SQL Web Reporter User Guide

Visual Click Software, Inc.

Table of Contents

Introduction

This user guide will assist you in getting started with the CPTRAX SQL Web Reporter. The CPTRAX SQL Web Reporter will allow you to query a Microsoft SQL Server or SQL Express Server and view the results of your query in an easy to use interface.

The CPTRAX SQL Web Reporter shows you details about your environment that have been collected by the CPTRAX Server Agent. The data can be viewed as charts/charts as well as in a table similar to Microsoft Excel.

Getting Started

To get started simply open a browser and browse to the appropriate URL to reach the CPTRAX SQL Web Reporter. If the defaults were accepted during the configuration the URL will be:

HTTP://CPTRAXWEB

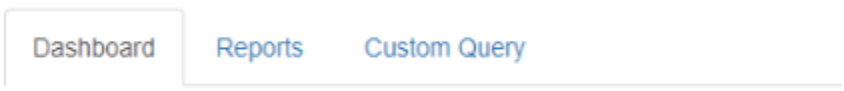
Since the URL is configurable, you may have to reach out to your administrator to find the appropriate URL.

CPTRAX SQL Web Reporter

The CPTRAX SQL Web Reporter is made up of three primary sections that are displayed as tabs in the web browser:

- Dashboard
- Reports
- Custom Query

Figure 1 shows an example of what you should expect.



Dashboard

The Dashboard is intended to provide quick insight into the events in the environment over the last 30 days. It includes the following:

- Active Directory Charts
- File System Charts
- Authentication Charts
- Group Policy Charts
- Summary Report

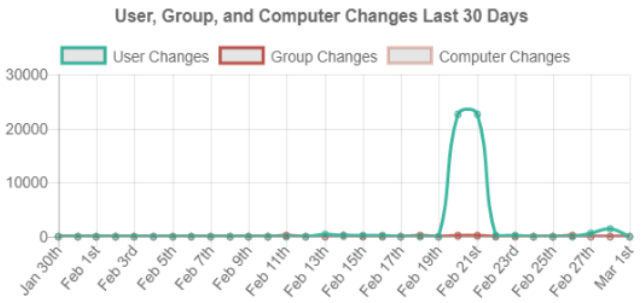
There are four types of charts under each chart sections:

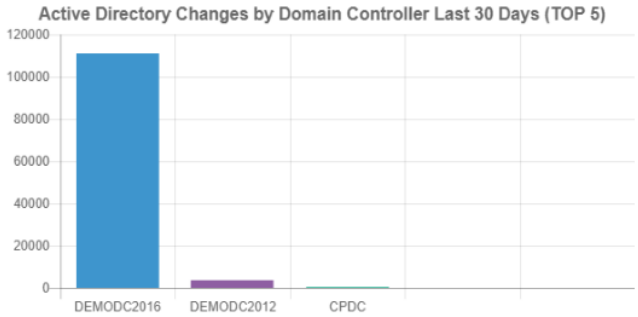
- Line Charts
- Bar Charts
- Horizontal Bar Charts
- Pie Charts

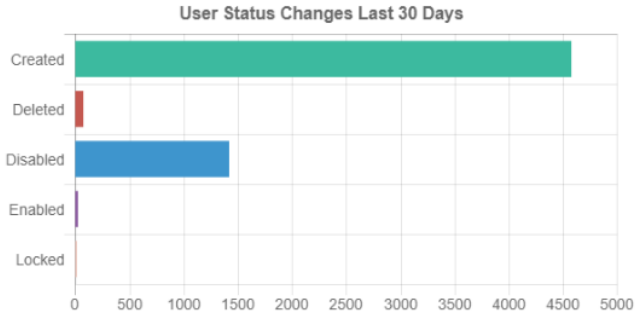
If you select an item on any chart's legend, you can remove that data from the chart temporarily. The data can be added back to the chart by selecting that item in the legend again.

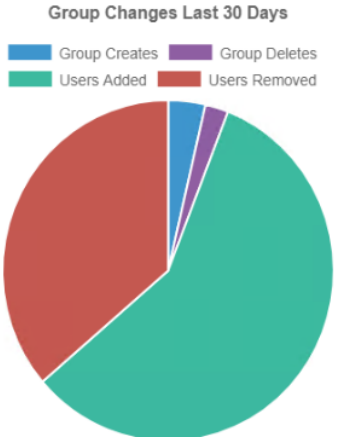
Active Directory Charts

Active Directory charts include data regarding any changes to Active Directory collected by the CPTRAX Server Agent. There are four Active Directory charts included with the CPTRAX SQL Web Reporter:







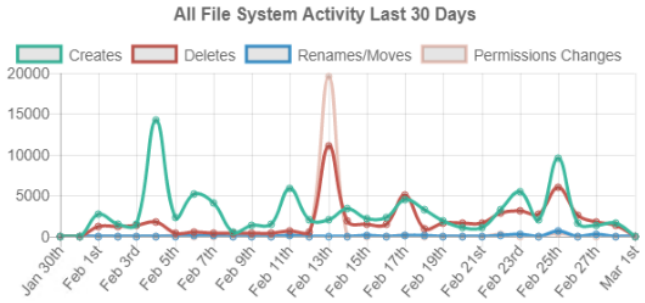


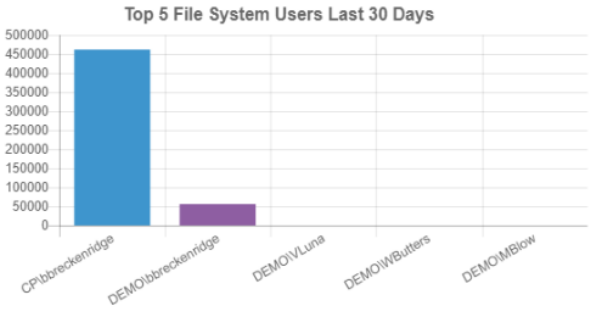
- User, Group, and Computer Changes Last 30 Days
  - Line chart
  - Includes all changes to users, groups and computers over the last 30 days.
  - Items in Legend can be selected to add/remove the data from the chart.
- Active Directory Changes by Domain Controller Last 30 Days (TOP 5)
  - Bar Chart
  - Includes the number of changes made per domain controller over the last 30 days.
  - It only shows the top 5 domain controllers with changes in the environment.
- User Status Changes Last 30 Days

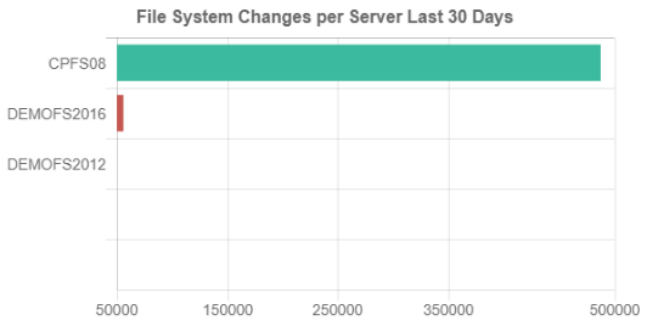
    - Horizontal Bar Chart
    - Includes counts of status changes for all users over the last 30 days. Status Changes include the following:
        - Enabled
        - Deleted
        - Disabled
        - Enabled
        - Locked
- Group Changes Last 30 Days
    - Pie Chart
    - Includes counts of group changes over the last 30 days. Changes included are:
        - New groups being created
        - Existing groups being deleted
        - Users being added to existing groups
        - Users being removed from existing groups
    - Items in Legend can be selected to add/remove the data from the graph.

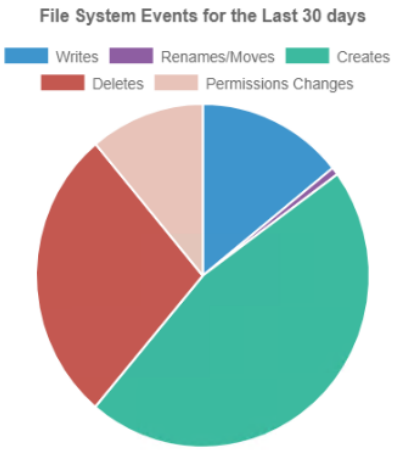
File System Charts

File System charts include data regarding any changes to the File System collected by the CPTRAX Server Agent. There are four File System charts included with the CPTRAX SQL Web Reporter:







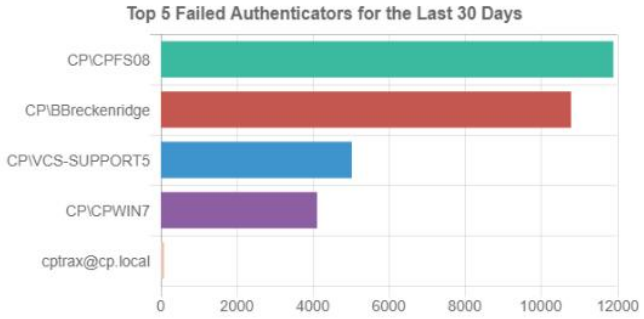


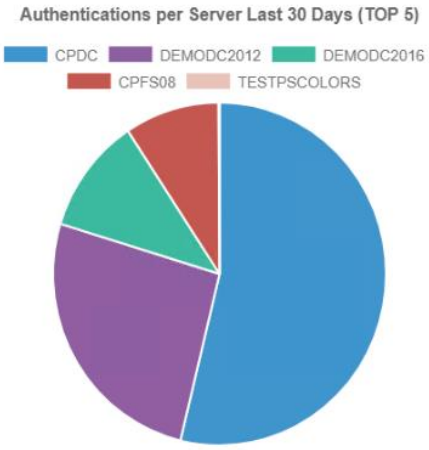
- All File System Activity Last 30 Days
  - Line Chart
  - Includes counts of File System changes over the Last 30 days. Changes included are:
    - Files/Folders Created
    - Files/Folders Deleted
    - Files/Folders Renamed/Moved
    - Files/Folders Permissions Changes
  - Items in Legend can be selected to add/remove the data from the graph.
- Top 5 File System Users Last 30 Days
  - Bar Chart

    - Includes counts of all file system activity for top 5 users over the last 30 days.
- File System Changes per Server Last 30 Days (TOP 5)
    - Horizontal Bar Chart
    - Includes the number of changes made per file server over the last 30 days.
    - It only shows the top 5 file servers with changes in the environment.
- File System Events for the Last 30 Days
    - Pie Chart
    - Includes the total number of file system events per activity type across all servers for the last 30 days. Activity Types included:
        - All Writes
        - All Renames/Moves
        - All Creates
        - All Deletes
        - All Permissions Changes
    - Items in Legend can be selected to add/remove the data from the graph.

Authentication Charts

Authentication charts include data regarding any successful or failed authentications collected by the CPTRAX Server Agent. There are four Authentication charts included with the CPTRAX SQL Web Reporter:



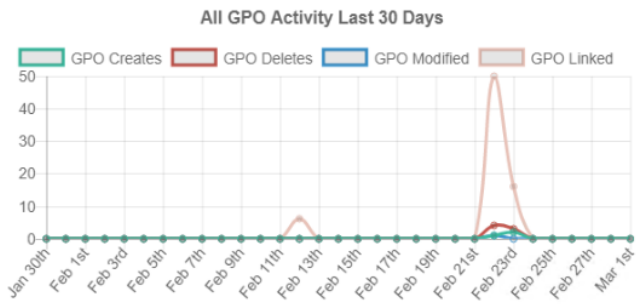


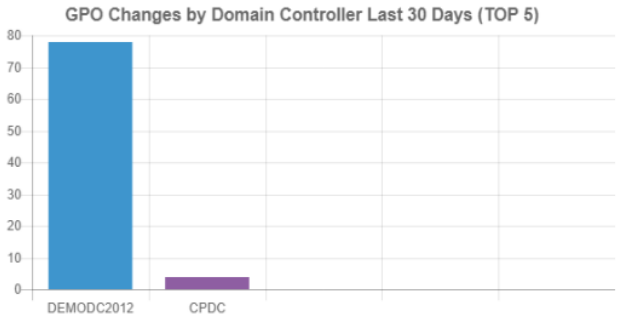
- Authentication Events Last 30 Days
  - Line Chart
  - Includes the total number of authentication events per activity type over the last 30 days. Activity types included:
    - Successful Logons
    - Failed Logons
    - Account Lockouts
  - Items in Legend can be selected to add/remove the data from the graph.
- Top 5 Authenticators for the Last 30 Days
  - Bar Chart
  - Includes the top 5 user's successful authentication count over the last 30 days.

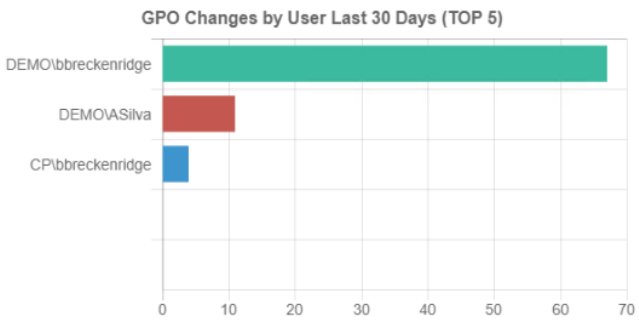
- Top 5 Failed Authenticators for the Last 30 Days
  - Horizontal Bar Chart
  - Includes top 5 user's failed authentication count over the last 30 days.
- Authentications per Server Last 30 Days (TOP 5)
  - Pie Chart
  - Includes authentication counts per Domain Controller for the top 5 Domain Controllers
  - Items in Legend can be selected to add/remove the data from the graph.

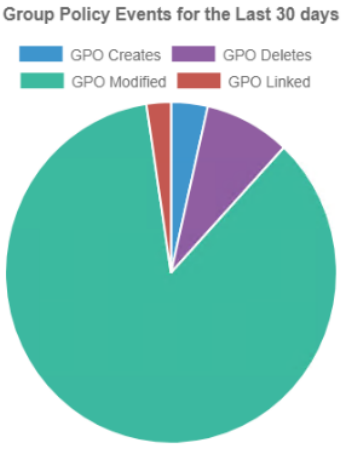
Group Policy Charts

Group Policy charts include data regarding any Group Policy changes collected by the CPTRAX Server Agent. There are four Group Policy charts included with the CPTRAX SQL Web Reporter:







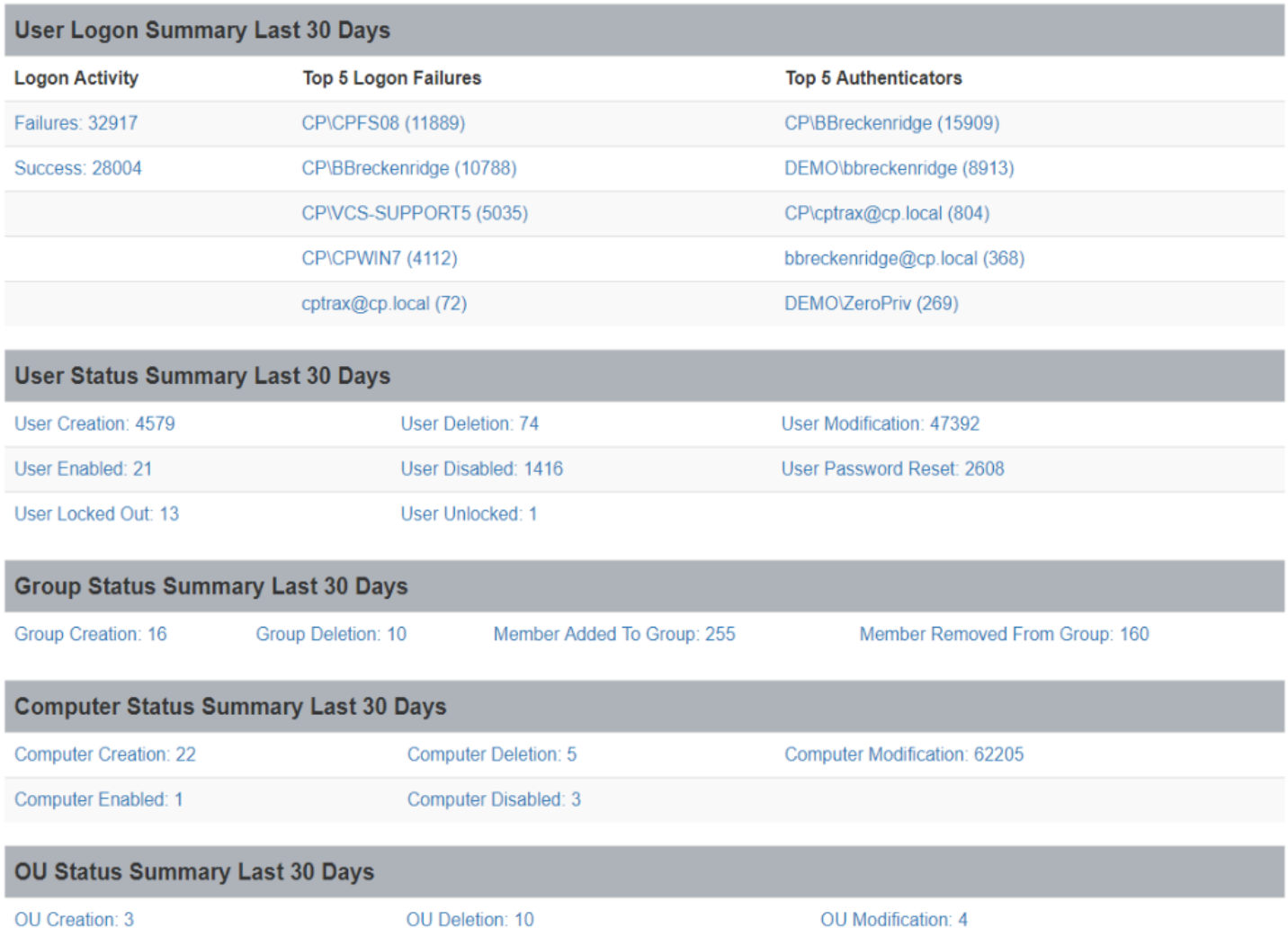


- All GPO Activity Last 30 Days
  - Line Chart

    - Includes total number of Group Policy changes over the last 30 days. Activity types included:
        - Group Policy Object Creations
        - Group Policy Object Deletions
        - Group Policy Object Modifications
        - Group Policy Objects being Linked/Unlinked
    - Items in Legend can be selected to add/remove the data from the graph.
- GPO Changes by Domain Controller Last 30 Days (TOP 5)
    - Bar Chart
    - Includes all Group Policy changes per domain controller for the top 5 domain controllers recording GPO changes.
- GPO Changes by User Last Days (TOP 5)
    - Horizontal Bar Chart
    - Includes all Group Policy changes per user for the top 5 users making GPO changes.
- GPO Events for the Last 30 Days
    - Pie Chart
    - Includes counts for Group Policy activities over the last 30 days. Activity types included:
        - Group Policy Objects Creations
        - Group Policy Objects Deletions
        - Group Policy OBjects Modifications
        - Group Policy Objects being Linked/Unlinked
    - Items in Legend can be selected to add/remove the data from the graph.

Summary Report

The Summary section of the CPTRAX SQL Web Reporter is meant to give administrators and auditors insight into the overall activity in the environment. It includes sections for different types of activities with various statistics related to those activities. If you click on a statistic it will show you the report that resulted in the statistic.



User Logon Summary Last 30 Days

Logon Activity	Top 5 Logon Failures	Top 5 Authenticators
Failures: 32917	CP\CPFS08 (11889)	CP\BBreckenridge (15909)
Success: 28004	CP\BBreckenridge (10788)	DEMO\bbreckenridge (8913)
	CP\VCS-SUPPORT5 (5035)	CP\cptrax@cp.local (804)
	CP\CPWIN7 (4112)	bbreckenridge@cp.local (368)
	cptrax@cp.local (72)	DEMO\ZeroPriv (269)

User Status Summary Last 30 Days

User Creation: 4579	User Deletion: 74	User Modification: 47392
User Enabled: 21	User Disabled: 1416	User Password Reset: 2608
User Locked Out: 13	User Unlocked: 1	

Group Status Summary Last 30 Days

Group Creation: 16	Group Deletion: 10	Member Added To Group: 255	Member Removed From Group: 160

Computer Status Summary Last 30 Days

Computer Creation: 22	Computer Deletion: 5	Computer Modification: 62205
Computer Enabled: 1	Computer Disabled: 3	

OU Status Summary Last 30 Days

OU Creation: 3	OU Deletion: 10	OU Modification: 4

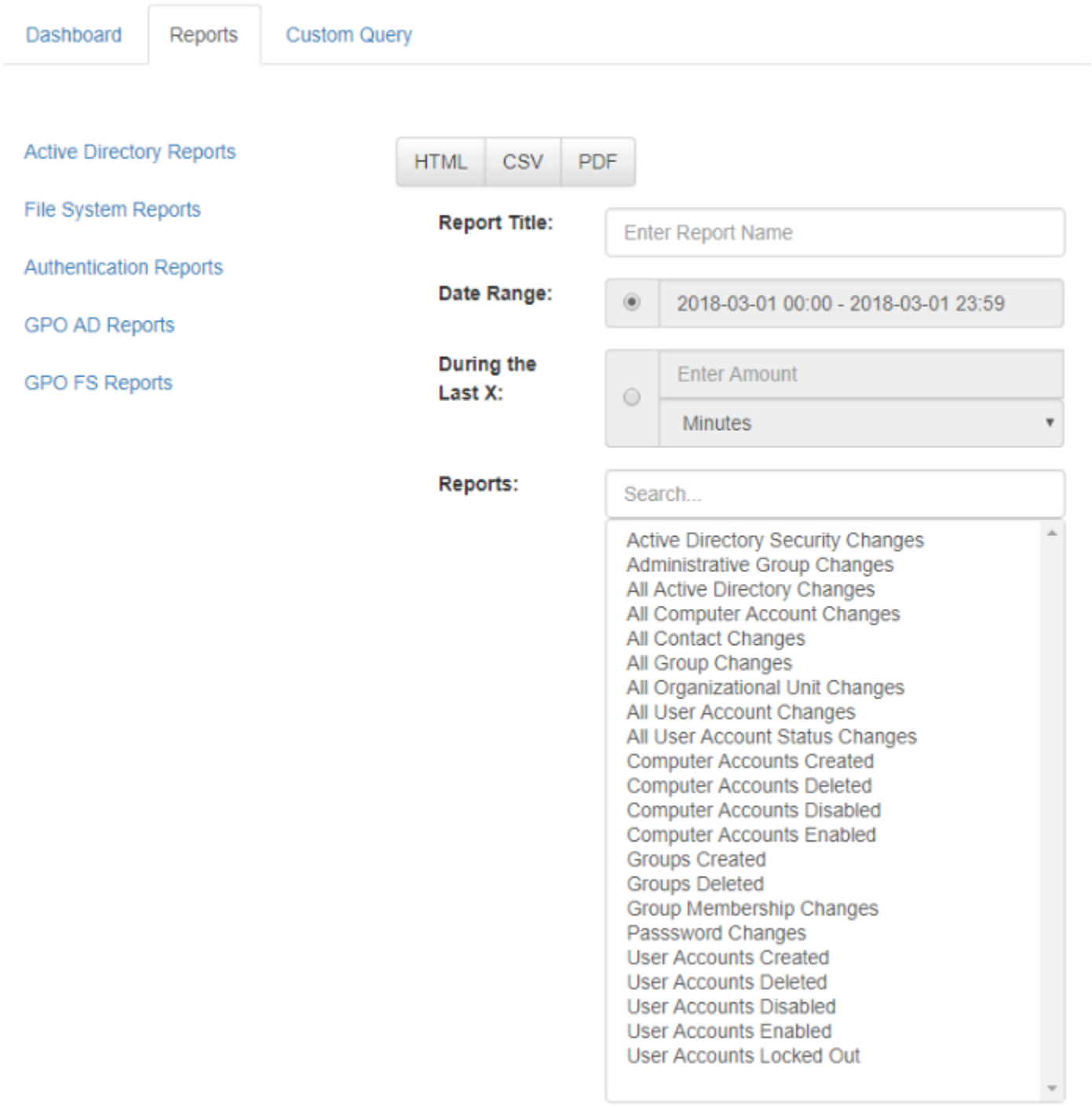
All Sections of the Summary Report:

- User Logon Summary Last 30 Days
    - Logon Activity
        - Total Count of all Failed Logons Last 30 Days
        - Total Count of all Successful Logons Last 30 Days
    - Top 5 Logon Failures
        - Top 5 User/Computer Accounts for total number of failed logons during the last 30 days.
        - Top 5 User/Computer Accounts for total number of successful logons during the last 30 days.
- User Status Summary Last 30 Days
    - Count of all users created during the last 30 days.
    - Count of all users deleted during the last 30 days.
    - Count of all users modified during the last 30 days.
    - Count of all users enabled during the last 30 days.
    - Count of all users disabled during the last 30 days.
    - Count of all password changes during the last 30 days.
    - Count of all users locked out during the last 30 days.
    - Count of all users unlocked during the last 30 days.
- Group Status Summary Last 30 Days
    - Count of all groups created during the last 30 days.
    - Count of all groups deleted during the last 30 days.
    - Count of members added to groups during the last 30 days.
    - Count of members removed from groups during the last 30 days.
- Computer Status Summary Last 30 Days
    - Count of all computers created during the last 30 days.
    - Count of all computers deleted during the last 30 days.
    - Count of all computers modified during the last 30 days.
    - Count of all computers enabled during the last 30 days.
    - Count of all computers disabled during the last 30 days.
- OU Status Summary Last 30 Days
    - Count of all organizational units created during the last 30 days.
    - Count of all organizational units deleted during the last 30 days.

    - Count of all organizational units modified during the last 30 days.
- GPO Status Summary Last 30 Days
    - Count of all group policy objects created during the last 30 days.
    - Count of all group policy objects deleted during the last 30 days.
    - Count of all group policy objects modified during the last 30 days.
    - Count of all group policy objects linked or unlinked during the last 30 days.
    - Count of all changes to the Default Domain group policy object during the last 30 days.
- File System Summary Last 30 Days
    - Count of all file/folder creations during the last 30 days.
    - Count of all file/folder deletions during the last 30 days.
    - Count of all file/folder permissions changes during the last 30 days.
    - Count of all file/folder writes during the last 30 days.
    - Count of all file/folder renames and moves during the last 30 days.

Reports

The reports section is made up of five sub sections that include common reports required for day to day auditing and regulatory compliance. There are several reports included in each section. In each section you can select a date range and the report you would like to run and then select “Run Report”.



Active Directory Reports

The Active Directory Reports section includes various Active Directory reports to assist with day to day auditing and regulatory compliance. The reports included are:

- Active Directory Security Changes
    - Includes any change to the ntSecurityDescriptor attribute. This attribute is modified when user or group permissions change within Active Directory.
- Administrative Group Changes
    - Includes any changes to the following administrative groups:
        - Domain Admins
        - Enterprise Admins
        - Schema Admins
        - Account Operators
        - Server Operators
        - Backup Operators
- All Active Directory Changes
    - Includes all changes to all objects in Active Directory.
- All Computer Account Changes
    - Includes all changes to computer objects in Active Directory.
- All Contact Changes
    - Includes all changes to contact objects in Active Directory.
- All Group Changes
    - Includes all changes to group objects in Active Directory
- All Organizational Unit Changes
    - Includes all changes to organizational units in Active Directory
- All User Account Changes
    - Includes all changes to user objects in Active Directory.
- All User Account Status Changes
    - Includes all user objects being disabled, enabled, locked out or unlocked in Active Directory.
- Computer Accounts Created

    - Includes all computer objects created in Active Directory.
- Computer Accounts Deleted
    - Includes all computer objects deleted in Active Directory.
- Computer Accounts Disabled
    - Includes all computer objects disabled in Active Directory.
- Computer Accounts Enabled
    - Includes all computer objects enabled in Active Directory.
- Groups Created
    - Includes all group objects created in Active Directory.
- Groups Deleted
    - Includes all group objects deleted in Active Directory.
- Group Membership Changes
    - Includes all group membership changes in Active Directory.
- Password Changes
    - Includes all password changes in Active Directory.
- User Accounts Created
    - Includes all user objects created in Active Directory.
- User Accounts Deleted
    - Includes all user objects deleted in Active Directory.
- User Accounts Disabled
    - Includes all user objects disabled in Active Directory.
- User Accounts Enabled
    - Includes all user objects enabled in Active Directory.
- User Accounts Locked Out
    - Includes all user objects locked out in Active Directory.

File System Reports

The File System Reports section includes various File System reports to assist with day to day auditing and regulatory compliance. The reports included are:

- All File Changes
    - Includes all file changes across all file servers.
- All File System Changes

    - Includes all file system changes across all file servers. (Files & Folders)
- All Folder changes
    - Includes all folder changes across all file servers.
- Created Files
    - Includes all created files across all file servers.
- Created Files and Folders
    - Includes all created files and folders across all file servers.
- Created Folders
    - Includes all created folders across all file servers.
- Deleted Files
    - Includes all deleted files across all file servers.
- Deleted Files and Folders
    - Includes all deleted files and folders across all file servers.
- Deleted Folders
    - Includes all deleted folders across all file servers.
- Renamed Files
    - Includes all renamed files across all file servers.
- Renamed Files and Folders
    - Includes all renamed files and folders across all file servers.
- Renamed Folders
    - Includes all renamed folders across all file servers.
- Permissions Changes
    - Includes all permissions changes across all file servers.

Authentication Reports

The Authentication Reports section includes various Authentication reports to assist with day to day auditing and regulatory compliance. The reports included are:

- Authentication History
    - Includes all successful authentication history for Active Directory.
- Failed Authentication History
    - Includes all failed authentication history for Active Directory.

- Failed Authentications – Bad Account Name
    - Includes all failed authentications for Active Directory where the user entered a username that didn't exist in Active Directory.
- Failed Authentications – Bad Password
    - Includes all failed authentications for Active directory where the user entered an incorrect password.
- Workstation Locks and Unlocks
    - Includes all workstation locks and unlocks and any local password changes on workstations.

GPO AD Reports

The GPO AD Reports section includes various GPO AD reports to assist with day to day auditing and regulatory compliance. The reports included are:

- GPO Changes
    - Includes all GPO changes made through the Group Policy Management Console.
- Default Domain Policy Changes
    - Includes all changes to the Default Domain Group Policy Object through the Group Policy Management Console.

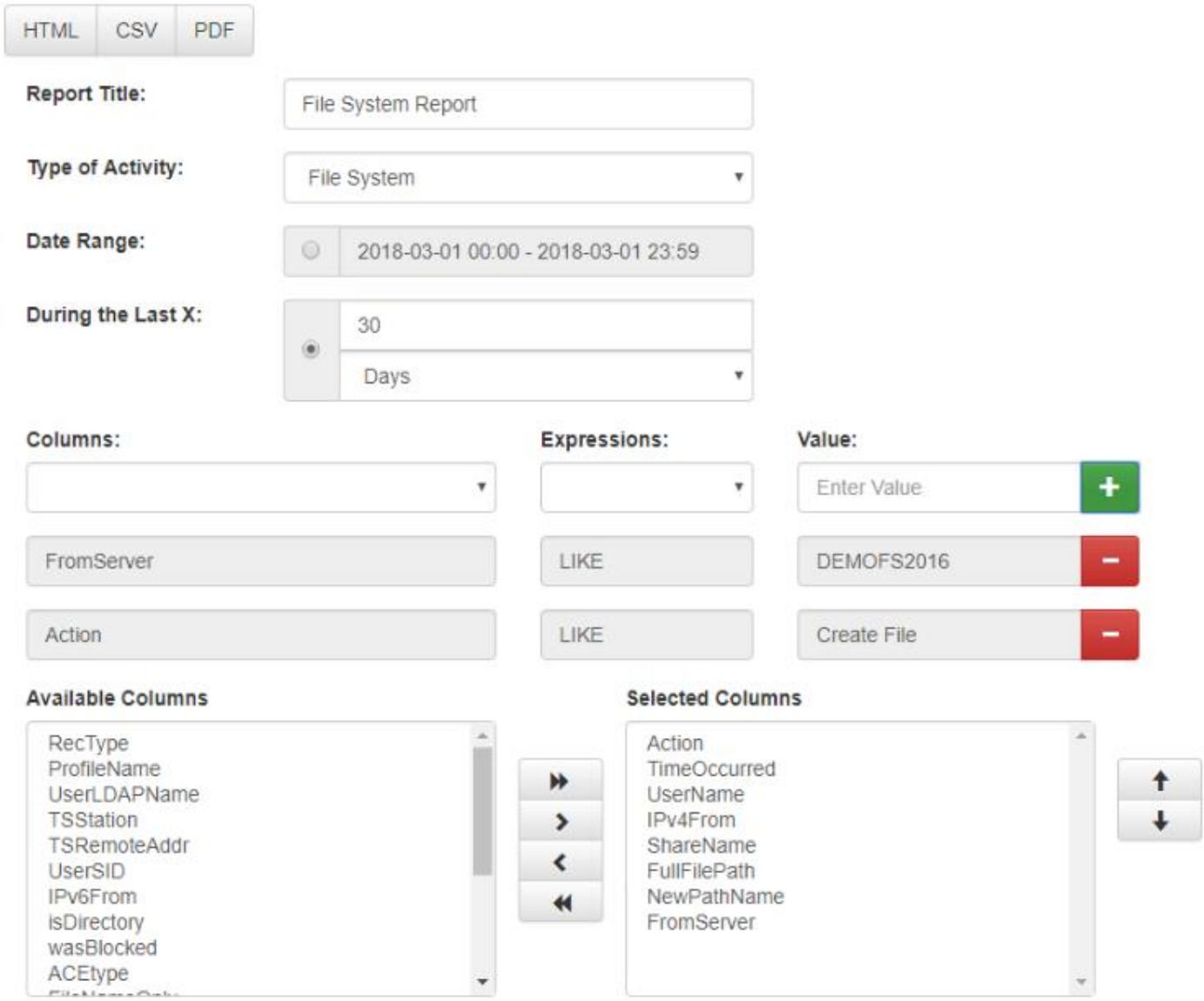
GPO FS Reports

The GPO FS Reports section includes various GPO FS reports to assist with day to day auditing and regulatory compliance. The reports included are:

- GPO Changes
    - Includes all changes to the files related to Group Policy Objects.
- Default Domain Policy Changes
    - Includes all changes to the files related to the Default Domain Group Policy Object.

Custom Query

The Custom Query Section allows the user to run custom queries against the SQL Server.



The options are:

- Report Title
  - This is a custom name the user can give the report. It will be included at the top of the results page and in the tab text in the browser tab.
- Type of Activity
  - Authentication
  - File System

    - Active Directory
    - GPO AD Changes
    - GPO FS Changes
- Date Range
    - Select your date range from the calendar GUI.
- During the Last X
    - Set a value and the period to run reports for the Last 30 Days for example.
- Filters
    - Filter any number of columns
    - Each filter is made up of a Column, an Expression, and a Value
- Available Columns
    - Columns that are available to include in the report, but are not currently included in the report.
- Selected Columns
    - Columns that are currently included in the report.
- Run Report
    - Select HTML, CSV, or PDF to run the report and receive the results in the specified format.

Query Results Page

The query results page will display the results from any query ran by the user. There are several ways to manipulate the results once they have completely loaded.

- Show/Hide Columns
    - Allows the user to dynamically show/hide columns that were selected when the report was ran.
- Share the results as CSV or an HTML link that can be e-mailed, bookmarked, or linked to on an internal portal.
- Search All Columns for a Value
    - The search box in the top right allows the user to search all columns for a particular value. The value is assumed to have wildcards on each

side, so search for the letters OU would find any value with “OU” anywhere throughout the value.

- Drag and Drop Columns
    - The user can left click and hold on any column name, then drag right or left to change the order of the columns.
- Sort Columns Ascending/Descending
    - A single left click on any column name will result in the column being sorted.
- Highlight/Select Rows
    - The user can select any number/combination of rows by left clicking on the rows with shift/ctrl selected on the keyboard. Works the same as selecting 1 or more objects in Windows Explorer.
- Search Individual Columns for a Value
    - At the bottom of each column is a field so you can search that single column for a value. The value is assumed to have wildcards on each side, so search for the letters OU would find any value with “OU” anywhere throughout the value. The TimeOccurred column provides a calendar GUI to assist with filtering on date/time.