

## **User Guide**

Revised in Oct, 2019



# **BrowseReporter**

**Version 5.4.2**

**Employee Monitoring Software**

# BrowseReporter User Guide - Table of Contents

<b>1.0 Introduction to BrowseReporter .....</b>	<b>5</b>
1.1 CurrentWare Components .....	6
1.2 System Requirements .....	7
1.3 Installing the CurrentWare Server, Console and Solutions .....	8
1.4 Installing the CurrentWare Clients .....	9
1.4.1 Local CurrentWare Client Install.....	9
1.4.2 Remote Client Install .....	10
1.4.3 Deploy CurrentWare Client by Command Line .....	12
1.4.4 Deploy CurrentWare Client with a Third-Party Software Delivery Tool or Active Directory	12
1.5 Configuring the CurrentWare Client to Connect to the CurrentWare Server over the Internet (Port Forwarding) .....	13
1.5.1 Preparing Your CurrentWare Server .....	13
1.5.2 Installing the CurrentWare Client .....	13
1.6 Upgrading the CurrentWare Clients.....	14
1.6.1 Automatic Upgrade of the CurrentWare Clients.....	14
1.6.2 Manual Upgrade of the CurrentWare Clients .....	15
1.7 Standalone Installation.....	15
1.7.1 Installing the CurrentWare Console, Server and Solution .....	15
1.7.2 Installing the CurrentWare Client .....	15
1.7.3 Password Protect the CurrentWare Console .....	15
1.8 Connecting CurrentWare to your SQL server.....	16
1.8.1 Migrating your Existing CurrentWare Data from Firebird to SQL Server.....	17
<b>2.0 CurrentWare Console Overview .....</b>	<b>18</b>
2.1 Client and Group Management.....	19
2.2 Redirect Clients .....	20
2.3 Client Settings .....	22
2.4 Troubleshooting.....	26
2.5 Operators.....	28
2.5.1 Operator Permissions.....	29
2.6 Import Users .....	31
2.7 Database Backup Scheduler.....	33
2.8 Auto Delete Scheduler .....	34
2.9 Console Settings .....	35
2.10 Server Settings.....	37
2.11 Log Out.....	37
<b>3.0 Overview of BrowseReporter Functions .....</b>	<b>38</b>

<b>4.0 Run Report.....</b>	<b>39</b>
4.1 Report Profile .....	40
4.2 Report Type.....	40
4.3 Report Options .....	42
4.3.1 Select Mode.....	42
4.3.2 Rename Category.....	42
4.3.3 Options.....	43
4.3.4 Idle Time Limit .....	43
4.3.5 Reporting Period.....	43
4.3.6 Output .....	43
<b>5.0 Request Latest Data .....</b>	<b>44</b>
<b>6.0 Add Custom Logo.....</b>	<b>45</b>
<b>7.0 URL Tracking Scheduler .....</b>	<b>45</b>
<b>8.0 Exclusion List.....</b>	<b>46</b>
<b>9.0 Email Reports .....</b>	<b>48</b>
9.0.1 Email Report Options .....	50
<b>9.1 Email Alerts .....</b>	<b>50</b>
<b>9.2 Email Settings .....</b>	<b>53</b>
<b>10.0 Export URLs .....</b>	<b>54</b>
<b>11.0 Delete Data.....</b>	<b>55</b>
<b>12.0 Remote Screen Capture .....</b>	<b>56</b>
<b>13.0 Tracking Options .....</b>	<b>57</b>
13.1 Tracking Options .....	57
13.2 Upload Settings .....	57
13.2.1 Auto Upload .....	58
13.2.2 Manual Upload.....	58
<b>14.0 BrowseReporter Client Settings .....</b>	<b>60</b>
<b>15.0 CurrentWare Server Manager .....</b>	<b>61</b>
15.1 Changing the CurrentWare Client and Console Port.....	61
15.2 Stopping the CurrentWare Server Service .....	63
15.3 CurrentWare Database Selection .....	63
15.4 Upgrading the CurrentWare Database .....	64
15.5 Compress the CurrentWare Database.....	64
15.6 Archive and Restore the CurrentWare Database .....	65
15.7 Repairing the CurrentWare Database.....	66
15.8 Reset Primary Key .....	67
15.9 Advanced.....	67

<b>16.0 Licensing .....</b>	<b>69</b>
16.1 Register Your Permanent License key .....	69
16.2 License Management.....	70
16.2.1 Managing Your CurrentWare Licenses .....	70
<b>17.0 Uninstall CurrentWare Server, Console and Solutions .....</b>	<b>71</b>
17.1 Uninstalling the CurrentWare Solutions .....	71
17.2 Uninstalling the CurrentWare Server and Console.....	71
<b>18.0 Uninstall CurrentWare Client.....</b>	<b>72</b>
18.1 Uninstall CurrentWare Client from the Console.....	72
18.2 Uninstall CurrentWare Client on the Workstation by Command Line.....	73
18.3 Uninstall CurrentWare Client on the Workstation from the Client Configuration Window.....	73
<b>19.0 Technical Support.....</b>	<b>74</b>
<b>20.0 Contacts.....</b>	<b>75</b>

# 1.0 Introduction to BrowseReporter

BrowseReporter is an easy to use reporting tool designed to allow department managers, team leaders, teachers and lecturers to monitor user Internet browsing activity.

BrowseReporter provides the facility to generate reports and graphs at both the computer and user level. In depth information of the sites visited and the time spent at these sites are presented. Detailed reports, summary level reports and graphs can be generated.

In addition to tracking Internet activity, BrowseReporter also includes bandwidth monitoring and remote screen capture functions.

## 1.1 CurrentWare Components

There are four primary components in the CurrentWare Console

### CurrentWare Server

This component includes a server Service and database. It houses all the data for the configuration and settings. The CurrentWare Server is the central hub for the CurrentWare Consoles and the CurrentWare Clients to connect to. A Firebird database is used for the data storage.

### CurrentWare Console

This component is the management console that the administrator uses to control the functionalities of the CurrentWare Solutions. The administrator will be able to see the connection status of their CurrentWare Clients within the CurrentWare Console.

Multiple consoles can be installed on the same network. Multiple authentications can be assigned to different users to allow or restrict the full functionality of the console.

**NOTE:** the CurrentWare Server and the Console components are commonly installed on the same computer. Additional CurrentWare Consoles may be installed on other administrators' computers.

### CurrentWare Solutions

This component contains different functionalities based on the solution that you are installing. After the installation of a CurrentWare solution, the solution's functions will be embedded on the right-hand side of the CurrentWare Console.

- **BrowseControl:** Web Filtering
- **BrowseReporter:** Internet Tracking and Reporting
- **AccessPatrol:** Endpoint Device Security
- **enPowerManager:** Power Management

### CurrentWare Client

This component is to be installed on all computers that need to be managed by the CurrentWare Console. The CurrentWare Clients establish communication to the CurrentWare Server. The client is password protected and runs in stealth mode.

## 1.2 System Requirements

### Hardware Requirement

All components of the CurrentWare Console are supported on desktop computers and server computers with the following specifications.

- **Processor:** any CPU running i3 or similar or faster
- **Memory:** At least 4GB of RAM
- **Disk Space:** At least 500MB of disk space

### Software Requirement

All components of the CurrentWare Console are compatible with the following Operating Systems running 32-bit or 64-bit platform.

- **Windows 7 Professional and Ultimate**
- **Windows 8 and 8.1 Professional and Ultimate**
- **Windows 10 Pro and Enterprise**
- **Windows Server 2008, 2012, 2016**

## 1.3 Installing the CurrentWare Server, Console and Solutions

Follow the instructions below to install the CurrentWare Server, Console and Solutions.

### Before you begin your installation:

- Installation of all components must be done with an admin user account.
- The Server and Console components may be installed on the same computer.

### 1. Download the Setup Files

Download the CurrentWare setup files from our website:

<http://www.currentware.com/download/>

### 2. Select a Computer to Install the CurrentWare Server and Console

### 3. Install the CurrentWare Server and Console

1. Unzip the setup file that you downloaded from our website and run the **currentware.exe** to initiate the CurrentWare Console Installation Wizard.
2. Proceed to accept the **License Agreement**.
3. Put in your **User Information** (Full Name and Organization name) and select the software usage for “Anyone who uses this computer” or “Only for me”.
4. Now, select the **CurrentWare Components** that you want to install. For first time installation, click next. The install wizard will automatically select the CurrentWare Console and Server to be installed on your computer.
5. Select the **Solutions** that you want to install.
6. Type in the computer name (or IP address) of your CurrentWare Server. For first time installation, click next. The install wizard will automatically type in your Computer name.
7. The Installer will now proceed to install the CurrentWare Server, Console and the solution(s) on your computer.



## 1.4 Installing the CurrentWare Clients

Follow the instructions below to install the CurrentWare clients on the computers you want to manage. After a successful installation of the CurrentWare Clients, they will connect to your CurrentWare Server and automatically show up on your CurrentWare Console.

### Before you begin your installation:

- Installation of all components must be done with an admin user account.
- To successfully deploy the CurrentWare Client using the **Remote Client Install utility**, please temporarily disable the Windows Firewall on the client computers and disable Windows's Simple File Sharing.

There are four ways to deploy the CurrentWare Clients to your workstations.

1. **Local CurrentWare Client Install:** run the *cwClientSetup.exe* file on all the computers you want to manage.
2. **Remote Client Install:** use the built-in *Remote Client Install* tool on the CurrentWare Console to push the CurrentWare Client install to the computers.
3. **Deploy the CurrentWare Client by Command Line:** create a batch file that will install the CurrentWare Client. Run the batch file through *Active Directory* or *Login Script*.
4. **Deploy the CurrentWare Client with a Third-Party Software Delivery Tools:** use third-party software to deploy the *cwClientSetup.exe* file.

### 1.4.1 Local CurrentWare Client Install

This is the most standard method of installing the CurrentWare Client. Run the *cwClientSetup.exe* file on each computer you want to manage.

The *cwClientSetup.exe* file can be found on the computer that you have installed the CurrentWare Server. This set up file is stored under:

CurrentWare Client Setup File:

**C:\Program Files (x86)\CurrentWare\cwClient\cwClientSetup.exe**

When you run the *cwClientSetup.exe* on your managed computers, you will need to fill in the following information.

## 1. Computer Name or IP Address of the CurrentWare Server

Put in the Computer Name or IP address of the CurrentWare Server that you want the client to connect to. Ensure that the managed workstations can establish connections to the CurrentWare Server.

Upon the completion of your CurrentWare Client installation, it will automatically connect to your CurrentWare Console.

### 1.4.2 Remote Client Install

#### Before you begin your installation:

- Disable UAC (User Account Control) and Windows Firewall on the client computers


CurrentWare Clients can be remotely installed from the Console. The remote installer can be found on the console under the menu **Install > Remote Client Install**.

1. Browse for the path of the CurrentWare Client setup file, cwClientSetup.exe, on your computer. By default, this file is located in the following folder on the server computer:

**C:\Program Files(x86)\CurrentWare\cwClient\cwClientSetup.exe**

2. Enter the **Computer name or IP address** of the CurrentWare Server.
3. Select the option to enable or disable **reboot** after the installation (the recommended option is to enable reboot).
4. Select the computers you want to install the CurrentWare Client on:
  - a. You can enter the IP address manually, or
  - b. Click on the Search button to allow CurrentWare to look for the computers on your network, or
  - c. Import from a text file that contains a list of your computers' names or IP addresses.
5. Enter the username and password of an account that has administrative rights to the computers you are installing to.
  - a. If you are a domain admin, put in the username in the format of **Domain\Administrator**
6. The CurrentWare Client will now be deployed to the designated computers.

Remote Client Install

 **Remote Client Install**  
Deployment of the CurrentWare Client to the computers on your network

**Installer Path**

Select the path of the client setup file

C:\Program Files (x86)\CurrentWare\cwClient\cwClientSetup.exe Browse Save

*(The default location of the client setup file is: %Program Files (x86)%\CurrentWare\cwClient\)*

**CurrentWare Server Settings**

CurrentWare Server    
*IP address or Computer name*

**Reboot Option**

☐ Reboot client systems after installation

Reboot Delay:  minutes

**Note:** Please disable the Firewall and UAC on the target computers. Next Cancel

The First screen of the Remote Client Install Window.

If you are encountering the following error messages during the remote client installation, visit this page for help:

<https://www.currentware.com/faqs/remote-client-install/>

### 1.4.3 Deploy CurrentWare Client by Command Line

The CurrentWare client file can be deployed through a single command line. Below is a list of switches you can along with the command line to deploy the CurrentWare client with the configurations of your choice.

```
e:\cwClientSetup.exe /qn USERPARAMS="-p Admin -ds 192.168.1.100 " /l  
e:\install.log /norestart
```

#### Switches:

-p	Required parameter (password is Admin)
-ds	CurrentWare Server IP address or Computer name
-rp	New Password (Optional)
-sp	Confirm Password (Optional)
/qn	Quiet Install
/l	Create a log file during the install. Specify the location and name of the log file.
/norestart	Prevents the installer to restart the client computer

In the above example, the network drive is assigned with the letter e:\. The CurrentWare Client set up file is stored on the network drive and the install log file will be created on the network drive after the installation.

### 1.4.4 Deploy CurrentWare Client with a Third-Party Software Delivery Tool or Active Directory

The CurrentWare Client is packaged as an .exe file and a .msi file. You can find the .msi file as a separate download link from our download page. You can use your company's system deployment tools to deploy the CurrentWare client to your workstations.

#### Deploy by Customizing the cwClientSetup.msi File

You can take the existing cwClientSetup.msi file and customize it with the proper CurrentWare Server Computer name and other parameters before you deploy the file.

Use a MSI editor (for example, the Orca MSI editor) and modify the following table within the cwClientSetup.exe file:

Table Property	Property USERPARAMS	Value "-p Admin -ds 192.168.1.100"
-------------------	------------------------	---------------------------------------

Change the IP address in the value field to the IP address of your CurrentWare Server.

Deploy the .msi file using a Software Delivery Tool or through Active Directory.

## 1.5 Configuring the CurrentWare Client to Connect to the CurrentWare Server over the Internet (Port Forwarding)

To connect your CurrentWare Clients to the CurrentWare Server over the Internet, you will need to port forward the CurrentWare traffic from your network's router to the CurrentWare Server computer.

### 1.5.1 Preparing Your CurrentWare Server

First, you will need to set up your CurrentWare Server on a network that has a **Public Static IP address** (obtained from your Internet service provider).

Then, you will need to configure your router's setting. On your router's configuration page, go to the Port Forwarding Settings and forward the traffic from the following ports to the IP address of your CurrentWare Server computer.

- **8990 (TCP and UDP)**
- **8991 (TCP and UDP)**
- **8992 (TCP and UDP)**
- **3050 (TCP and UDP)**
- **1024 (TCP and UDP)**
- **1433 (TCP and UDP)** – for SQL Server database only

### 1.5.2 Installing the CurrentWare Client

Install the CurrentWare Client by running the cwClientSetup.exe file on the Client computer. During the installation, put in the **Public IP address, hostname or DDNS** of the CurrentWare Server's Network.



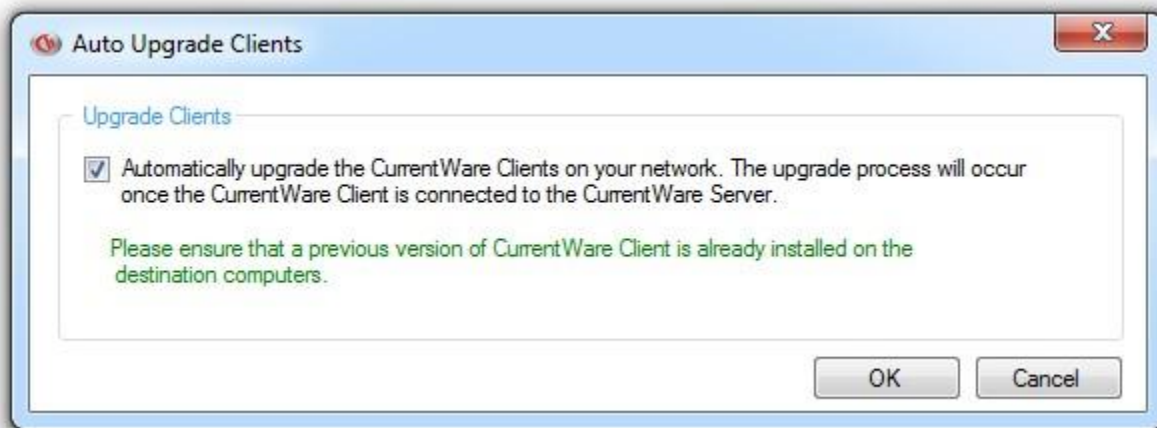
## 1.6 Upgrading the CurrentWare Clients

There are two ways to upgrade the CurrentWare clients in version 4 – Automatic upgrade or Manual upgrade.

### 1.6.1 Automatic Upgrade of the CurrentWare Clients

The client upgrade process can be automated when you upgrade any version of the CurrentWare client to the latest version.

1. On the CurrentWare Console, go to **Install > Auto Upgrade Clients**.
2. Click on the “**Automatically upgrade the CurrentWare Clients on your network...**” checkbox and the CurrentWare Server will push the update to the clients.



The Client upgrade is automatic when this option is enabled.

## 1.6.2 Manual Upgrade of the CurrentWare Clients

The client upgrade method can be done manually by running the cwClientSetup.exe file on each computer that has a CurrentWare client installed.

## 1.7 Standalone Installation

**Standalone:** Installing the CurrentWare Server, Console and Client on the same computer.

### 1.7.1 Installing the CurrentWare Console, Server and Solution

1. Run the CurrentWare.exe setup file.
2. Accept the terms in the License Agreement.
3. Select the Security Solutions you want to install.
  - a. AccessPatrol: Block USB and external devices.
  - b. BrowseControl: Web Filter and Application Blocking.
  - c. BrowseReporter: Internet Activity Tracking.
  - d. enPowerManager: Remote Power Management.
4. The Installer will proceed to install the CurrentWare Server, Console and Solutions onto your computer.

### 1.7.2 Installing the CurrentWare Client

1. Run the **cwClientSetup.exe** setup file.
2. When prompted for the CurrentWare Server, put in the word **loopback**. This will make the Client connect to itself.
3. Finish the installation.

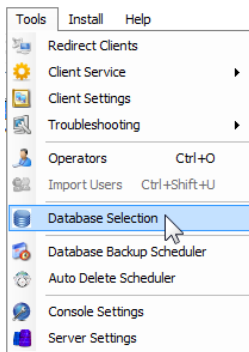
### 1.7.3 Password Protect the CurrentWare Console

1. Launch the CurrentWare Console.
2. Go to Tools > Operators.
3. Click on Add and add an operator with administrator role.
4. Once an administrator has been added, check the option "Enable Password Security".
5. The next time you launch the CurrentWare Console, it will ask you to enter the operator name and password.

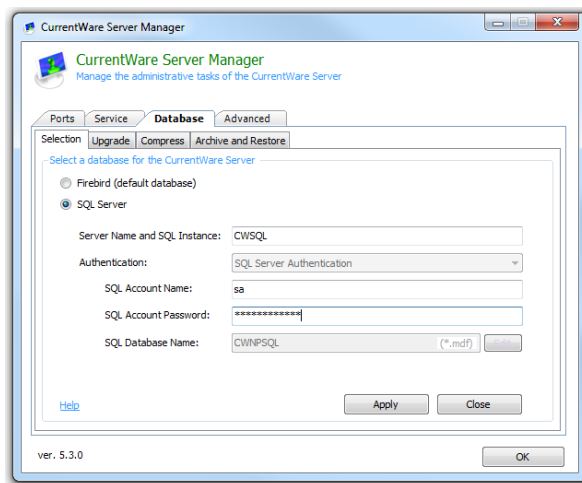
## 1.8 Connecting CurrentWare to your SQL server

The CurrentWare Server database is compatible with Microsoft SQL server (not included in the setup file). Follow the instructions below to connect your CurrentWare Server to your SQL server.

1. Open the CurrentWare Console.
2. Select *Tools > Database Selection*.



3. This will bring up the CurrentWare Server Manager.
4. Select *Database > Selection > SQL Server*.
5. Enter your SQL Server details:



- SQL Server name and Instance.
- Authentication:
  - i. For workgroup, SQL Server Authentication is required.
  - ii. For Domain, you can choose between SQL Server Authentication or Windows Authentication.



- Account name and password.
6. A new SQL database called *CWNPSQL.mdf* will be created on your SQL Server.
  7. (Optional): A prompt will appear to give you a choice to migrate your existing Firebird database to the new SQL database.

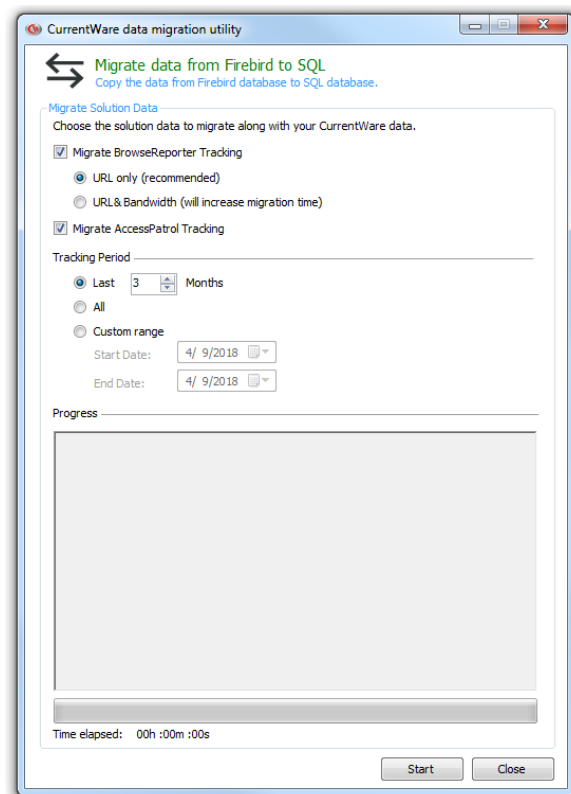
## 1.8.1 Migrating your Existing CurrentWare Data from Firebird to SQL Server

The data migration utility is presented after connecting your CurrentWare Server to a new SQL Server database.

File location: *\Program Files(x86)\CurrentWare\cwServer\CWDBMigration.exe*

The data migration utility will migrate all of the CurrentWare data from the Firebird to the SQL database. The following data can be included or excluded from the migration:

1. BrowseReporter Tracking Data: URL, Application and Bandwidth.
  - **NOTE:** Including bandwidth data will increase the migration time significantly.
2. AccessPatrol Tracking Data.

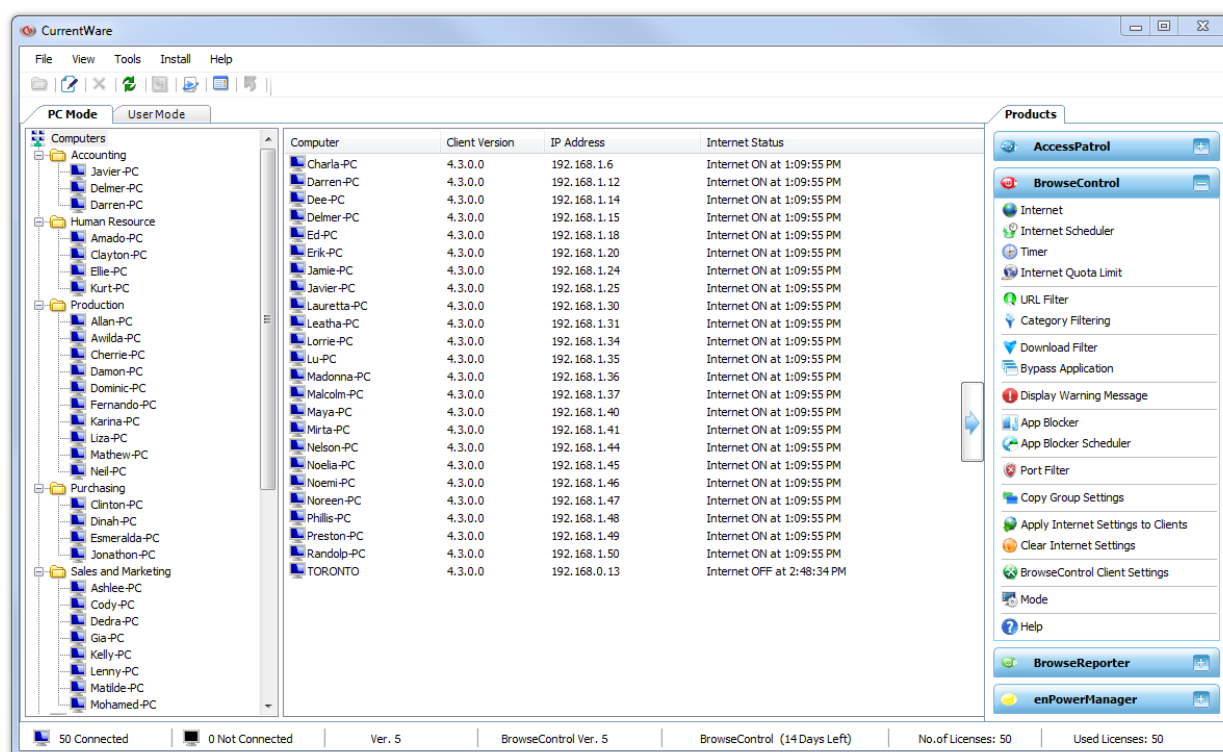


## 2.0 CurrentWare Console Overview

The CurrentWare Console is the manager that the administrators will use to control the managed workstations.

The CurrentWare Console contains the following functions:

- **Client and Group Management**
- **Redirect Clients**
- **Client Settings**
- **Operators**
- **Import Users**
- **Options**
- **Log Out**



The CurrentWare Console.

## 2.1 Client and Group Management

In computer mode, a connected client is represented by a blue computer icon, while an unconnected client is represented by a grey computer icon. In user mode, an active user is represented by a green user icon, while an inactive user is represented by an orange user icon. For ease of management, the workstations and users can be organized into groups.

### Create a New Group

To create a new group, from the menu, select **File > Add New Group**.

Or, right click on the computer pane in the CurrentWare console and select **Add New Group**.

### Rename a Group

To rename a group, from the menu, select **File > Rename**.

Or, right click on the computer pane in the CurrentWare console and select **Rename**.

### Delete a Group

To delete a group, from the menu, select **File > Delete**.

Or, right click on the computer pane in the CurrentWare console and select **Delete**.

### Move Computers/Users

On the CurrentWare Console, organization of the computers, users and groups can be accomplished by dragging and dropping the selected computer/user into the group. To facilitate the organization of a large number of computers, users or groups, you can use the **Move Computers/Users** function.

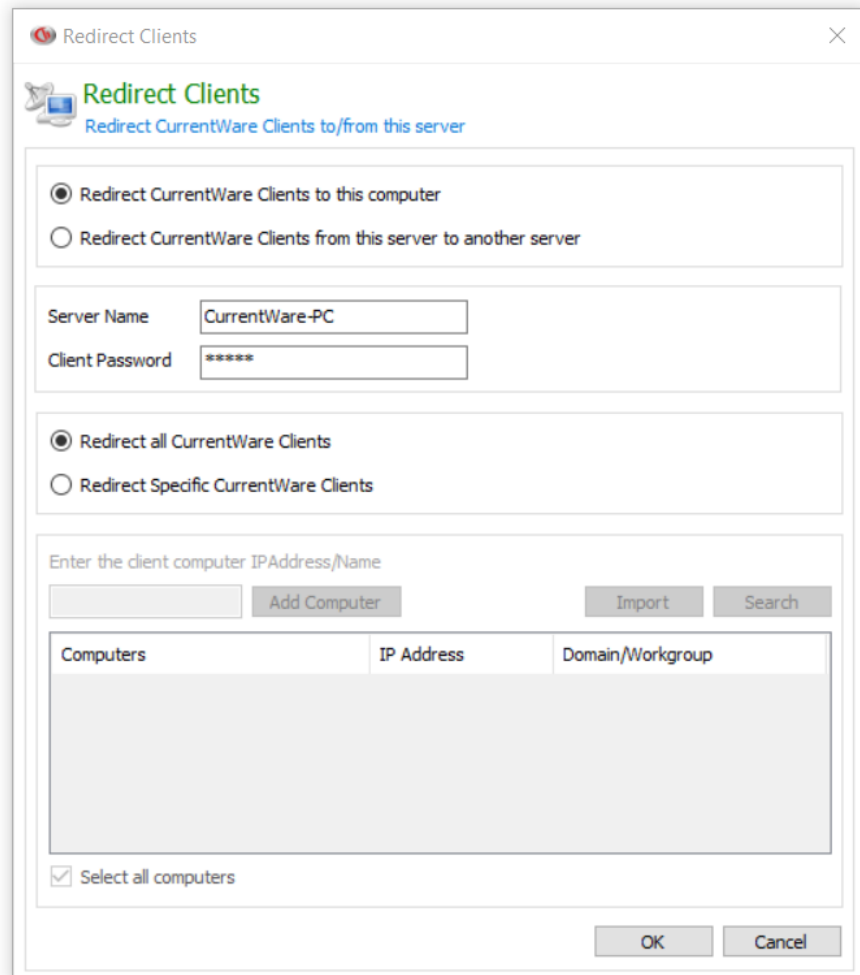
On the CurrentWare Console menu, select **File > Move Computer/Users**. The left-hand side contains the source folder and the right hand side contains the destination folder. Select the computer(s) you want to move from the source folder, and then select the destination folder. Click on the >> button to move the computers.

## 2.2 Redirect Clients

Redirect Client is used to move multiple CurrentWare Clients from one CurrentWare Server to another CurrentWare server.

### Redirect CurrentWare Clients to this computer

1. On the new CurrentWare Server, launch the CurrentWare Console and access the menu **Tools > Redirect Clients**.
2. Select the option **Redirect CurrentWare Clients to this computer**
3. Enter the CurrentWare Client password. The default password is Admin
4. Select Redirect All CurrentWare Clients.
5. Click on OK.
6. After a brief moment, the CurrentWare Clients will start connecting to this CurrentWare Server



Redirect Clients

Redirect CurrentWare Clients to/from this server

☒ Redirect CurrentWare Clients to this computer  
☐ Redirect CurrentWare Clients from this server to another server

Server Name: CurrentWare-PC  
Client Password: \*\*\*\*\*

☒ Redirect all CurrentWare Clients  
☐ Redirect Specific CurrentWare Clients

Enter the client computer IPAddress/Name

Add Computer Import Search

Computers	IP Address	Domain/Workgroup
-----------	------------	------------------

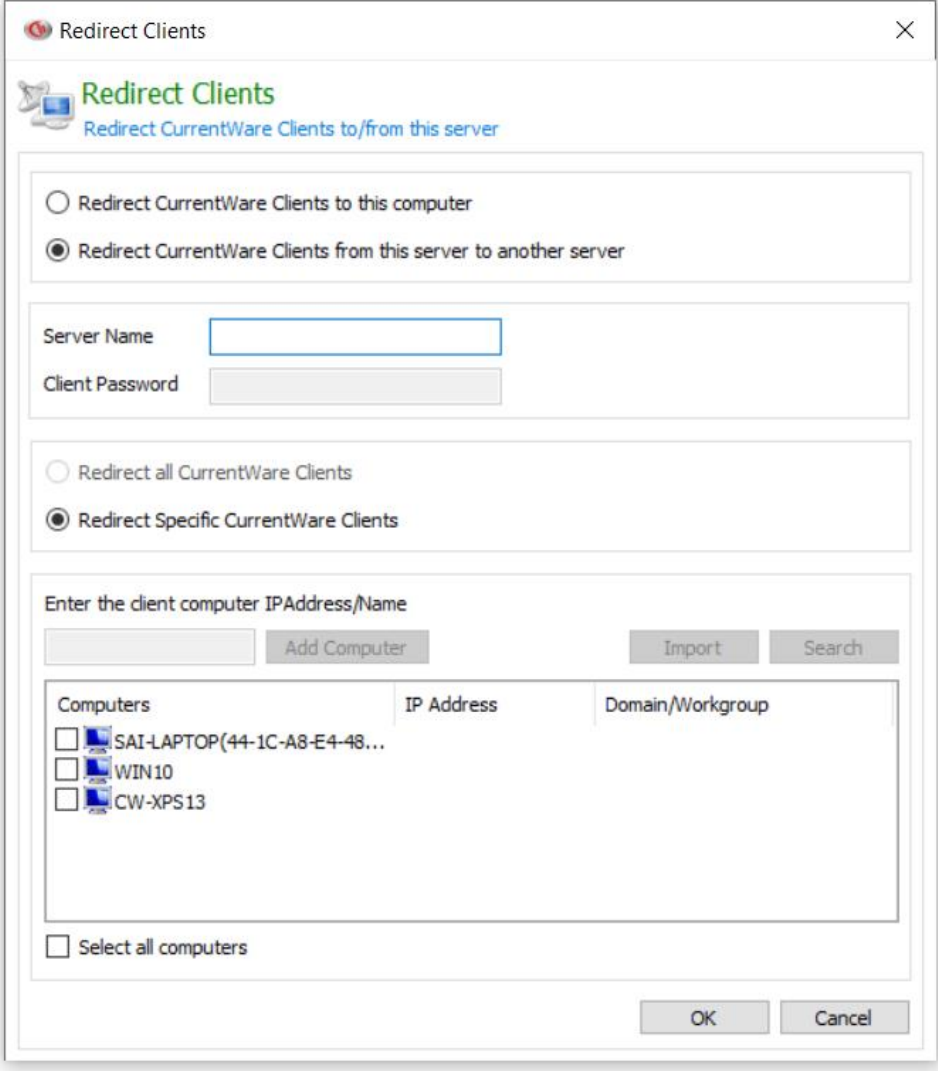
☒ Select all computers

OK Cancel

Redirect CurrentWare Clients to this CurrentWare Server.

## Redirect CurrentWare Clients from this server to another server

1. On the old CurrentWare Server, launch the CurrentWare Console and access the menu **Tools > Redirect Clients**.
2. Select the option **Redirect CurrentWare Clients from this server to another server**
3. Enter the name of the new CurrentWare Server
4. Select the computer you want to redirect to the new CurrentWare Server. Only connected computers can be redirected.
5. Click on OK.
6. After a brief moment, the CurrentWare Clients will start connecting to the new CurrentWare Server



Redirect Clients

Redirect CurrentWare Clients to/from this server

☐ Redirect CurrentWare Clients to this computer

☒ Redirect CurrentWare Clients from this server to another server

Server Name

Client Password

☐ Redirect all CurrentWare Clients

☒ Redirect Specific CurrentWare Clients

Enter the client computer IPAddress/Name

Add Computer Import Search

Computers	IP Address	Domain/Workgroup
<input type="checkbox"/> SAI-LAPTOP(44-1C-A8-E4-48...)		
<input type="checkbox"/> WIN10		
<input type="checkbox"/> CW-XPS13		

☐ Select all computers

OK Cancel

Redirect CurrentWare Clients that are connected from the old CurrentWare Server to a new CurrentWare Server.

## 2.3 Client Settings

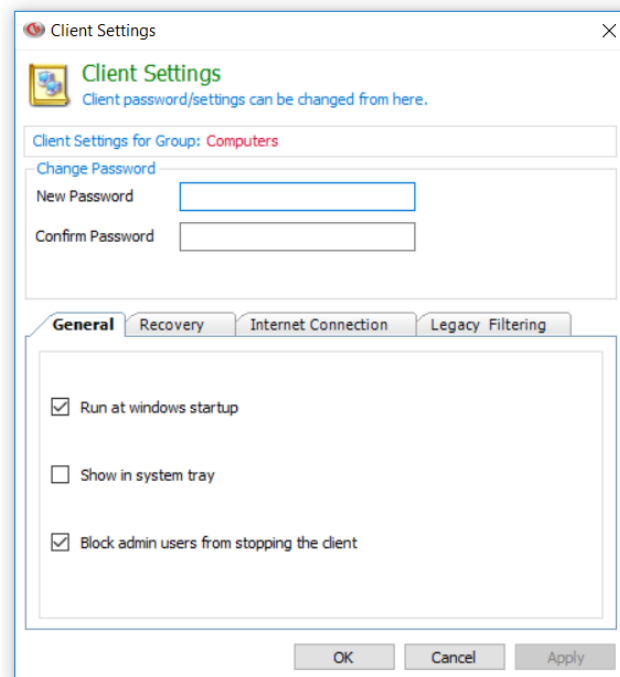
The CurrentWare Client settings can be modified in the CurrentWare Console under **Tools > Client Settings**. You can also right click on a group to find the Client Settings.

### Change Password

Put in the new CurrentWare Client password to replace the existing CurrentWare Client password. You will need to use the CurrentWare client password if you want to change the client settings, such as IP address or computer name of the CurrentWare Server or the port that the client uses to connect to the CurrentWare Server. By default, the case sensitive Client password is **Admin**.

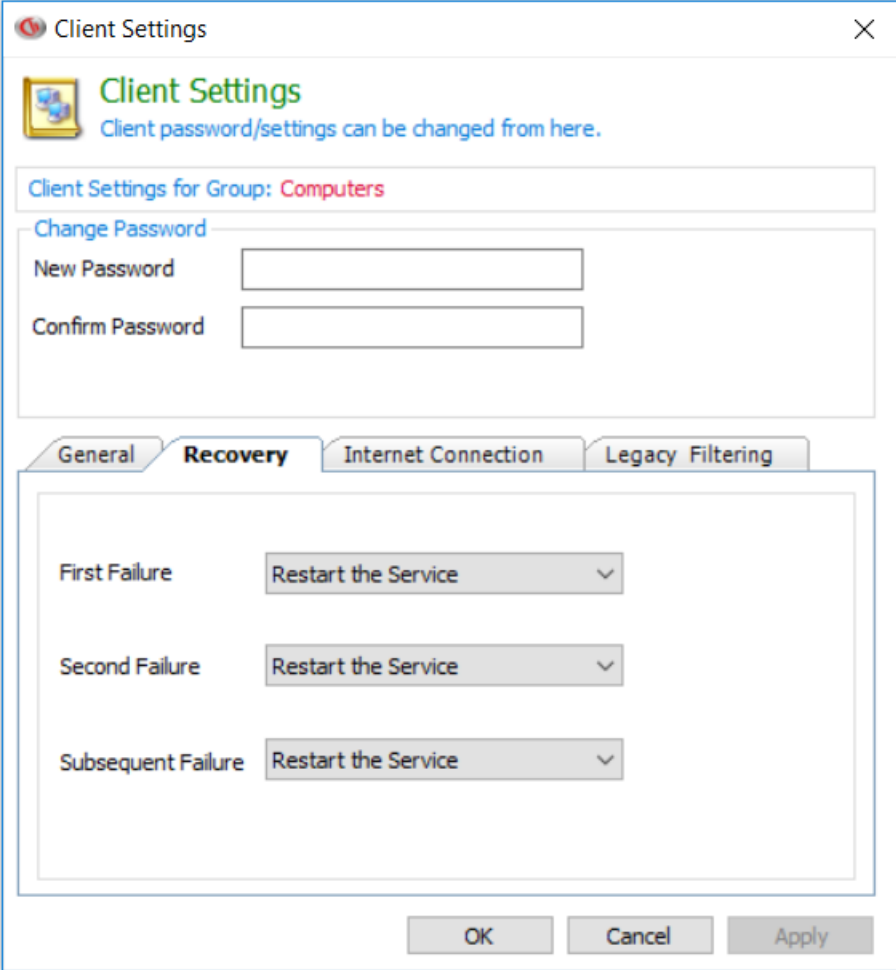
### General

- **Run at Windows Startup:** toggle the option to allow the CurrentWare client service to start every time the workstation boots up.
- **Show in System Tray:** toggle the option to display the CurrentWare icon in the system tray. When this option is enabled, the administrator can double click on the icon, put in the password, to access the CurrentWare Client configuration window.
- **Block admin users from stopping the client:** toggle the option to prevent the users of the workstation to stop the CurrentWare Client service or end the CurrentWare Client process.



## Recovery

- The recovery option is for the property of the CurrentWare Client. By default, the option is set to “Restart the Service”. If the CurrentWare Client service was stopped by Windows or software, the default action would be for the Client to restart itself so it can continue to operate. It is best practice to leave this option as “Restart the Service”.



The screenshot shows the 'Client Settings' dialog box with the 'Recovery' tab selected. The dialog has a title bar with a close button. Below the title bar is a header section with a 'Client Settings' icon and the text 'Client password/settings can be changed from here.' Below this is a section for 'Client Settings for Group: Computers' with a 'Change Password' link and two password input fields. The 'Recovery' tab is active, showing three failure scenarios: 'First Failure', 'Second Failure', and 'Subsequent Failure', each with a dropdown menu set to 'Restart the Service'. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

Client Settings

Client Settings for Group: Computers

Change Password

New Password

Confirm Password

General Recovery Internet Connection Legacy Filtering

First Failure Restart the Service

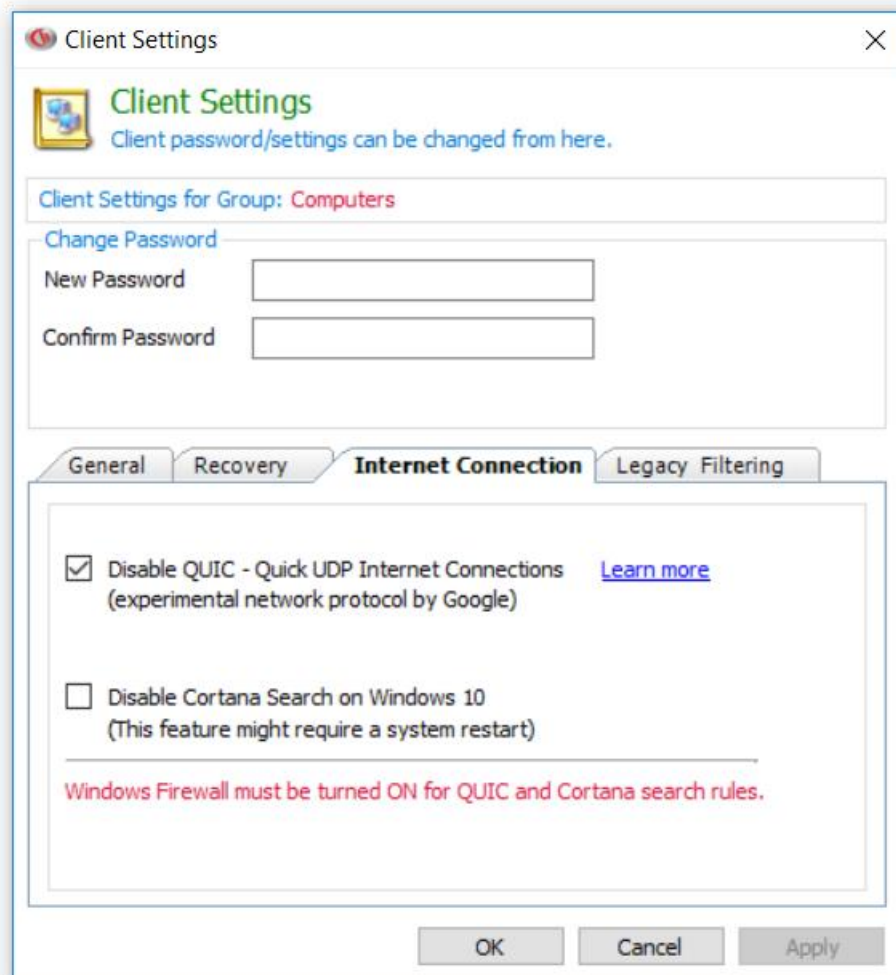
Second Failure Restart the Service

Subsequent Failure Restart the Service

OK Cancel Apply

## Internet Connection

- **Disable QUIC – Quick UDP Internet Connections (experimental network protocol by Google).** BrowseControl controls Internet using the TCP protocol. QUIC uses UDP for Internet traffic on Google Chrome. Since BrowseControl is not filtering the Internet traffic through UDP, QUIC can cause an issue with BrowseControl's filter. This option will disable QUIC on Google Chrome automatically.
- **Disable Cortana Search on Windows 10.** End users can use Windows 10's Cortana search to reach out to the Internet. By enabling this option, it will block the Firewall's outgoing port associated with Cortana and prevent Cortana searches from displaying results from the Internet.





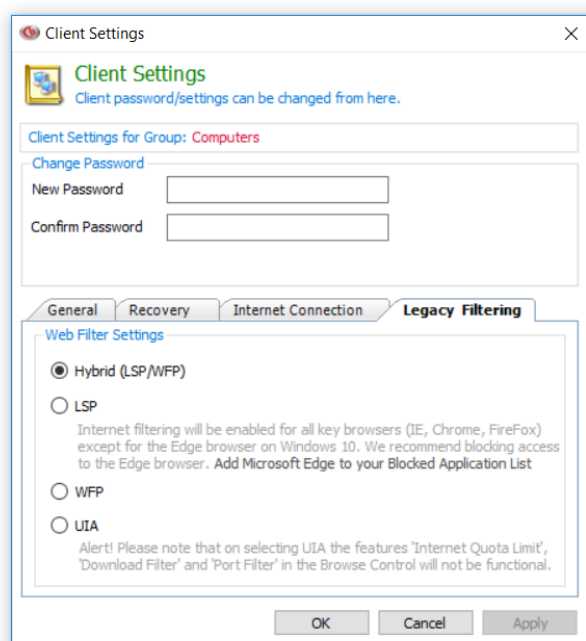
## Legacy Filtering

This setting applies to BrowseControl only.

- **Hybrid (LSP/WFP):** Depending on your client computer's operating system, BrowseControl will use LSP or WFP to filter Internet access.

For Windows 7, 8, 2008 and 2012, BrowseControl will filter internet using LSP. For Windows 10 and 2016, BrowseControl will filter Internet using WFP.

- **HTTPS Settings = Simple:** All web filtering (HTTP/HTTPS) in Hybrid (LSP/WFP).
  - **HTTPS Settings = Advanced:** All web filtering (HTTP/HTTPS) in UIA.
- **LSP:** BrowseControl will filter Internet on the client computers using LSP.
  - **HTTPS Settings = Simple:** All web filtering (HTTP/HTTPS) in WFP.
  - **HTTPS Settings = Advanced:** All web filtering (HTTP/HTTPS) in UIA.
- **WFP:** BrowseControl will filter Internet on the client computers using WFP.
  - **HTTPS Settings = Simple:** All web filtering (HTTP/HTTPS) in WFP.
  - **HTTPS Settings = Advanced:** All web filtering (HTTP/HTTPS) in UIA.
- **UIA:** BrowseControl will filter Internet on the client computers using UIA.
  - **HTTPS Settings = Simple:** automatically switch to Advanced.
  - **HTTPS Settings = Advanced:** All web filtering (HTTP/HTTPS) in UIA.

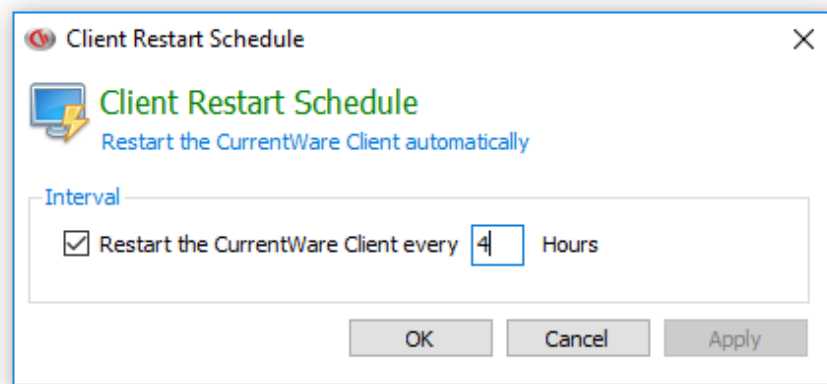


## 2.4 Troubleshooting

The troubleshooting option allows administrator to perform troubleshooting tasks to resolve errors that are related to the CurrentWare Client.

### Client Restart Schedule

Restarting the CurrentWare Client will resolve unexpected issues that can occur on the CurrentWare Client. This option will help the administrator restart the CurrentWare Client automatically during scheduled time.



Use the Client Restart Schedule to automatically restart the CurrentWare Clients.

### Viewing Log files

You can use the CurrentWare Console to remotely connect to a client computer to open the CurrentWare Client log files. The following CurrentWare Client log files are available to view remotely:

- **CurrentWare Client Log**
- **Upload Log**
- **Category Log**
- **Blocked URL Log**
- **Advanced Logs**
- **System Reports > Assets**

## CurrentWare Client Log

The CurrentWare Client log indicates the status of the Client. This log file can help identify connection issues and version conflicts.

## Upload Log

The upload log records the data, tracked by BrowseReporter, which is uploaded to the CurrentWare Server. This log file can help identify issues with BrowseReporter data upload.

## Category Log

The category log records the communication between the CurrentWare Client and the Category Filtering Server used by BrowseControl. If the Category Filtering restriction is not working properly, use this log to identify if the client is connected to the server.

## Blocked URL Log

The blocked URL log will show you the blocked websites that your end users attempted to access. You can use this log to identify additional websites (such as CDN, image server, CSS, etc.) to add to BrowseControl's Allowed list.

## Advanced Logs

Use the CurrentWare advanced log to troubleshoot specific issues that you are having with CurrentWare:

- CWSEmail.log
- CWSAPEmail.log
- CWSBRAAlertEmail.log
- CWUserActivity.log
- Advanced client and port connection logs (CltCommand.log, TSTLog8991.log, TSTLog8992.log)

**NOTE:** Enable advanced logs may cause your system to slow down. After collecting the log files for the technical support team, remember to disable the logging.

## System Reports > Assets

A .csv file containing all of your computer's computer name, IP address, MAC address, Client connection, last connected, last disconnected and user names.

## 2.5 Operators

Operators are used in the CurrentWare Console to assign console permissions to different users. The Operators utility is available on the CurrentWare Console under **Tools > Operators**. There are two types of operators in CurrentWare Console: Administrator and User.

- **Administrator type** has complete control over every computer, group and the solution's functionalities.
- **User type** has limitations defined by the administrator. These limitations include the solution's functionalities and group accesses.

### Password Protect the Console

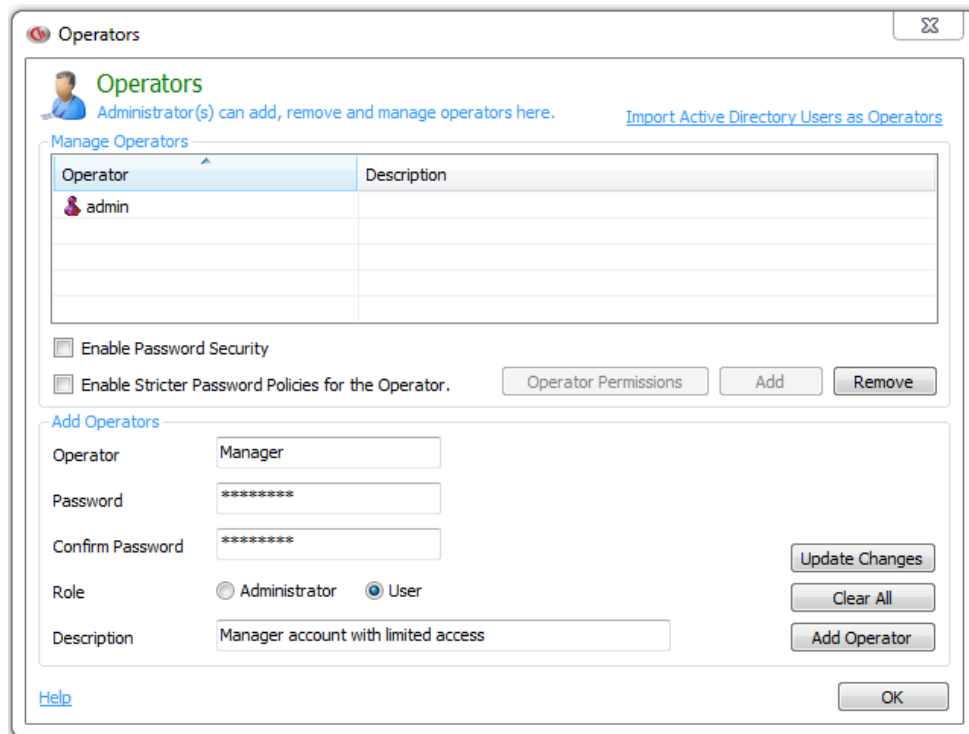
In order to password protect the console, operator accounts need to be created.

#### Creating an Operator:

1. Launch the CurrentWare Console.
2. On the menu select **Tools > Operators**.
3. Click on the **Add** button.
4. Fill in the name, password and description.
5. Select a role for this operator. While the **Administrator** role has access to all the features of CurrentWare, the **User** role only has the limited access to the solution's functionalities.
6. Click **OK** to create a new operator.

#### Enable Password Protected CurrentWare Console

1. Create an operator with the step above.
2. Check the option **Enable Password Security**.
3. Log out of the CurrentWare Console.
4. The next time you log into the CurrentWare Console, you will be prompted for a username and password.



Administrators have unlimited control. Users have limited controls.

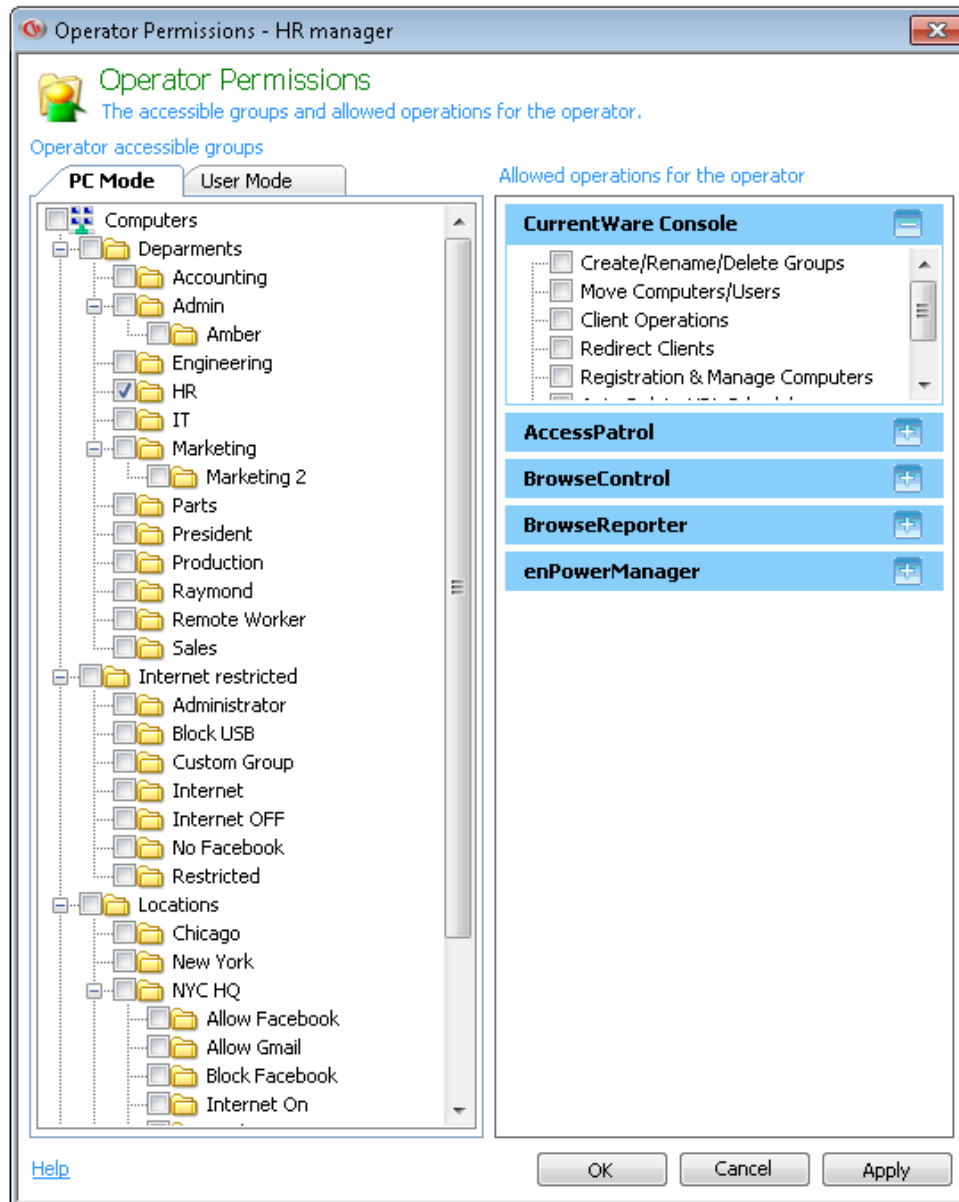
## 2.5.1 Operator Permissions

With operator permissions, you can assign each operator access to specific groups or specific solution operations.

This only applies to an operator with the user role. An operator with administrator role will have access to all groups and all operations.

### Assign Access to Groups

Check the checkbox next to the group that you want the operator to have access to. The operator will only be able to see the computers/users under the checked group.



## Assign Operations

Each solution along with the CurrentWare Console has specific operations you can assign to a user operator:

### CurrentWare Console Operations

- Create/Rename/Delete Groups
- Move Computers/Users
- Client Operations
- Redirect Clients
- Registration & Manage Computers

- Auto Delete URL Scheduler
- Track Assets

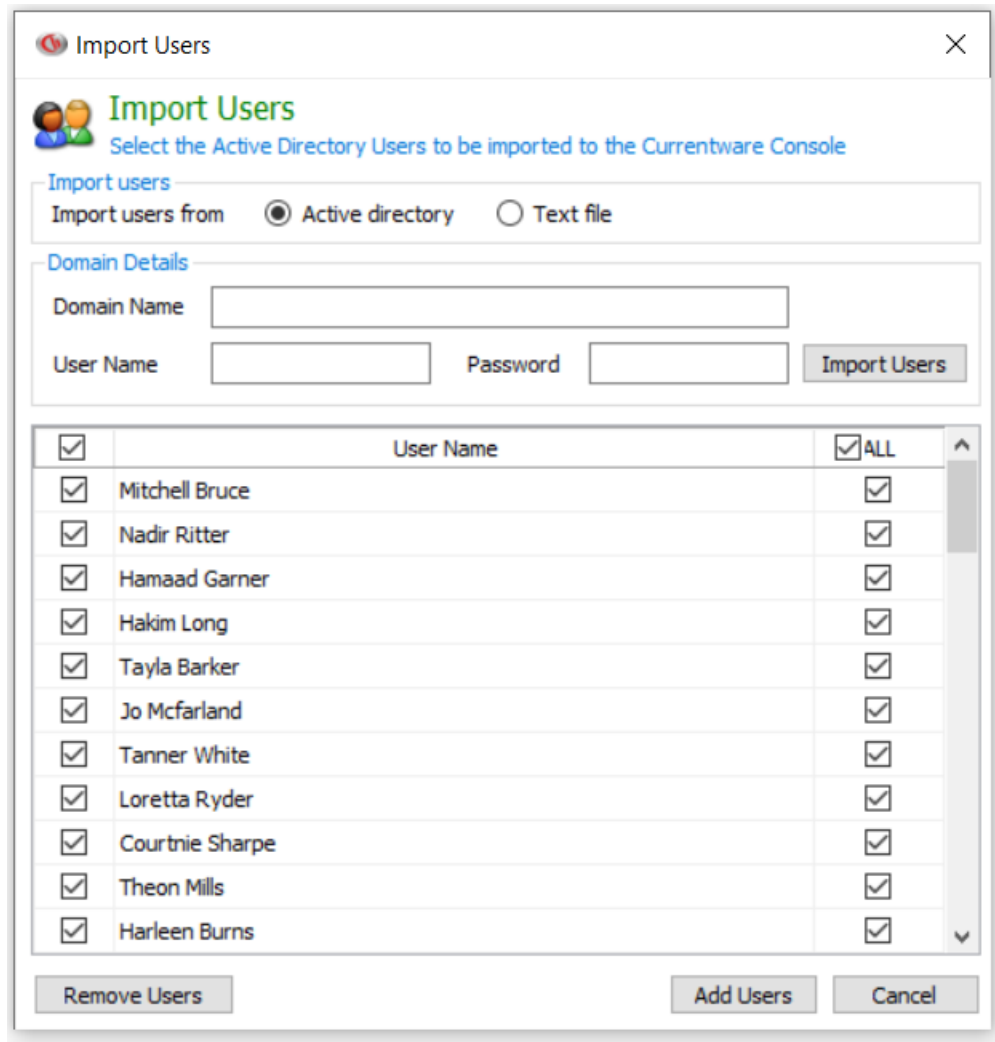
### BrowseControl Operations

- Internet Settings
- On/Off
- Scheduler
- Timer
- Internet Quota Limit
- URL Filter (Add, Remove, Import and Export)
- Category Filtering
- HTTPS Settings
- App Blocker (Add, Remove, Import, Export and Scheduler)
- Display Warning Message
- Port Filter
- Download Filter
- Copy Group Settings
- BrowseControl Client Settings

## 2.6 Import Users

The Import users function will import your existing Windows users from your Active Directory domain into the CurrentWare Console.

1. In order to import users, your CurrentWare Console must be in User Mode. Click on the tab called “User Mode” below the toolbar on the left-hand side to activate User Mode.
2. Click on **Tools > Import Users**
3. Select to Import from **Active Directory** or from a **Text File**
4. Enter the **Domain administrator** credential (Domain name, user name and password) and click on the Import Users button.
5. A list of your Active Directory Users will be populated in the window.
6. Select specific users you want to add to the CurrentWare Console or click on the checkbox **Select All Users**.
7. Click **Add Users** to add the selected users to the Console.



**Import Users**

Select the Active Directory Users to be imported to the Currentware Console

Import users from ☒ Active directory ☐ Text file

Domain Details

Domain Name

User Name  Password

<input checked="" type="checkbox"/>	User Name	<input checked="" type="checkbox"/> ALL
<input checked="" type="checkbox"/>	Mitchell Bruce	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Nadir Ritter	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Hamaad Garner	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Hakim Long	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Tayla Barker	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Jo Mcfarland	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Tanner White	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Loretta Ryder	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Courtne Sharpe	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Theon Mills	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Harleen Burns	<input checked="" type="checkbox"/>

Import Windows Users from Active Directory.

**NOTE:** When you import users from Active Directory to the CurrentWare Console as operators, the operator name will be the same as the username on active directory. However, the passwords cannot be retrieved directly from the Microsoft Active Directory for security purposes.

The new password for each operator is the username in lowercases. For example, if your Active Directory username is John, your CurrentWare operator password will be john.



## 2.7 Database Backup Scheduler

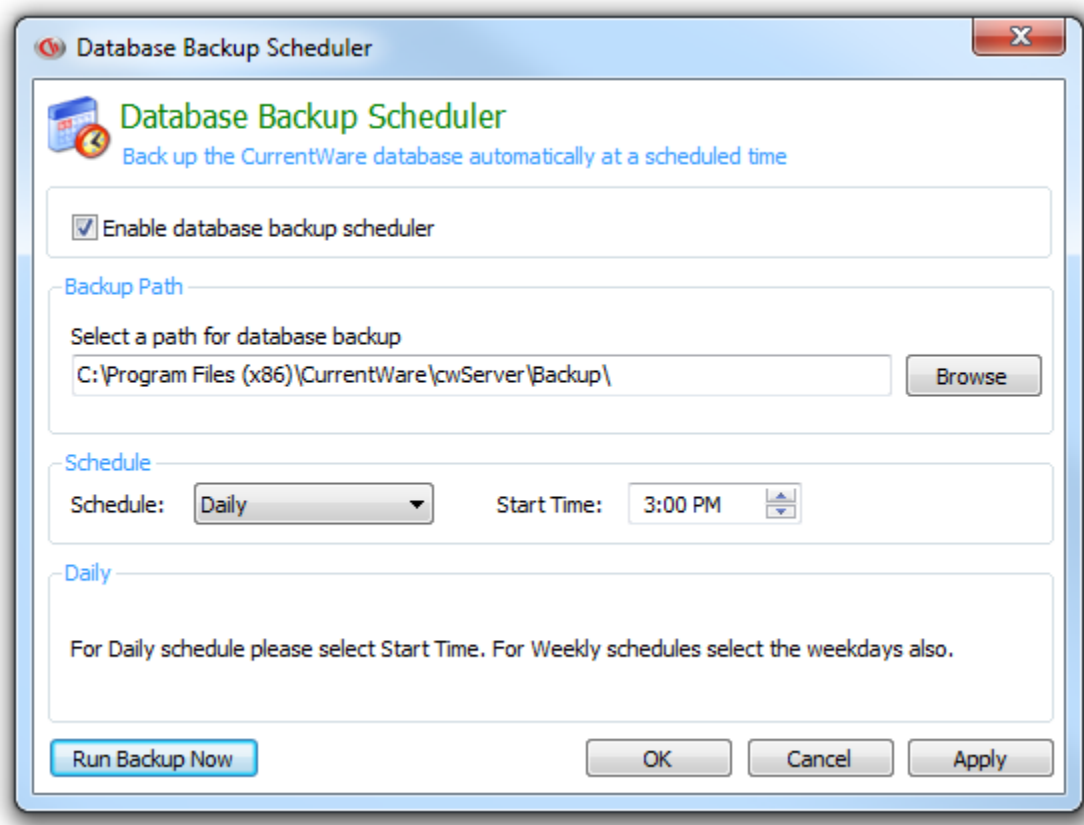
The Database Backup Scheduler automatically backs up the CurrentWare database (CWNPFB.CWD) at a scheduled time.

The database will be backed up into the following default directory:

\Program Files (x86)\CurrentWare\cwServer\Backup

Up to a maximum of 10 of the newest databases will be backed up into the folder.

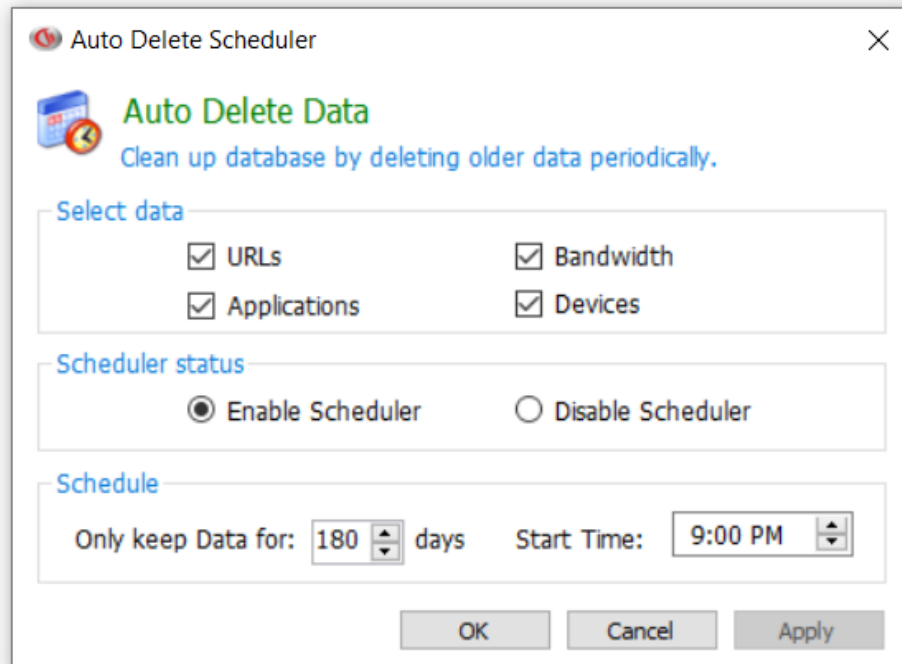
You can perform a one-time back up by clicking on the “Run Backup Now” button.



Automatically back up your database at a scheduled time.

## 2.8 Auto Delete Scheduler

Automatically delete URL, bandwidth, application and device histories from your database. An optimized database will improve the performance of the CurrentWare Console and reduce the time it takes to generate reports.



In this example, data older than 180 days will be deleted automatically every day at 9:00 PM.

**Only Keep Data for:** Select the number of days you want to keep your Internet data. The Auto Delete scheduler will automatically delete any data that are older than the day that you selected.

**Start Time:** The scheduler will be executed at this time. During the data cleanup, the Console may close briefly (depending on your database size, the time it takes for the cleanup will vary). After the cleanup is completed, you can resume using the CurrentWare Console.

The CurrentWare Server must be turned on at the Start Time for the cleanup process to happen.

**Database Compression to reduce file size:** Database compression is a heavy process and during the compression, the cwServer will be down. So, we do not perform compression each time the Auto delete scheduler is triggered. Instead, the compression only runs once every 3 schedules and only if the database is larger than 500 MB.

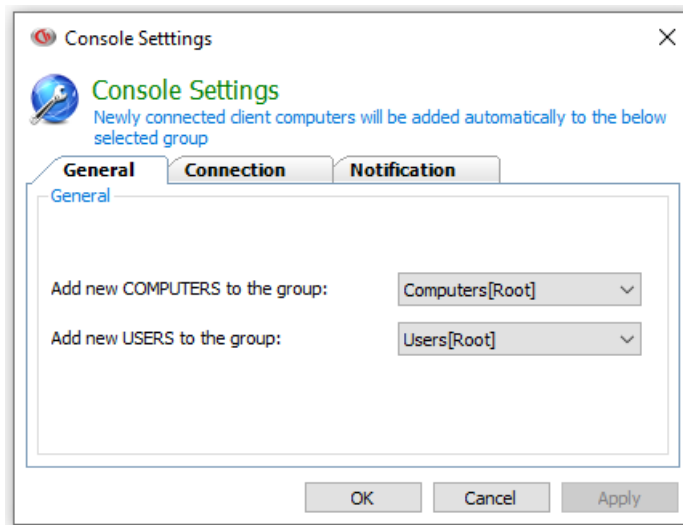
## 2.9 Console Settings

Details of the Console port and newly connected client management are available on the CurrentWare Console under **Tools > Console Settings**.

### General

**Add new Computers to the group:** define the group that a new computer will automatically be assigned to once it connects to the CurrentWare Server for the first time.

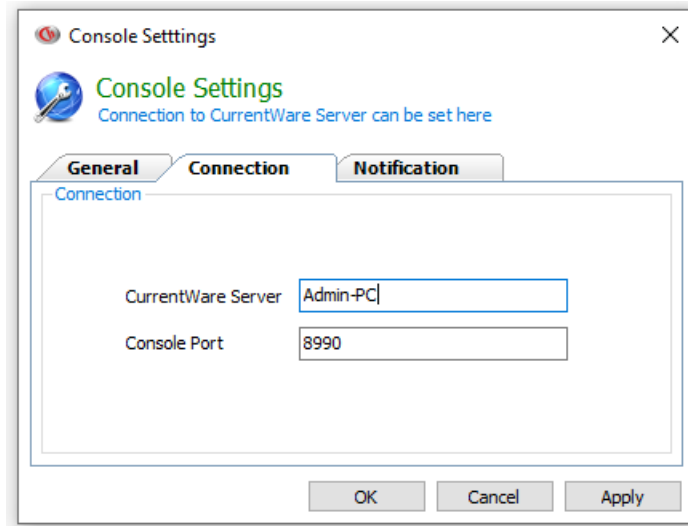
**Add new Users to the group:** define the group that a new user will automatically be assigned to once it is populated to the CurrentWare Server for the first time.



### Connection

**CurrentWare Server:** The computer name or the IP address of the CurrentWare Server that the CurrentWare Console is connected to.

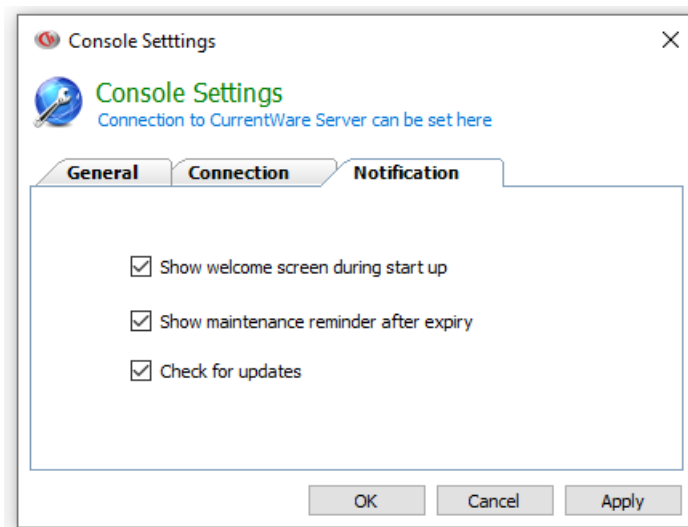
**Console Port:** The port that CurrentWare Console uses to connect to the CurrentWare Server. The default Console port is 8990.



## Notification

Enable/disable the following notifications:

- Show welcome screen during start up
- Show maintenance reminder after expiry
- Check for updates



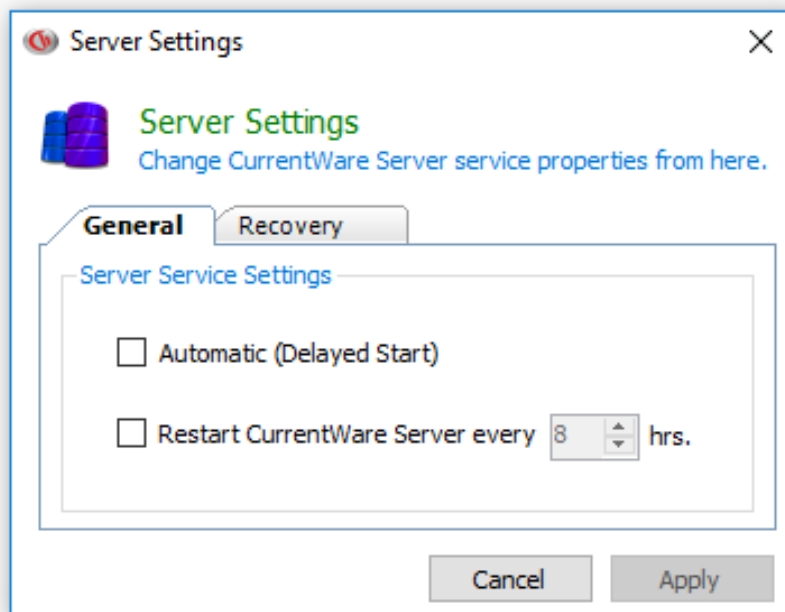
## 2.10 Server Settings

Use the Server Settings to change the CurrentWare Server service start up type and recovery mode.

### Server Service Settings

**Automatic (Delayed Start):** Enable this option if you are having issue with the CurrentWare Server service not starting during boot up.

**Restart CurrentWare Server Every 8 hours:** Enable this option to reset any CurrentWare Server service issues every 8 hours.



### Recovery

The CurrentWare Server service is set to “Restart the Service” if it runs into any failures. This will prevent the CurrentWare Server service from stopping unexpectedly.

## 2.11 Log Out

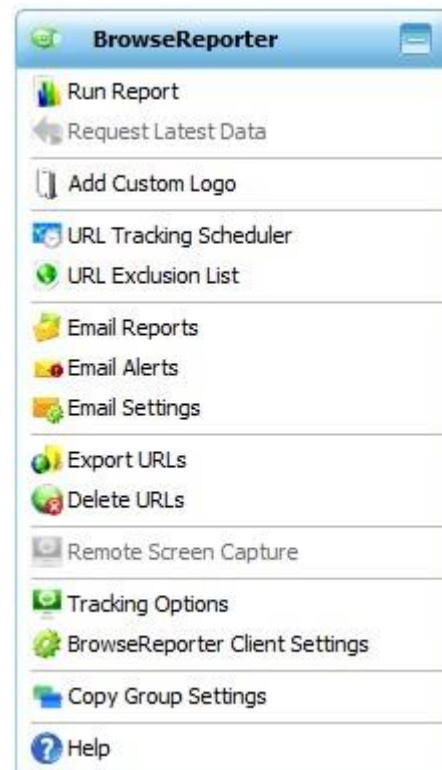
Log Out can be used to re-log into the Console with a different user name and password. This feature can be found under the menu **File → Logout**.

## 3.0 Overview of BrowseReporter Functions

BrowseReporter is an Internet tracking tool that allows an administrator to review the Internet activities of the network users.

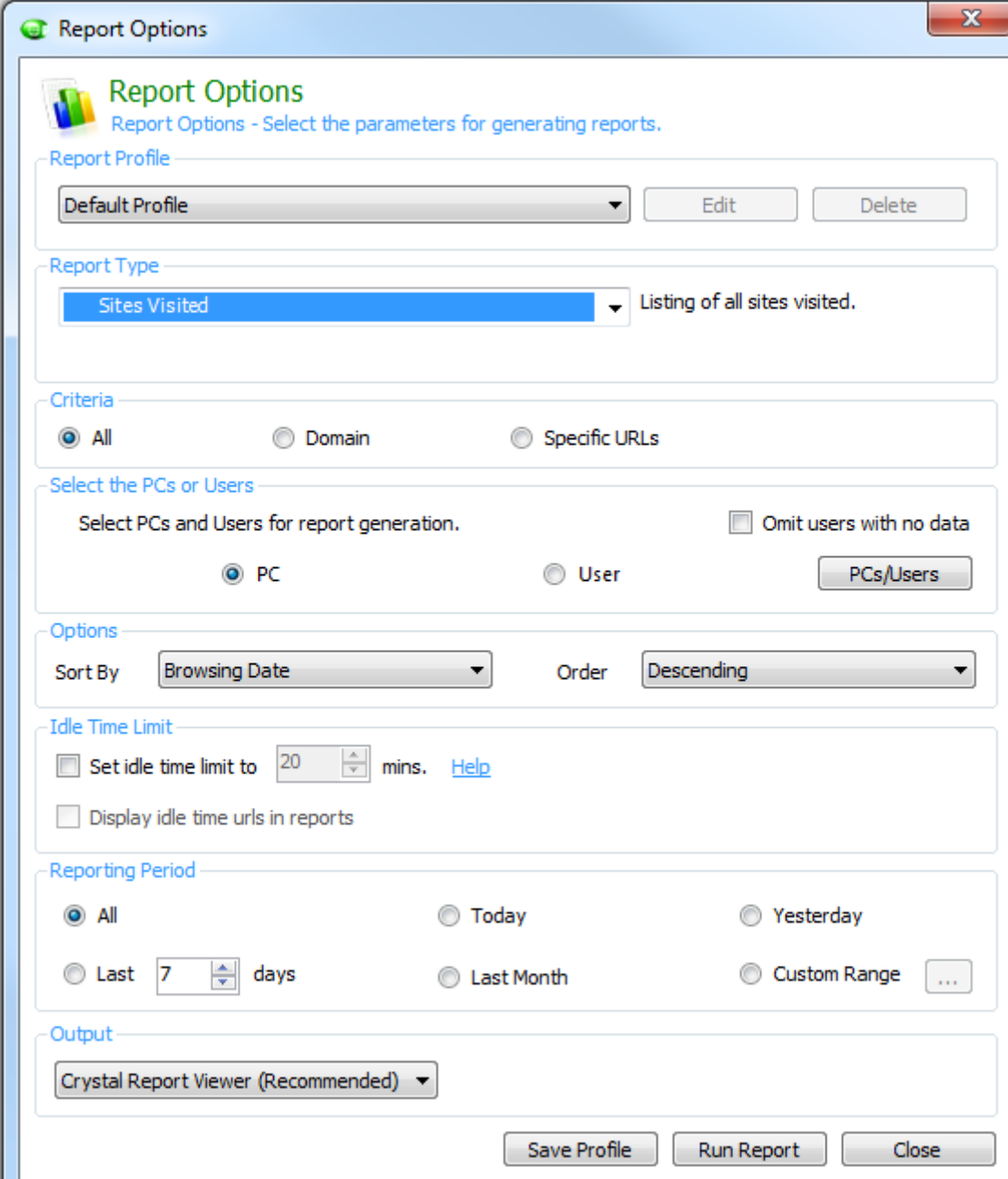
An overview of the BrowseReporter functions includes:

- **Run Report**
- **Request Latest Data**
- **Add Custom Logo**
- **URL Tracking Scheduler**
- **Exclusion List**
- **Email Reports**
- **Email Alerts**
- **Email Settings**
- **Export URLs**
- **Delete URLs**
- **Remote Screen Capture**
- **Tracking Option**
- **BrowseReporter Client Settings**
- **Copy Group Settings**



## 4.0 Run Report

The reports are the core components of BrowseReporter. The administrator can generate reports to view the Internet activities of his/her users.



The screenshot shows the 'Report Options' dialog box. It has a title bar with a close button (X). The main area is divided into several sections:

- Report Options**: A subtitle 'Report Options - Select the parameters for generating reports.' with a small icon of a bar chart.
- Report Profile**: A dropdown menu showing 'Default Profile', with 'Edit' and 'Delete' buttons.
- Report Type**: A dropdown menu showing 'Sites Visited', with a description 'Listing of all sites visited.'
- Criteria**: Three radio buttons: 'All' (selected), 'Domain', and 'Specific URLs'.
- Select the PCs or Users**: A section with the text 'Select PCs and Users for report generation.' and a checkbox 'Omit users with no data'. Below are radio buttons for 'PC' (selected) and 'User', and a 'PCs/Users' button.
- Options**: 'Sort By' dropdown set to 'Browsing Date', and 'Order' dropdown set to 'Descending'.
- Idle Time Limit**: A checkbox 'Set idle time limit to' followed by a spinner set to '20' and the text 'mins.' with a 'Help' link. Below is a checkbox 'Display idle time urls in reports'.
- Reporting Period**: Radio buttons for 'All' (selected), 'Today', 'Yesterday', 'Last' (with a spinner set to '7' and the text 'days'), 'Last Month', and 'Custom Range' (with an ellipsis button).
- Output**: A dropdown menu showing 'Crystal Report Viewer (Recommended)'.

At the bottom are three buttons: 'Save Profile', 'Run Report', and 'Close'.

## 4.1 Report Profile

Administrators can create different report profiles to use as shortcuts to reports and settings that they commonly use in BrowseReporter. A report profile will store the selection for report type, the computers or users selected options, idle time option and the reporting period.

### How to Create a Report Profile

1. Select **Run Report** on the BrowseReporter menu located on the right-hand side of the CurrentWare console.
2. Select the **Report** type.
3. Select the **computers or users** you want to generate for your report profile.
4. Select the **sorting** and ordering of your report.
5. Set an Idle Time Limit (optional).
6. Choose a reporting period.
7. Click on **Save Profile**.
8. Give a name to the report profile and click OK.

The profile is now saved and can be accessed for future report generation. To retrieve the report profile, simply select the report profile from the **Report Profile** list the next time you run a report.

## 4.2 Report Type

There are many different types of reports within BrowseReporter ranging from a detailed report that includes all the websites that the users visited (Sites Visited) to a graph that shows the top 10 domains that your network users are visiting. This is a list of all the Reports in BrowseReporter:

### Websites Visited

- **Sites Visited:** This report contains every single URL that your users have visited. You can choose to show domains only or specific URLs only.
- **Top (N) Domains by Browsing Time:** Summary view of a list of top domains that the computer or user has spent the most time on. (N) is a number that you can define in the Report options. There is an option to display a horizontal graph showing the top 10 domains.
- **Top (N) Domains by Hits:** Summary of hits by popular domains visited on a per computer or user basis. (N) is a number that you can define in the Report options.
- **Total Browsing Time:** Accumulated time spent on the Internet for each computer or user.
- **Keywords Searched by Hits:** Tracking of search engine keywords searched by your employees by the number of hits.



- **Keywords Searched by Time:** Tracking of search engine keywords and the date/time searched by user.
- **Employee Productivity Report:** Assign categories and websites that are productive or unproductive to your company in order to report the overall efficiency of your employees.
- **Graph – Hourly Active Browsing Time:** A graphical display of the accumulated Internet browsing time for users for each hour of the day.
- **Graph – Weekly Active Browsing Time:** A graph that shows the accumulated Internet browsing time for users for each day of the week.
- **Graph – Top 10 PCs by Active Browsing Time:** A graph of the top 10 computers on your network that spent the most time on the Internet.
- **Graph – Top 10 Users by Active Browsing Time:** A graph of the top 10 users on your network that spent the most time on the Internet.
- **Graph – Top 10 Domains by Active Browsing Time:** A graph of the top 10 domains on your network that your computers or users visited most frequently by hits.

### Categories Visited

- **URL Categories Visited:** Detail of domains visited and the category that they belong to with the duration of each visit on a per computer or user basis
- **Top N Categories by Browsing Time:** Summary view of a list of top categories that the computer or user has spent the most time on.
- **Category Drill Down:** Detailed view of each category and their top users.
- **Social Media Activity:** Display activities exclusively from the social media category.

### Bandwidth Usage

- **Bandwidth Usage by URL:** Bandwidth sent or received by the computers or users with details of each URL.
- **Daily Bandwidth Usage:** Accumulated daily bandwidth consumption for the time period.
- **Total Bandwidth Usage by PC/User:** Accumulated bandwidth consumption of all the selected computers and users.

### Application Usage

- **Top N Application Usage:** Summary of time spent for applications on a per computer or user basis. (N) is a number that you can define in the Report options.

- **Specific Application Usage:** Display time spent report containing only the applications that you have specified.
- **Application Usage by Hour (with Graph):** A graph of the top applications time spent for each computer or user. Includes a tabular summary of time spent on each application grouped into hourly basis. (N) is a number that you can define in the Report options.

## 4.3 Report Options

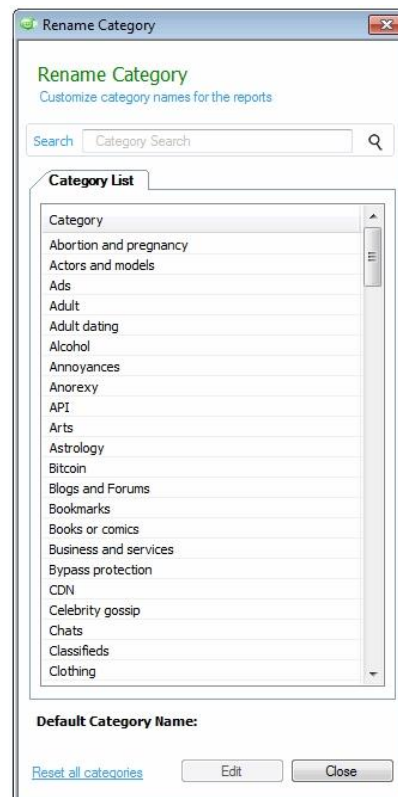
The BrowseReporter Report Options utility allows you to customize the report on the basis of specific criteria.

### 4.3.1 Select Mode

Select the computers or users to generate a BrowseReporter report on. You can select an individual computer, multiple computers and a group of computers. The same selection applies for the users.

### 4.3.2 Rename Category

This option is only available for category reports. Rename the default category names to a new name that will appear on the category reports.



### 4.3.3 Options

The BrowseReporter report options allow you to select the sorting and ordering of the report. You can sort by URL, Browsing Date, Browsing Time, Active Time, Domains, Hits, Date, Bandwidth Sent and Bandwidth Received.

Reports can be sorted by ascending or descending order.

### 4.3.4 Idle Time Limit

The Idle time limit filters out web sessions that are perceived to be inactive or idle from the final report. This function is optional and the time limit value is defined by the administrator. The URLs with a web session period longer than the idle time limit will not be displayed in the reports.

#### Set Idle Time Limit

When enabled, the BrowseReporter will look for all browsing sessions that are longer than the idle time limit value and exclude it from the report.

#### Display Idle Time URLs in Reports

When enabled along with the “Set idle time limit” option, the BrowseReporter will look for all browsing sessions that are longer than the idle time limit value and add a red asterisk indicator \* before the entry in the report.

### 4.3.5 Reporting Period

Select the time and date period for the report. The reporting period options are as follow:

- All
- Today
- Yesterday
- Last 7 Days (can be customized to any days)
- Last Month
- Custom Range (by Date and Time)

### 4.3.6 Output

You can choose to output some reports in .CSV format for easy access on your spreadsheet program such as Microsoft Excel.

The reports that are compatible with this option are:

- Sites Visited
- Keyword Searched by Time
- URL Categories Visited

## 5.0 Request Latest Data

The Internet data tracked by BrowseReporter is initially stored locally on the CurrentWare Client computer. This data must be uploaded to the CurrentWare Server before the administrator can generate a report.

The CurrentWare Server automatically requests the latest data from the CurrentWare Client workstation when the CurrentWare Client is connected.

The administrator can manually request the data from the client computer by clicking on the Request Latest Data button.

### How to Request the Latest Data From a Computer

1. Select the desired computer.
2. Click on **Request Latest Data** under the BrowseReporter tab.
3. Select the computer that you have selected in step 1.
4. A window will appear with the upload progress.
5. Click OK when the upload is finished.

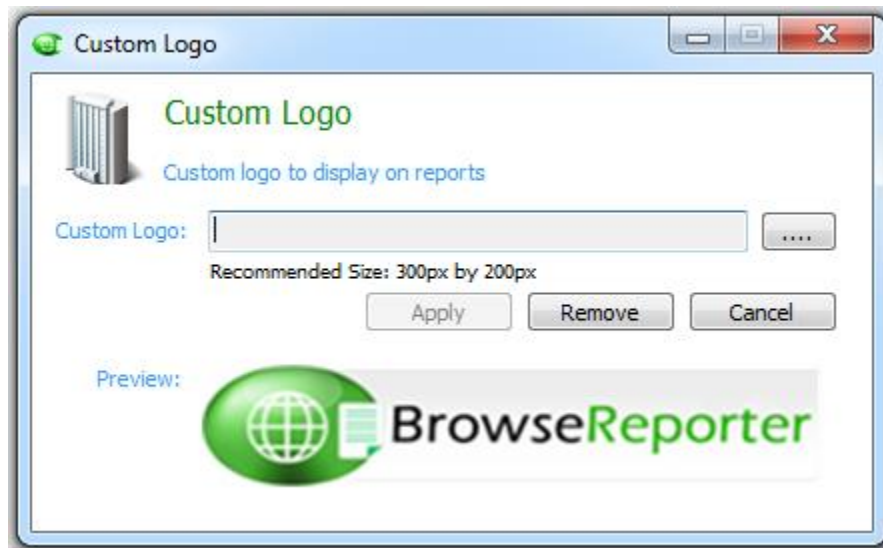
### How to Manually Upload Data and Disable Auto Upload

1. From the BrowseReporter menu, select Tracking Options.
2. Under the Upload Settings option, select Manual Upload.
3. Click Apply.
4. Select a folder that you want to manually upload data.
5. Click Request Latest Data.
6. Select a list of computers that you want to manually upload data.
7. Click on the >> button to bring the computer to the Request Latest Data List.
8. Click on Request Data to perform the upload.
9. You will see a window displaying the Upload Status.

## 6.0 Add Custom Logo

Add a custom logo to your BrowseReporter reports. The custom logo will appear on the header of all of your reports.

For the best resolution, we recommend using a logo that is 3:2 ratio and ideally 300px by 200px.



## 7.0 URL Tracking Scheduler

Collecting URL information at all times may be unnecessary. For example, managers may only be interested to track browsing activity during business hours.

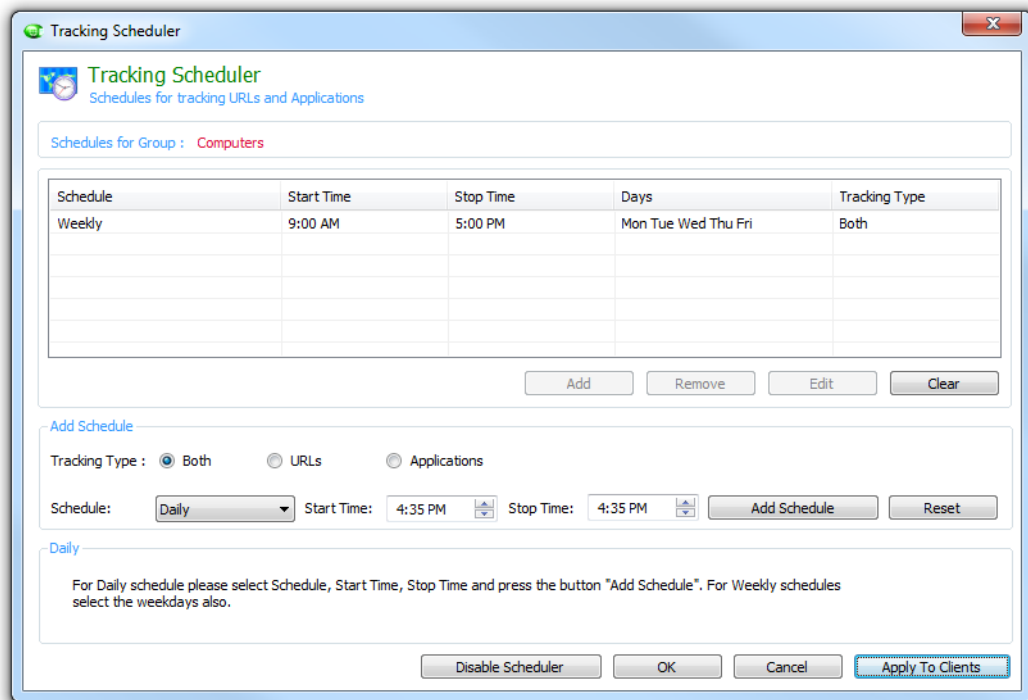
Through the URL Tracking Scheduler, you can schedule the date and time ranges for collecting the Internet browsing activity. Outside of these schedules, no browsing data will be collected. This also helps to maintain the database size. Below is an example of how to use the URL Tracking Scheduler.

**Scenario:** Track URLs only during work hours.

**Predefined work hours:** 9:00 AM to 5:00 PM. BrowseReporter will track Internet activities only during the work hours.

1. Launch the URL Tacking Scheduler by selecting **URL Tracking Scheduler** under the BrowseReporter tab on the right-hand side of the CurrentWare Console.
2. Click on the **Add** button.
3. Select Daily.

4. Set the start time as 9:00 AM and the stop time as 5:00 PM.
5. Click on **Add Schedule**.
6. Click on **Enable Scheduler**.
7. Click on Apply.
8. BrowseReporter will now only track the Internet activities of the computers or users in this group during the scheduled time.

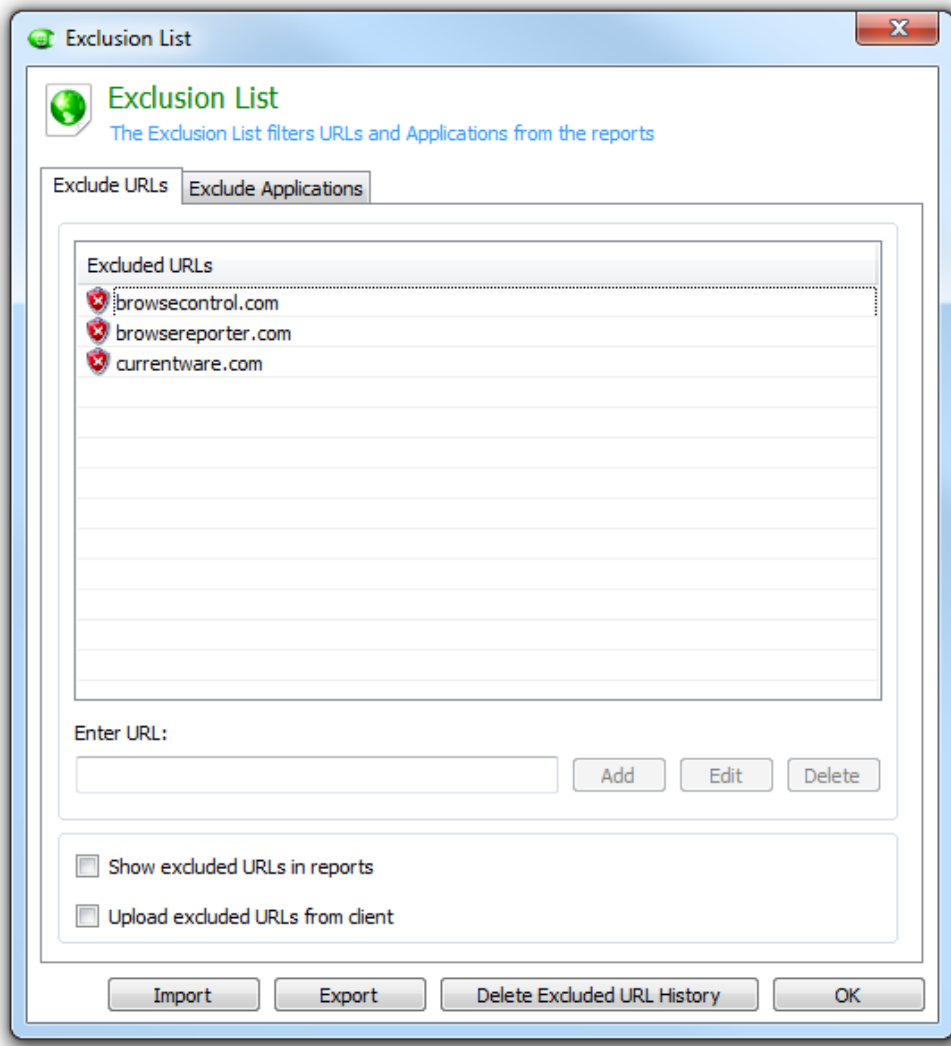


The URL Tracking Scheduler will only track Internet activity during the specified time range.

## 8.0 Exclusion List

When monitoring the browsing activity of users, it may be necessary to purge the tracking of authorized URLs and applications. Adding “authorized” URLs and applications to the Exclusion List will filter them out from the reports.

To access the Exclusion List, under the BrowseReporter tab on the right-hand side of the CurrentWare Console, click on Exclusion List.



### Show Excluded URLs/Applications in Reports:

By enabling this checkbox, all URLs and applications defined under the exclusion list will be listed in the reports.

### Upload Excluded URLs/Applications from client:

When this option is disabled, URLs and applications under the Excluded List will not be uploaded from the client database to the central database. This option will permanently erase the excluded URLs and applications on the client's local database before any data is uploaded to the server.

### Delete Excluded URL/Application History

When you click on this button, BrowseReporter will delete all the excluded URLs and applications from the CurrentWare database.

## Import and Export

A copy of the excluded URL and application list can be saved by exporting it to a text file. You can also import a text file that contains a list of URLs and applications you want to exclude into the Excluded List.

In the text file, each entry must be separated by a line break.

## 9.0 Email Reports

Through the Email Reports feature, the BrowseReporter reports can automatically be generated and emailed to the administrator periodically. This eliminates having to rely on the manual process of creating reports.


To access Email Reports, under the BrowseReporter tab, click on **Email Reports**.

### How to Create a Schedule for Email Reports:

**NOTE:** You must have your email settings configured and a report profile created before creating an email report schedule.

1. Under the BrowseReporter tab on the right-hand side of the console, select **Email Reports**.
2. Click on the **Create Schedule** button.
3. Define the **email address** of the recipient of the reports.
4. Select a **Report profile**. A report profile is created in Run Report.
5. Define the **Schedule type (daily, weekly or monthly)** of the email report.
6. Define the **Time** of the email delivery.
7. The report will be sent in PDF format.




**Email Reports**  
 Email Reports - To create report profile

Assign schedule(s) for Emailing reports
 

Email Address	Report Profile	Format	Time	Days
tech@company.com	Bandwidth Usage Monthly...	PDF	10:45 AM	Sat
CEO@company.com	Weekly Sites Visited Report	PDF	5:00 PM	Fri
User@company.com	Daily Summary	PDF	6:00 PM	
Manager@company.com	Application Usage - Devel...	PDF	6:00 PM	Fri

Option
 

Create Schedule
 Delete
 Edit

Assign schedule(s) for Emailing reports
 

Email reports to

Report profile
 

-----Select Profile-----
 [Help](#)

 Report format
 

PDF

Schedule
 

Daily

 Time
 

10:45 AM

Add Schedule
 Clear

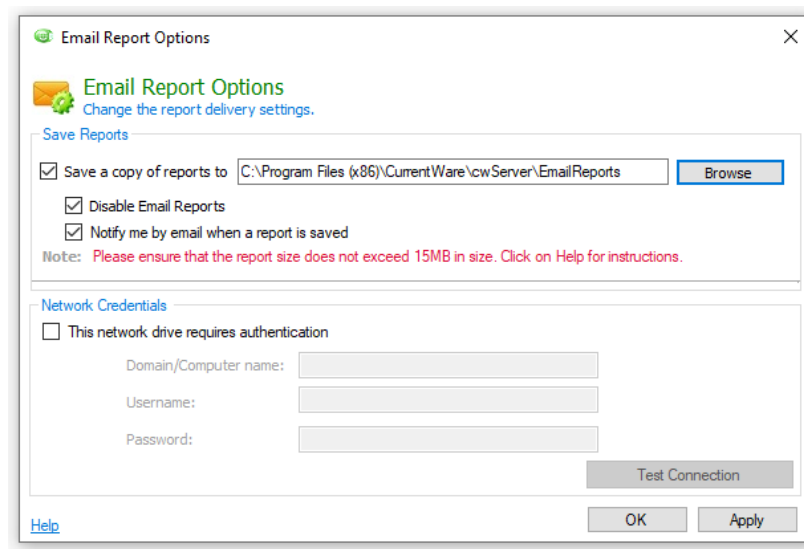
To Email Reports on a regular basis, create a schedule, include the recipient(s) Email address(s), select a Report Profile and the time to send the Email.

OK
 Cancel
 Apply

## 9.0.1 Email Report Options

This option will allow you to save a copy of the report onto your computer during the scheduled email report delivery.

If you check the “disable email reports” option, it will save a copy of the report at the scheduled time and it won’t send out an email. When this option is checked, you don’t have to enter a recipient email address.

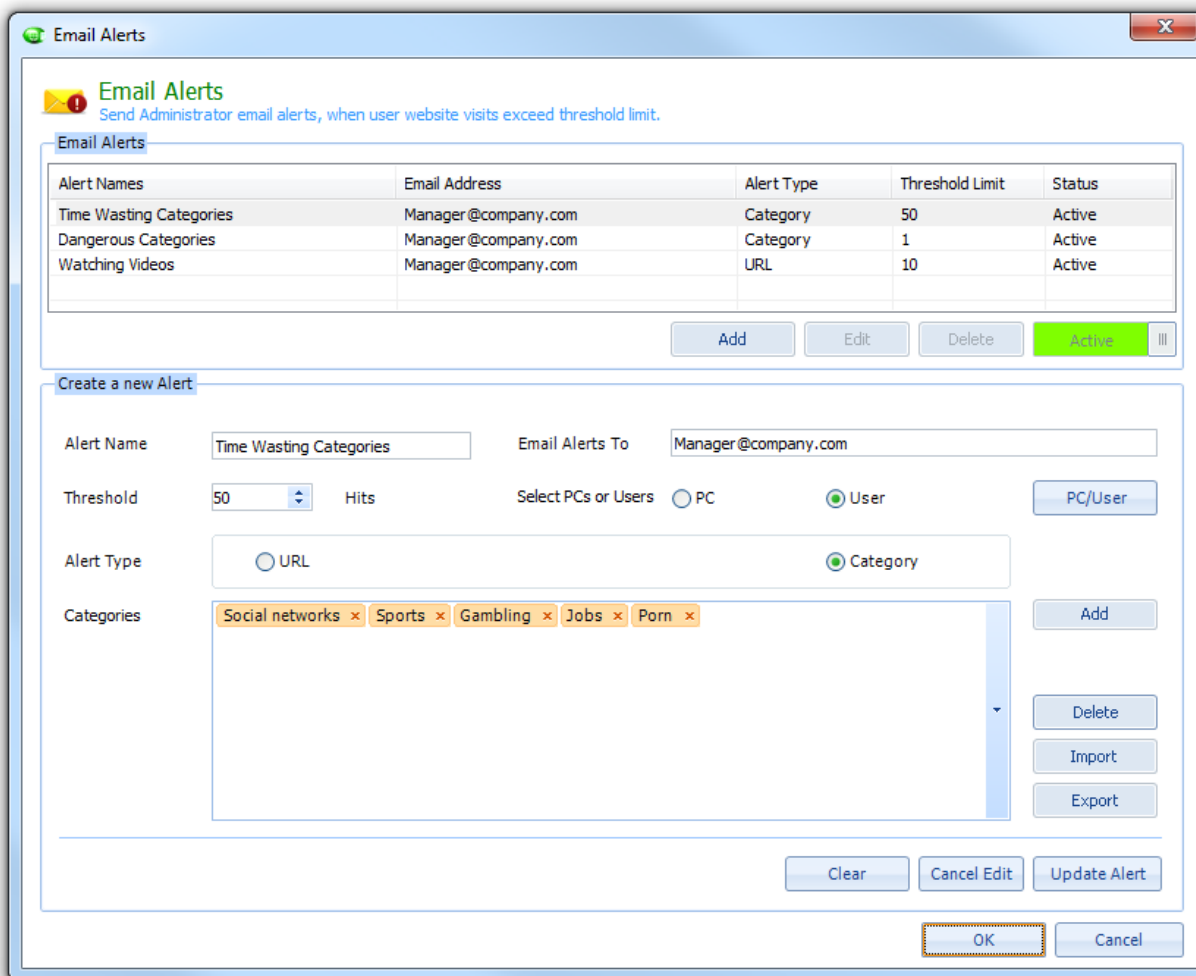


## 9.1 Email Alerts

Setup an email notification alert to be notified of when a user breaches any of the defined settings.

This real time alert warns of potential trouble as it is happening.

A message is immediately triggered to administrators to help them respond immediately to excessive web abuse on valuable company time. Alert notification contains specifics about website infringements, allowing the administrator to immediately identify the user or client machine.



Alert Names	Email Address	Alert Type	Threshold Limit	Status
Time Wasting Categories	Manager@company.com	Category	50	Active
Dangerous Categories	Manager@company.com	Category	1	Active
Watching Videos	Manager@company.com	URL	10	Active

**Create a new Alert**

Alert Name:  Email Alerts To:

Threshold:  Hits:  Select PCs or Users: ☐ PC ☒ User

Alert Type: ☐ URL ☒ Category

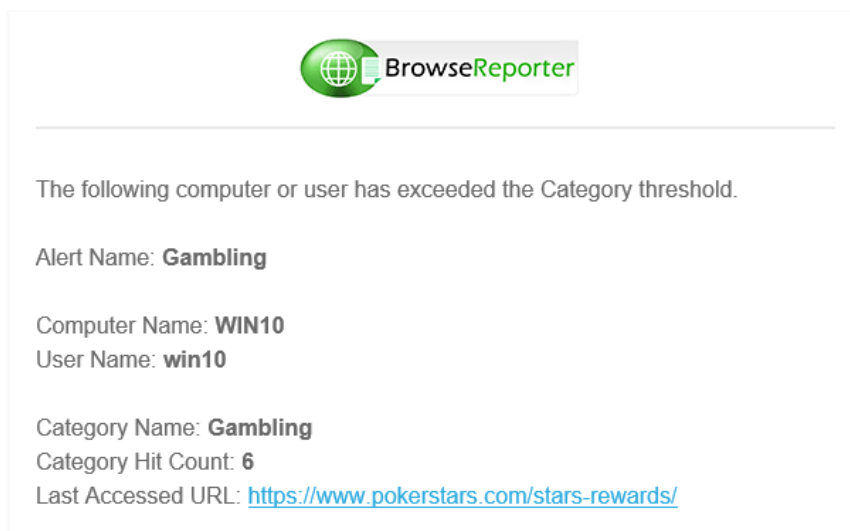
Categories:

## How to create an Email Alert:

**NOTE:** You must have your email settings configured before creating an email alert.

1. Under the BrowseReporter tab on the right-hand side of the console, select **Email Alerts**.
2. Click on the **Create Alert** button.
3. Put in the **Alert Name** and an **email address** of the recipient of the reports.
4. Define a **Threshold**.
5. Choose the alert type that you want to monitor – **URL** or **Category**.
6. Select the **PCs** or **Users** that you want to monitor.
7. For URL alert, an email is sent out for each URL that has reached the threshold.
8. For Category alert, an email is sent out for each category that has reached the threshold.

An example of the email alert received by the recipient:

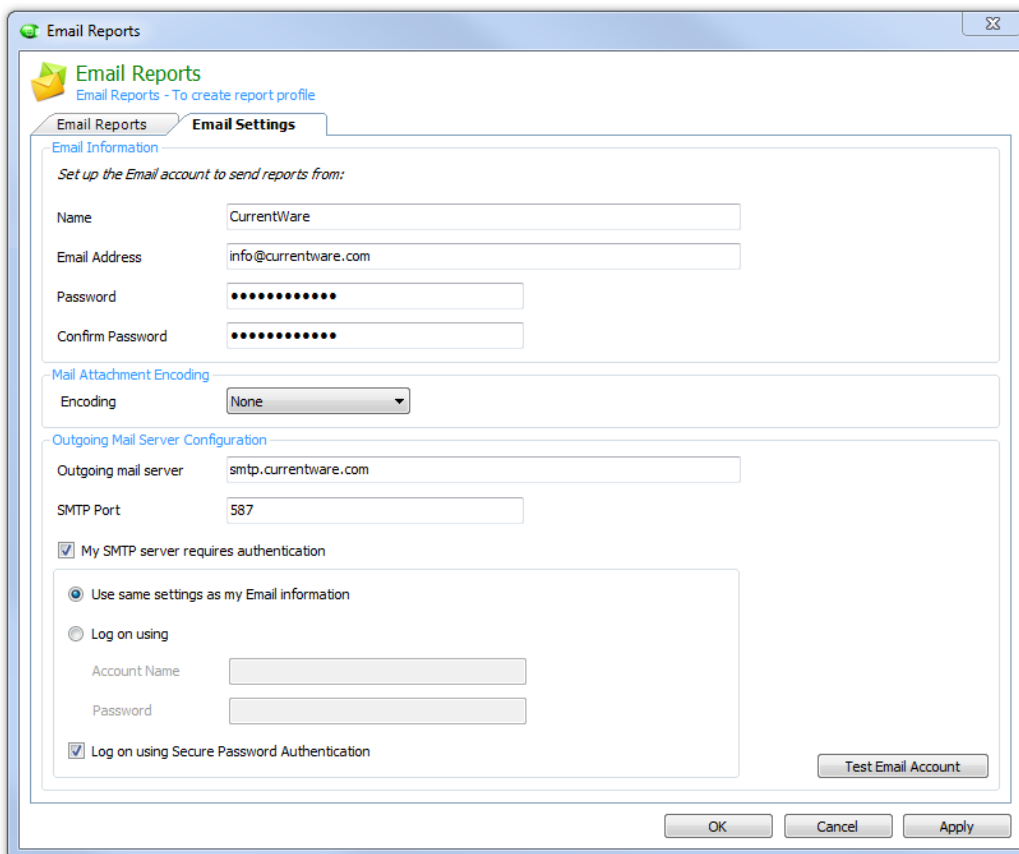


## 9.2 Email Settings

Under the Email Settings tab, enter the email configuration that is required to successfully send the reports to the administrator.

### How to Configure Your Email Settings

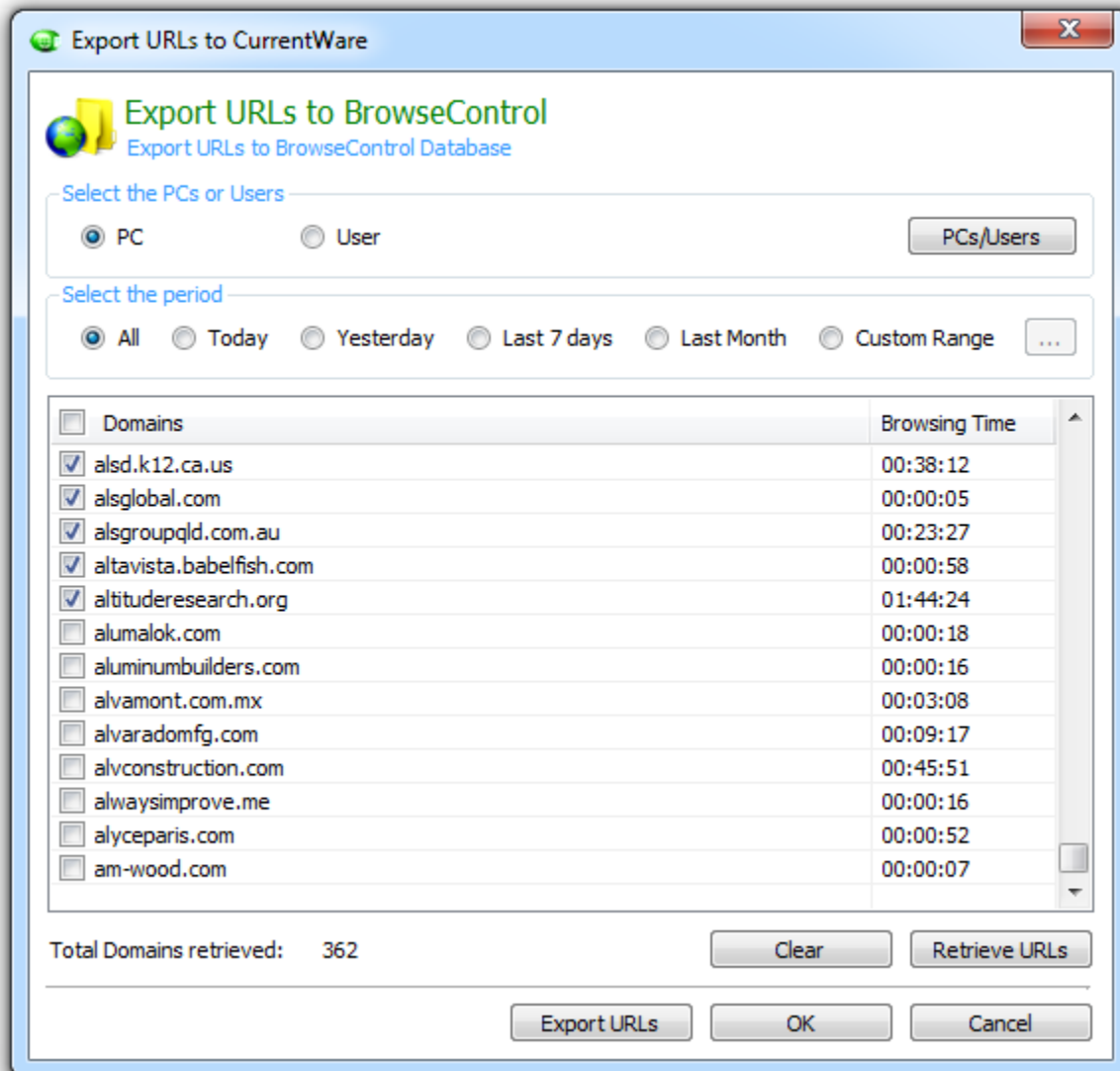
1. Enter the appropriate email Information, including the **name**, **email address** and the **password** for your email address.
2. Define the **outgoing mail server** that your email account uses to send email. The default SMTP port that BrowseReporter uses to send email is port 25.
3. Enable **mail server authentication** if your email server requires the authentication.
4. You can also use web email services, such as Gmail/ Hotmail/ Yahoo mail, to generate email notifications. These web email services usually require mail server authentication.
5. To test the validity of the email account information, click on the **Test Email Account** button to ensure that the reports will be emailed successfully.
6. Click on the Apply button.



## 10.0 Export URLs

The **Export URLs** feature allows the administrator to export a list of domains from the BrowseReporter reports directly to the BrowseControl URL filter list.

BrowseControl is a separate CurrentWare solution that controls the Internet access of your users. By integrating the URLs from BrowseReporter, administrators will be able to use the tracked URLs to control the Internet access of the users.



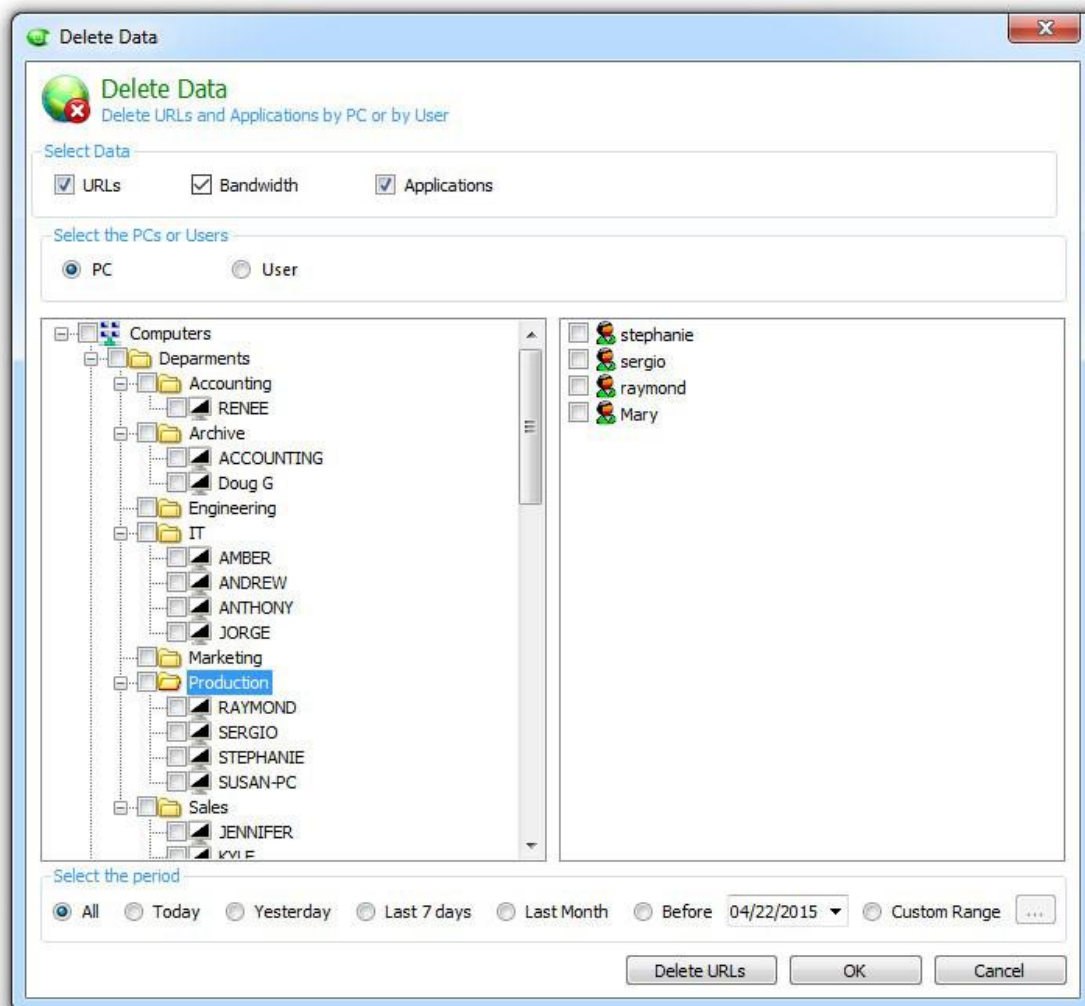
Export the URL directly to the BrowseControl URL filter.

## 11.0 Delete Data

The administrator can delete specific URLs and application histories from the BrowseReporter database.

To Delete data from the BrowseReporter database:

1. From the BrowseReporter tab, click on Delete Data.
2. Select the computers or users that you want to delete the data from.
3. Specify the time period to delete the data from.



Select the data that you want to delete from BrowseReporter.

## 12.0 Remote Screen Capture

Track your user's activity by capturing screenshots of their computers. Identify users who are spending excessive amounts of company/school time on unauthorized sites, chats, games etc.

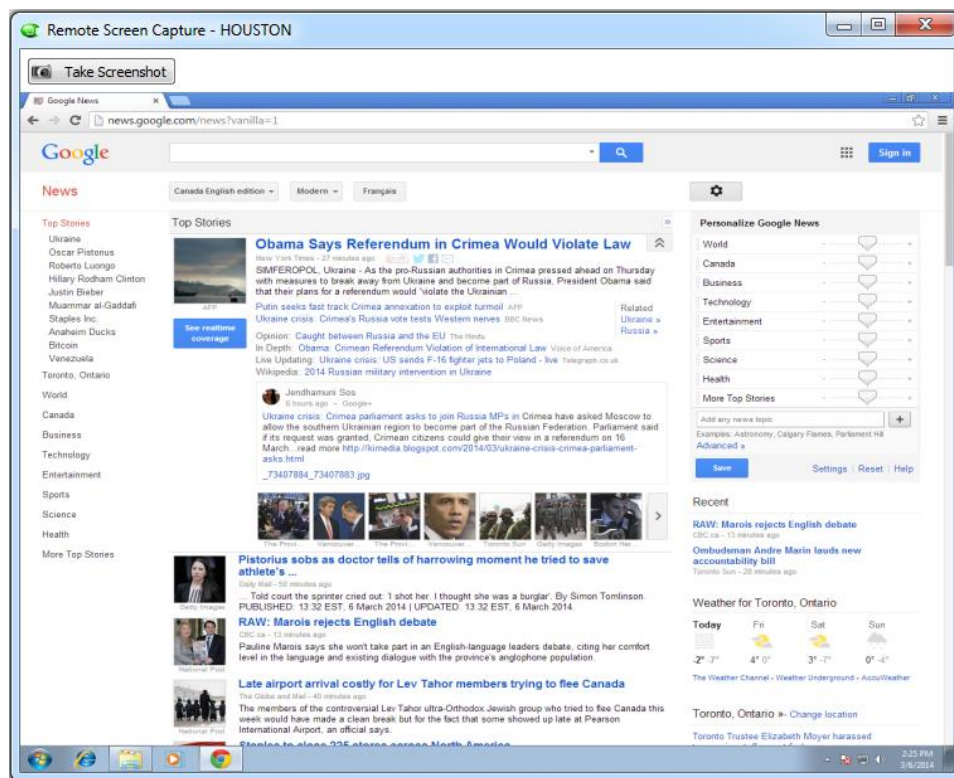
To take a screenshot for future references, simply click on the "Take Screenshot" button and type in the file name and file directory you want to save the screenshot at.

For computers with more than one monitor, remote screen capture supports dual screen monitors.

### How to use Remote Screen Capture

1. Select the computer on the left-hand panel of the CurrentWare console.
2. Under the **BrowseReporter** tab, click on the **remote screen capture** button.
3. A window will now appear to display the screen of the remote computer.

**NOTE:** Ensure that port 1024 is open on the client system to allow for screen capturing.

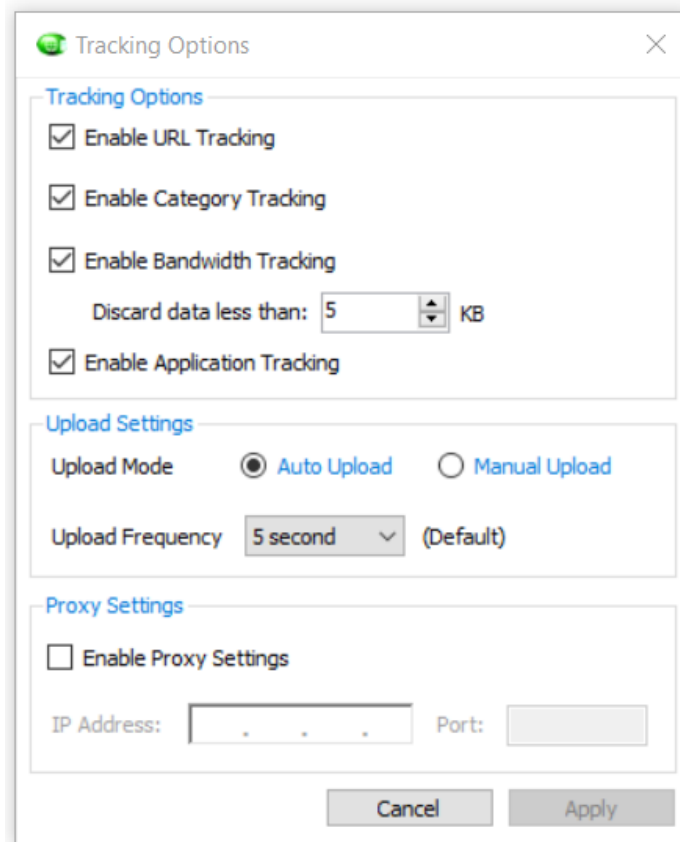


With Remote Screen Capture, you will be able to see what your users are doing on their computer in real time.



## 13.0 Tracking Options

Four options are available to change the behavior of BrowseReporter's tracking process.



The screenshot shows a dialog box titled "Tracking Options" with a close button (X) in the top right corner. The dialog is divided into three sections: "Tracking Options", "Upload Settings", and "Proxy Settings".

- Tracking Options:** Contains four checked checkboxes: "Enable URL Tracking", "Enable Category Tracking", "Enable Bandwidth Tracking", and "Enable Application Tracking". Below these is a "Discard data less than:" field with a value of "5" and a unit of "KB".
- Upload Settings:** Contains an "Upload Mode" section with two radio buttons: "Auto Upload" (selected) and "Manual Upload". Below this is an "Upload Frequency" section with a dropdown menu set to "5 second" and the text "(Default)".
- Proxy Settings:** Contains an unchecked checkbox "Enable Proxy Settings". Below this are two input fields: "IP Address:" (with a placeholder ". . .") and "Port:" (with a placeholder " ").

At the bottom of the dialog are two buttons: "Cancel" and "Apply".

### 13.1 Tracking Options

Toggle the tracking status of BrowseReporter

- **Enable URL Tracking**
- **Enable Bandwidth Tracking**
- **Enable Category Tracking**
- **Enable Application Tracking**

### 13.2 Upload Settings

Change the upload mode to determine how data is uploaded from the CurrentWare Client to the CurrentWare Server.

### 13.2.1 Auto Upload

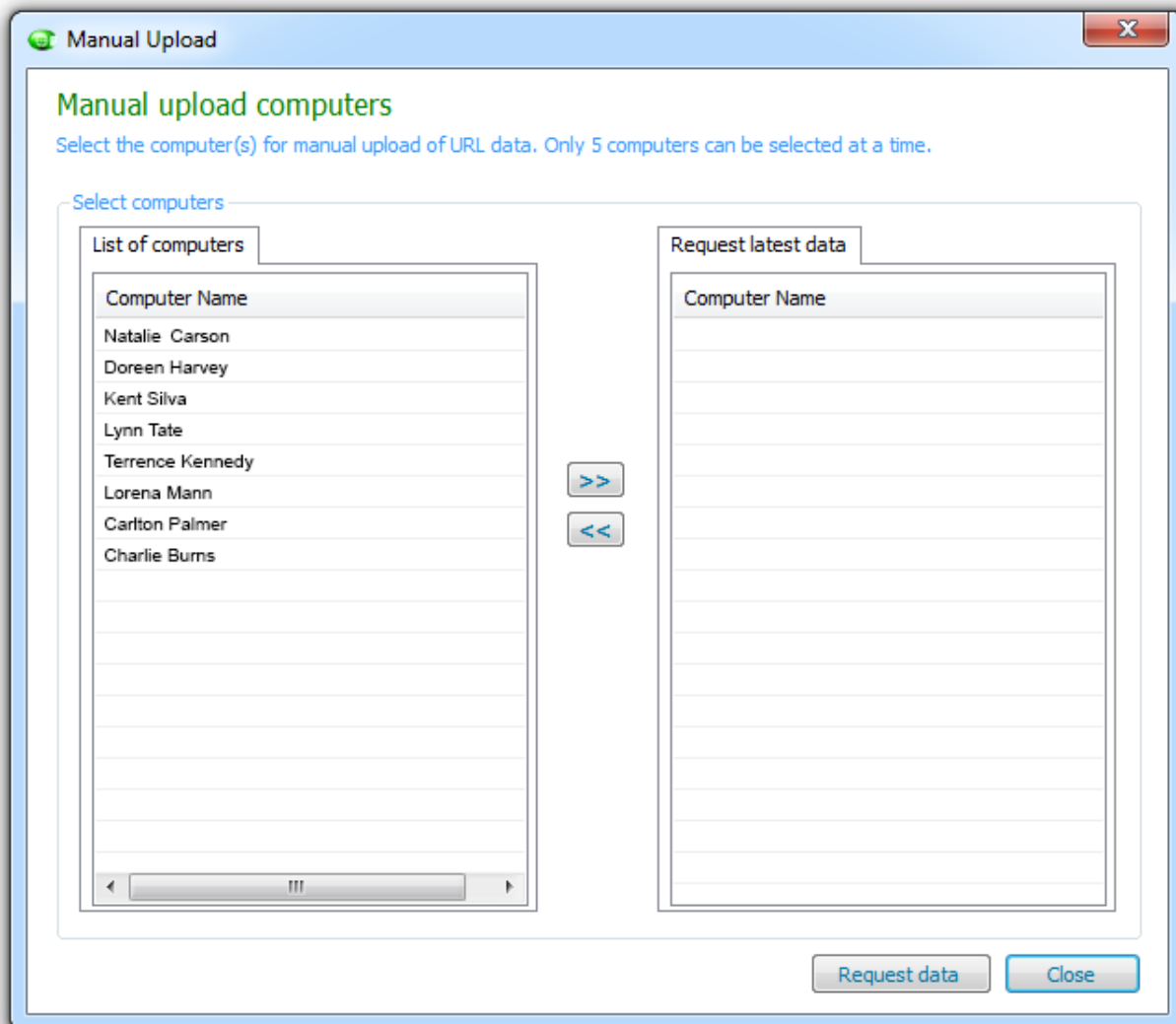
Auto upload will automatically upload data from the CurrentWare Client to the CurrentWare Server in cycles. The interval is defined by the **Upload frequency** (in minutes).

### 13.2.2 Manual Upload

Manual upload allows the administrator to select specific computers to upload data from. The data upload will occur manually and the administrator must remember to perform the upload.

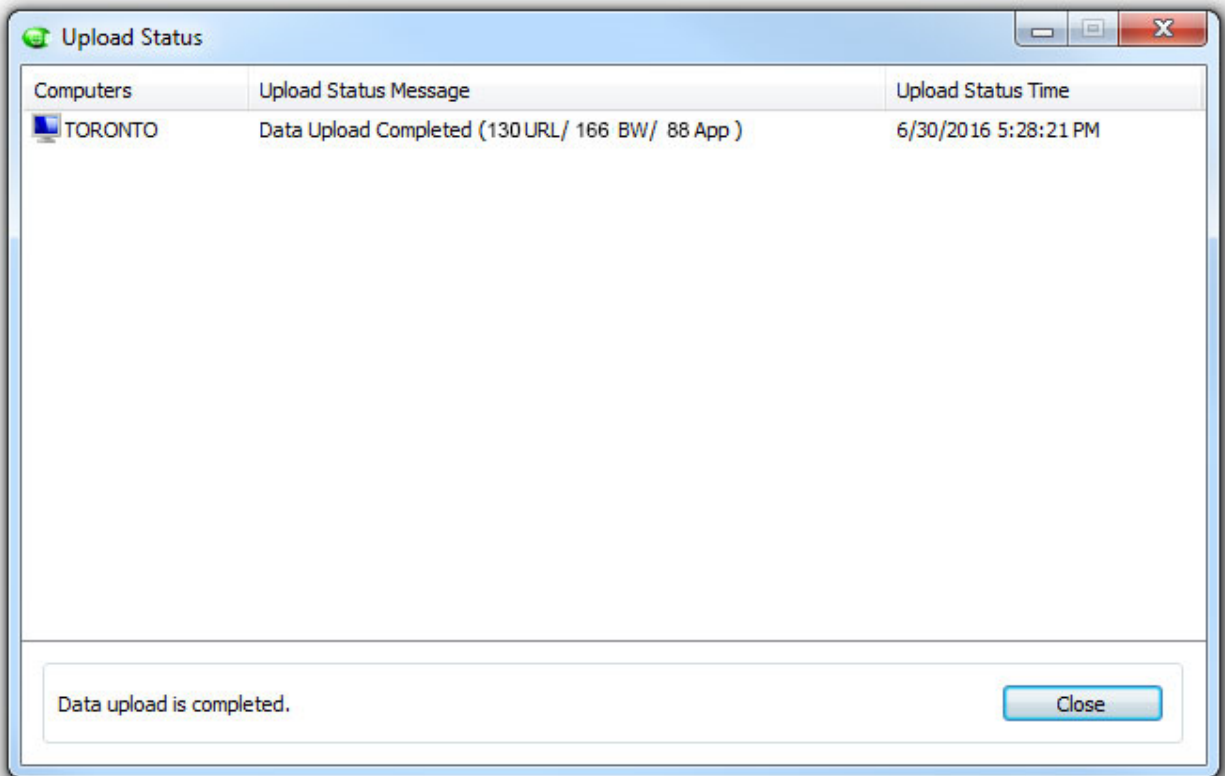
This option is suitable for large networks to reduce bandwidth bottleneck. Since auto upload will automatically upload data from all the computers, resulting in all the client computers connecting to the Server at once. Manual upload gives the administrator control on which group of computers to perform the upload from. This will reduce network traffic congestion to the CurrentWare Server.

Once Manual Upload is enabled, the “Request Latest data” option will no longer be greyed out.



## Upload Status

The upload status will display the upload progress and report the number of URLs uploaded from the CurrentWare Client to the CurrentWare Server along with the upload status time.



## 14.0 BrowseReporter Client Settings

### Offsite Management

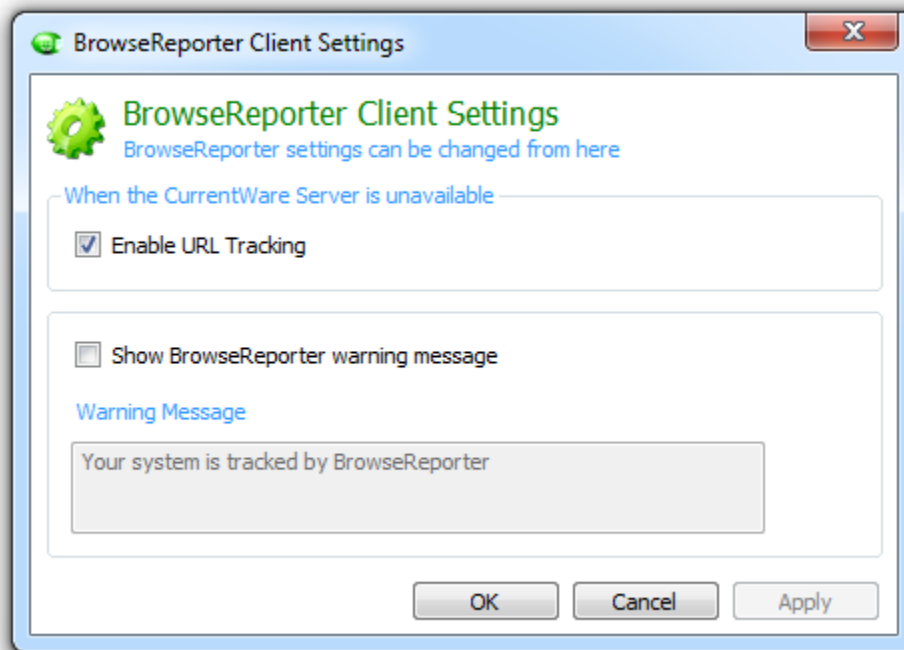
BrowseReporter will still track the Internet activities of a workstation if the CurrentWare Server is unavailable.

For example, if the Client/Server computer is taken outside the network, BrowseReporter will track the data into the client database. When the server is available, it will resume uploading the data.

### Show BrowseReporter Warning Message

The administrator has the option to display a warning message on the client computer.

If this option is enabled, the warning message will appear on the client computer when the users log on to their computers.



BrowseReporter Client Settings.

## 15.0 CurrentWare Server Manager

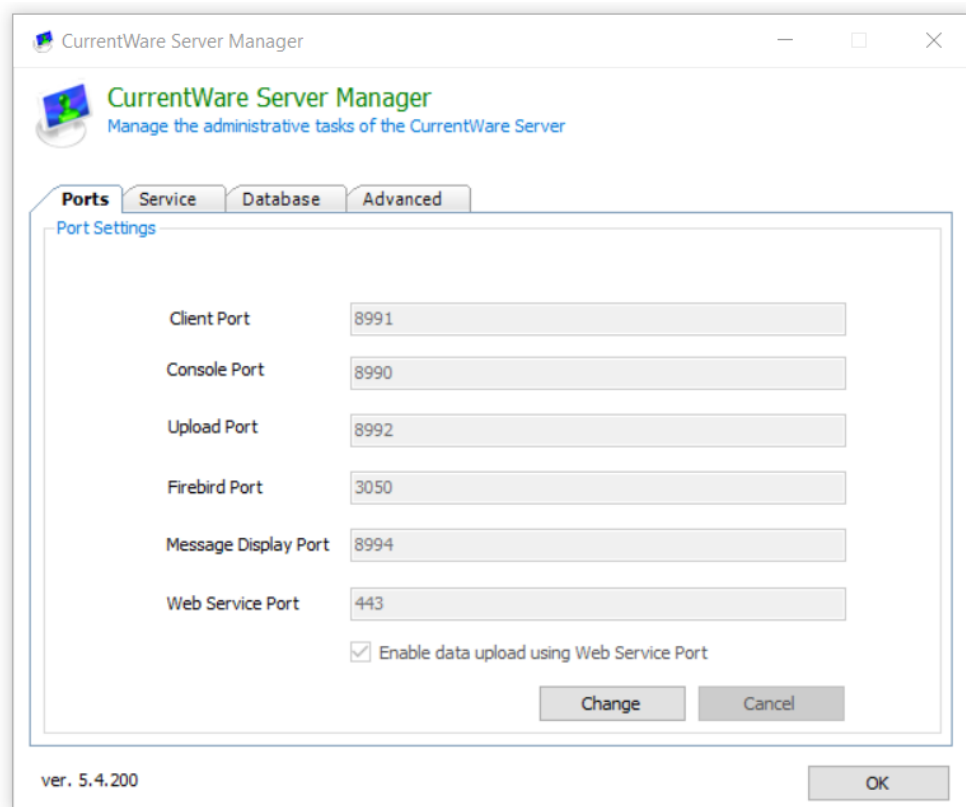
The CurrentWare Server Manager is used to manage the administrative tasks of the CurrentWare Server.

To access the Server Manager, click on the **Start Menu > Programs > CurrentWare > CurrentWare Server Manager**.

### 15.1 Changing the CurrentWare Client and Console Port

Changes to the Client and Console ports may be required to establish the connections between the CurrentWare server, clients and consoles. For example, if you are using a program that is already utilizing the ports that CurrentWare uses, then you will need to change the ports. Otherwise, please do not modify the Client and Console ports.

The default ports are listed in the screenshot below.

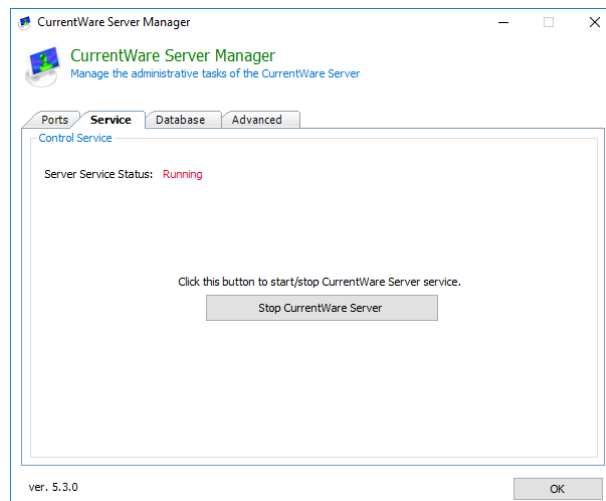


CurrentWare Server Manager.

- **Client Port:** the port connection between the CurrentWare Client and the CurrentWare Server.
- **Console Port:** the port connection between the CurrentWare Client and the CurrentWare Consoles.
- **Upload Port:** the port used to upload BrowseReporter (URL, BW and APP) and AccessPatrol data from the CurrentWare Client to the CurrentWare Server.
- **Firebird Port:** the port connection between the CurrentWare Server and the Firebird database.
- **Message Display Port:** the port used by BrowseControl's Web Filter (UIA) to display the warning messages.
- **Web Service Port:** the alternative port used to upload BrowseReporter (URL, BW and APP) and AccessPatrol data from the CurrentWare Client to the CurrentWare Server.

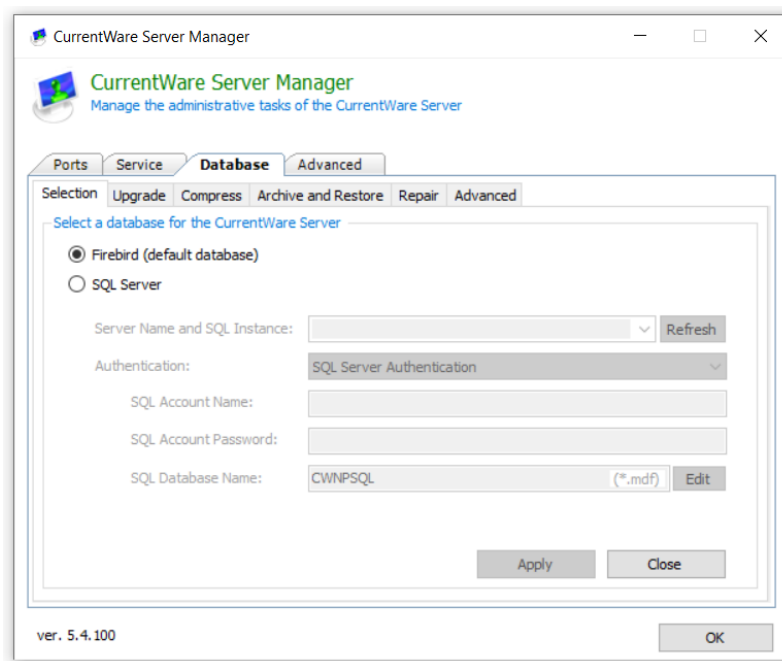
## 15.2 Stopping the CurrentWare Server Service

To stop the CurrentWare Server, under the Service tab, click on the button “Stop CurrentWare Server”.



## 15.3 CurrentWare Database Selection

Database selection lets you choose between using the default Firebird database or your own SQL Server.



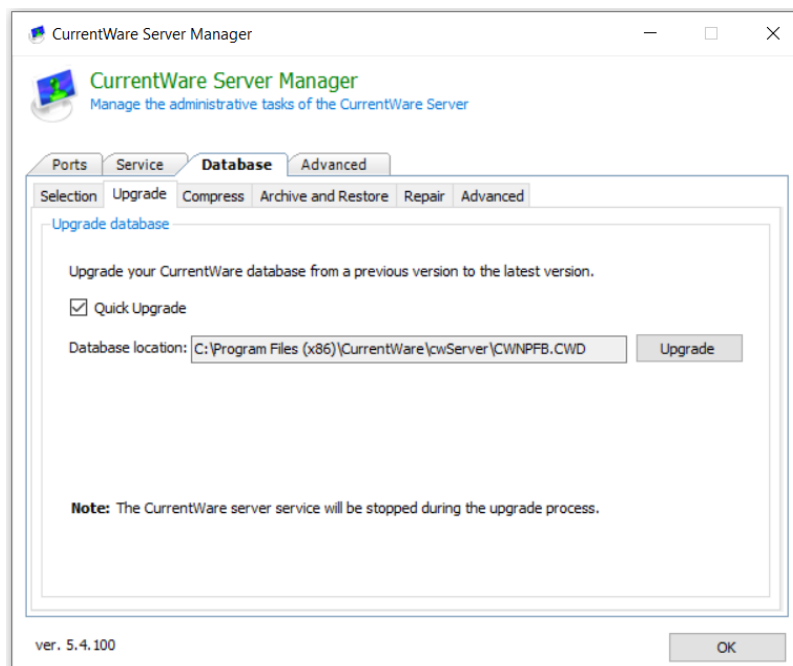
## 15.4 Upgrading the CurrentWare Database

Use this option to upgrade an older CurrentWare database to the same version as the CurrentWare Server.

The CurrentWare database file must be located in:

*C:\Program Files(x86)\CurrentWare\cwServer\CWNPFB.CWD*

**Quick Upgrade:** Use this option to perform a quick upgrade of the CurrentWare database. If you run into any issues with the database upgrade, uncheck this option and try again.



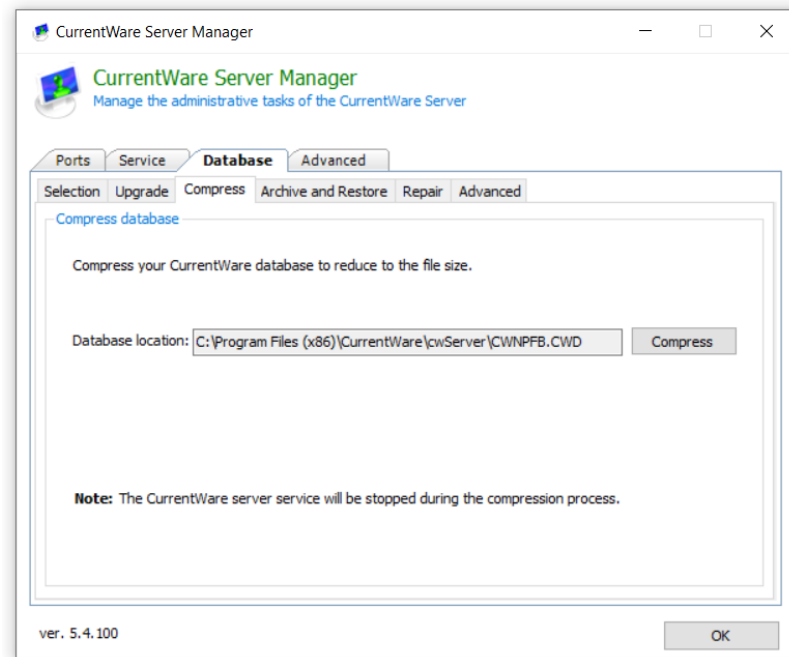
## 15.5 Compress the CurrentWare Database

It is recommended that database compression be performed on a regular basis.

**To compress your CurrentWare database:**

1. Make sure you have closed the **CurrentWare** Console.
2. Go to the Start menu > Programs > CurrentWare > CurrentWare Server Manager.
3. Under the **Compress** tab, click on the **browse** button and search for your CurrentWare database. By default, the database is located under **C:\Program Files\CurrentWare\cwServer\CWNPFB.CWD**
4. Click on the **Compress** button to begin compressing your database.





## 15.6 Archive and Restore the CurrentWare Database

Archiving the CurrentWare database will create a copy of your existing database. However, all tracking data from the existing live database will be deleted.

**NOTE:** Archiving will create a copy of the current database. After the archiving process is completed, the Internet tracking data for BrowseReporter will be deleted. All Computer and User data will be maintained but the corresponding monitoring data will be removed.

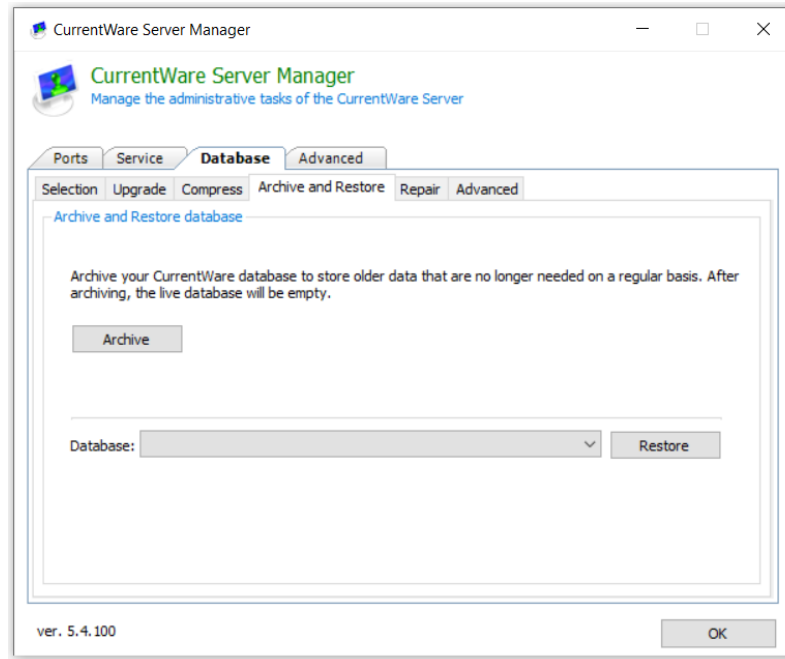
### To Archive your CurrentWare Database:

1. Under the **Archive and Restore** tab, click on the **Archive** button.
2. A copy of your database will be created under **C:\Program Files\CurrentWare\cwServer\Archive\**

Restoring the database will put your current database back to the state it was prior to archiving. The current database will be replaced with the archived database. It is advised that you archive your current database before restoring to a previous database, should you need to retrieve the original data.

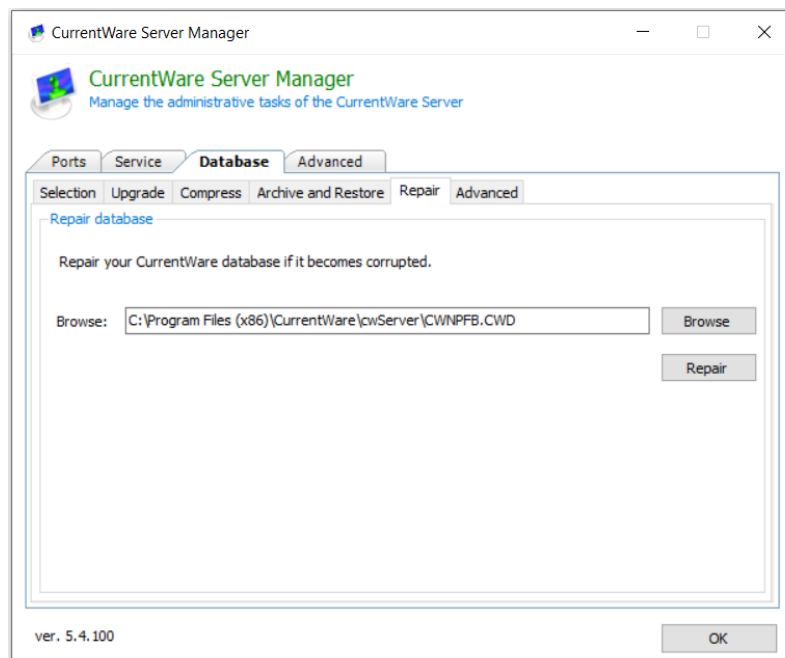
### Restoring an Archived Database:

1. Under the **Archive and Restore** tab, select the database that you want to restore from the drop-down menu
2. Click on the **Restore** button to begin the process of restoring your archived database.



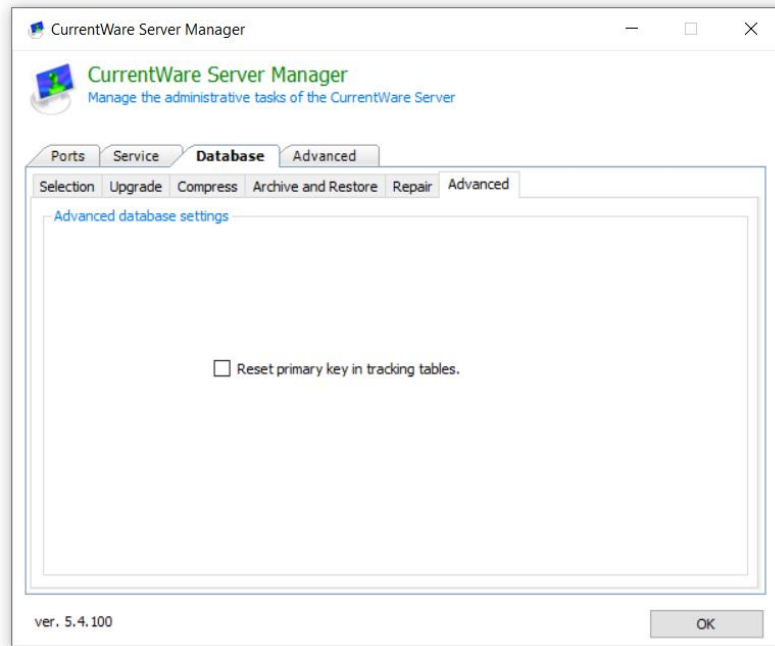
## 15.7 Repairing the CurrentWare Database

When you are unable to start the cwServer because the CWNPFb database has been corrupted, use this option to repair your existing database.



## 15.8 Reset Primary Key

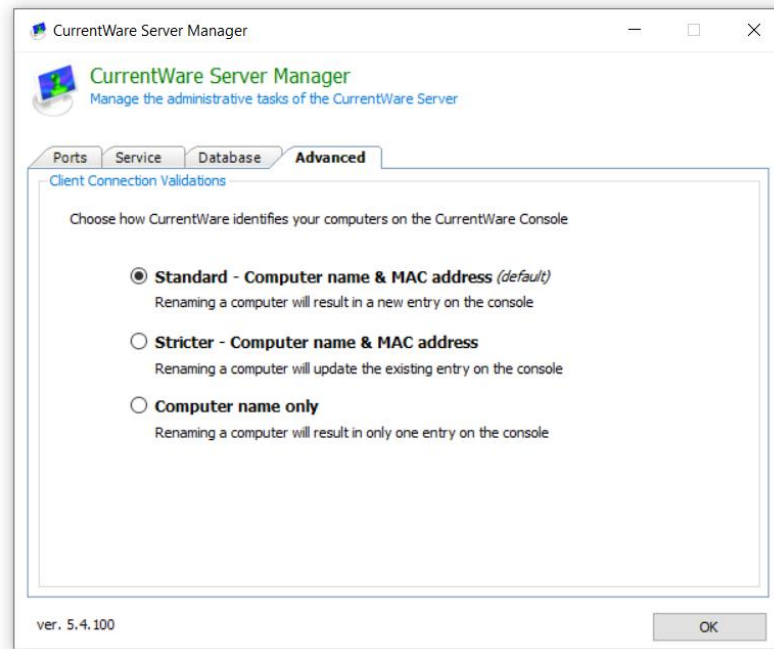
Advanced troubleshooting option for resetting primary key used for the data upload process. Only make changes to this option if it was recommended by the CurrentWare support team.



## 15.9 Advanced

Enabling Stricter client connection handshake will add another layer of validation to the client connection process.

- **Standard – Computer Name & MAC Address (default)**  
Renaming a computer will result in a new computer entry on the CurrentWare Console.
- **Stricter – Computer name & MAC Address**  
Renaming a computer will update the existing computer's name on the CurrentWare Console if the MAC address matches an existing computer.
- **Computer Name Only**  
Renaming a computer will always result in a new computer entry on the CurrentWare Console.



## 16.0 Licensing

CurrentWare Solutions are licensed on a per-computer basis for client management.

The evaluation copy of CurrentWare is functional on a maximum of 10 computers for 14 days.

### 16.1 Register Your Permanent License key

After you have purchased BrowseControl, BrowseReporter, enPowerManager or AccessPatrol from CurrentWare, you will receive an email from our licensing department containing your license key information, which includes the following fields:

1. **Organization's Name**
2. **Number of Licenses**
3. **License key**

To register your license key, follow the steps below:

1. Launch the CurrentWare Console.
2. Go to **Help > Licensing**.
3. From the Solutions drop down box, select the **Solution** .
4. Copy your **Organization's name, number of licenses and Activation Code** from the licensing email sent to you.
5. Click on the **Register** Button.
6. Your CurrentWare Console has now been registered.
7. Click on **Next** to manage the computers you want to apply the license keys to.

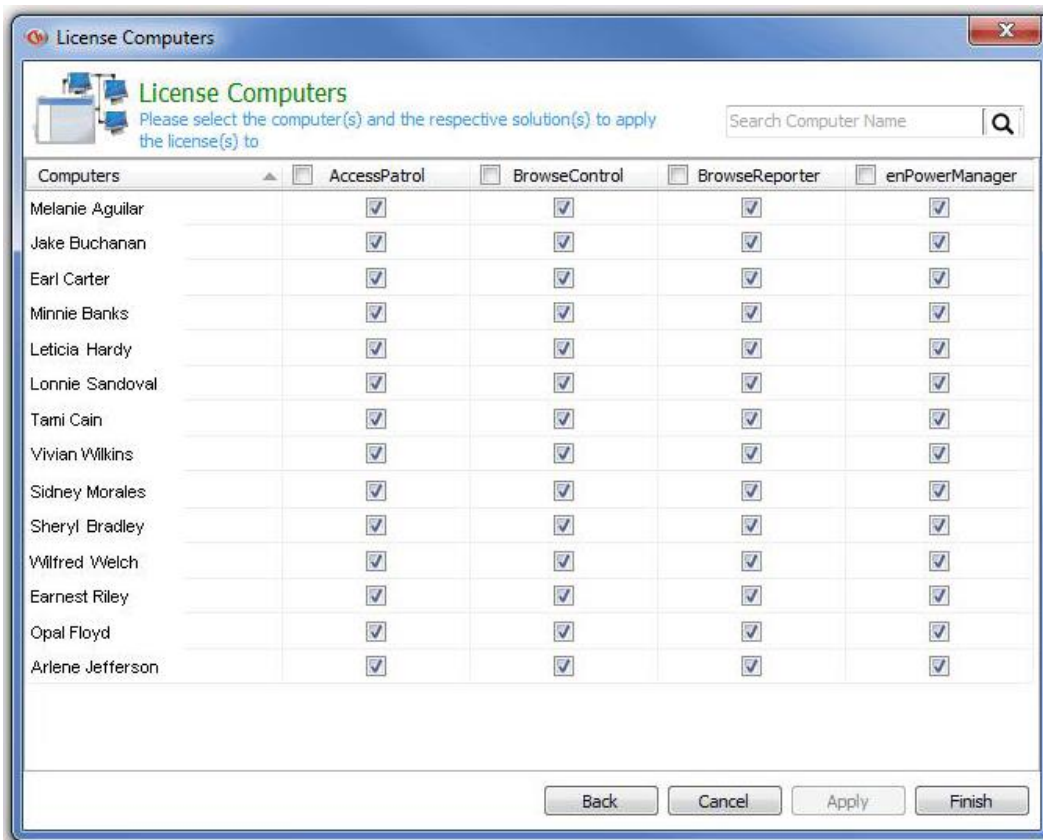
## 16.2 License Management

The License Computers console allows the administrator to select the computers to assign the CurrentWare license to. Depending on the installed status of your CurrentWare clients, the licensing process can be automatic or manual.

### 16.2.1 Managing Your CurrentWare Licenses

You will need to manage your CurrentWare Licenses if you have applied your license key before installing your CurrentWare Clients.

1. After you install your CurrentWare Clients, launch your CurrentWare Console.
2. Go to **Help > Licensing**.
3. Fill in the fields for the Organization name, solution, mode of license, number of licenses and license key.
4. Click **next**.
5. Now the **License Computers** window will appear. This is where you assign your licenses to your computers. Click on the checkbox to assign a license key to your computer.



Manage your CurrentWare Licenses.

## 17.0 Uninstall CurrentWare Server, Console and Solutions

### 17.1 Uninstalling the CurrentWare Solutions

1. On the CurrentWare Console, go to Help > Licensing.
2. Select the solution you want to remove and click the “Remove button”.
3. The CurrentWare Console will restart and the selected solution will be removed.

### 17.2 Uninstalling the CurrentWare Server and Console

The CurrentWare Console and Server can be removed from the Control Panel.

1. Go to Control Panel > Programs > Uninstall a Program.
2. Select CurrentWare and click “Uninstall”.
3. The CurrentWare Server and Console will be uninstalled.

## 18.0 Uninstall CurrentWare Client

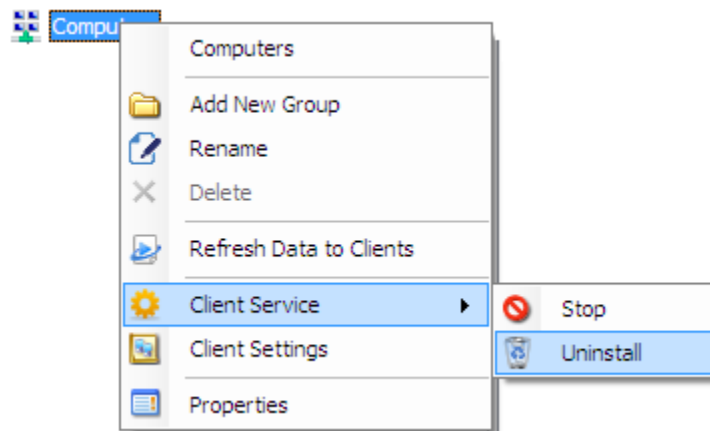
The CurrentWare Client can be uninstalled by three different methods:

- **Uninstall CurrentWare Client from the Console.**
- **Uninstall CurrentWare Client on the workstation by command line.**
- **Uninstall CurrentWare Client on the workstation from the Client Configuration Window.**

### 18.1 Uninstall CurrentWare Client from the Console

Follow the steps below to uninstall the CurrentWare Client remotely from the CurrentWare Console.

1. Launch the CurrentWare Console.
2. Right click on the computer or the group of computers that you want to uninstall, select **Client Service > Uninstall**.
3. The client will proceed to uninstall
4. A reboot will be prompted. It is recommended to restart the computer.





## 18.2 Uninstall CurrentWare Client on the Workstation by Command Line

Follow the steps below to uninstall the CurrentWare Client locally on the workstation by running a command line.

You need to have your CurrentWare Client password in order to uninstall the CurrentWare Client by command line.

On your CurrentWare Client computer, go to start menu > run > type in the following (for Windows 7, go to the run command box):

**For 32-bit Windows PC**

**C:\Windows\SysWOW64\wcsystck\CwClient.exe -p Admin -u**

**For 64-bit Windows PC**

**C:\Windows\SysWOW64\wcsystck\CwClient.exe -p Admin -u**

\*The word "Admin" in the command is the CurrentWare Client password. Admin is the default CurrentWare Client password. If you changed the CurrentWare Client password during the installation, replace Admin with your CurrentWare Client password.

## 18.3 Uninstall CurrentWare Client on the Workstation from the Client Configuration Window

Follow the steps below to uninstall the CurrentWare Client locally on the workstation from the CurrentWare client configuration Window.

1. On the Client computer, go to C:\Windows\System32\wcsystck (for 32-bit computers) or C:\Windows\SysWOW64\wcsystck (for 64-bit computers).
2. Double click on cwagent.exe.
3. When prompted for the CurrentWare Client password, type it in (Admin is the default CurrentWare Client password. If you changed the CurrentWare Client password during the installation, please replace Admin with your CurrentWare Client password).
4. In the CurrentWare Client Configuration Window, click on the Uninstall button to uninstall the CurrentWare client from your workstation.

## 19.0 Technical Support

There are several ways to reach our technical support team.

**By Email:** Send us an email at [support@currentware.com](mailto:support@currentware.com)

**By Phone:** Call us at 613-368-4300.

Our hotline is available between 8 AM to 6 PM EST on weekdays.

**Live Chat:** Chat with a live agent on our website at <https://www.currentware.com>

Our live chat is 24/7.

## 20.0 Contacts

### USA

**Codework Inc**

1623, Military Rd #556, Niagara Falls, NY 14304-1745, United States of America

Tel: 613-368-4300

Fax: 866-929-9808

Email: [info@currentware.com](mailto:info@currentware.com)

### CANADA

**CurrentWare Inc**

PO Box 30024 King St PO, Toronto, Ontario, M5V 0A3, Canada

Tel: 613-368-4300

Fax: 866-929-9808

Email: [info@currentware.com](mailto:info@currentware.com)

### EUROPE

**CurrentWare Inc**

PO Box 30024 King St PO, Toronto, Ontario, M5V 0A3, Canada

Tel: 613-368-4300

Fax: 866-929-9808

Email: [info@currentware.com](mailto:info@currentware.com)

### ASIA

**Codework Solutions Pvt Ltd,**

'Thapasya', Infopark, Kakkanad, Kochi, Kerala, India – 682030

Tel: +91-484-4055678

Fax: +91-484-4061003

Email: [info@codework.com](mailto:info@codework.com)

### OTHER COUNTRIES

Please email [info@currentware.com](mailto:info@currentware.com) for the name of a local reseller in your country.