

User Guide

Revised in March, 2017



BrowseReporter

Version 5.1.4

Web Monitoring Tool

BrowseReporter User Guide - Table of Contents

1.0 Introduction to BrowseReporter	5
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 Terminal Server Setup	16
1.8.1 BrowseControl and Terminal Server	16
2.0 CurrentWare Console Overview.....	17
2.1 Client and Group Management.....	18
2.2 Redirect Clients	19
2.3 Client Settings	20
2.4 Troubleshooting.....	22
2.5 Operators	24
2.6 Import Users	25
2.7 Database Backup Scheduler.....	27
2.8 Auto Delete Scheduler	28
2.9 Options	29
2.10 Server Settings.....	31
2.11 Log Out.....	32
3.0 Overview of BrowseReporter Functions	33

4.0 Run Report.....	34
4.1 Report Profile	35
4.2 Report Type.....	35
4.3 Report Options	37
4.3.1 Select Mode.....	37
4.3.2 Rename Category.....	37
4.3.3 Options.....	38
4.3.4 Idle Time Limit	38
4.3.5 Reporting Period.....	38
5.0 Request Latest Data	39
6.0 Add Custom Logo.....	40
7.0 URL Tracking Scheduler	40
8.0 Exclusion List.....	41
9.0 Email Reports.....	43
9.1 Email Alerts	44
9.2 Email Settings	46
10.0 Export URLs	48
11.0 Delete Data.....	49
12.0 Remote Screen Capture	50
13.0 Tracking Options	51
13.1 Tracking Options	51
13.2 Upload Settings	51
13.2.1 Auto Upload.....	52
13.2.2 Manual Upload.....	52
14.0 BrowseReporter Client Settings	54
15.0 CurrentWare Server Manager	55
15.1 Changing the CurrentWare Client and Console Port.....	55
15.2 Stopping the CurrentWare Server Service	56
15.3 Compress the CurrentWare Database.....	56
15.4 Archive and Restore the CurrentWare Database	57
16.0 Licensing	58
16.1 Register your Permanent License key	58
16.2 License Management.....	59
16.2.1 Managing your CurrentWare Licenses.....	59
17.0 Uninstall CurrentWare Server, Console and Solutions	60
17.1 Uninstalling the CurrentWare Solutions	60
17.2 Uninstalling the CurrentWare Server and Console.....	60

18.0 Uninstall CurrentWare Client.....	61
18.1 Uninstall CurrentWare Client from the Console.....	61
18.2 Uninstall CurrentWare Client on the workstation by command line	62
18.3 Uninstall CurrentWare Client on the workstation from the Client Configuration Window.....	62
19.0 Technical Support.....	63
20.0 Contacts.....	64
USA.....	64
CANADA	64
EUROPE	64
ASIA	64
OTHER COUNTRIES	64

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

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 Window's Simple File Sharing.

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

1. **Local CurrentWare Client Install:** run the *cwClient.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 *cwClient.exe* file.

1.4.1 Local CurrentWare Client Install

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

The *cwClient.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\cwClient.exe

When you run the *cwClient.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.

2. CurrentWare Client Password (Optional)

The CurrentWare Client password is used to configure the CurrentWare Client settings. If you do not put in a custom CurrentWare Client password, then the default password is “Admin” (without the quote; case sensitive).

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

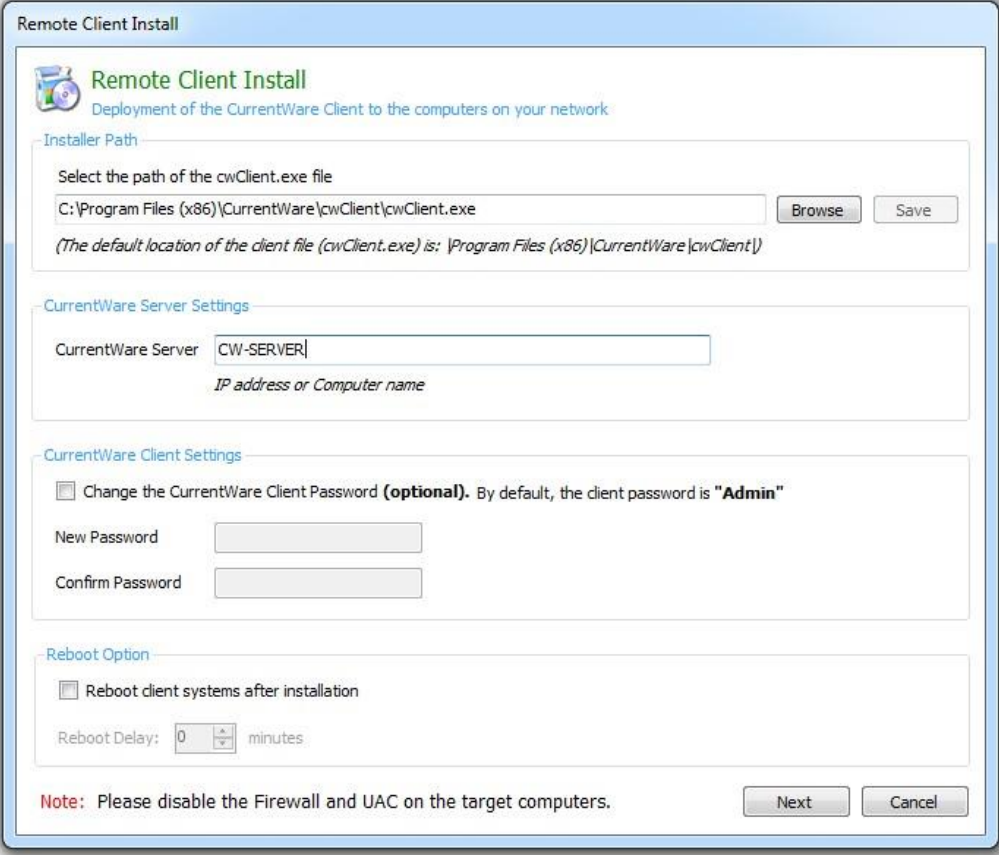
CurrentWare Clients can be remotely installed from the Console. The remote installer can be found on the console under the menu **Install > Remote Client Install**.

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

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

2. Enter the **Computer name or IP address** of the CurrentWare Server.
3. (Optional): Change the **CurrentWare Client password**.
4. Select the option to enable or disable **reboot** after the installation (the recommended option is to enable reboot).
5. 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.
6. 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**
7. The CurrentWare Client will now be deployed to the designated computers.



The screenshot shows the 'Remote Client Install' window. It has a title bar 'Remote Client Install' and a subtitle 'Deployment of the CurrentWare Client to the computers on your network'. The window is divided into several sections: 'Installer Path' with a text box for the path to 'cwClient.exe' (defaulting to 'C:\Program Files (x86)\CurrentWare\cwClient\cwClient.exe') and 'Browse'/'Save' buttons; 'CurrentWare Server Settings' with a text box for the server name (defaulting to 'CW-SERVER') and a note 'IP address or Computer name'; 'CurrentWare Client Settings' with a checkbox for 'Change the CurrentWare Client Password (optional)' (checked), and fields for 'New Password' and 'Confirm Password'; and 'Reboot Option' with a checkbox for 'Reboot client systems after installation' (checked) and a 'Reboot Delay' spinner set to '0' minutes. A 'Note' at the bottom states 'Please disable the Firewall and UAC on the target computers.' and there are 'Next' and 'Cancel' buttons.

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:

<http://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:\cwClient.exe /qn USERPARAMS="-p Admin -ds 192.168.1.100 -rp  
password -sp password" /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 cwClient.msi file

You can take the existing cwClient.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 cwClient.exe file:

Table	Property	Value
Property	USERPARAMS	"-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)

1.5.2 Installing the CurrentWare Client

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



The image shows a screenshot of the 'CurrentWare Client Setup' window. The window has a title bar with the text 'CurrentWare Client Setup' and standard Windows window controls. The main area is divided into two sections. On the left is a red graphic with the CurrentWare logo and a 3D box. On the right is the 'CurrentWare Client configuration' section. It contains three input fields: the first is for the IP address / Computer Name (with '205.145.10.133' entered), the second is for the CurrentWare Client password (with 'Admin' entered), and the third is for the new password (with 'Admin' entered). Below these fields are three buttons: '< Back', 'Next >', and 'Cancel'. The version 'Version: 5.1' is displayed at the bottom left.

CurrentWare Client Setup

CurrentWare Client configuration

Enter the IP address / Computer Name where the CurrentWare Server is installed. 205.145.10.133

Enter the CurrentWare Client password. The default password is 'Admin' (case sensitive). Admin

OPTIONAL - To change the default password, please enter the new password max 15 characters. Admin

Please confirm the password. Admin

Version: 5.1

< Back Next > Cancel

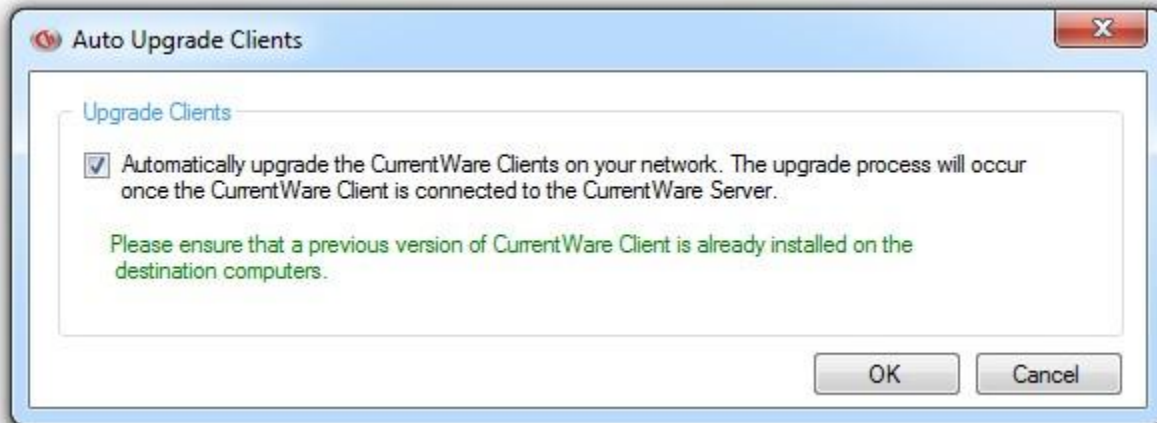
1.6 Upgrading the CurrentWare Clients

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 cwClient.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 **cwClient.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 Terminal Server Setup

The CurrentWare Console is compatible with Windows Terminal Server. The terminal server installation is the same as a normal CurrentWare Console installation.

The following Solutions are compatible with Terminal Server:

- **BrowseControl**
- **BrowseReporter**

1.8.1 BrowseControl and Terminal Server

In order to view the users on your Terminal Server, you must change your CurrentWare Console from PC mode to User mode.

On the CurrentWare Console, expand the BrowseControl tab on the right hand side. Click on the Mode button. Select User mode and click Apply. You are now using BrowseControl in User Mode.

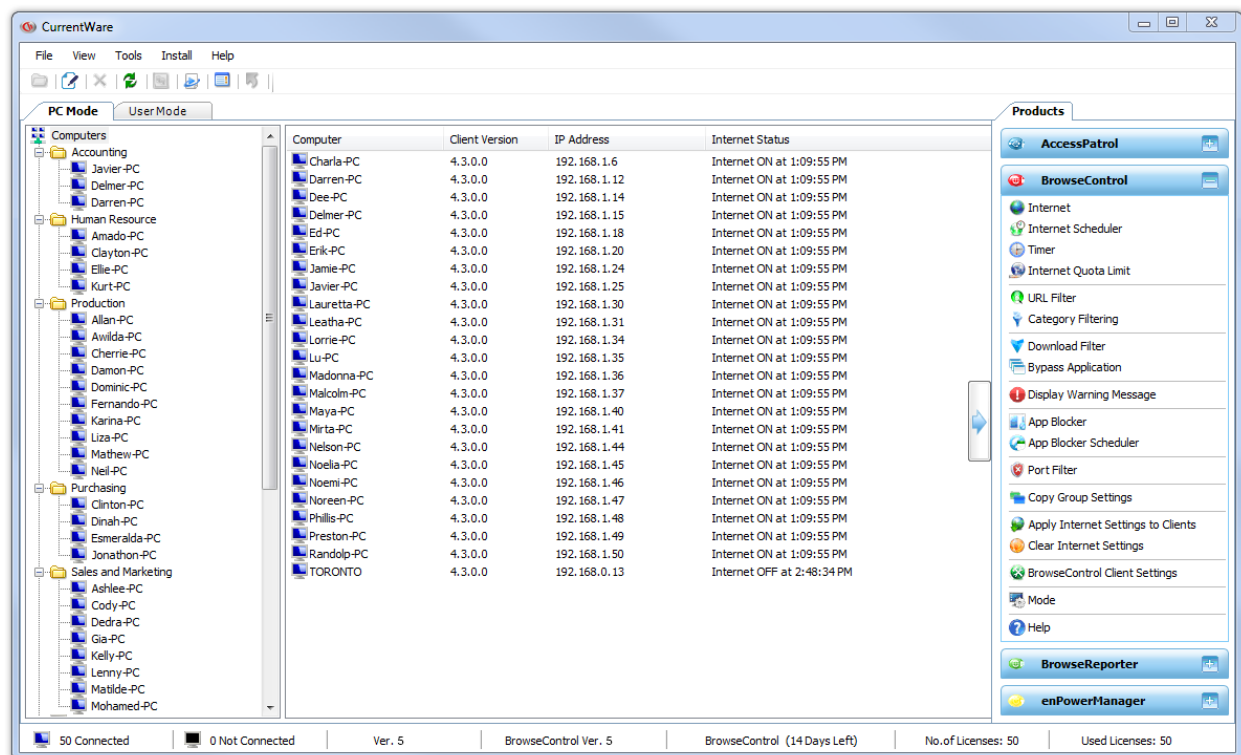
Once you are in user mode, your Terminal Server users will be listed under the User Mode tab automatically after they log onto the terminal server for the first time.

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.

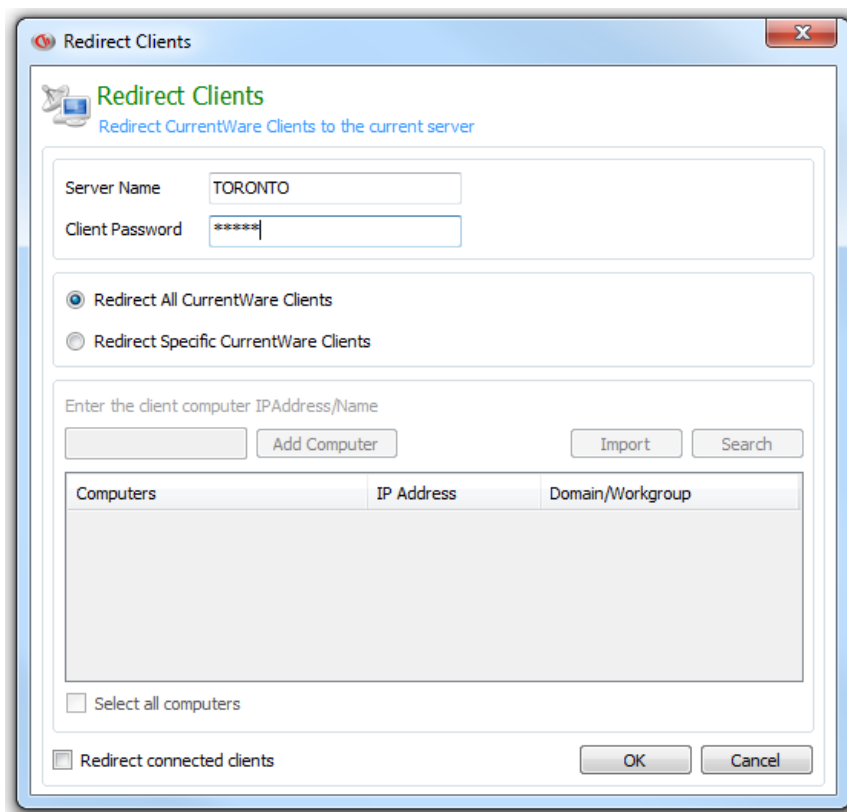
On the CurrentWare Console menu, select **File > Move Computer/Users**. The left hand side contains the source folder and the right hand side contains the destination folder. Select the computer(s) you want to move from the source folder, and then select the destination folder. Click on the >> button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

2.2 Redirect Clients

Redirect Clients is usually used when there are more than one CurrentWare Servers installed on your network. It is used to connect the CurrentWare Clients from another CurrentWare Server to the current CurrentWare server. Essentially, the redirect clients tool, transfers the CurrentWare Clients from one server to another.

Scenario: I need to transfer all of my CurrentWare Clients from my old server to the new server.

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



Redirect CurrentWare Clients that are connected to one CurrentWare Server
to another CurrentWare Server

2.3 Client Settings

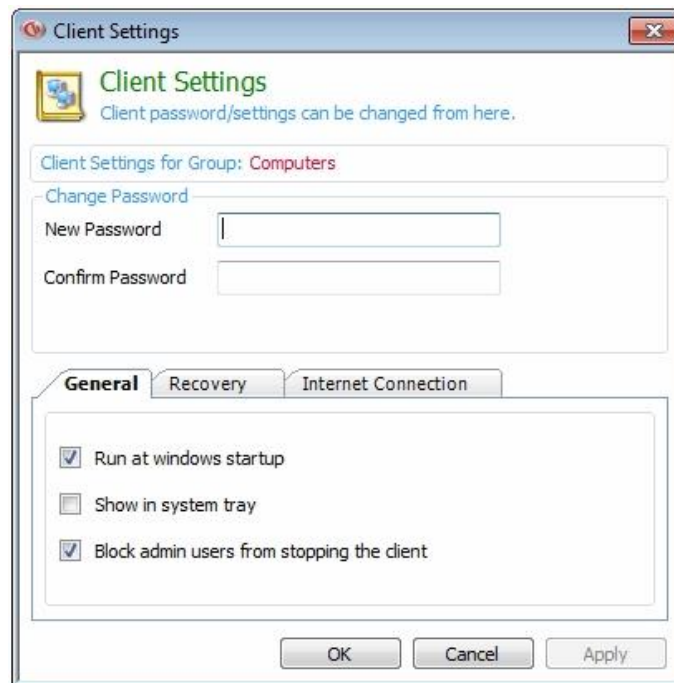
The CurrentWare Client settings can be modified in the CurrentWare Console under **Tools > Client Settings**. You can also right click on a group to find the Client Settings.

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 use to connect to the CurrentWare Server. By default the case sensitive Client password is **Admin**.

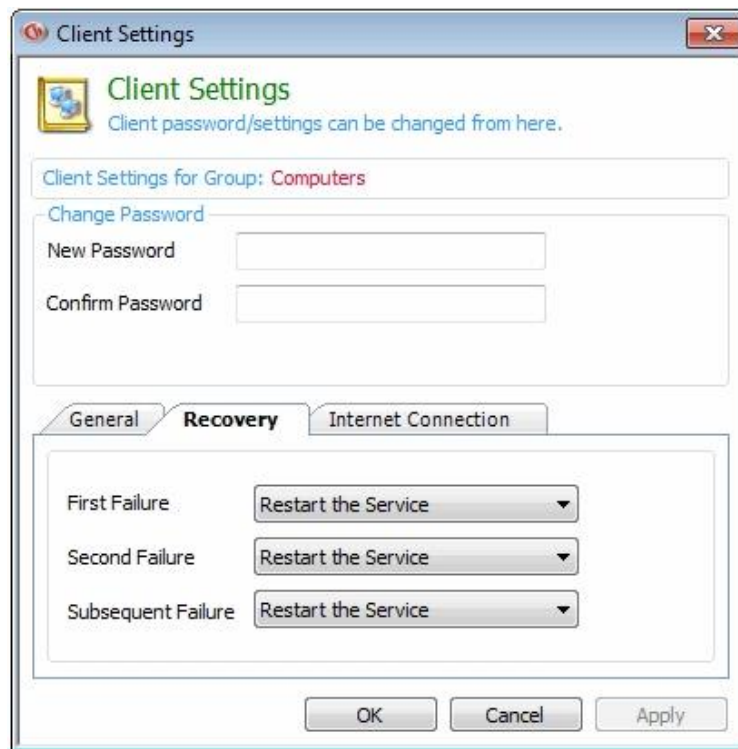
General

- **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.



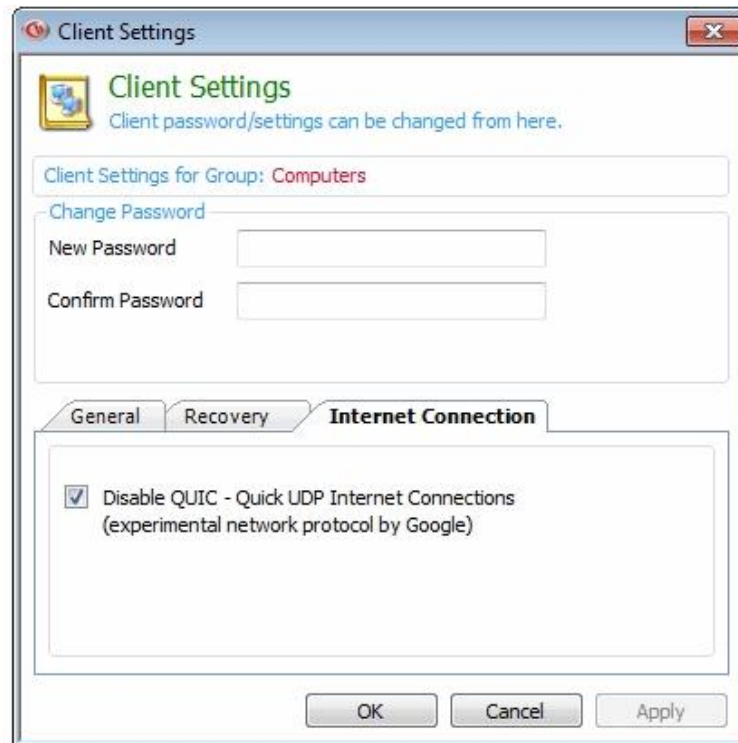
Recovery

- 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 another 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”.



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.

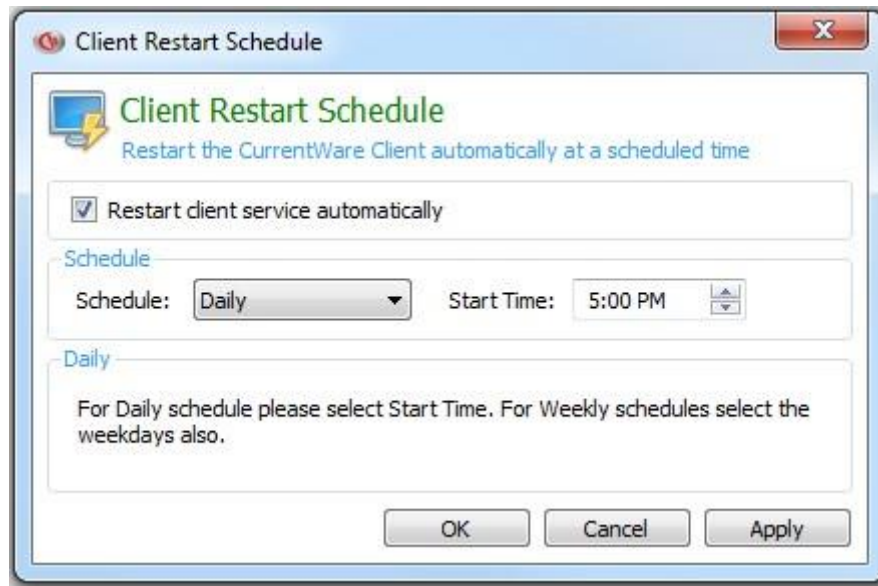


2.4 Troubleshooting

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**

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.

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.

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.

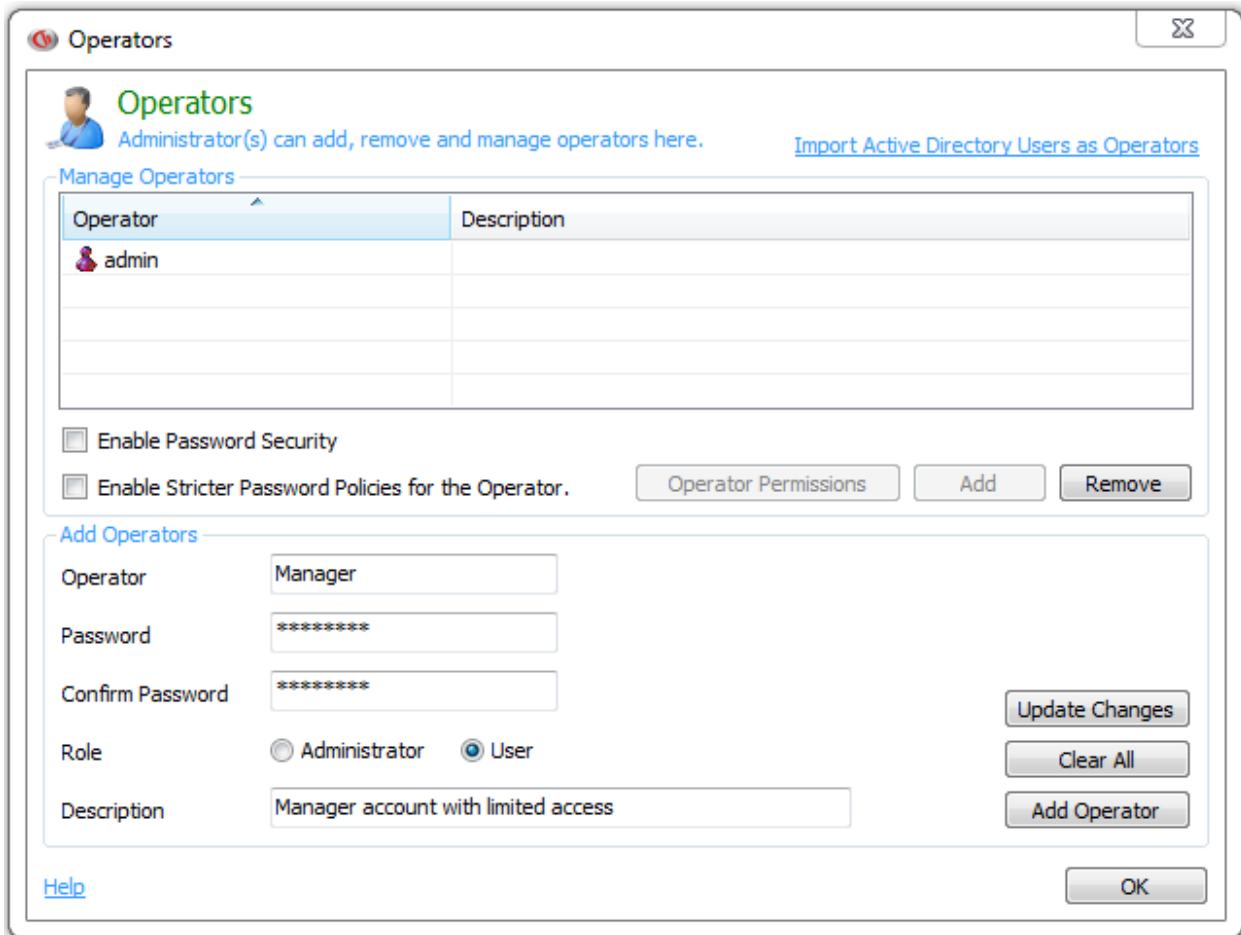
Creating an Operator:

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.



Operators

Administrator(s) can add, remove and manage operators here. [Import Active Directory Users as Operators](#)

Manage Operators

Operator	Description
admin	

☐ Enable Password Security
☐ Enable Stricter Password Policies for the Operator.

Operator Permissions

Add Operators

Operator:

Password:

Confirm Password:

Role: ☐ Administrator ☒ User

Description:

[Help](#)

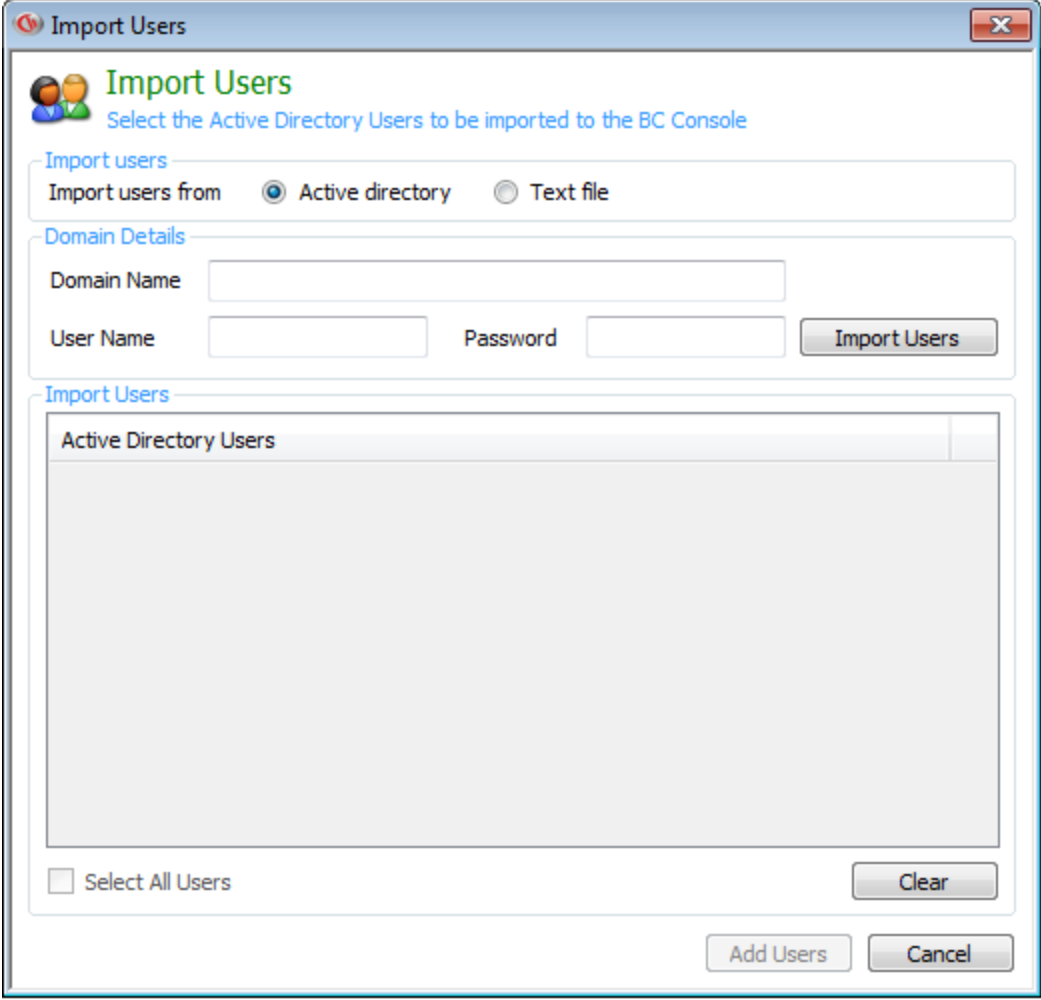
Administrators have unlimited control. Users have limited controls

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 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

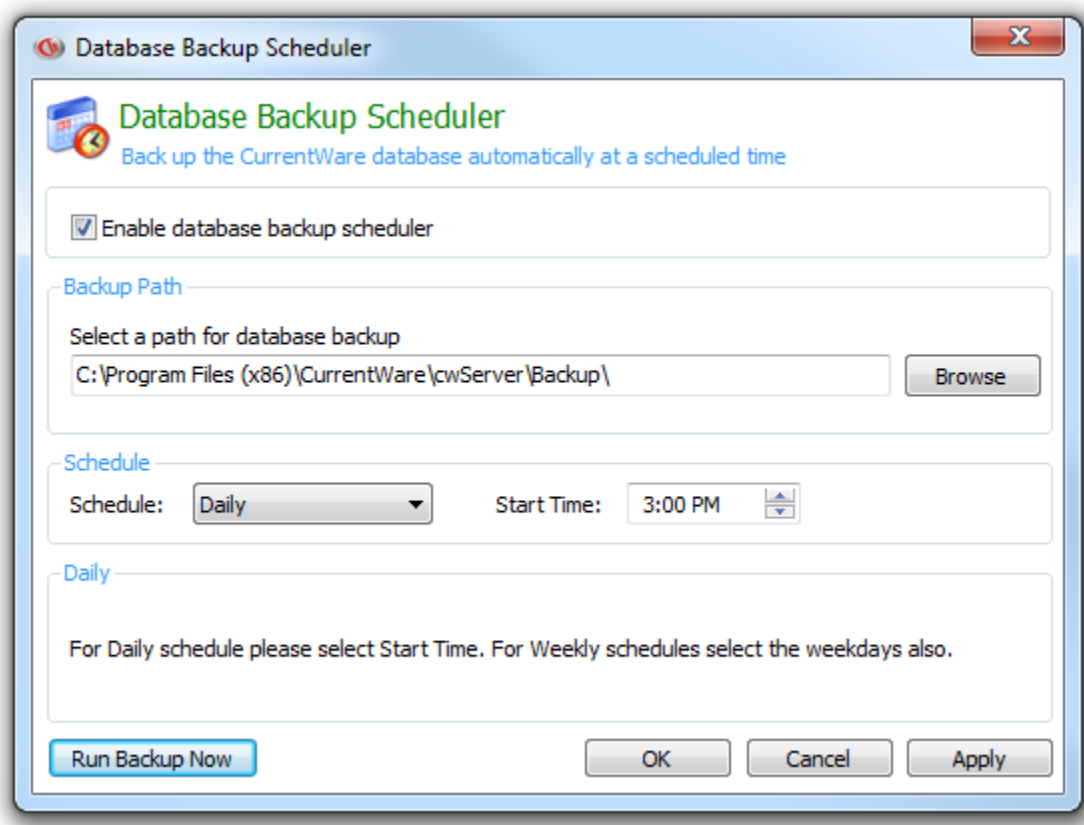
The Database Backup Scheduler automatically backs up the CurrentWare database (CWNPF.B.CWD) at a scheduled time.

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.

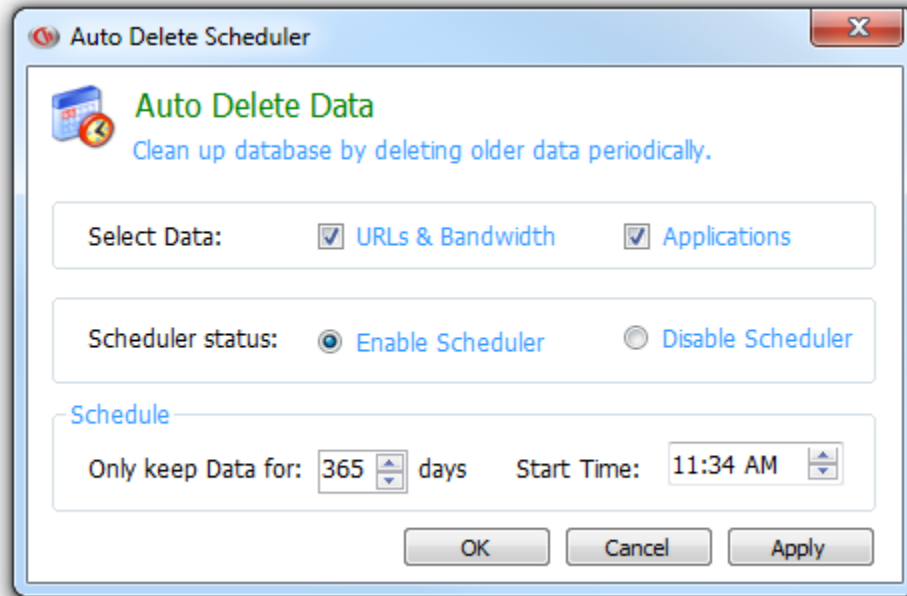
You can perform a one-time back up by clicking on the “Run Backup Now” button.



Automatically back up your database at a scheduled time

2.8 Auto Delete Scheduler

Automatically delete URL, bandwidth and application 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 90 days will be deleted automatically every day at 12:30 PM

Only Keep URLs 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.

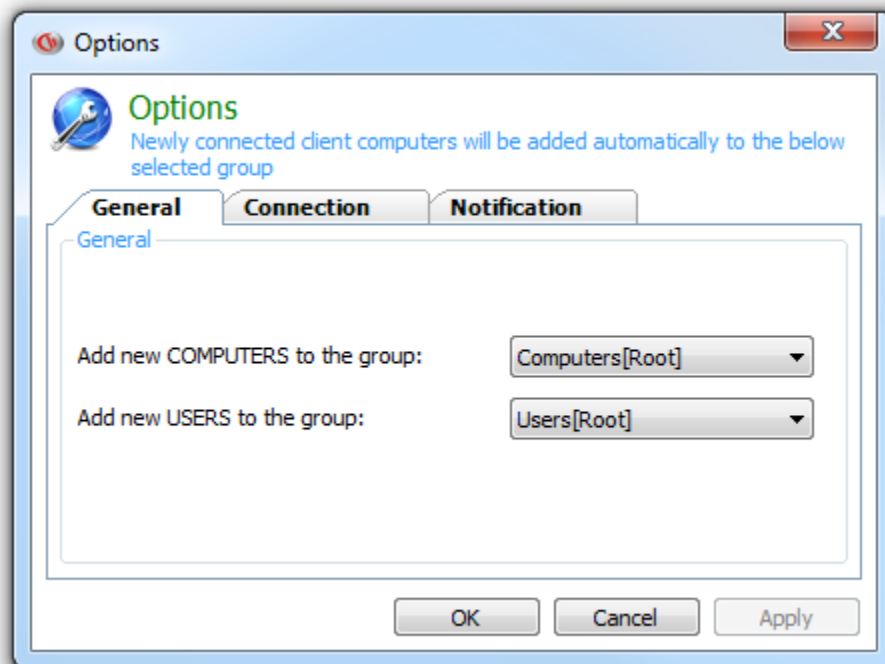
2.9 Options

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

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.

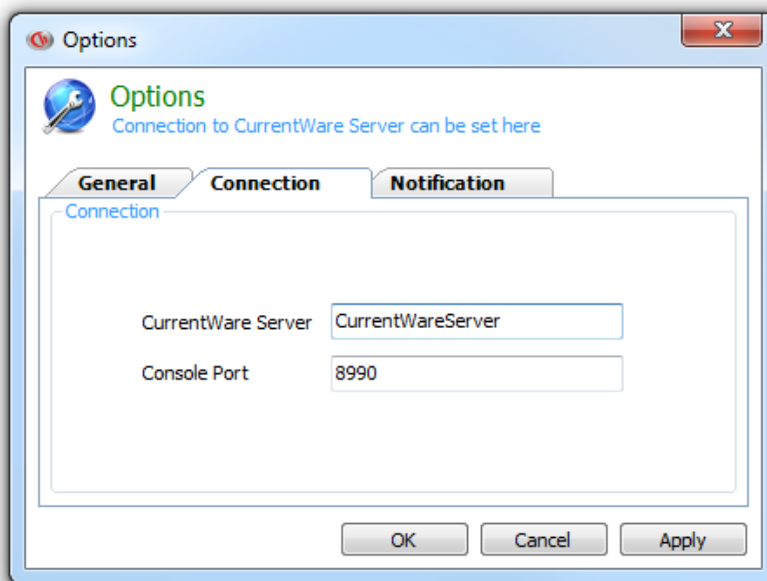
Add new Users to the group: define the group that a new user will automatically be assigned to once it is populated to the CurrentWare Server for the first time.



Connection

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

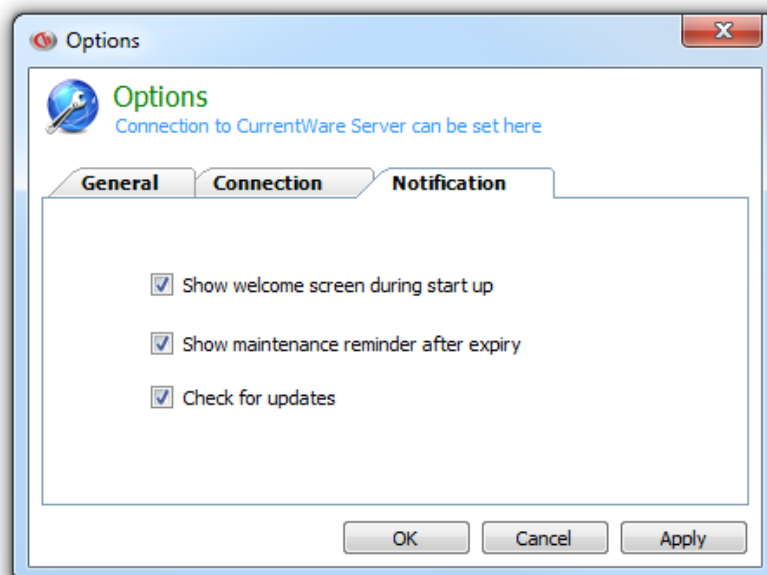
Console Port: The port that CurrentWare Console uses to connect to the CurrentWare Server. The default Console port is 8990.



Notification

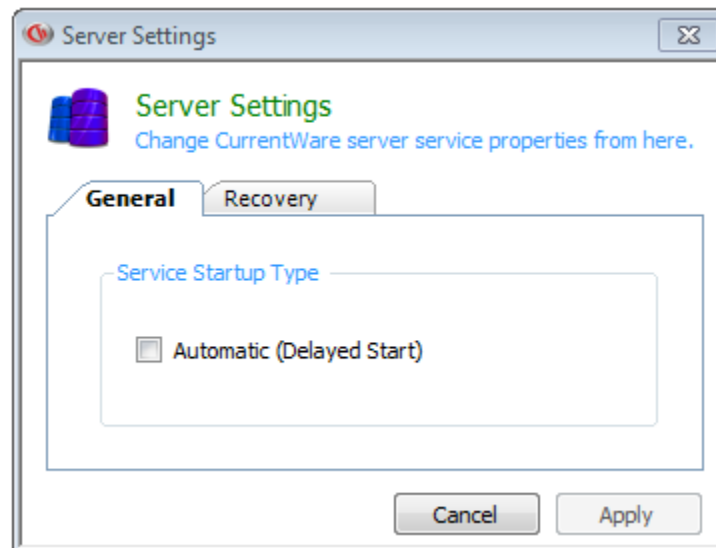
Enable/disable the following notifications:

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



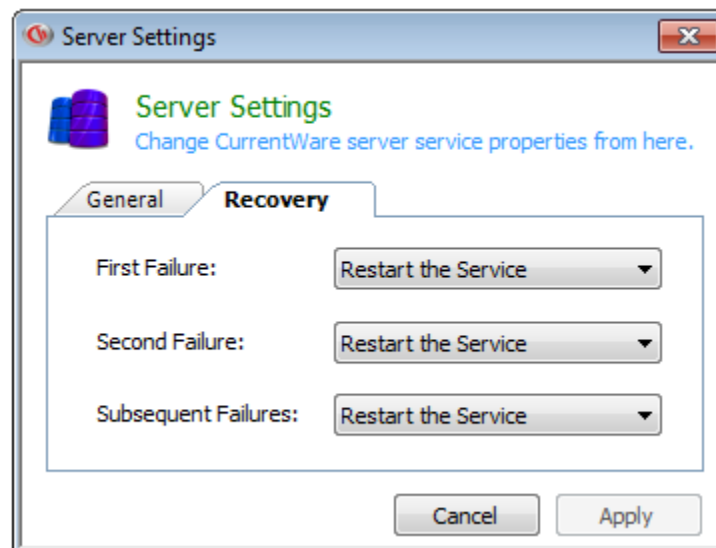
2.10 Server Settings

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



Service Startup Type

Toggle the option “Automatic (Delayed Start)” to change the CurrentWare Server service start up type. Enable this option if your CurrentWare Server service is not starting up automatically during system boot up.



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

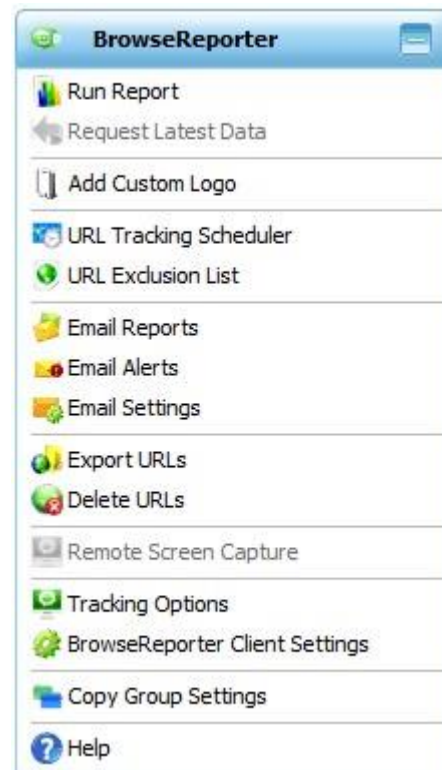
Log Out can be used to re-log into the Console with a different user name and password. This feature can be found under the menu **File → Logout**.

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.

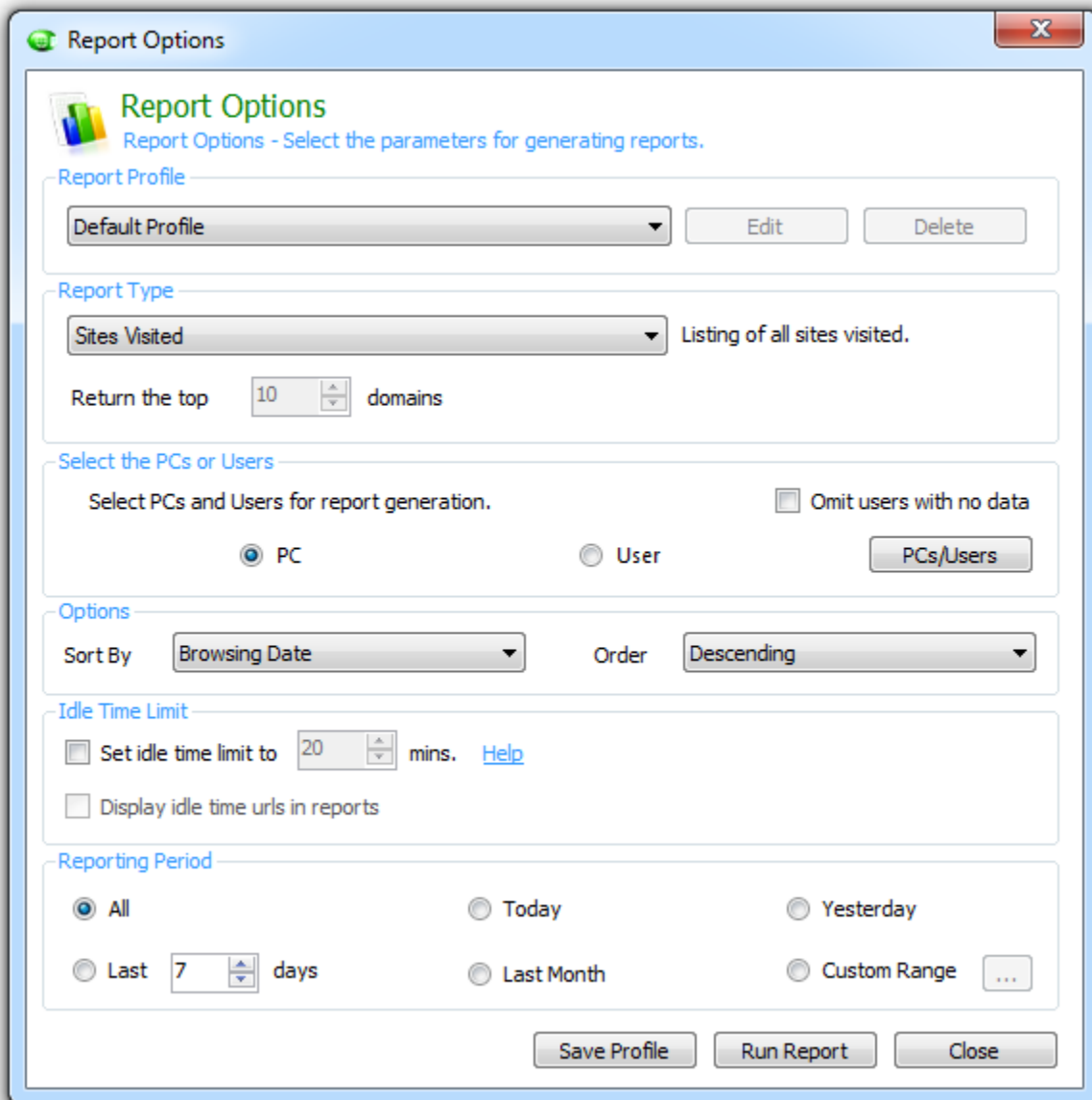
An overview of the BrowseReporter functions includes:

- **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.



Report Options

Report Options - Select the parameters for generating reports.

Report Profile

Default Profile

Report Type

Sites Visited Listing of all sites visited.

Return the top 10 domains

Select the PCs or Users

Select PCs and Users for report generation. ☐ Omit users with no data

☒ PC ☐ User

Options

Sort By Browsing Date Order Descending

Idle Time Limit

☐ Set idle time limit to 20 mins. [Help](#)

☐ Display idle time urls in reports

Reporting Period

☒ All ☐ Today ☐ Yesterday

☐ Last 7 days ☐ Last Month ☐ Custom Range ...

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.
- **Keyword Tracking (Hit):** Tracking of search engine keywords searched by your employees by the number of hits

- **Keyword Tracking (Time):** Tracking of search engine keywords and the date/time searched by your employees
- **Employee Productivity Report:** assign categories and websites that are productive or unproductive to your company, to access the overall efficiency of your employees.
- **Graph – Hourly Browsing Time:** a graphical display of the accumulated Internet browsing time for users for each hour of the day.
- **Graph – Weekly Browsing Time:** a graph that shows the accumulated Internet browsing time for users for each day of the week.
- **Graph – Top 10 Computers by 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 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 Hits:** 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 of your computer or user. Includes a tabular summary of time spent on each applications grouped into hourly basis. (N) is a number that you can define in the Report options..

4.3 Report Options

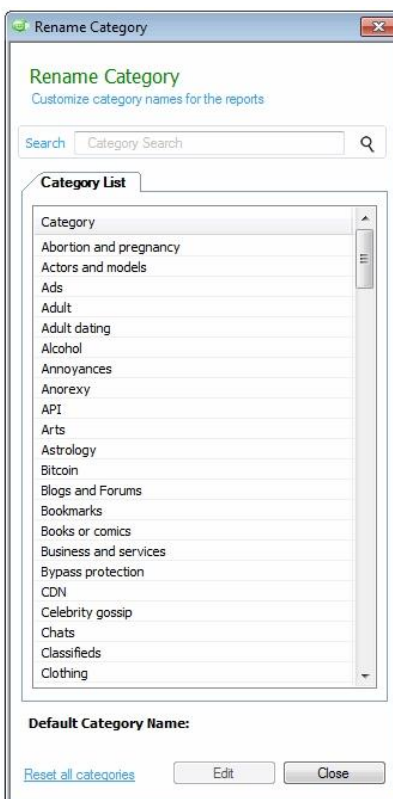
The BrowseReporter Report Options utility allows you to customize the report on the basis of specific criteria.

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)

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.

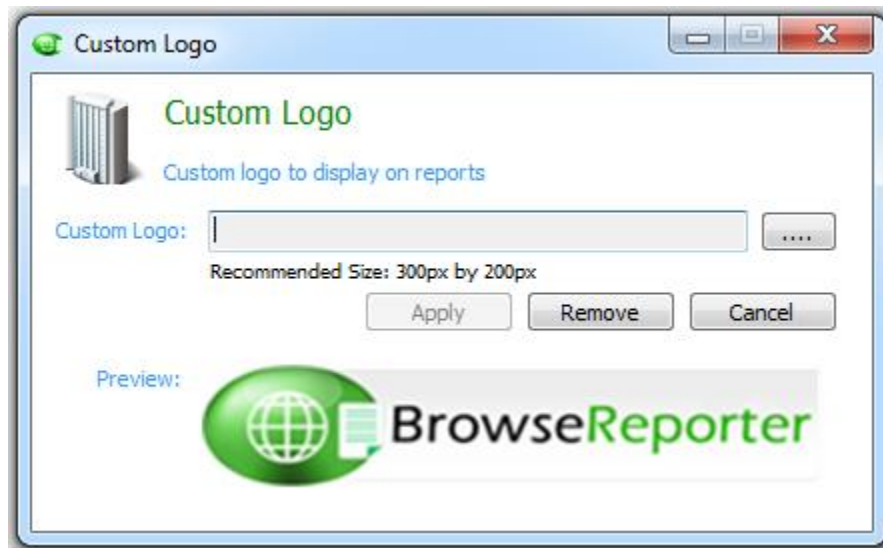
How to Manually Upload Data and disable Auto Upload

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.

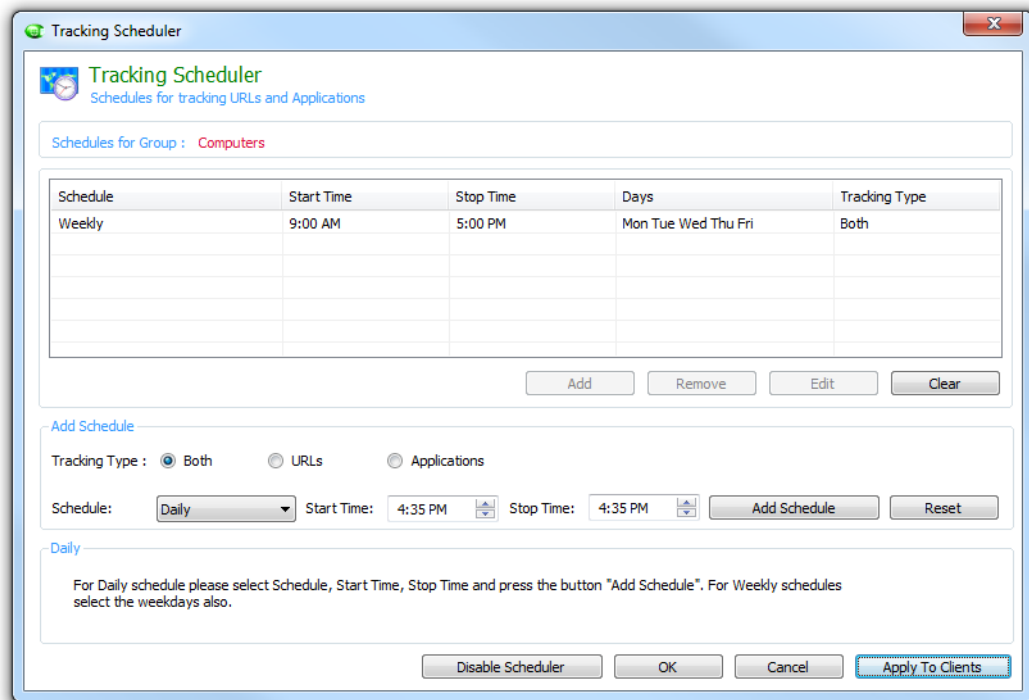
Through the URL Tracking Scheduler, you can schedule the date and time ranges for collecting the Internet browsing activity. Outside of these schedules, no browsing data will be collected. This also helps to maintain the database size. Below is an example of how to use the URL Tracking Scheduler.

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 clicking on **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 during the scheduled time.

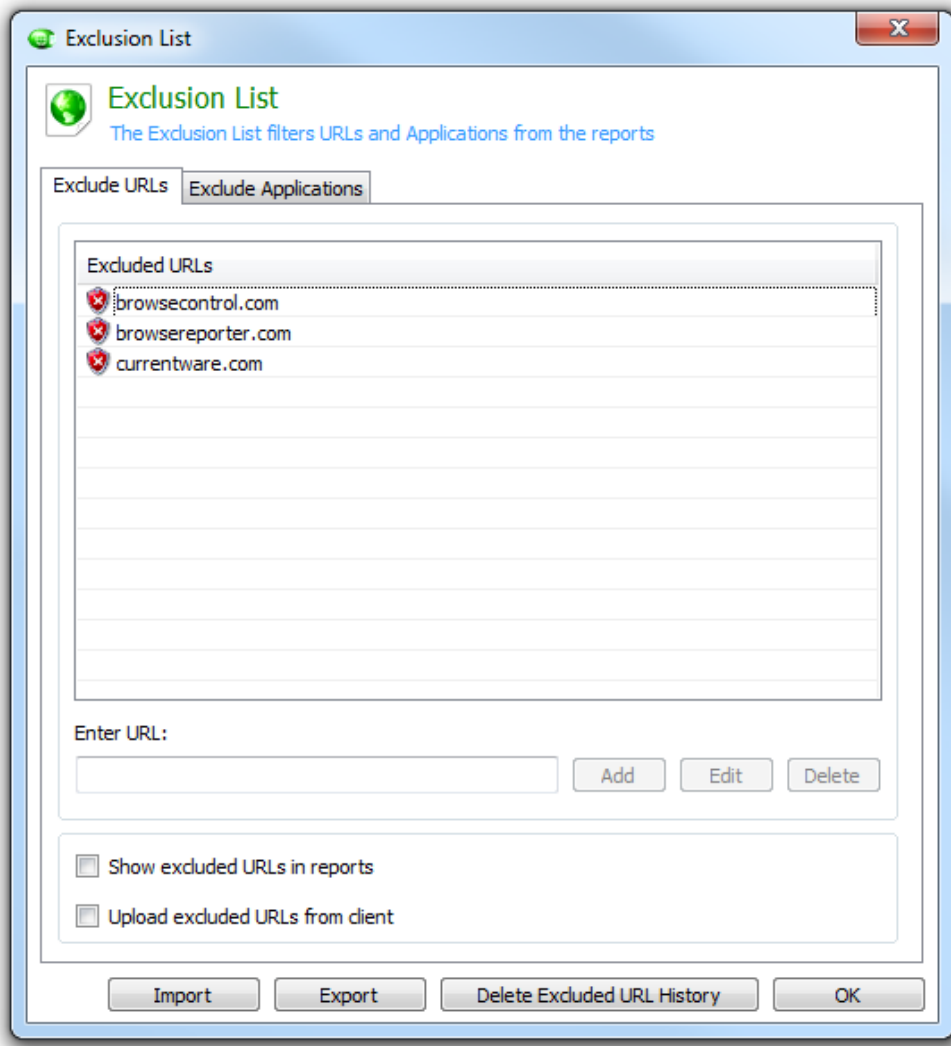


The URL Tracking Scheduler will only track Internet activity during the specified time range

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

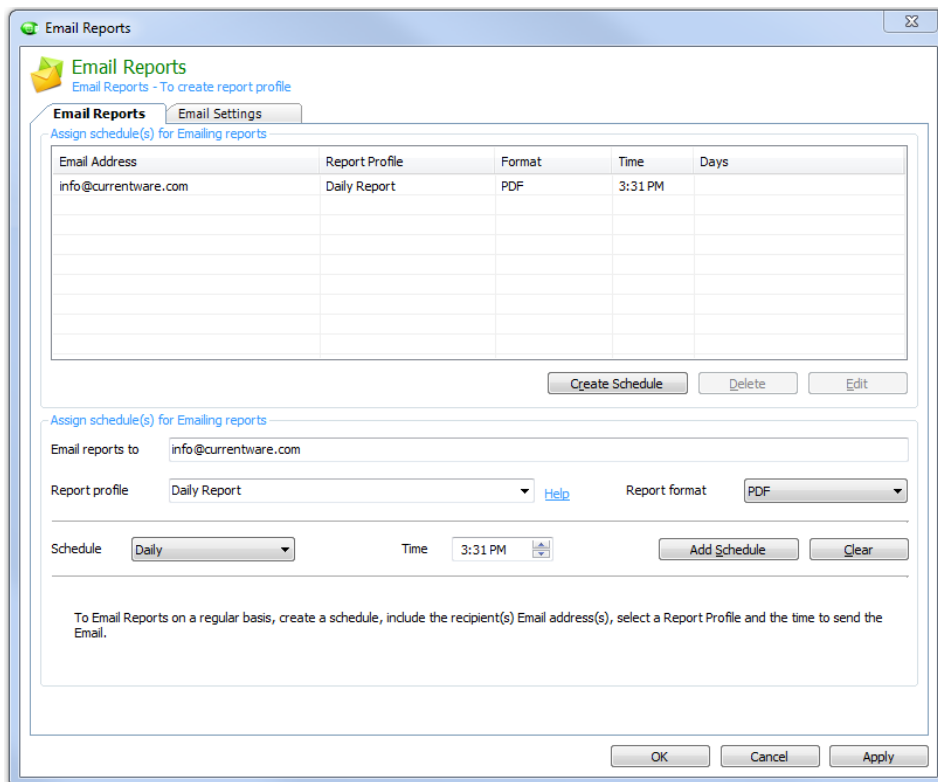
Through the Email Reports feature, the BrowseReporter reports can automatically be generated and emailed to the administrator periodically. This eliminates having to rely on the manual process of creating reports.

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

How to create a schedule for e-mail 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** to generate a report of your choice. A report profile is created in the Report Options menu item.
5. Define the **schedule type (daily or weekly)** of the email report.
6. Define the delivery **time** of the email report.
7. The Internet report will be sent in a PDF format.



Email Reports
Email Reports - To create report profile

Email Reports | Email Settings

Assign schedule(s) for Emailing reports

Email Address	Report Profile	Format	Time	Days
info@currentware.com	Daily Report	PDF	3:31 PM	

Create Schedule | Delete | Edit

Assign schedule(s) for Emailing reports

Email reports to:

Report profile: [Help](#) | Report format:

Schedule: | Time: | 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

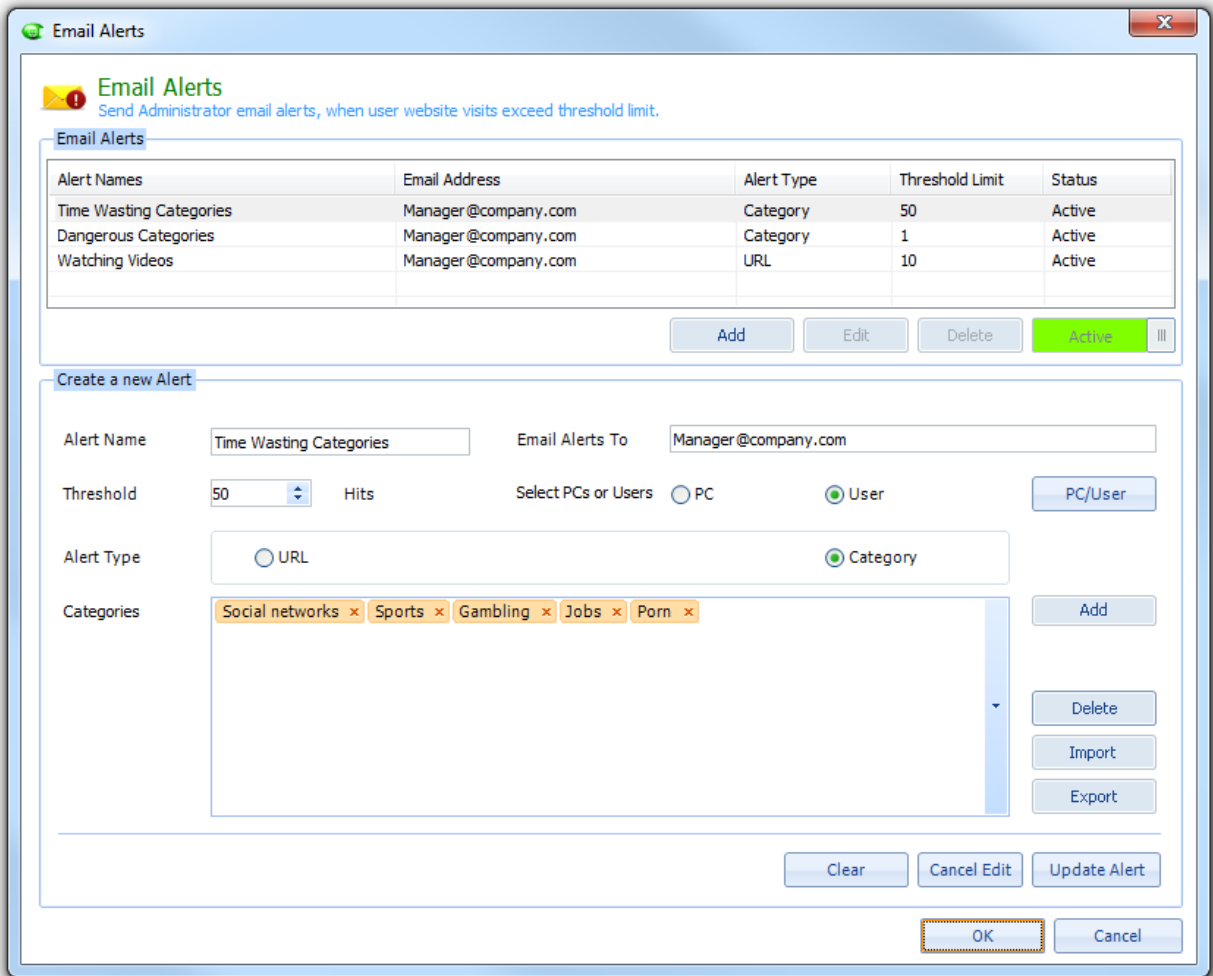
9.1 Email Alerts

Setup an email notification alert, every time a user exceeds a limit based off specific websites visited.

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

A message is immediately triggered to the authorities, 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.

Real time email alerts help you to respond immediately to excessive web abuse on valuable company time.



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: Social networks x Sports x Gambling x Jobs x Porn x

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:



The following computer or user has exceeded the URL threshold:

Alert Name: **Excessive Distractions**

Computer Name: **TORONTO**

User Name: **codework**

Domain Name: **espnfc.us**

URL Hit Count: **20**

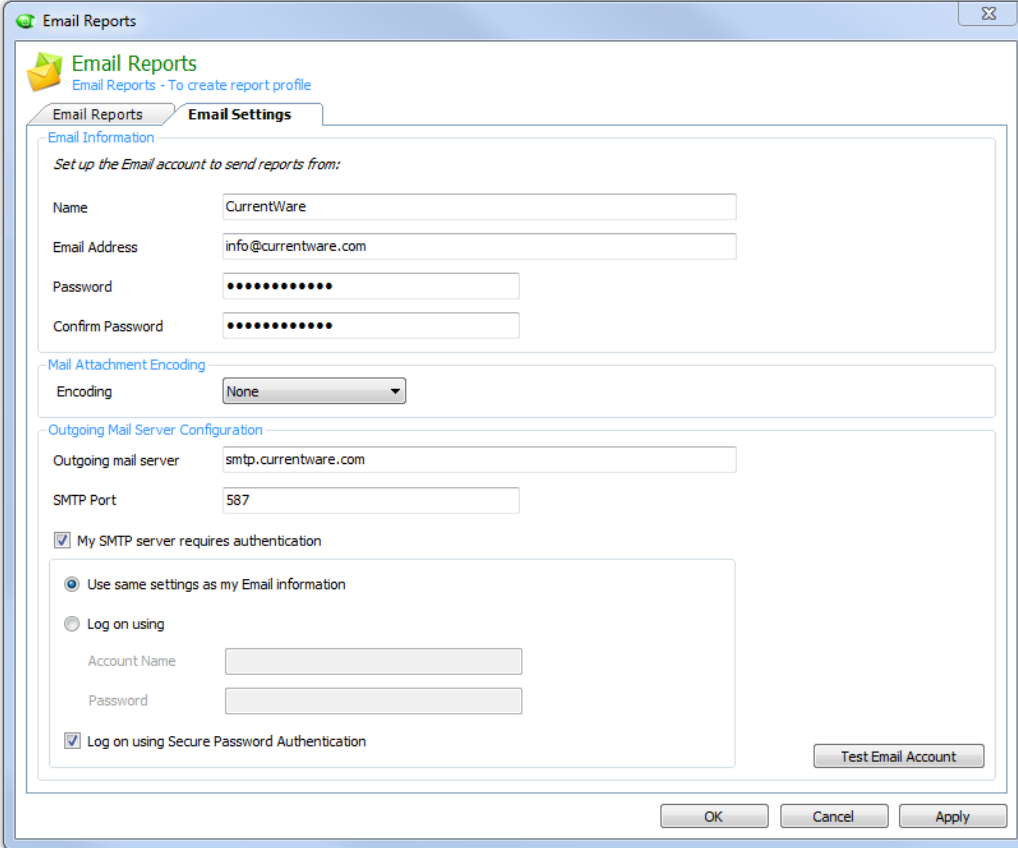
9.2 Email Settings

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



The image shows a screenshot of the 'Email Reports' application window, specifically the 'Email Settings' tab. The window has a title bar with the text 'Email Reports' and a close button. Inside the window, there is a sub-header 'Email Reports' with a small icon and the text 'Email Reports - To create report profile'. Below this, there are two tabs: 'Email Reports' and 'Email Settings', with 'Email Settings' being the active tab. The 'Email Settings' tab contains three main sections: 'Email Information', 'Mail Attachment Encoding', and 'Outgoing Mail Server Configuration'. The 'Email Information' section has a sub-header 'Set up the Email account to send reports from:' and four input fields: 'Name' (CurrentWare), 'Email Address' (info@currentware.com), 'Password' (masked with dots), and 'Confirm Password' (masked with dots). The 'Mail Attachment Encoding' section has a sub-header 'Mail Attachment Encoding' and a dropdown menu for 'Encoding' set to 'None'. The 'Outgoing Mail Server Configuration' section has a sub-header 'Outgoing Mail Server Configuration' and two input fields: 'Outgoing mail server' (smtp.currentware.com) and 'SMTP Port' (587). Below these fields, there is a checkbox 'My SMTP server requires authentication' which is checked. Under this checkbox, there are two radio buttons: 'Use same settings as my Email information' (selected) and 'Log on using'. The 'Log on using' option has two input fields: 'Account Name' and 'Password'. At the bottom of the 'Outgoing Mail Server Configuration' section, there is a checkbox 'Log on using Secure Password Authentication' which is checked. A 'Test Email Account' button is located at the bottom right of the 'Outgoing Mail Server Configuration' section. At the bottom of the window, there are three buttons: 'OK', 'Cancel', and 'Apply'.

Email Reports

Email Reports - To create report profile

Email Reports Email Settings

Email Information

Set up the Email account to send reports from:

Name CurrentWare

Email Address info@currentware.com

Password

Confirm Password

Mail Attachment Encoding

Encoding None

Outgoing Mail Server Configuration

Outgoing mail server smtp.currentware.com

SMTP Port 587

☒ My SMTP server requires authentication

☒ Use same settings as my Email information

☐ Log on using

Account Name

Password

☒ Log on using Secure Password Authentication

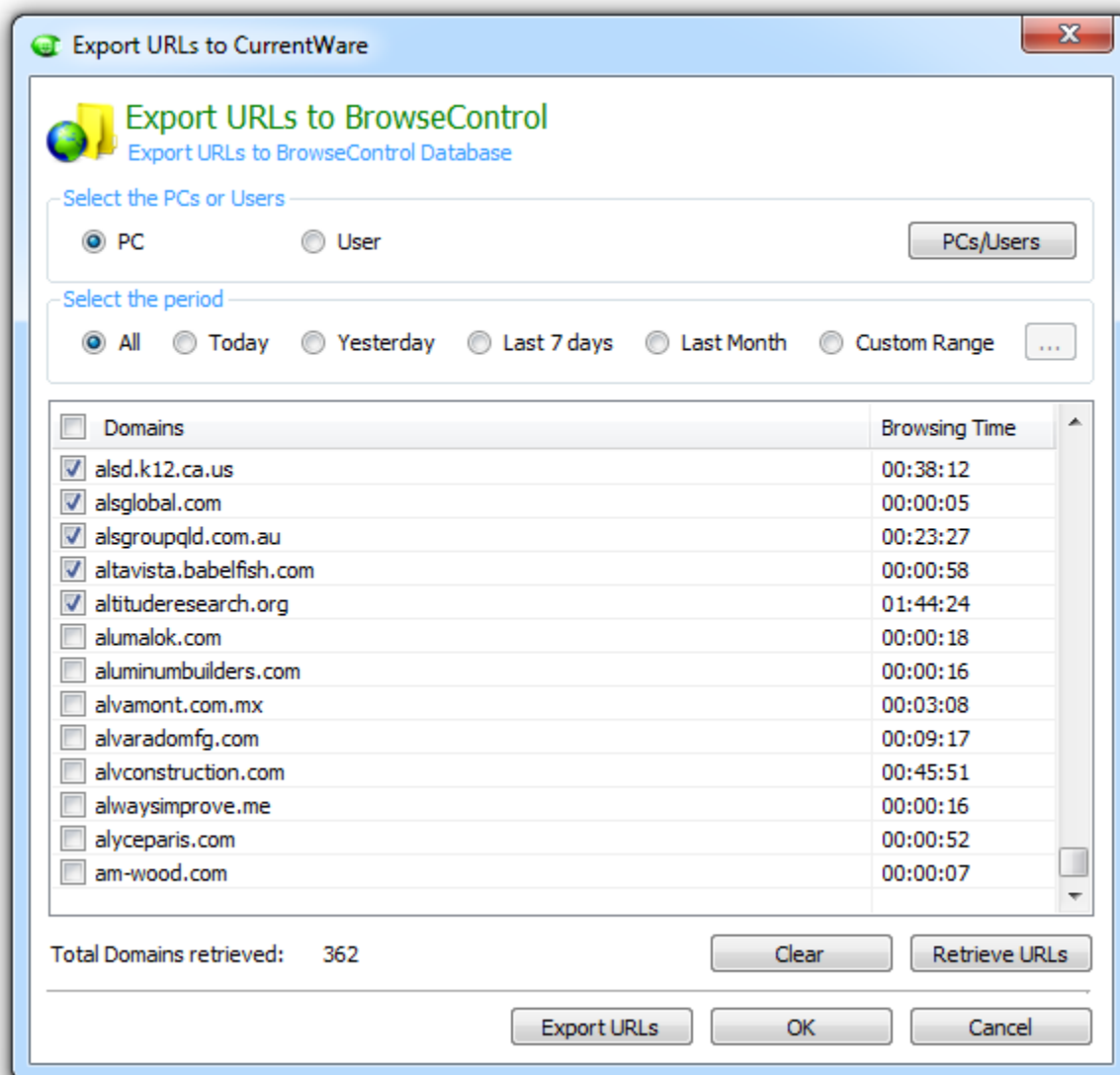
Test Email Account

OK Cancel Apply

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's 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.



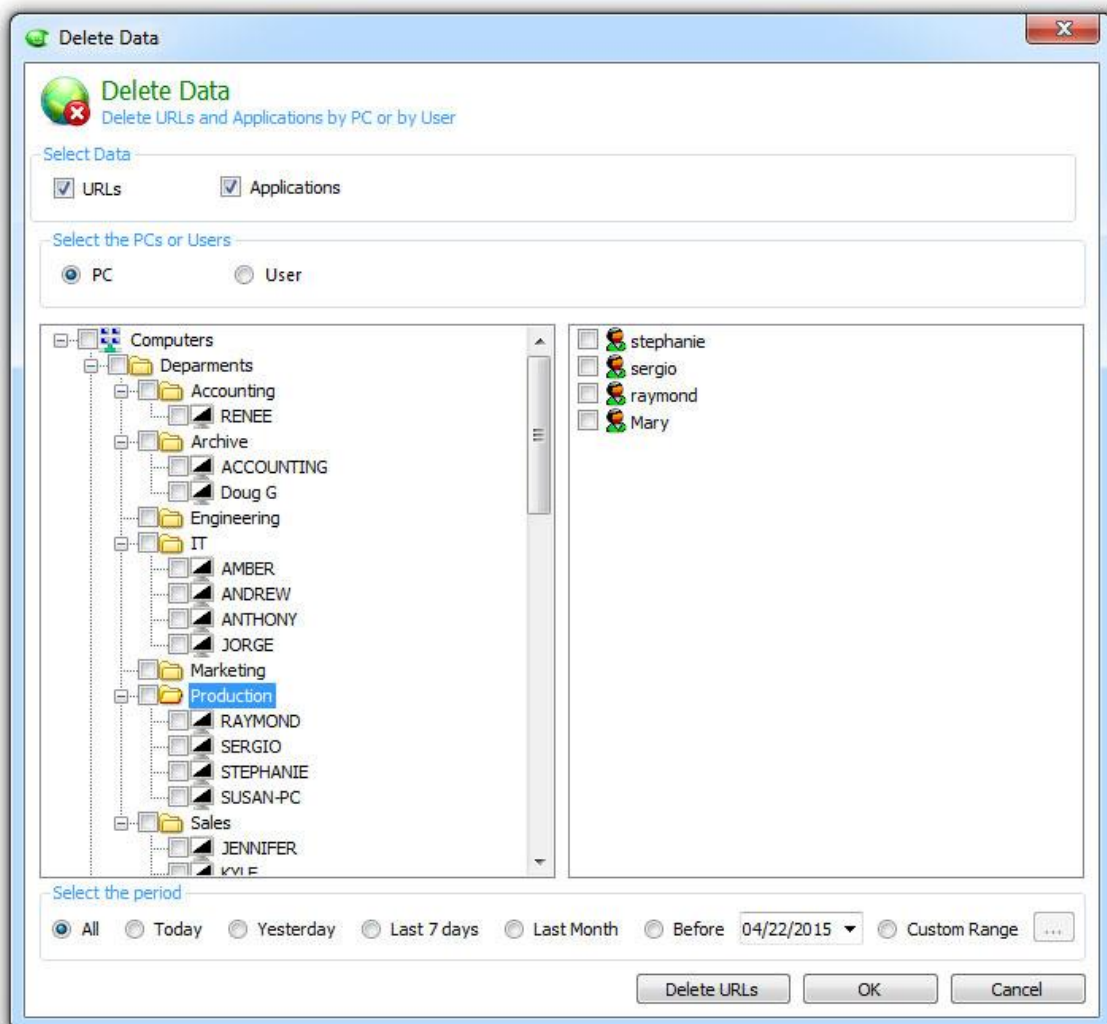
Export the URL directly to the BrowseControl URL filter

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.

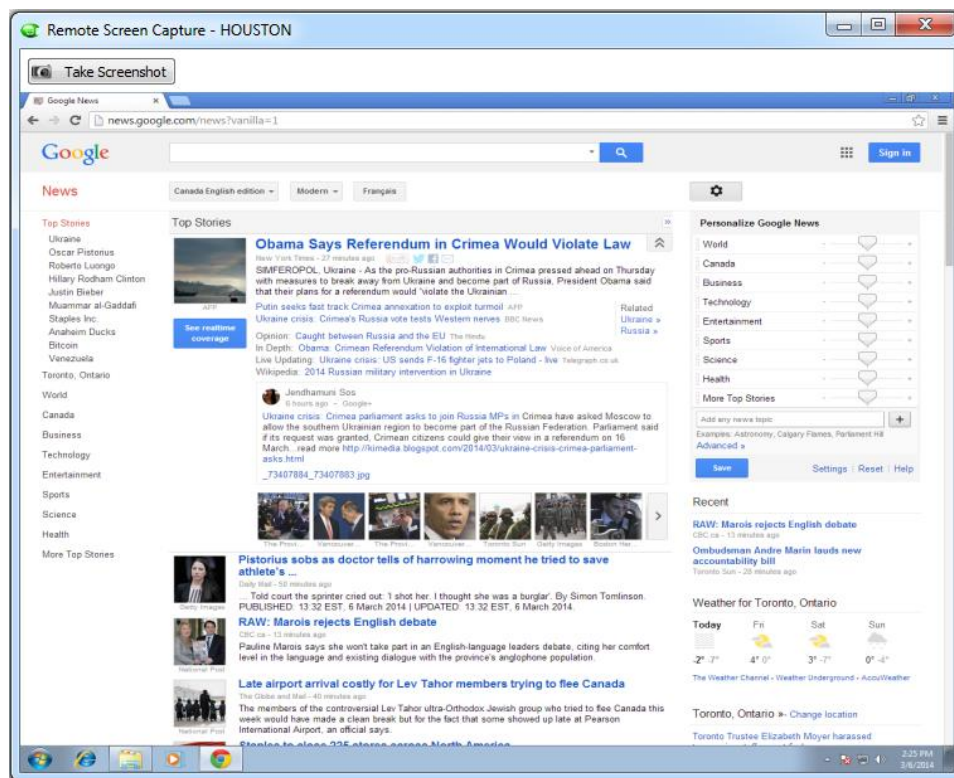
To take a screenshot for future references, simply click on the "Take Screenshot" button and type in the file name and file directory you want to save the screenshot at.

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

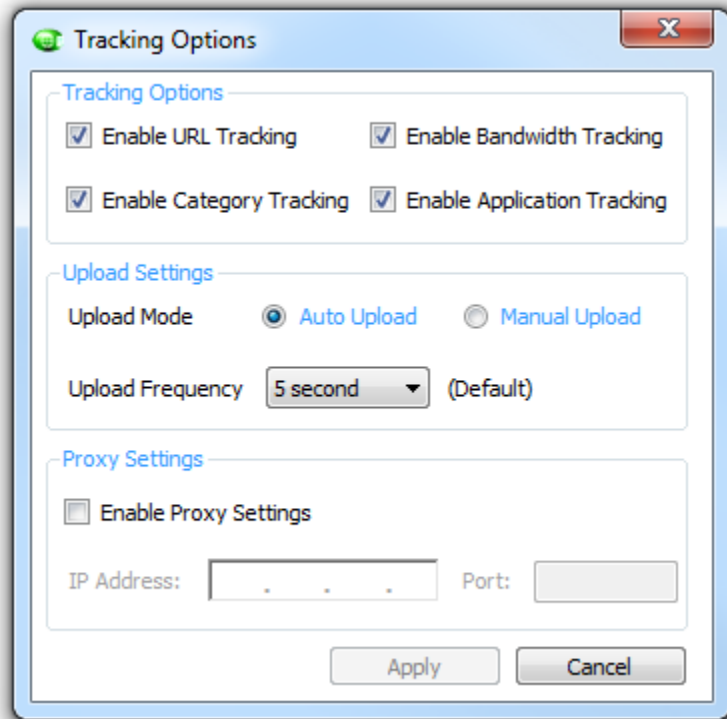
Note: ensure that port 1024 is open on the client system, to allow for screen capturing.



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.



13.1 Tracking Options

Toggle the tracking status of BrowseReporter

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

NOTE: Bandwidth Tracking is not enabled by default. Open the Tracking Option and enable this option if you would like to keep track of bandwidth traffic on your network.

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

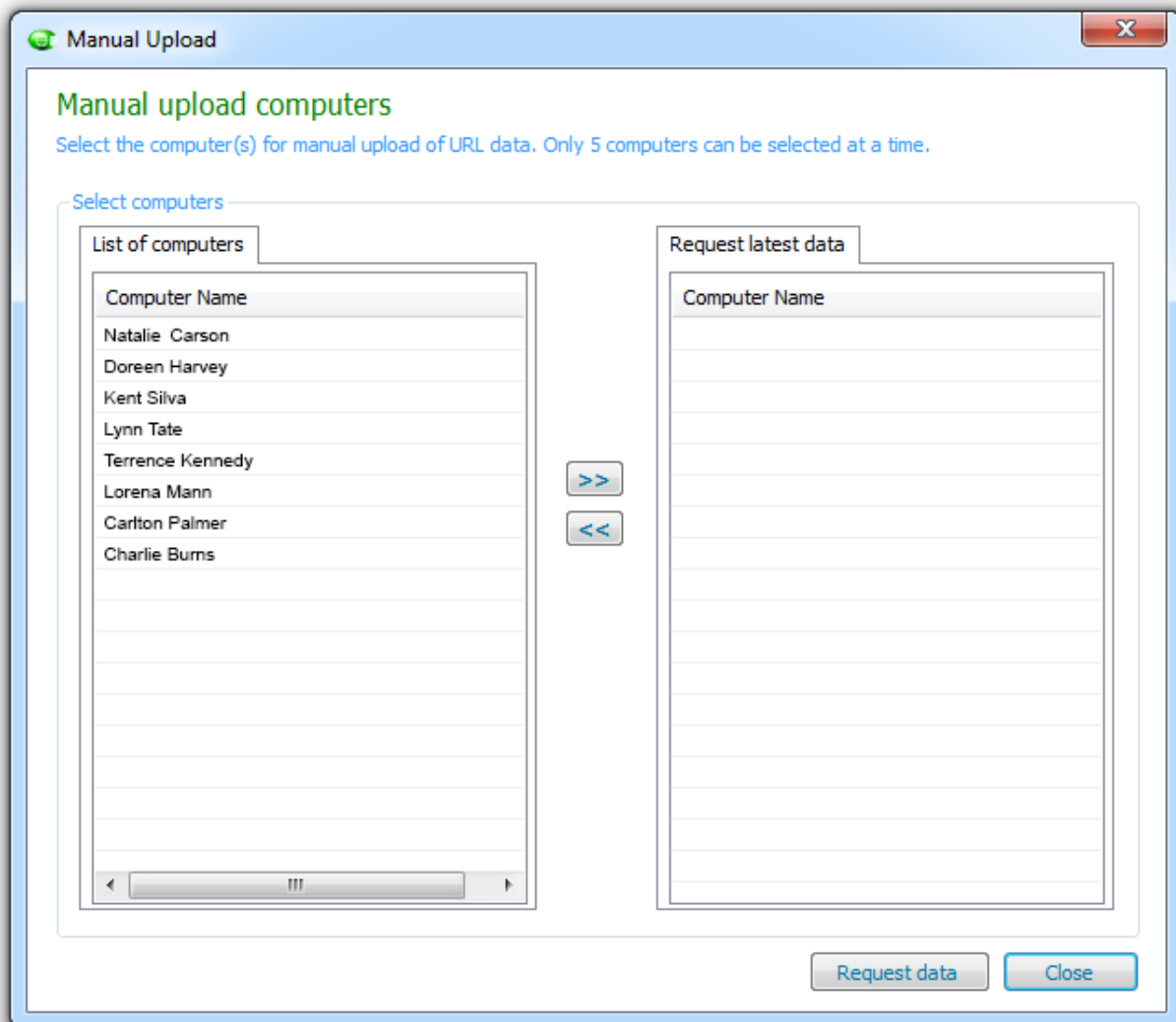
Auto upload will automatically upload data from the CurrentWare Client to the CurrentWare Server in cycles. The interval is defined by the **Upload frequency** (in minutes)

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.

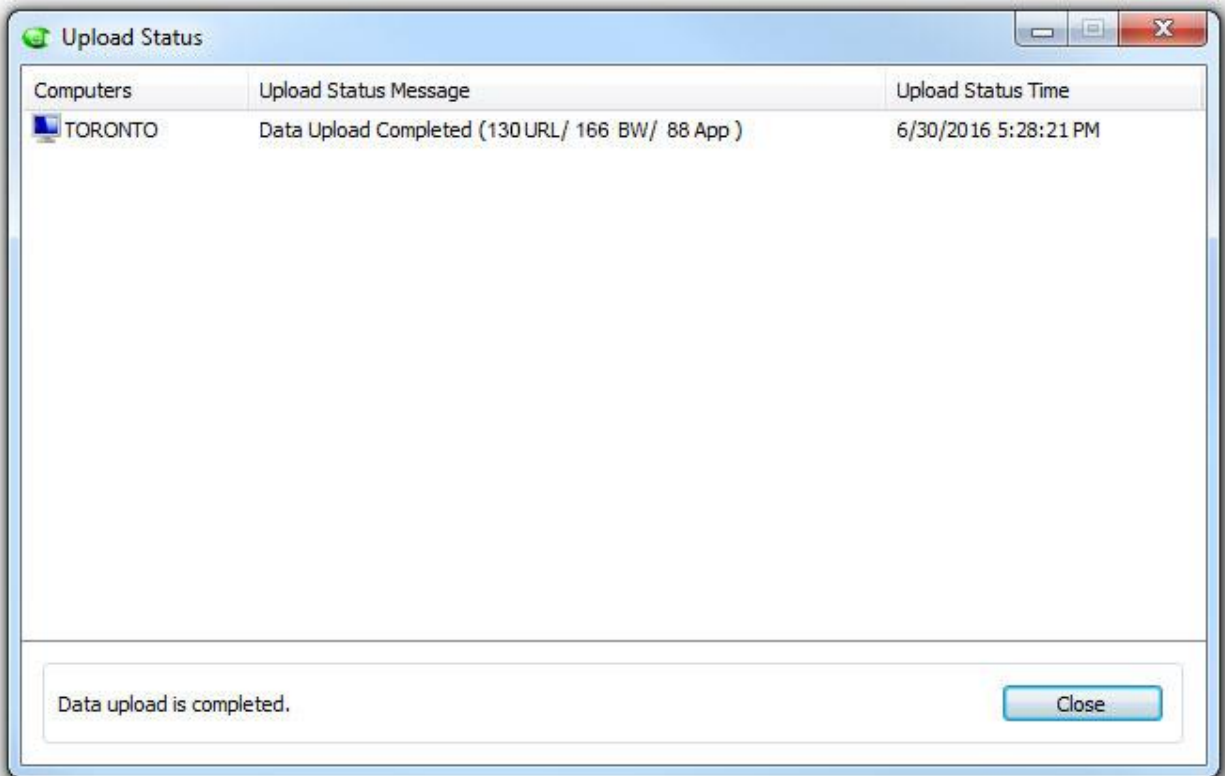
This option is suitable for large network to reduce bandwidth bottleneck. Since auto upload will automatically upload data from all the computers, resulting in all the client computers connecting to the Server at once. Manual upload give the administrator control on which group of computers to perform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

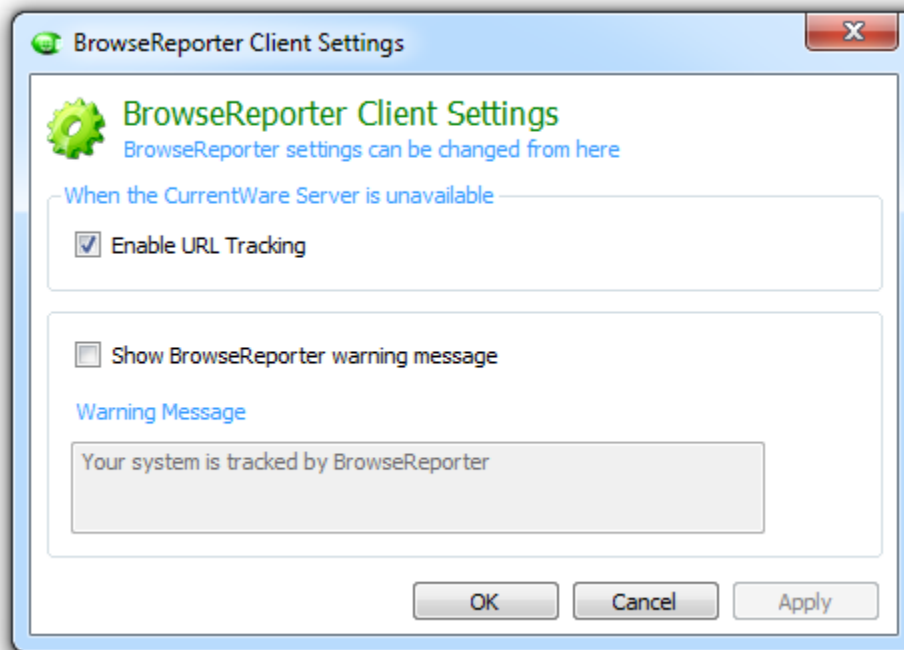
BrowseReporter will still track the Internet activities of a workstation if the CurrentWare Server is unavailable.

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

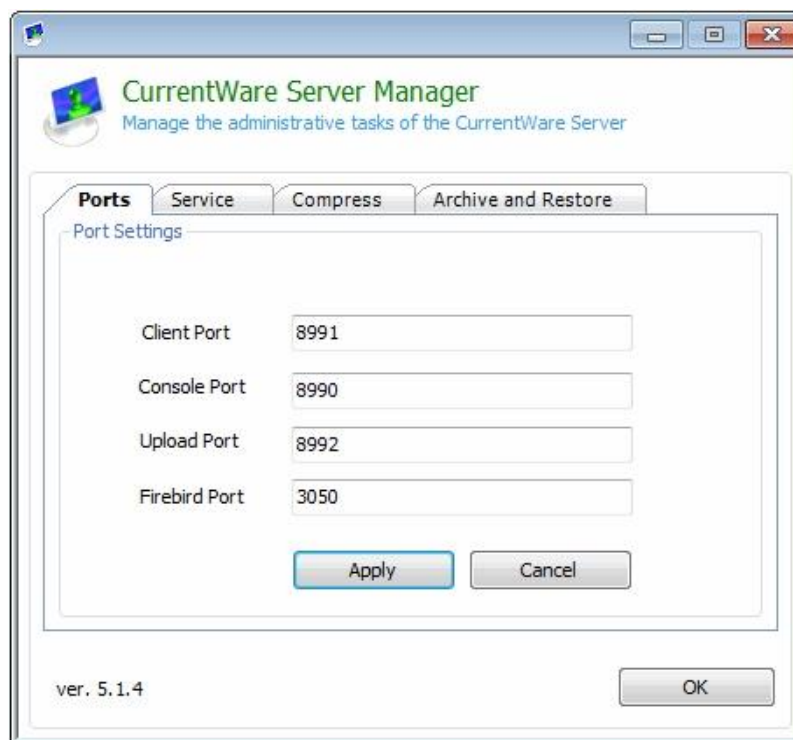
The CurrentWare Server Manager is used to manage the administrative tasks of the CurrentWare Server.

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.

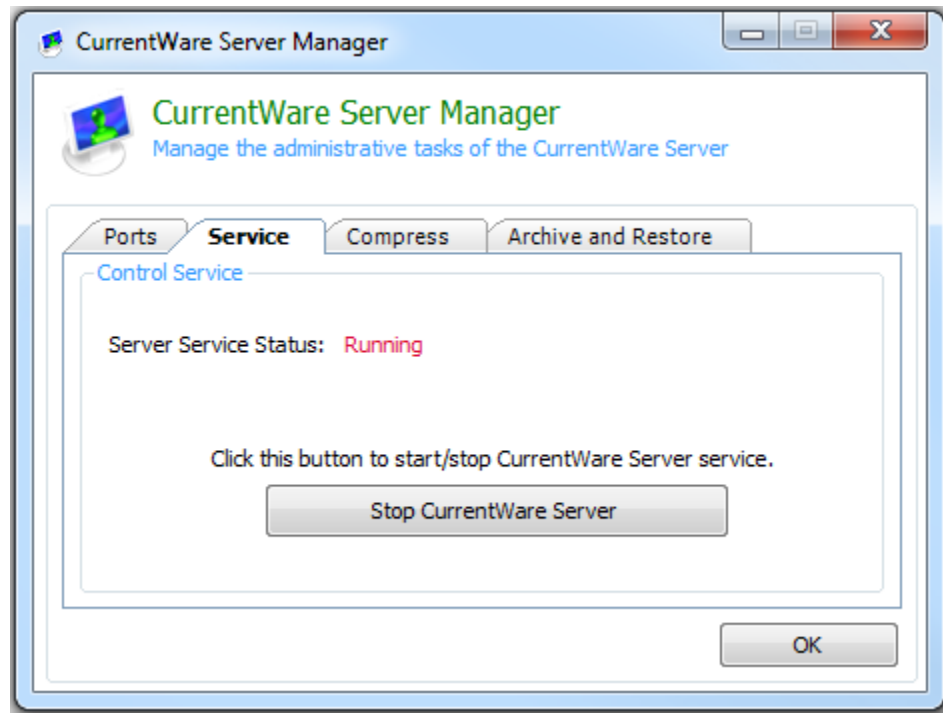
The default ports are listed in the screenshot below.



CurrentWare Server Manager

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 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.

15.4 Archive and Restore the CurrentWare Database

In order to maintain optimal database performance, it is recommended that the CurrentWare database be archived on a regular basis. 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.

16.0 Licensing

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

The evaluation copy of BrowseControl 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.

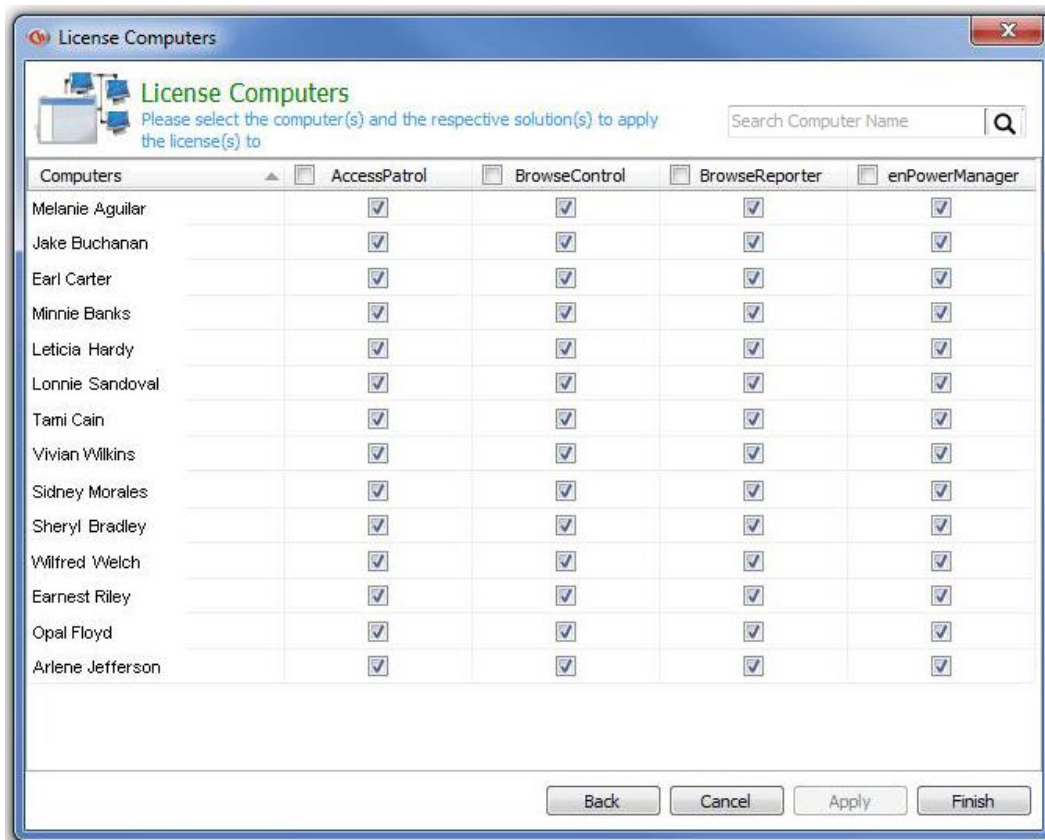
16.2 License Management

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

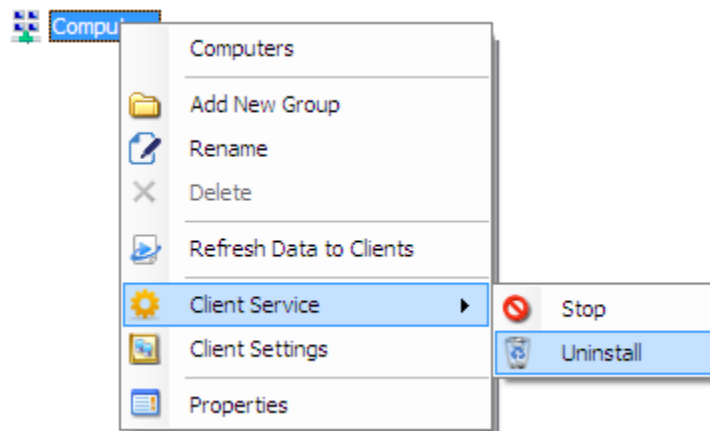
The CurrentWare Client can be uninstalled by three different methods:

- **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\System32\Cwclient.exe -p Admin -u

For 64-bit Windows PC

C:\Windows\SysWOW64\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 (for 32-bit computers) or C:\Windows\SysWOW64 (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

For technical support of CurrentWare, please contact us at info@currentware.com.

20.0 Contacts

USA

CurrentWare (a division of 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

CANADA

CurrentWare (a division of Codework Inc.)

55 Hawktree Ridge, Ottawa, K2J 5N7, Canada

Tel: 613-368-4300

Fax: 866-929-9808

Email: info@currentware.com

EUROPE

CurrentWare (a division of Codework Inc.)

55 Hawktree Ridge, Ottawa, K2J 5N7, Canada

Tel: 613-368-4300

Fax: 866-929-9808

Email: 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

OTHER COUNTRIES

Please email info@currentware.com for the name of a local reseller in your country.