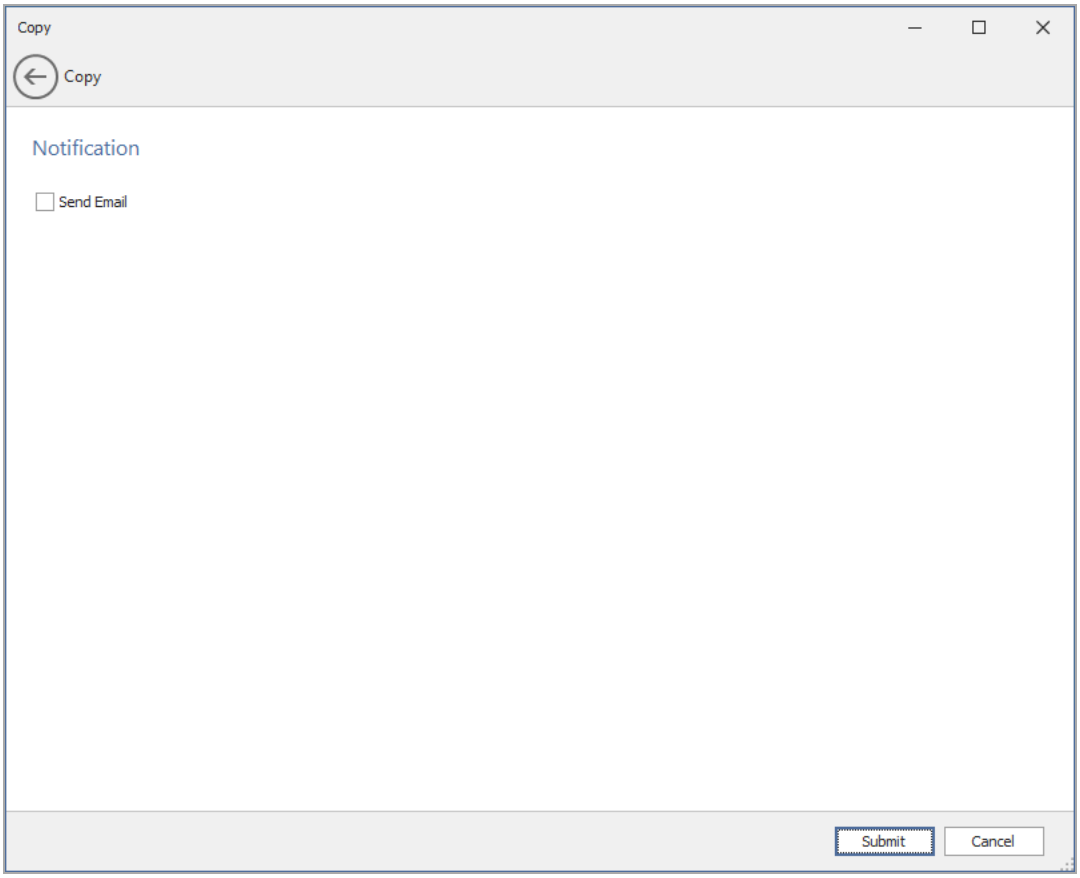
  ```
  \\sp.cctec.org\Public\HQ\HQSHARE\Finance\Data\Gnance
  ```

  and you select *Discard Leftmost Source Path Levels* and specify *2*, the files would be copied to:

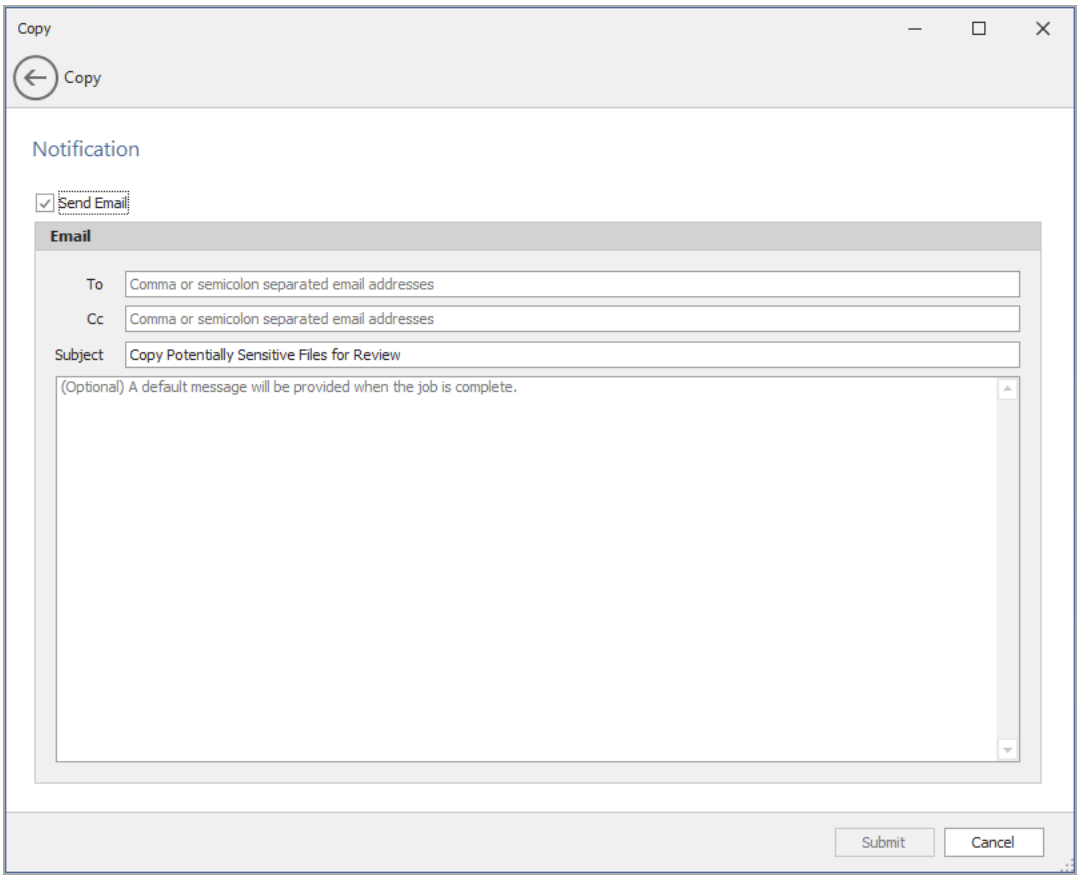
  ```
  \\sp.cctec.org\Public\HQ\HQSHARE\Finance\Data\Gnance\HQ\HQSHARE\Finance\Data\
  ```

The fields in the *Example* region will specify where files will be copied according to the options you select.

6. Click *Next*.



7. (Optional) If you want an email notification sent to someone once the files have been copied, specify the recipients and the email message in the fields provided.

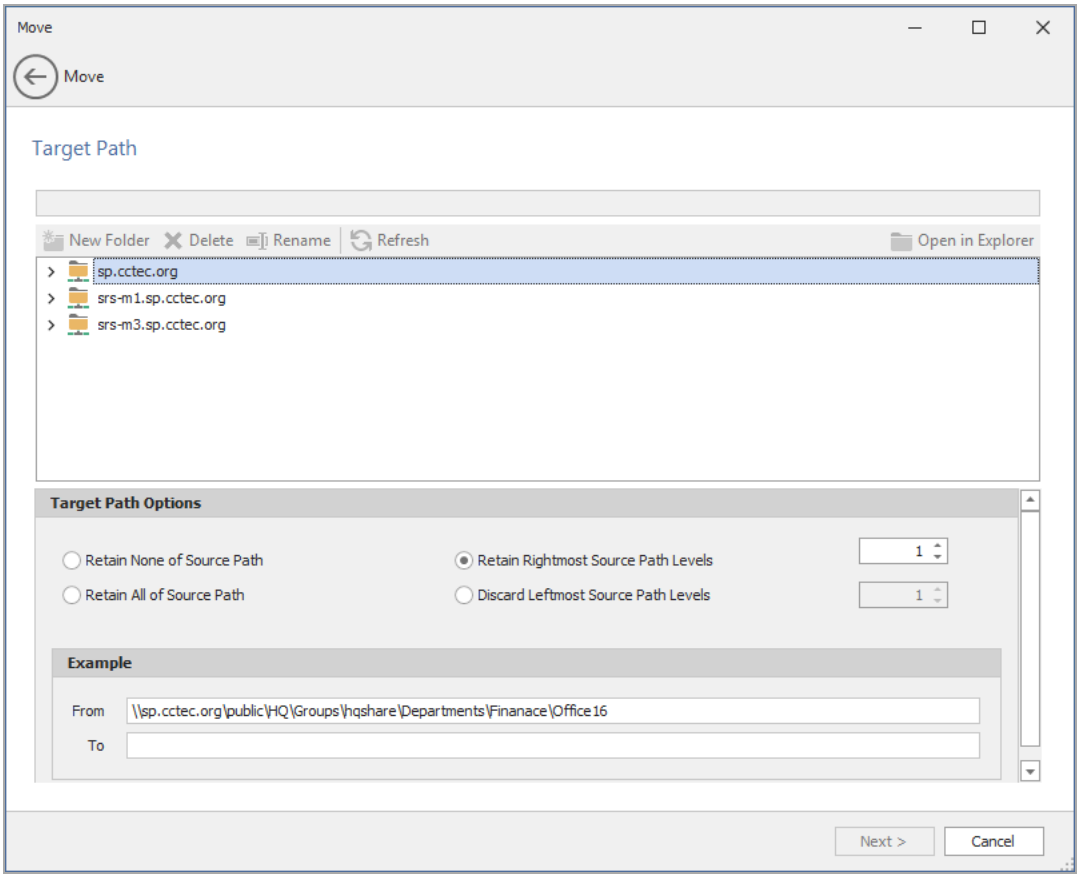
8. 

9. Click *Submit*.

1.8.3 - Move

This option moves files specified in each of the entries you select to a new a location specified by the Data Owner.

1. In the *Description* field, specify the purpose of the move operation and click *Next*.



2. In the upper pane, browse to specify the location where the files will be moved.
3. In the *Target Path Options* region, select one of the following:
   - **Retain None of Source Path:** Moves files to the specified location without creating any subdirectories to store the moved files.

     For example, if you were moving files from the following location:

     `\\sp.cctec.org\Public\HQ\HQSHARE\Finance\Data`

     to

     `\\sp.cctec.org\Public\HQ\HQSHARE\Finance\Data\Gnance`

     The moved files would be located in the `Gnance` folder where other files might be located.
   - **Retain Rightmost Source Path Levels:** This option moves the files to a location according to the number of levels you specify.

     For example, if you were moving files from the following location:

     `\\sp.cctec.org\Public\HQ\HQSHARE\Finance\Data`

to

```
\\sp.cctec.org\Public\HQ\HQSHARE\Finance\Data\Gnance
```

and you select *Retain Rightmost Source Path Levels* and specify *1*,

the files would be moved to a new folder one level deeper in the path. The name of the new folder comes from the folder name one level higher in the current file path. So the files would be moved to:

```
\\sp.cctec.org\Public\HQ\HQSHARE\Finance\Data\Gnance\Data
```

- **Retain All of Source Path:** This option moves the files to a subdirectory in the specified folder using a duplicate path where the files are stored.

  For example, if you were moving files from the following location:

  ```
  \\sp.cctec.org\Public\HQ\HQSHARE\Finance\Data
  ```

  to

  ```
  \\sp.cctec.org\Public\HQ\HQSHARE\Finance\Data\Gnance
  ```

  the files would be moved to:

  ```
  \\sp.cctec.org\Public\HQ\HQSHARE\Finance\Data\Gnance\sp.cctec.org\Public\HQ\HQSHARE\Finance\Data\
  ```

- **Discard Leftmost Source Path Levels:** This option moves files to a subdirectory in the specified folder, based on the path where the files are stored, and the specified levels in the leftmost portion of the file path that you discard.

  For example, if you were moving files from the following location:

  ```
  \\sp.cctec.org\Public\HQ\HQSHARE\Finance\Data
  ```

  to

  ```
  \\sp.cctec.org\Public\HQ\HQSHARE\Finance\Data\Gnance
  ```

  and you select *Discard Leftmost Source Path Levels* and specify *2*,

  the files would be moved to:

  ```
  \\sp.cctec.org\Public\HQ\HQSHARE\Finance\Data\Gnance\HQ\HQSHARE\Finance\Data\
  ```

The fields in the *Example* region will specify where files will be moved according to the options you select.

4. Click *Next*.
5. (Optional) If you want an email notification sent to someone once the files have been moved, specify the recipients and the email message in the fields provided.
6. Click *Submit*.

1.8.4 - Delete

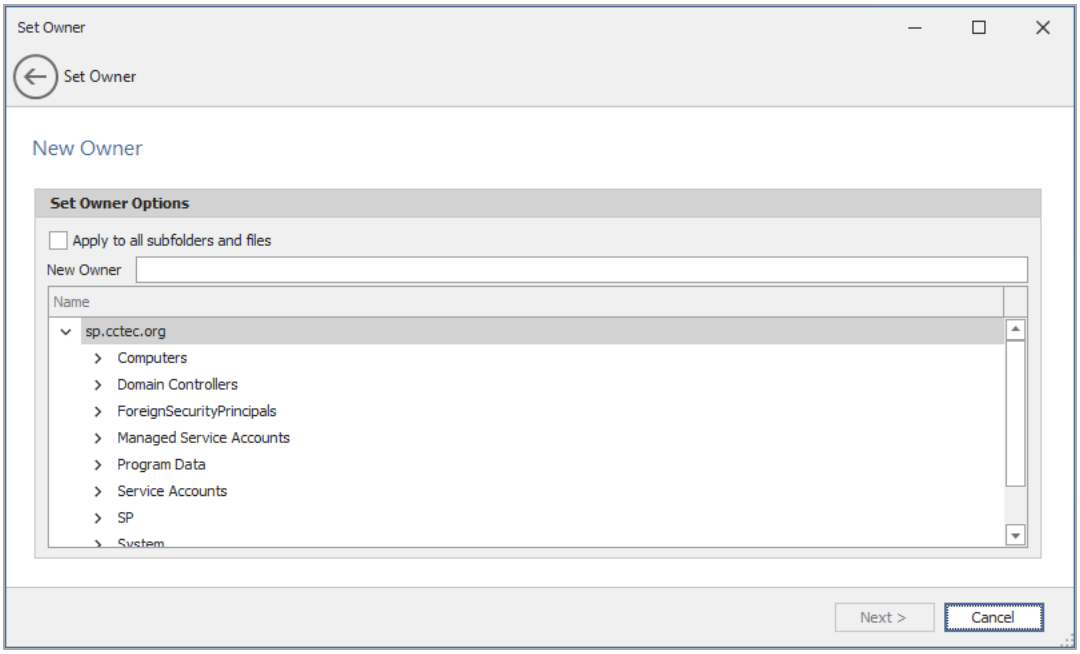
This option deletes files and folders specified in each of the entries you select.

1. In the *Description* field, specify the purpose of the delete operation and click *Next*.
2. (Optional) If you want an email notification sent to someone once the files have been deleted, specify the recipients and the email message in the fields provided.
3. Click *Submit*.

1.8.5 - Set Owner

This option allows the Data Owner to change the ownership of selected folders.

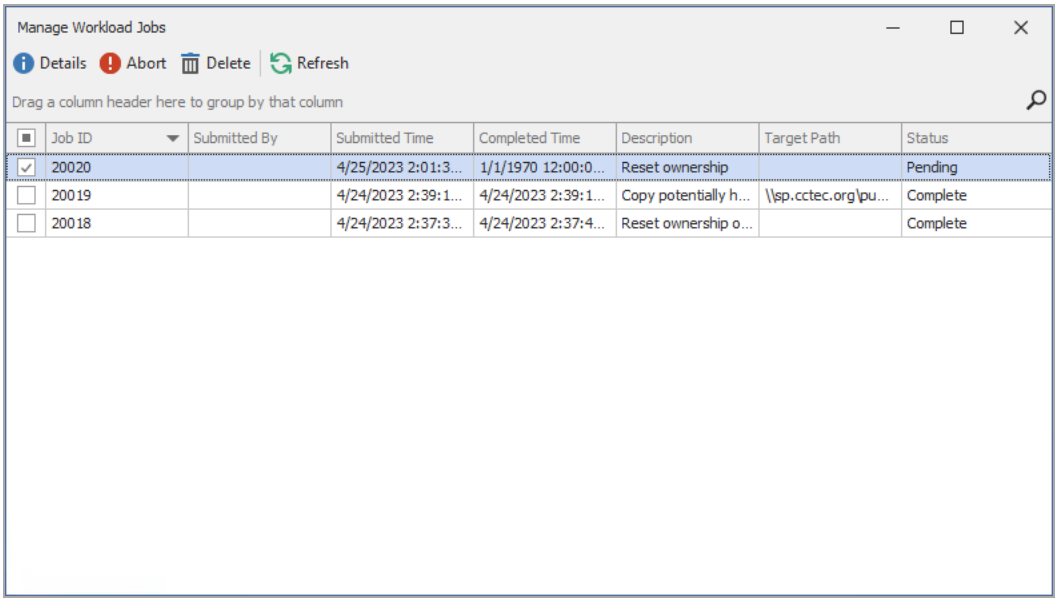
1. In the *Description* filed, specify the purpose of the Set Owner operation and click *Next*.



2. Specify the new owner by either typing the username or locating the User object.
    a. Click *Apply to Subfolders* if you want the user you specify to be the owner of all of the folder's subfolders.
3. Click *Next*.
4. (Optional) If you want an email notification sent to someone once the file ownership has been changed, specify the recipients and the email message in the fields provided.
5. Click *Submit*.

1.8.6 - Managing Workload Jobs

Clicking the *Jobs* tile brings up a list of Workload jobs.



From here, you can double-click a job to see more details, abort a pending job, or remove jobs from the list.

If you're a member of the File Dynamics Admins group, you will see the jobs for all users. If you are a regular user, you will see only the jobs that you have submitted.