User Guide

Revised in Oct, 2019

BrowseControl

Version 5.4.2

Web Filtering Software

BrowseControl User Guide - Table of Contents

1.0 Introduction to BrowseControl

BrowseControl is an easy to use **Web Filtering software** that restricts Internet access and enforces web usage policies across your network.

From a centralized Console, you can enable and disable Internet access of your employees or students instantly.

Use the **Blocked List** to block access to time wasting websites such as Facebook.com, Youtube.com and Netflix.com. To enforce stricter access, use the **Allowed List** to allow your users to only browse to authorized websites.

BrowseControl Web Filter is effective at filtering both HTTP and HTTPS sites. Use the Internet scheduler to choose when you would like to block Internet access.

BrowseControl comes with an **Application Blocker**. Eliminate the distractions from applications that are unnecessary time wasters. Block these applications to focus on aligning your users to your business goals.

This guide will help you better understand the features of BrowseControl and assist you in configuring your network to restrict Internet access.

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 Window'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:

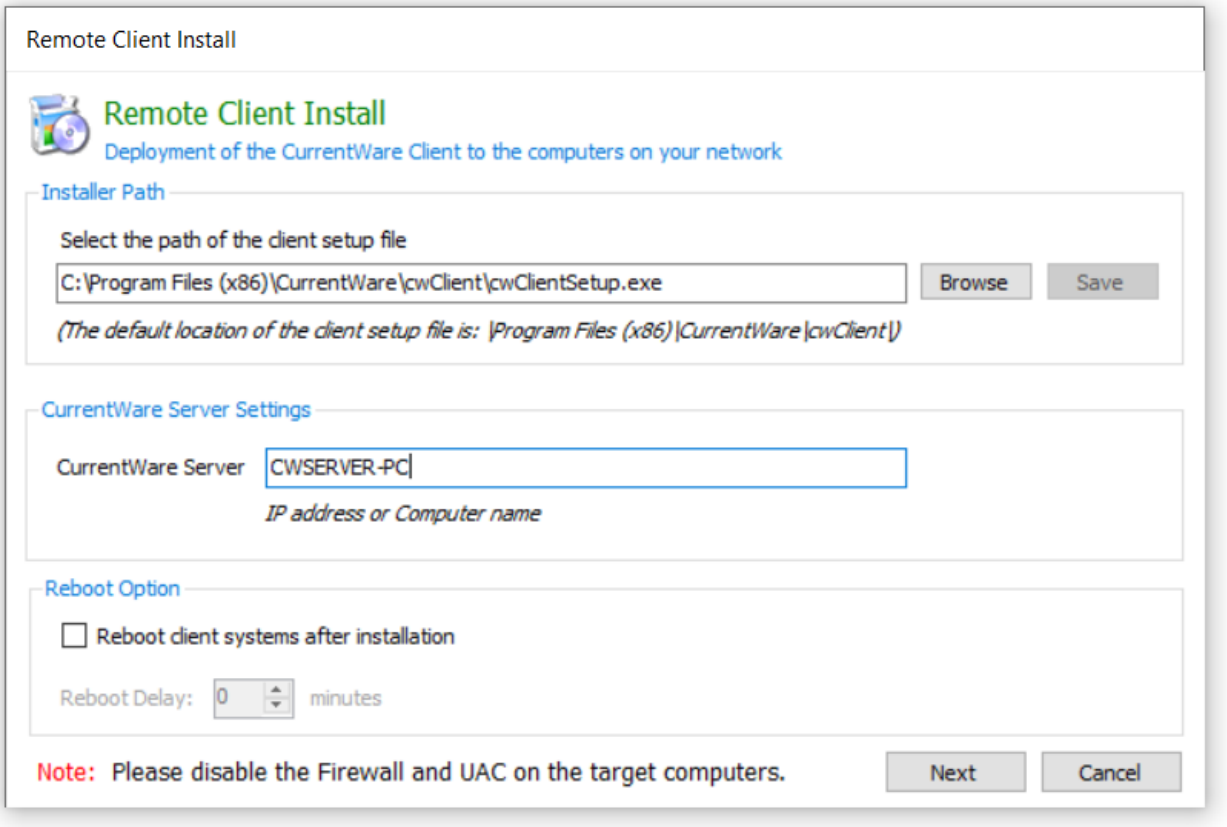
- Disable UAC (User Account Control) and Windows Firewall on the client computers

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 of 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.



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 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 cwClientSetup.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)**
- **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.

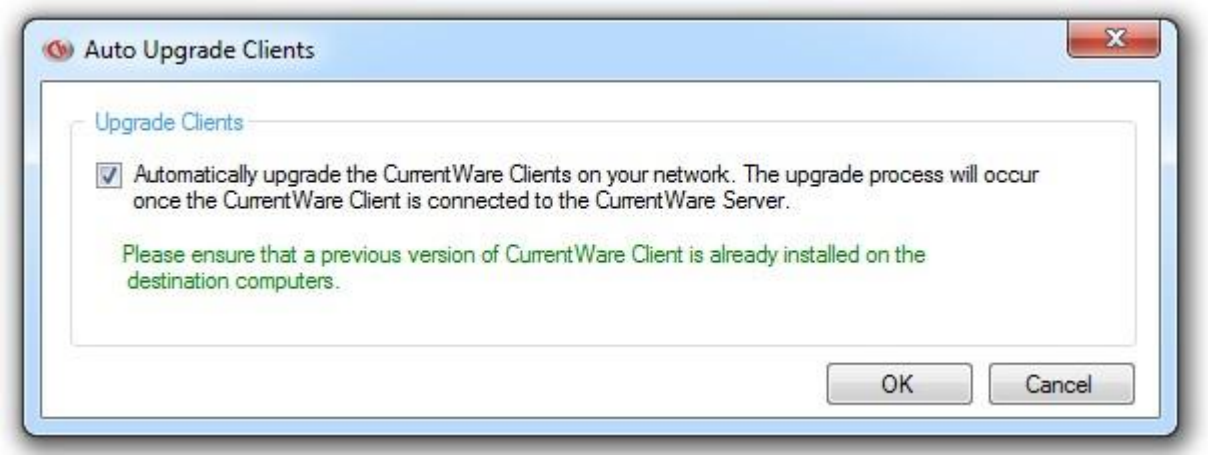
1.6 Upgrading the CurrentWare Clients

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.

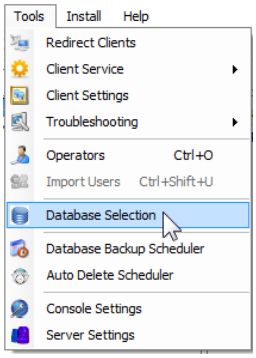
1.7.3 Password Protect the CurrentWare Console

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.

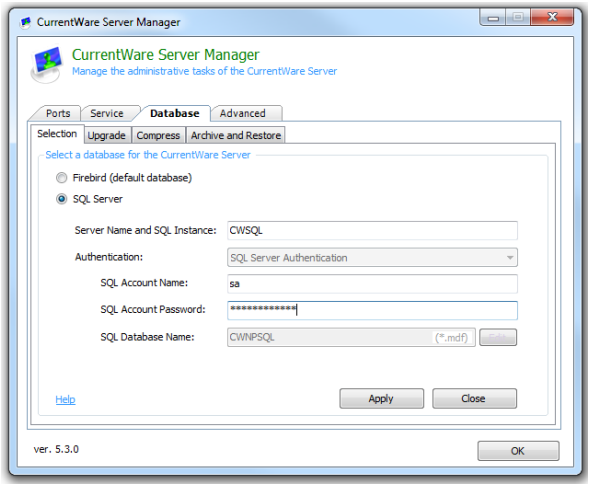
1.8 Connecting CurrentWare to your SQL server

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.

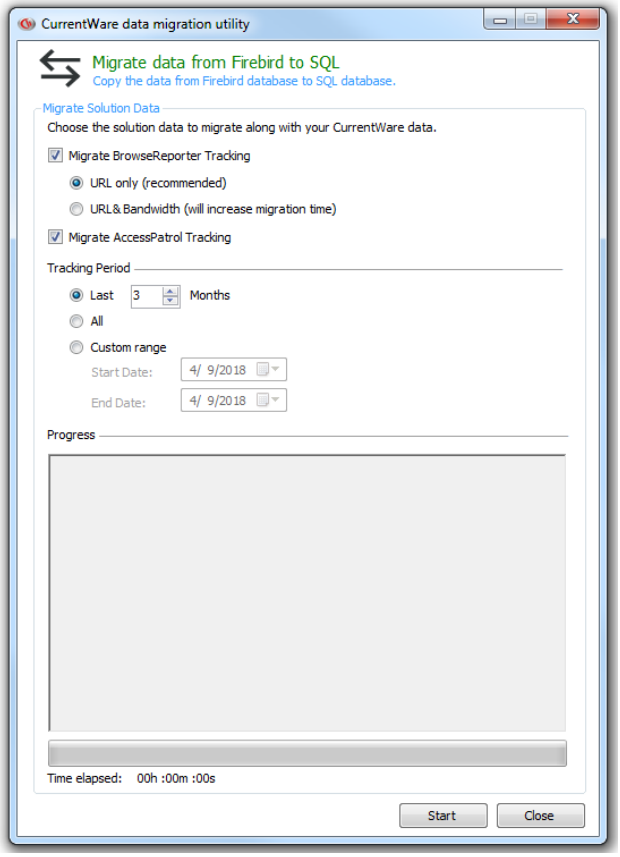
1.8.1 Migrating your Existing CurrentWare Data from Firebird to SQL Server

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.

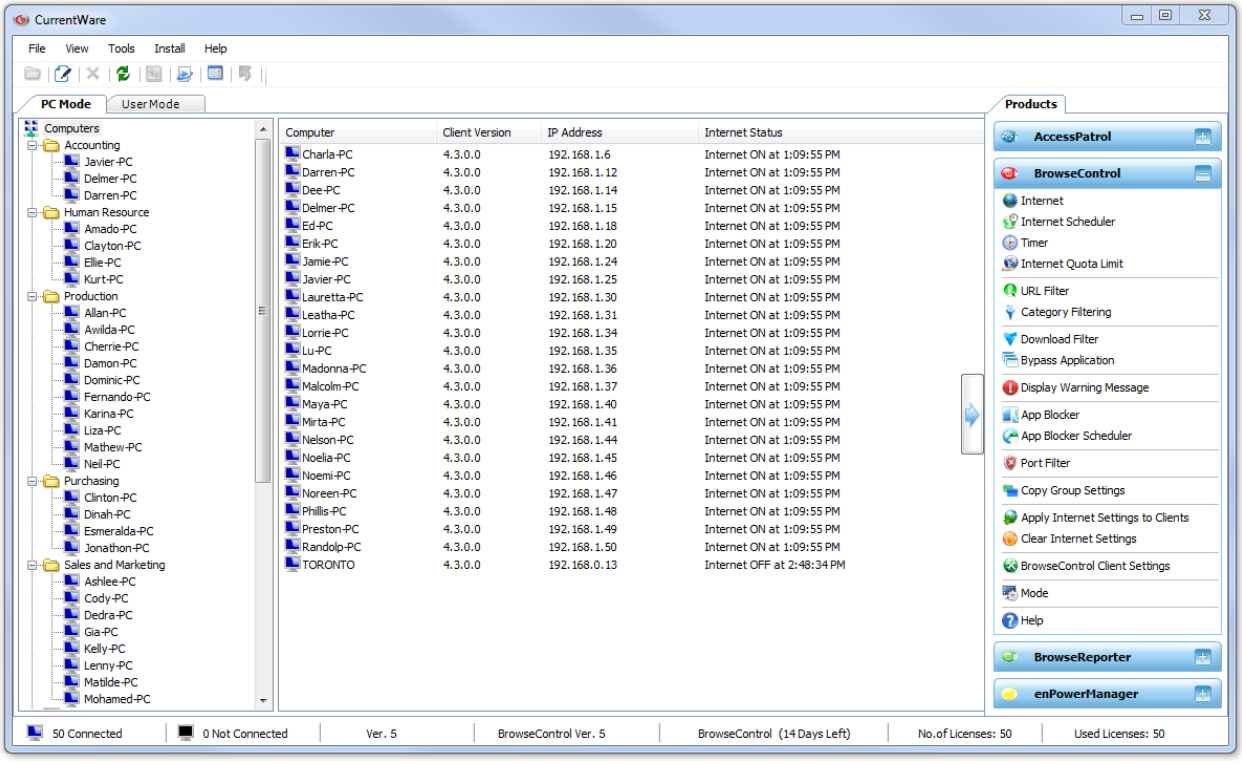


2.0 CurrentWare Console Overview

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.

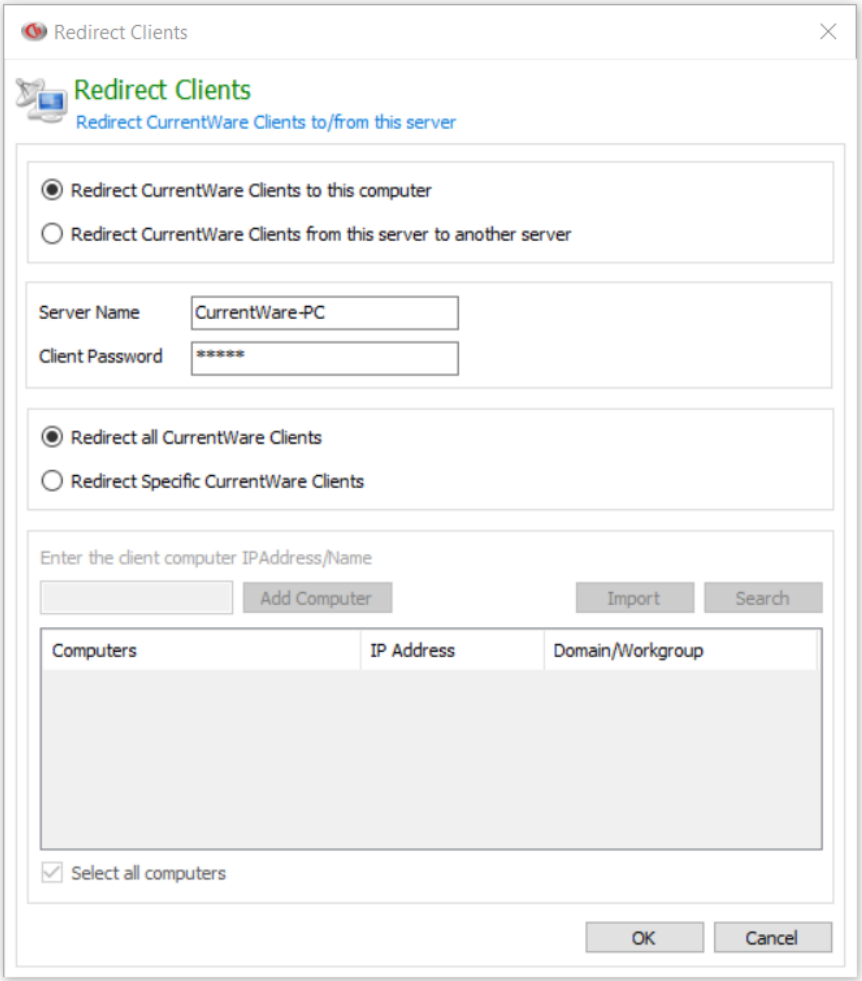
On the CurrentWare Console menu, select **File > Move Computer/Users**. The left-hand side contains the source folder and the right hand side contains the destination folder. Select the computer(s) you want to move from the source folder, and then select the destination folder. Click on the **>>** button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

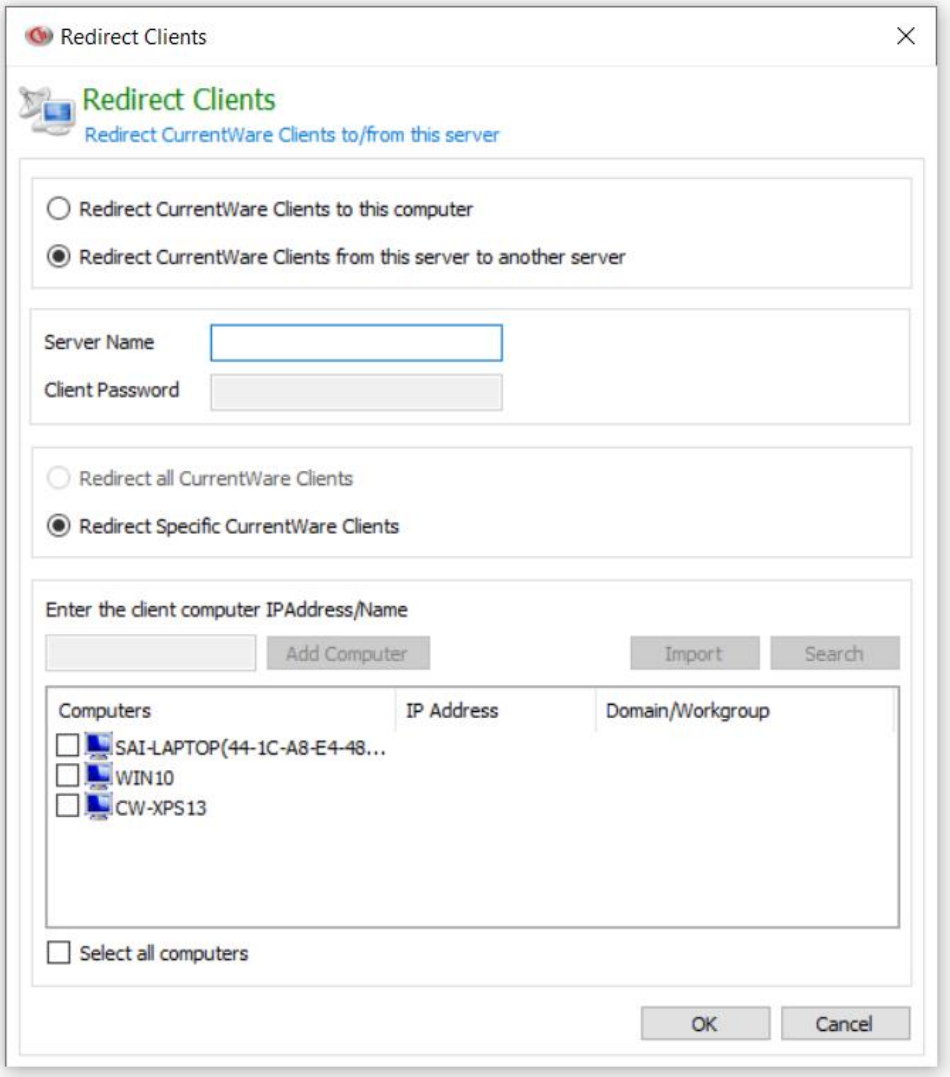
1. On the new CurrentWare Server, launch the CurrentWare Console and access the menu **Tools > Redirect Clients**.
2. Select the option **Redirect CurrentWare Clients to this computer**
3. Enter the CurrentWare Client password. The default password is Admin
4. Select Redirect All CurrentWare Clients.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



Redirect 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 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

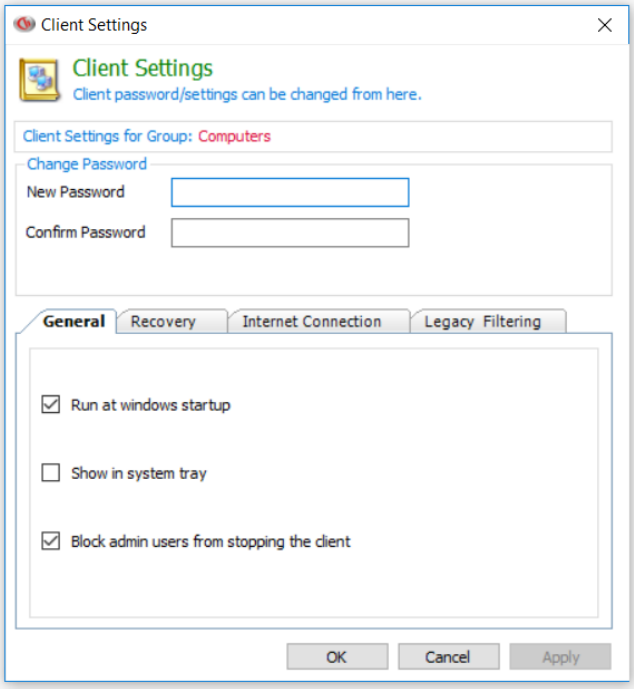
Put in the new CurrentWare Client password to replace the existing CurrentWare Client password. You will need to use the CurrentWare client password if you want to change the client settings, such as IP address or computer name of the CurrentWare Server or the port that the client uses to connect to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

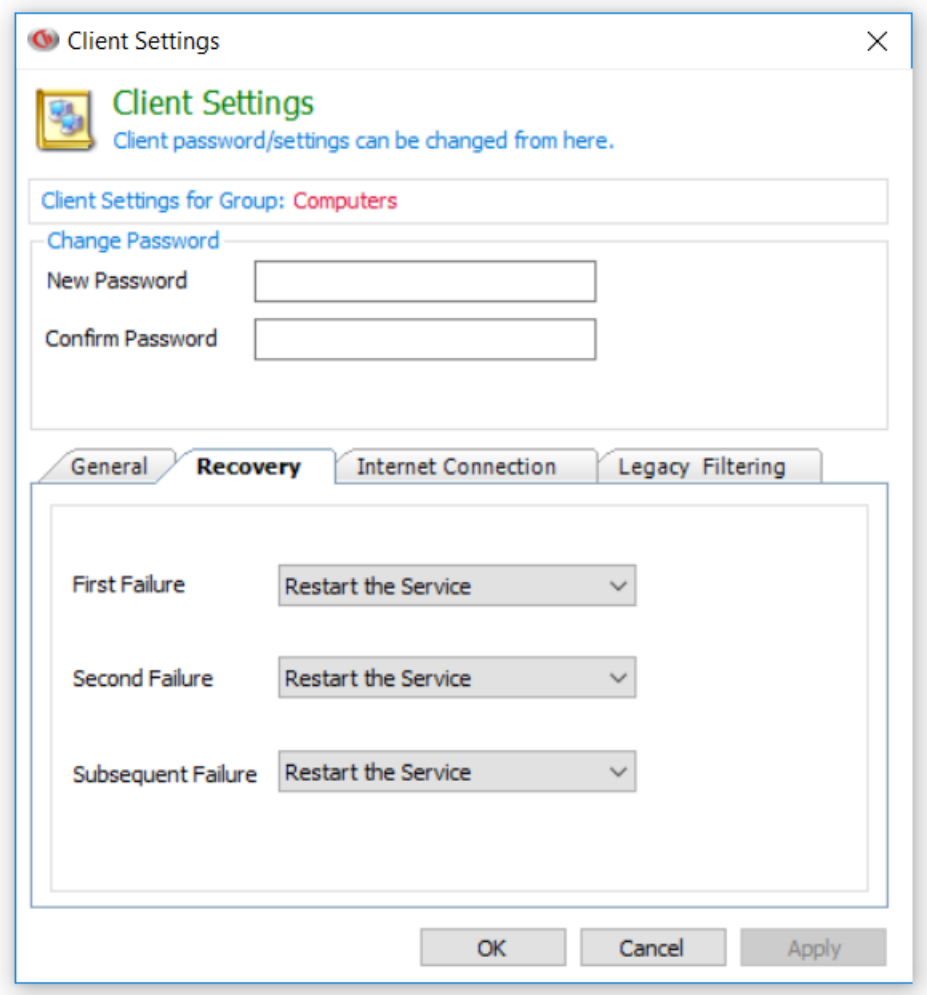
- **Show in System Tray:** toggle the option to display the CurrentWare icon in the system tray. When this option is enabled, the administrator can double click on the icon, put in the password, to access the CurrentWare Client configuration window.

- **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

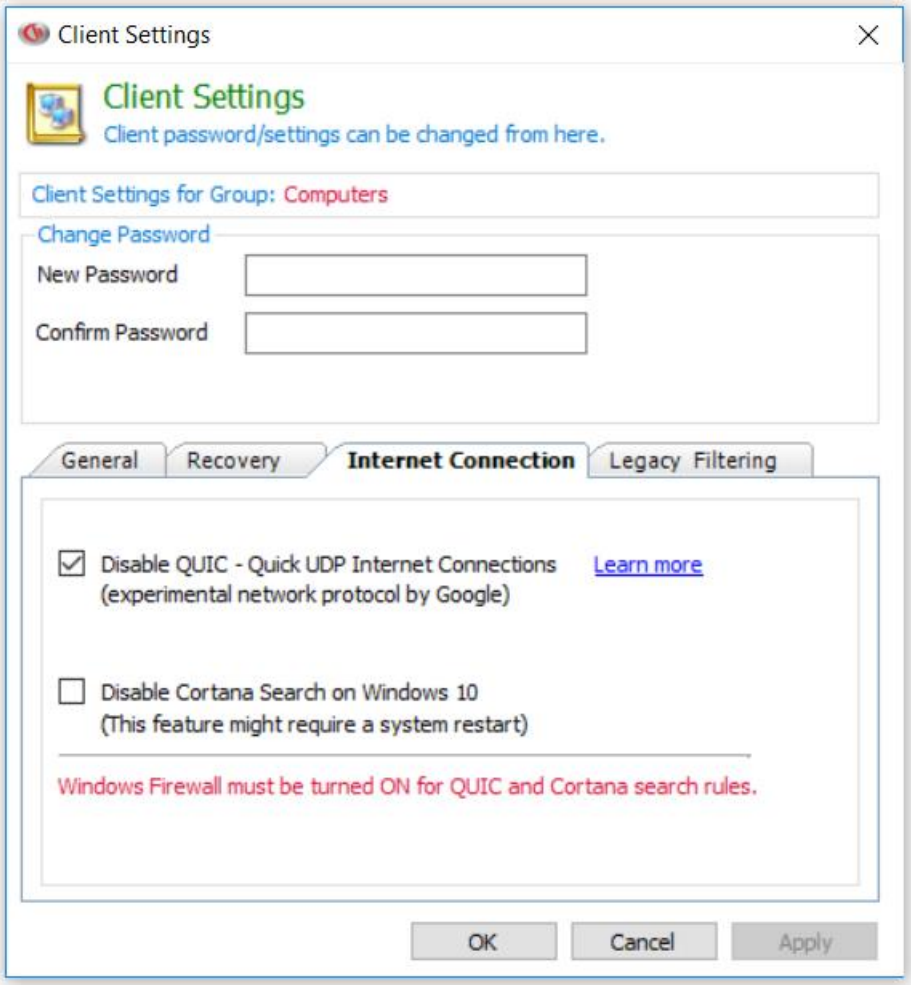
- The recovery option is for the property of the CurrentWare Client. By default, the option is set to “Restart the Service”. If the CurrentWare Client service was stopped by Windows or software, the default action would be for the Client to restart itself so it can continue to operate. It is best practice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



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.

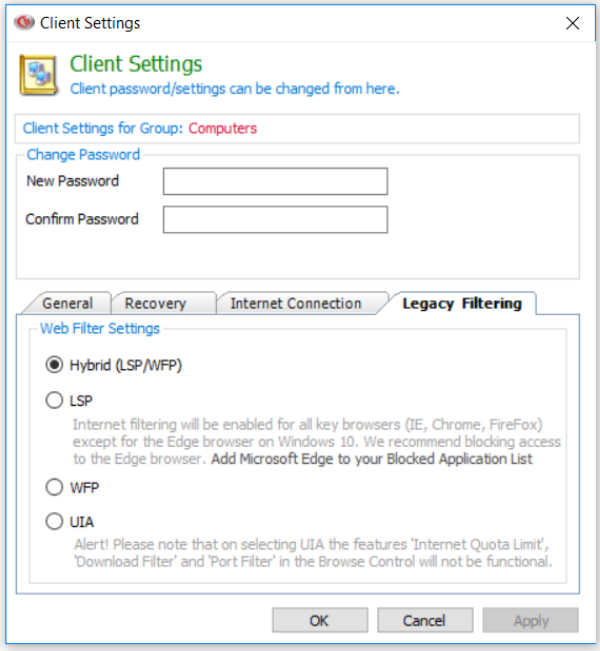
  - **HTTPS Settings = Simple:** All web filtering (HTTP/HTTPS) in WFP.
  - **HTTPS Settings = Advanced:** All web filtering (HTTP/HTTPS) in UIA.

- **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.

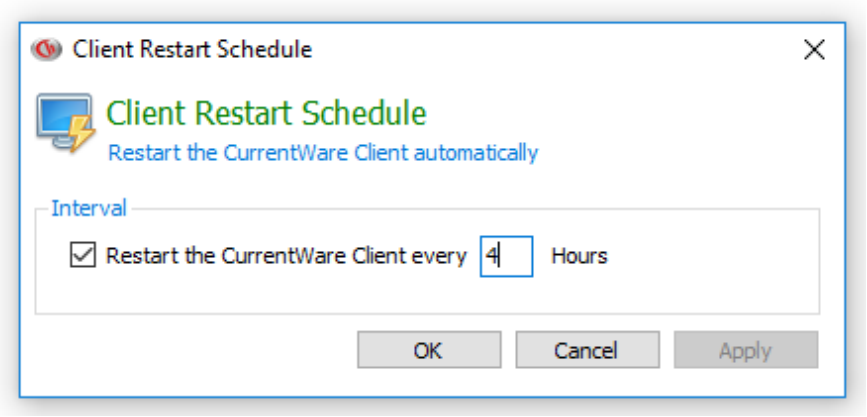


2.4 Troubleshooting

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

NOTE: Enabling 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

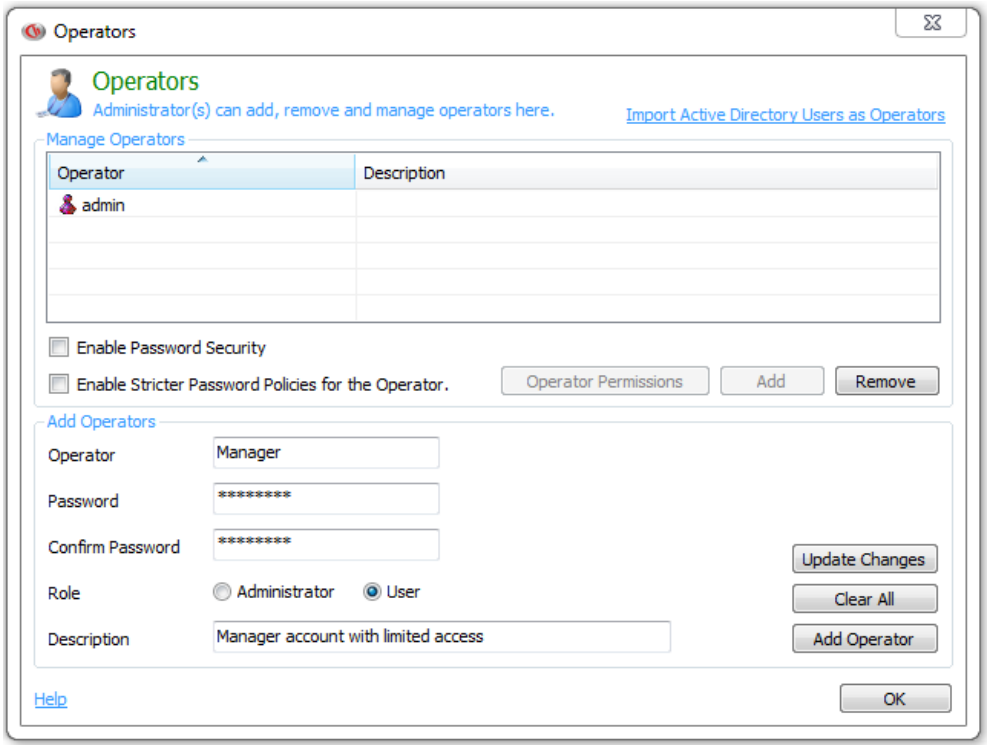
In order to password protect the console, operator accounts need to be created.

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.

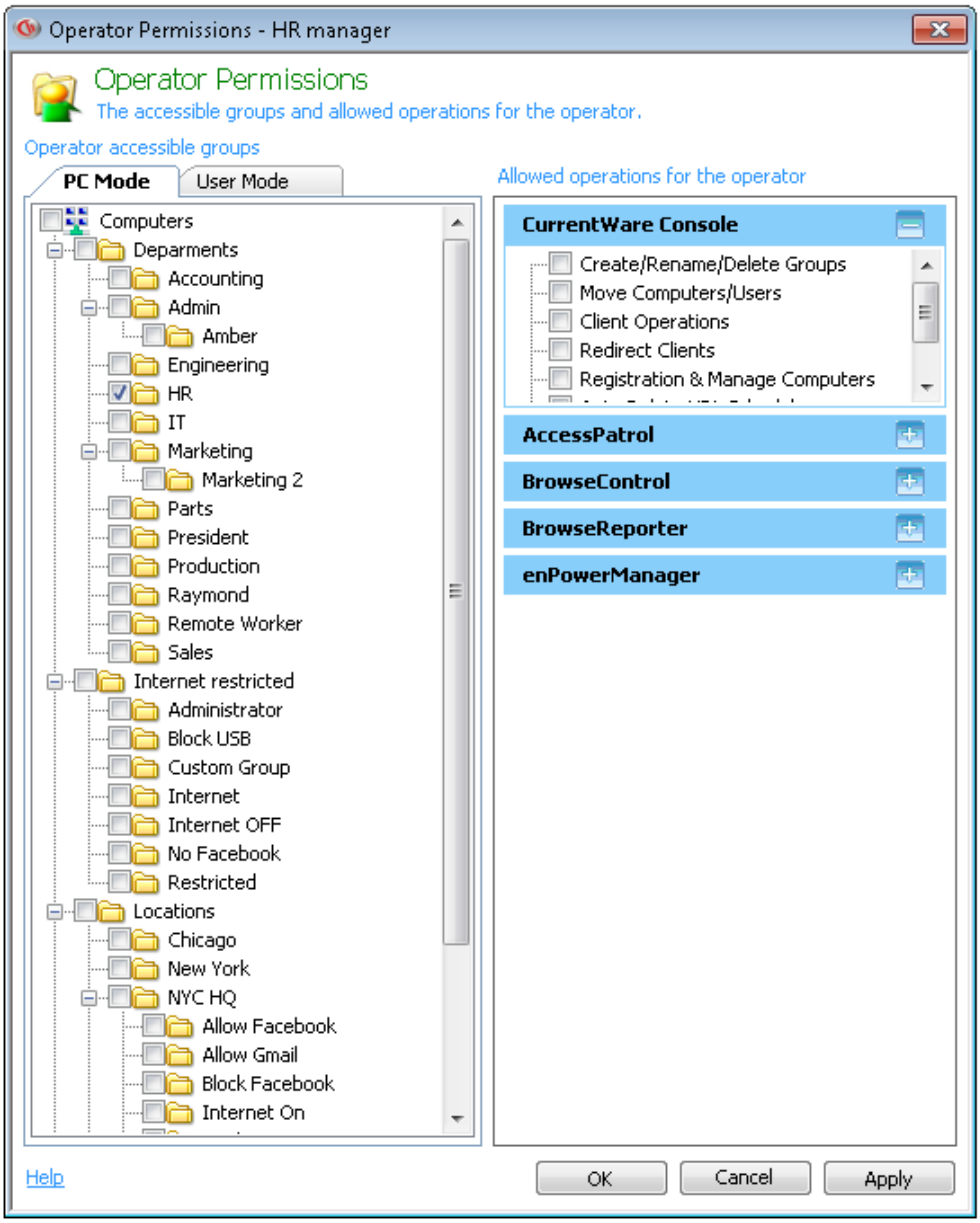
2.5.1 Operator Permissions

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

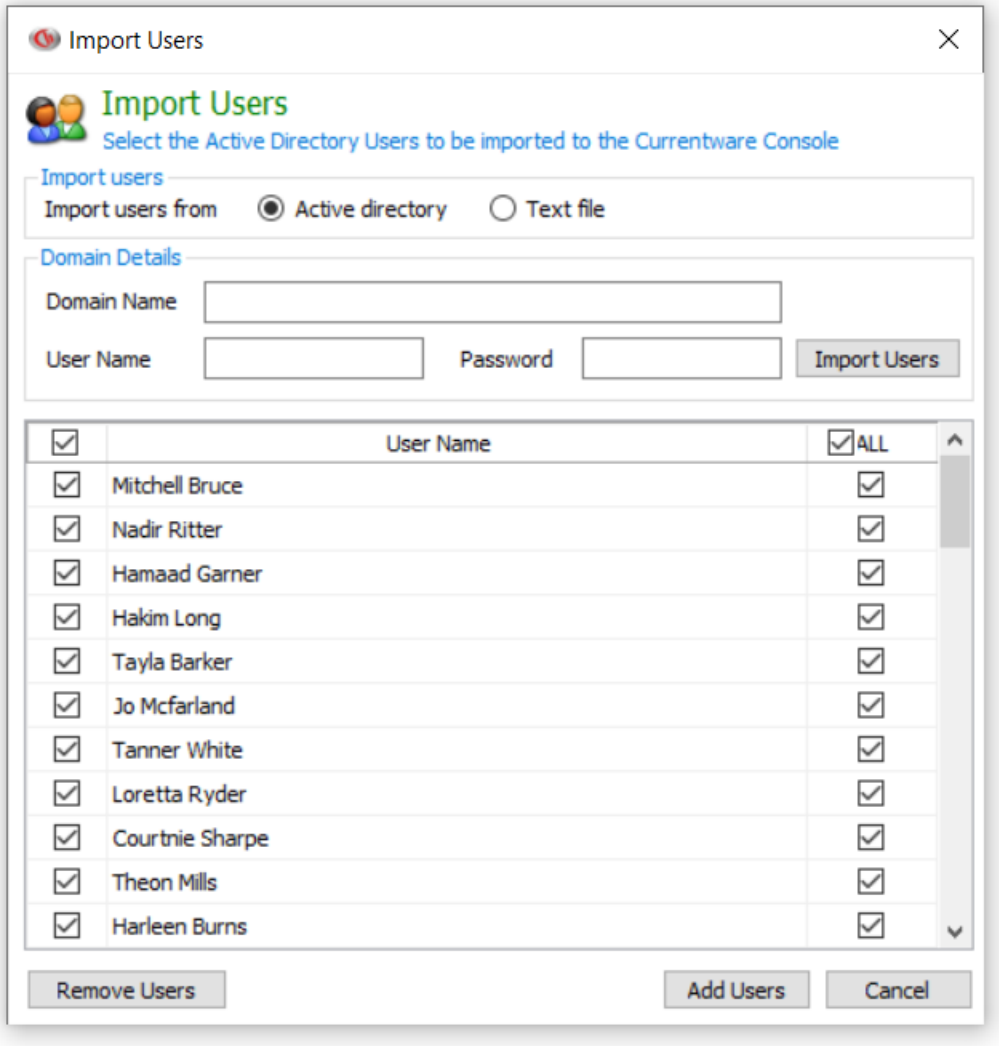
BrowseControl Operations

- 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 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

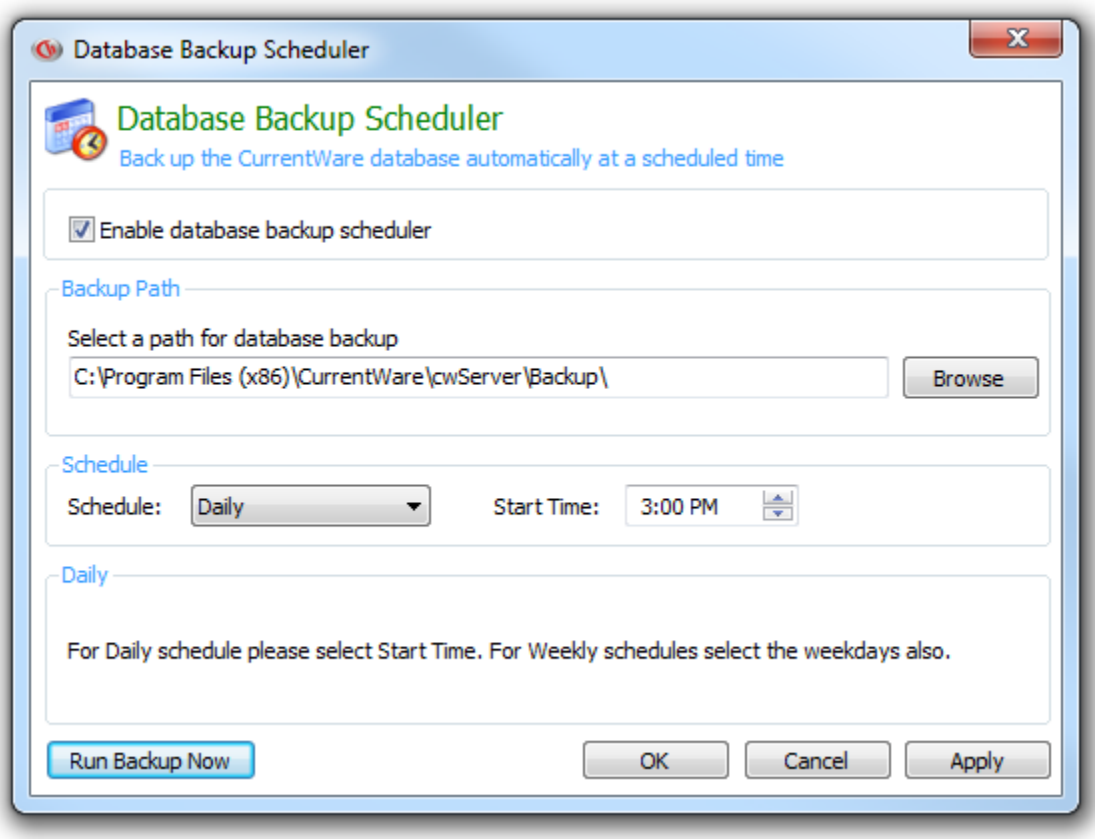
The Database Backup Scheduler automatically backs up the CurrentWare database (CWNPFB.CWD) at a scheduled time.

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.

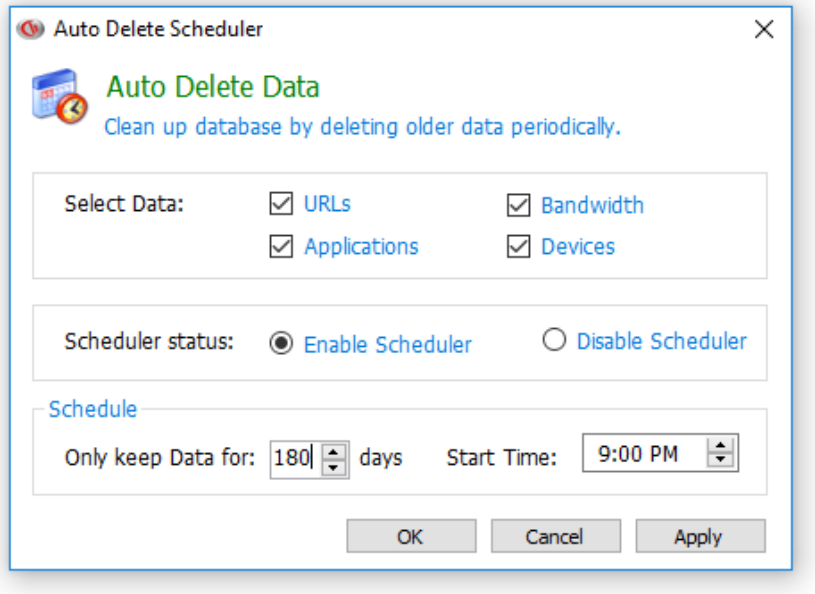
You can perform a one-time back up by clicking on the “Run Backup Now” button.



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 is 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 run once every 3 schedules and only if the database is larger than 500 MB.

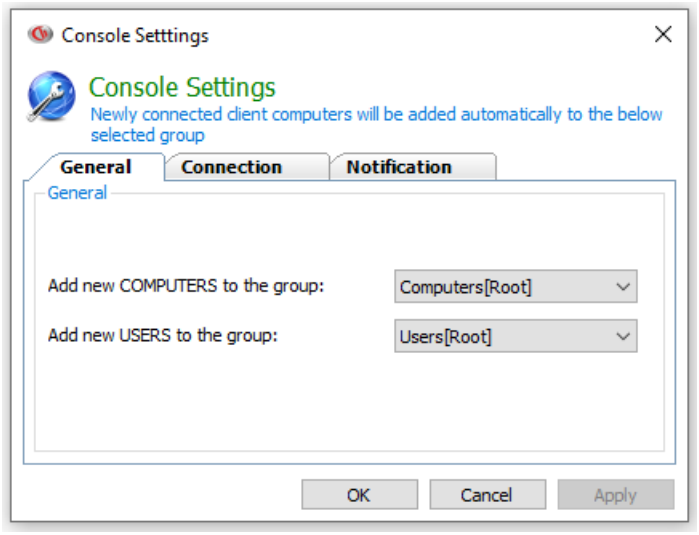
2.9 Console Settings

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.

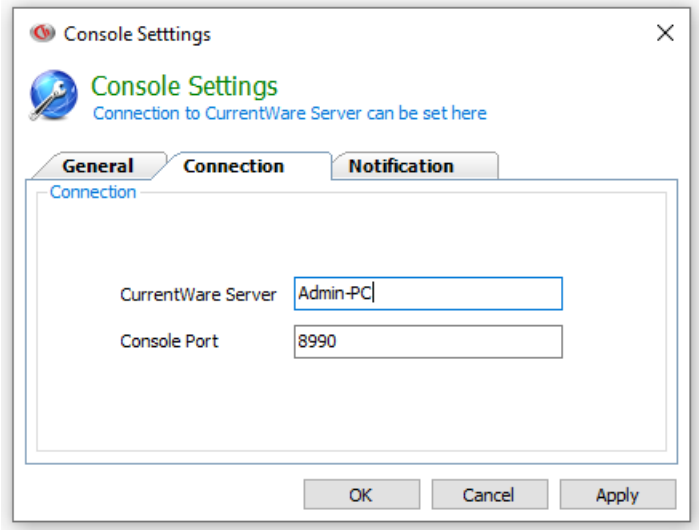
Add new Users to the group: define the group that a new user will automatically be assigned to once it is populated to the CurrentWare Server for the first time.



Connection

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

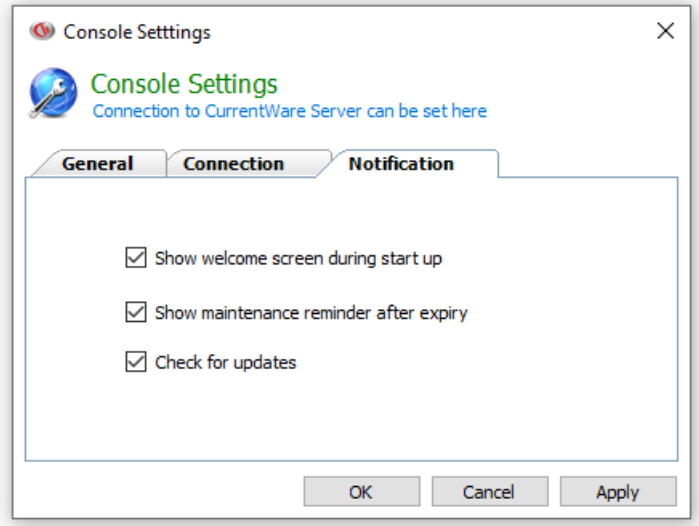
Console Port: The port that CurrentWare Console uses to connect to the CurrentWare Server. The default Console port is 8990.



Notification

Enable/disable the following notifications:

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



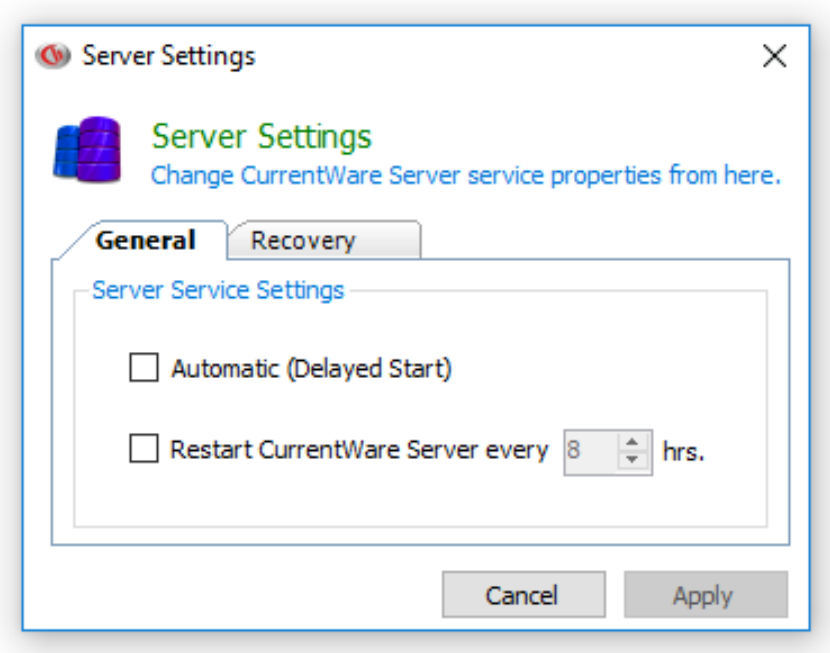
2.10 Server Settings

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

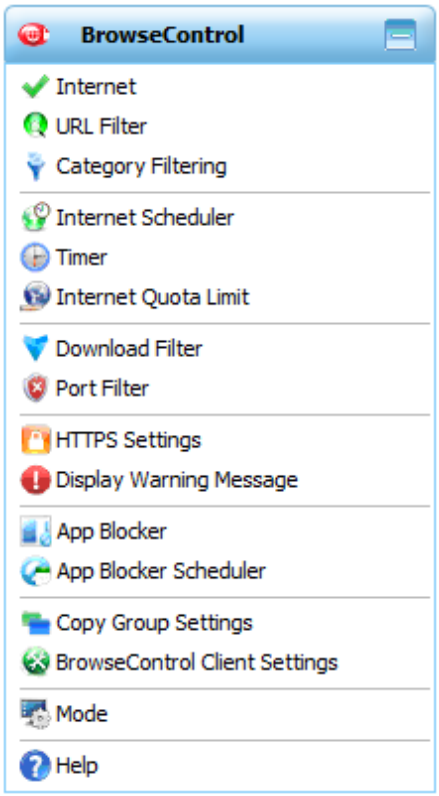
Log Out can be used to re-log into the Console with a different user name and password. This feature can be found under the menu **File → Logout**.

3.0 Overview of BrowseControl Functions

BrowseControl is an Internet restriction tool that allows an administrator to control the Internet access of your users.

An overview of the BrowseControl functions includes:

- **Controlling the Internet**
- **Block Websites Based on Categories**
- **Schedule Internet Restrictions**
- **Application Blocker**



BrowseControl Solution Feature set.

4.0 Controlling Internet Access

BrowseControl provides three different methods for controlling a client's Internet access.

- **Internet ON/OFF**
- **URL Filter**
- **Category Filtering**

All three settings can be applied at a group level. The Internet ON/OFF feature can also be applied to an individual computer/user.

4.1 Turning the Internet ON/OFF

The BrowseControl Console allows for direct control of Internet access privileges for a group of clients or an individual computer/user.

	URL Filter	**Category Filtering**
Internet ON	**Blocked List:** block specific websites **Allowed List:** allow websites that may be blocked from Category Filtering	Block websites from blocked categories
Internet OFF	**Allowed List:** only allow specific websites	Not applied

To force the Internet policy to all clients in a group, select the group on the left-hand tree of the Console. Under the BrowseControl menu on the right-hand side of the CurrentWare Console, click on Internet and select on or off.

NOTE: Groups do not inherit settings from their parent groups. Each of the groups stores the CurrentWare settings independently.

5.0 URL Filter

Under URL Filter, you can define your URL Allowed List or Blocked List. With the URL Filter, you can customize specific websites that your users are allowed or not allowed to go to.

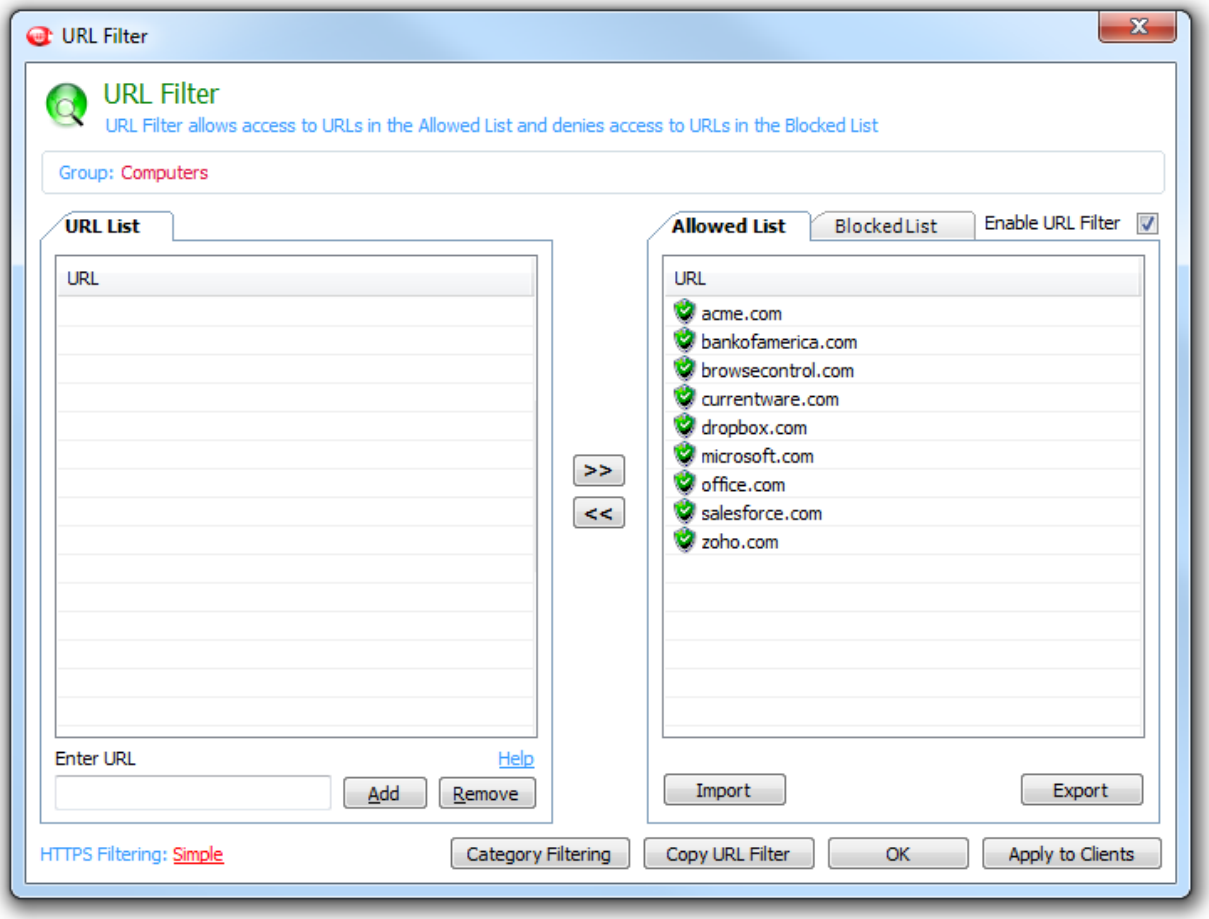
5.1 Allowed List

BrowseControl has the functionality to allow access to certain web sites when the Internet connection has been turned OFF.

The Allowed list is configured at the group level. Different allowed lists can be configured for different groups of computers and users.

How to Create an Allowed List for Your Group

1. Select the group for which you want to create the Allowed list for.
2. Under the BrowseControl menu on the right-hand side of the CurrentWare Console, click on **Internet** and select **OFF**. This will disable their Internet access completely.
3. Under the BrowseControl menu, click on **URL Filter** to modify your Allowed list.
4. Enter the URLs that you want to allow in the text box on the bottom left hand corner of the window. Click on the **Add** button.
5. Click the "**Allowed list**" tab on the right pane.
6. Select all the URLs you wish to make available to the Client computers,
7. Click on the  button to move the entries to the Allowed List on the right pane.
8. Click **Apply to Clients.**



Users will have access to the websites on the Allowed List.

5.2 Blocked List

BrowseControl has the functionality to prevent access to certain web sites when the Internet connection has been turned ON.

The Blocked list is configured at the group level. Different blocked list can be configured for different groups of computers and users.

How to Create a Blocked List for Your Group

1. Select the group for which you want to create the Blocked list for.
2. Under the BrowseControl menu on the right-hand side of the CurrentWare Console, click on **Internet** and select **ON**.
3. Under the BrowseControl menu, click on **URL Filter** to modify your Blocked list.

4. Enter the URLs that you want to block in the text box on the bottom left hand corner of the window. Click on the **Add** button.
5. Click the "**Blocked list**" tab on the right pane.
6. Select all the URLs you wish to deny access to for the Client computers,
7. Click on the  button to move the entries to the **Blocked List** on the right pane.
8. Click **Apply to Clients.**

Users will not have access to the websites on the Blocked List.

5.2.1 Importing URLs to the Allowed List or Blocked List by Text File

1. Under the BrowseControl menu, click on **URL Filter.**
2. Click on the List (Allowed List or Blocked List) that you want to import the URLs to.

3. Click on the **Import button** and browse to the text file that contains your URLs. Within the text file you are able to import, each URL should be listed on a new line.
4. Click **Apply to Clients.**

5.2.2 Exporting URLs from the Allowed List or Blocked List by Text File

1. Under the BrowseControl menu, click on **URL Filter.**
2. Click on the List (Allowed List or Blocked List) that you want to export the URLs to.
3. Click on the **Export button** and browse to the text file that contains your URLs. Within the text file you are able to export, each URL will be listed on a new line.
4. Click **Apply to Clients.**

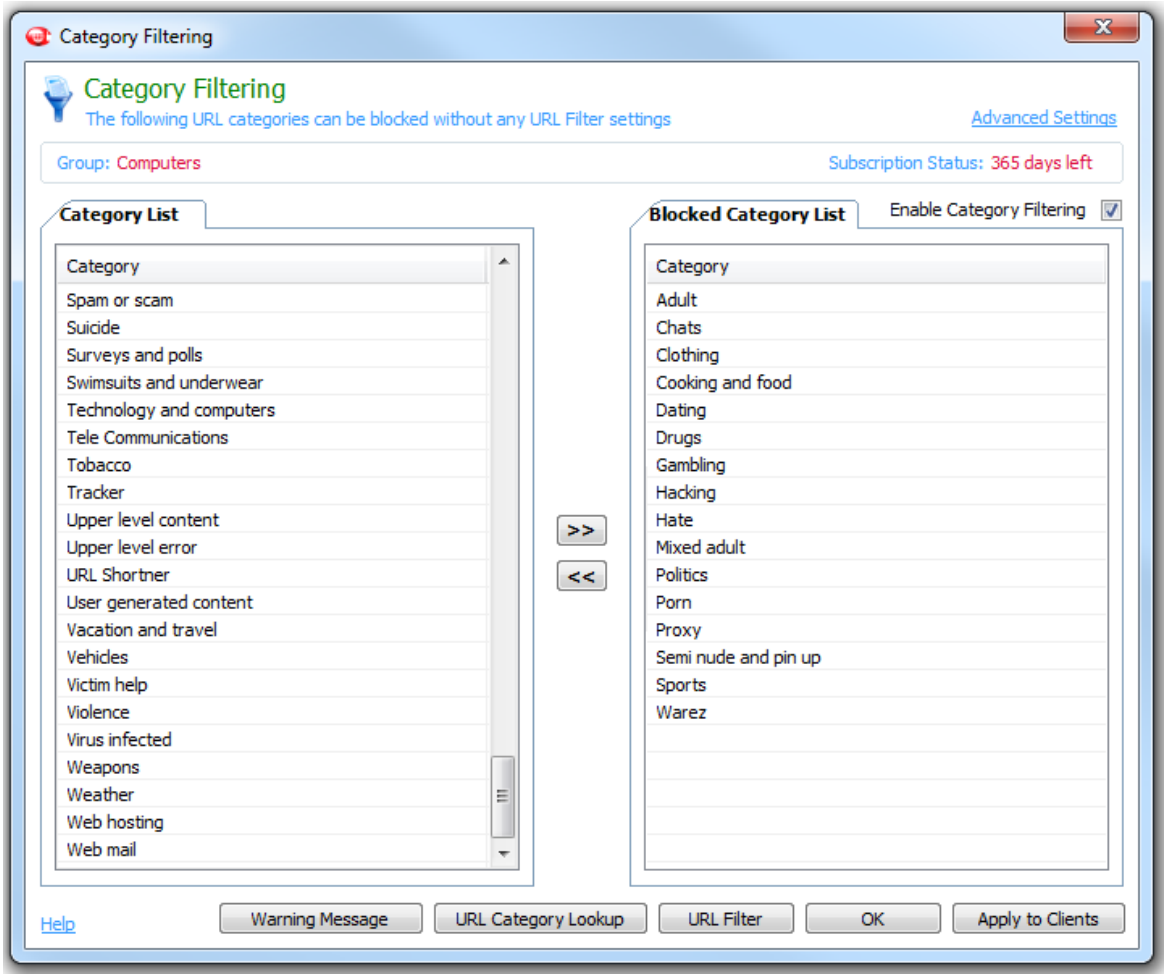
6.0 Category Filtering

CurrentWare's extensive Category Filtering, comprising of a diverse listing of more than 100+ URL categories, provides the added control of managing website accessibility beyond your blocked list.

From the central Console, administrators can instantly implement Internet restriction policies at the user or computer level. The laborious task of blocking millions of objectionable websites is instantly facilitated by simply selecting categories to be blocked from a range of 100+ URL Category filters.

You can choose from 100+ Categories that will block your users from accessing certain URLs. Find out more about each category from this page: http://www.currentware.com/browsecontrol/url-category-database/

NOTE: A separate paid subscription is required to use Category Filtering with BrowseControl. Please contact our sales representative (info@currentware.com) for further pricing inquiry.

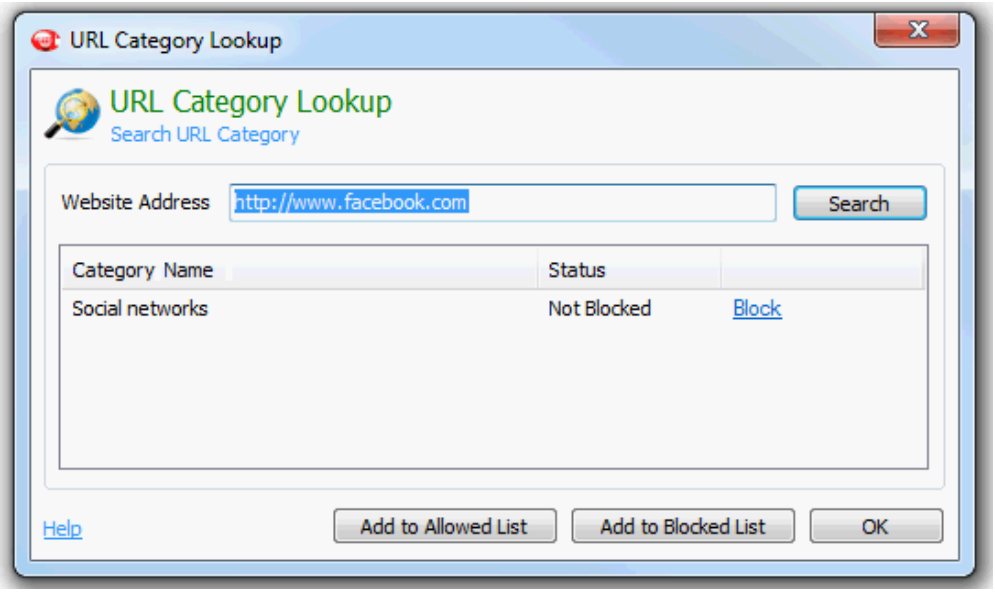


How to Block Websites using Category Filtering

1. Under the BrowseControl menu on the right-hand side of the CurrentWare console, select **Category Filtering.**
2. Select the **Categories** under the Category List that you would like to block.
3. Click on the  button to bring the selected categories to the Blocked Category List.
4. Click on the **Apply to Clients** button to restrict your users from accessing the websites from the blocked categories.

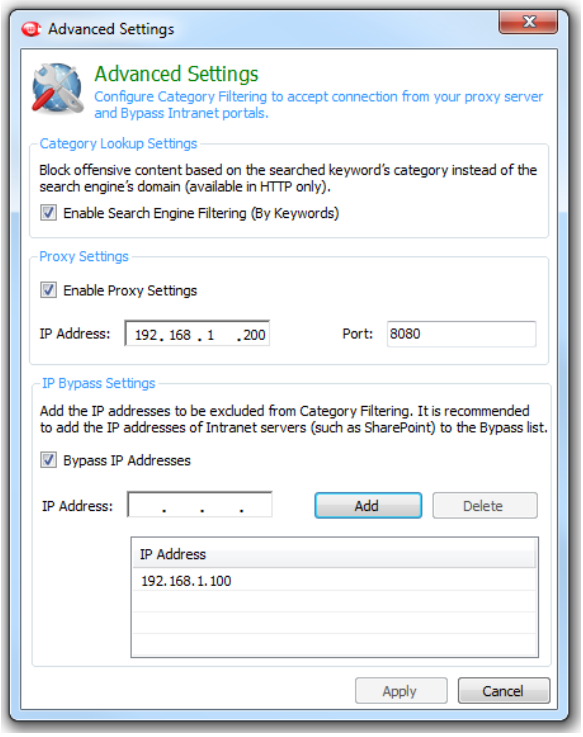
How to Lookup Websites and Their Corresponding Category Listing

1. Under the BrowseControl menu on the right-hand side of the CurrentWare console, select **Category Filtering.**
2. Click on the **URL Category Lookup** button.
3. Type in the **URL of the website** that you want to look up.
4. Click on the **Search** button.
5. The Category that the website is listed in and the Blocked status will be shown in the result.
6. From this window, you can block the entire category by clicking on the **Block** link.
7. You can also add this website directly to the **Allowed list** or **Blocked list.**



6.1 Category Filtering Advanced Settings

Advanced Settings allow you to enable Search Engine Filtering, enable Proxy Settings and Bypass IP addresses.



Enable Search Engine Filtering (By Keywords)

When this option is enabled, search queries from search engines will be categorized according to the keywords.

For example, if someone searches for anything related to basketball, the URL will be categorized as Sports. This option is only available in search engines with HTTP protocol (i.e. Bing.com, AOL.com and Ask.com).

Enable Proxy Settings

In order to categorize URL traffic from a proxy server, you must add the IP address and the port of the proxy server.

IP Bypass Settings

If your users are using any Intranet (such as Microsoft SharePoint, IBM Websphere), you will need to enable IP Bypass Settings and add the IP addresses of your intranet portals onto the bypass list.

7.0 Scheduling Internet Access

There are three ways to schedule Internet access using BrowseControl:

- **Internet Scheduler**
- **Timer**
- **Internet Quota Limit**

7.1 Internet Scheduler

Schedules can be created to allow Internet access at specific times. This is a Group specific setting.

Creating an Internet Schedule

1. Highlight the group you want to assign a scheduler to and select **Internet Scheduler** under the BrowseControl menu on the right-hand side of the CurrentWare Console.
2. Click on the **Add** button to create a new schedule.
3. Select the **Schedule Start and Stop Times.**
4. Select the **Schedule type**:

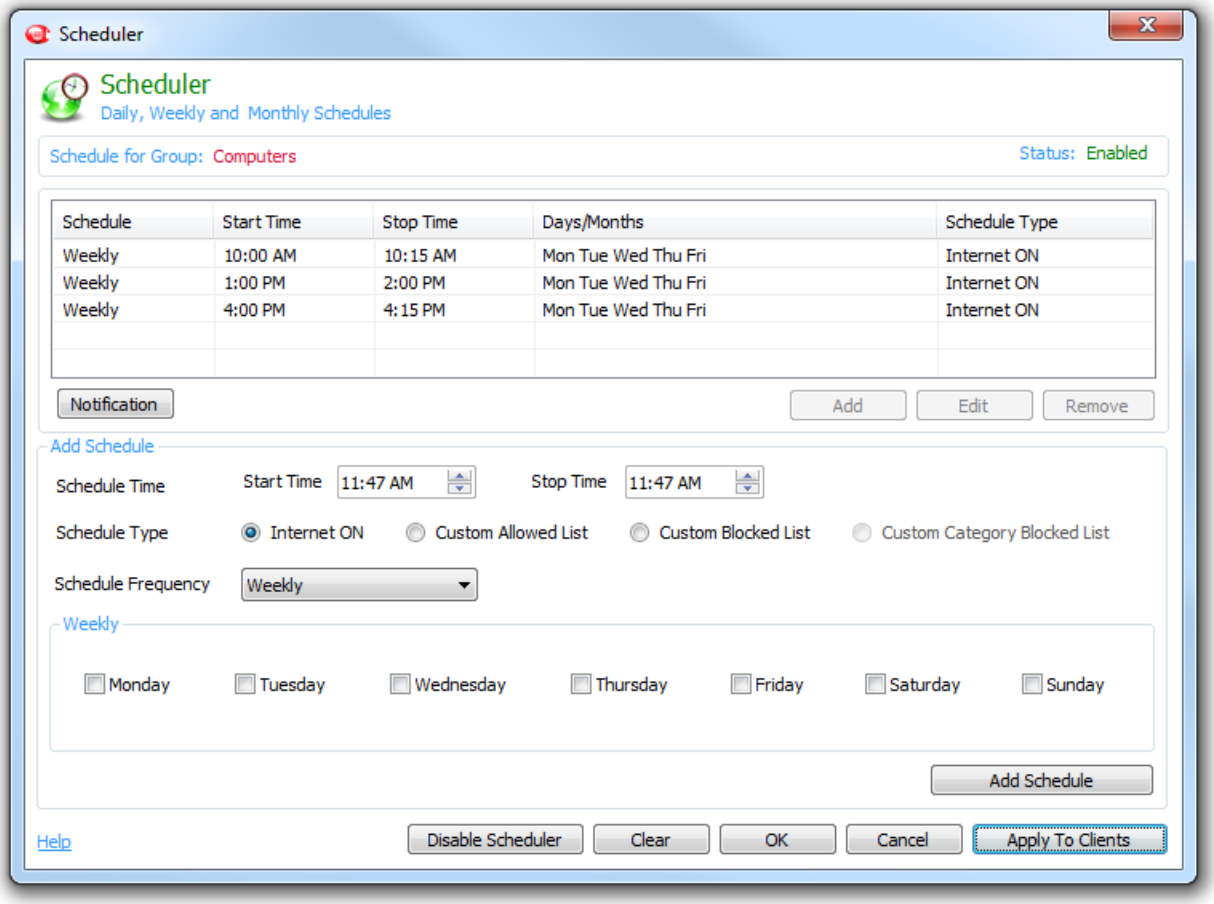
    - **Internet ON**: users will have full Internet access. The websites listed in the Blocked list (in URL Filter) will still be blocked.
    - **Custom Allowed List**: users will only have access to the websites listed in the Custom Allowed List plus the websites on the Allowed List (in URL Filter).
    - **Custom Blocked List**: users will not have access to websites on the Custom Blocked List.
    - **Custom Category Blocked List**: users will not have access to categories on the Custom Blocked List.

5. Select the **Schedule Frequency:** Daily, Weekly or Monthly.
6. Click on the **Add Schedule** button to create the Internet Schedule.

    - If a schedule type of **Custom Allowed List** was selected, then click on the Custom Allowed List hyperlink listed under the Schedule Type column to add the authorized URLs.

- If a schedule type of **Custom Blocked List** was selected, then click on the Custom Blocked List hyperlink listed under the Schedule Type column to add the restricted URLs.
- Up to 20 different Internet schedules can be set per Group.

7. Click on **Enable Scheduler.**
8. Click on **Apply to Clients.**



The Internet Scheduler sets the time for the Internet access to go on and off.

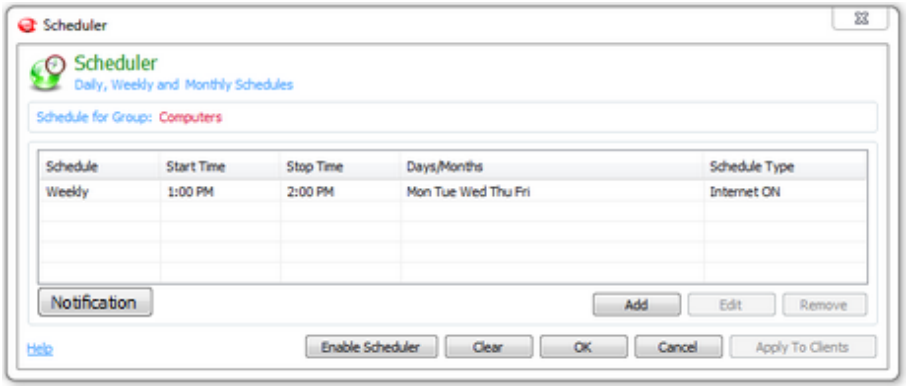
Internet Scheduler Scenarios

Companies enforce different Internet policies during different times of the day. Below are a few examples that you can use to set up the Internet scheduler suitable for your network.

Internet ON
If you selected Internet On, then the PC/user will have full Internet access until the stop time is reached. The period during the stop time and the next start time, the Internet will be set to off. The original Allowed list and Blocked list from the URL filter is still active.

Internet ON example:

- Internet ON during lunch time (*1:00 P.M. to 2:00 P.M.*)

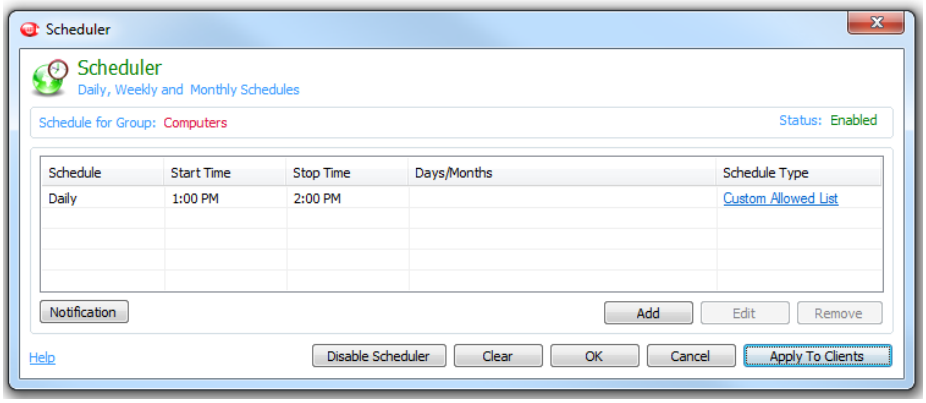


The Internet is set to ON during lunch. All other times, the Internet is OFF.

Custom Allowed List
If you selected Custom Allowed list, then the PC/user will have access to the original Allowed list **and**, on top of that, they will have access to the websites you defined on the Custom Allowed list (Internet scheduler) during the defined time period.

Custom Allowed List example:

- During standard hours (*before 1:00 P.M. and after 2:00 P.M.*), the user will have access to the websites on the original Allowed list.
- During lunch hours (*1:00 P.M. to 2:00 P.M.*), the user will have access to the websites on the original Allowed list **and** the websites on the Custom Allowed list.



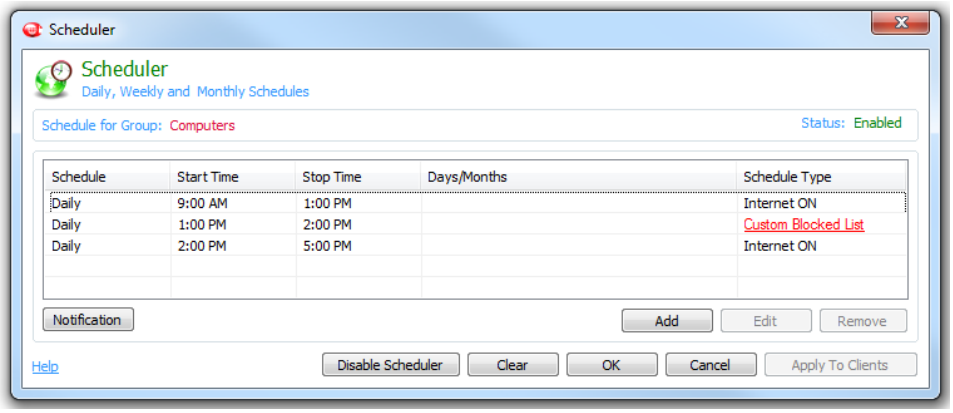
Custom Allowed list is used during lunch hour to add additional websites to the Allowed list.

Custom Blocked List

If you selected Custom Blocked list, then the PC/user will not have access to the websites on the custom blocked list during the defined time period.

Custom Blocked List example:

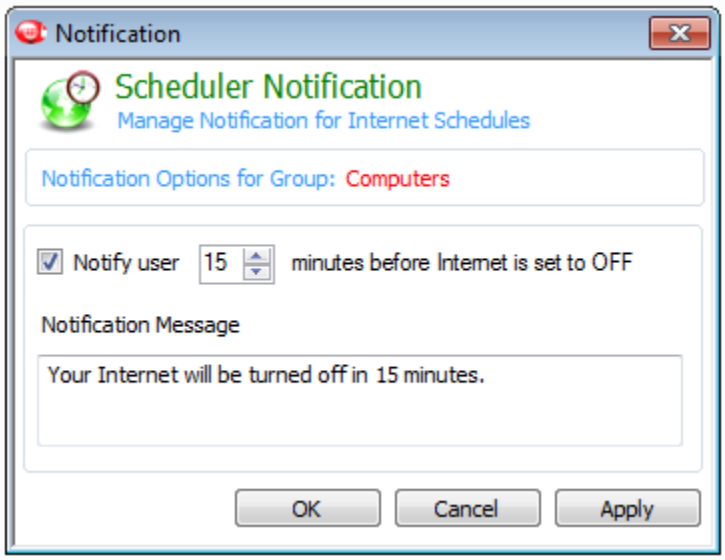
- During standard hours (*9:00 A.M. to 1:00 P.M. and 2:00 P.M. to 5:00 P.M.*), the user will not have access to the websites from the original Blocked list under the URL filter
- During lunch hours (*1:00 P.M. to 2:00 P.M.*), the user will have not have access to the websites from the Custom Blocked list under the Internet scheduler.



The user's websites are restricted by two different Blocked lists at different times: the original Blocked list is active during office hours and the Custom blocked list is active during lunch hours.

Scheduler Notification

Notify end users when the scheduler is about to turn Internet off. The notification will be displayed briefly at the system tray on the lower right corner. Administrators can customize the content of the notification message and when it will be displayed.

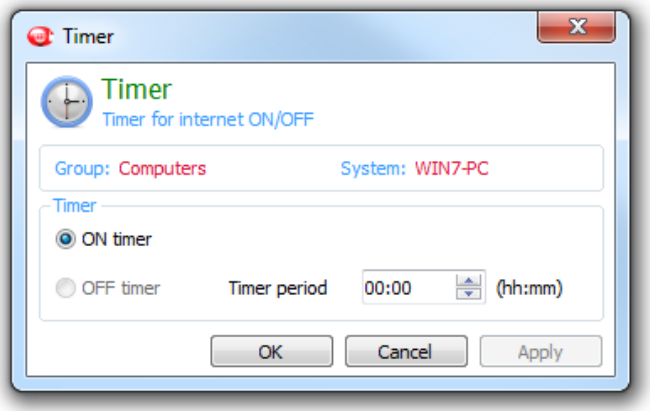


7.2 Timer

The Timer feature allows you to assign Internet ON or OFF permissions on an ad hoc basis. For example, if a Client PC/User is set to Internet ON at a specific time and you would like to temporarily block their Internet access, the Timer feature will allow you to set Internet to OFF for a specific amount of time. Once the timer has expired, the Internet settings will return to the previous Internet mode (ON/OFF or Schedule). The timer can be set for a whole group or an individual client.

1. To enable the Timer, highlight the group that you want to set the timer to and select Timer under the BrowseControl menu on the right-hand side of the CurrentWare Console.
2. The Timer screen will be displayed.
3. If the Internet status is ON then BrowseControl will automatically choose OFF Timer or vice versa.
4. Set the timer period.
5. The format of the timer is HH:MM.

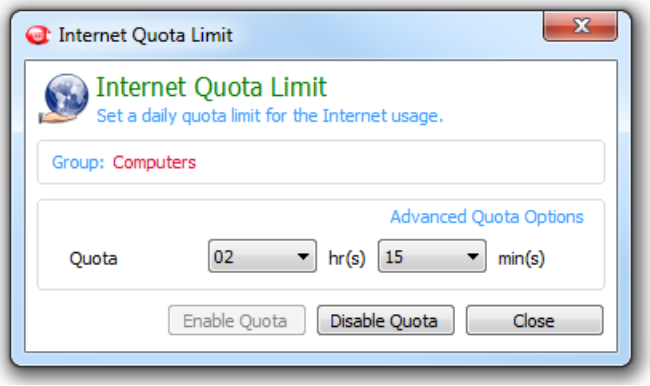
You can only use the Scheduler or the Timer one at a time. When in use, the Timer will temporarily override the Scheduler settings. Once the Timer has expired, the Scheduler will regain of the Internet settings for that group/client.



The Timer will temporary allow Internet access to the user for a predefined period of time.

7.3 Internet Quota Limit

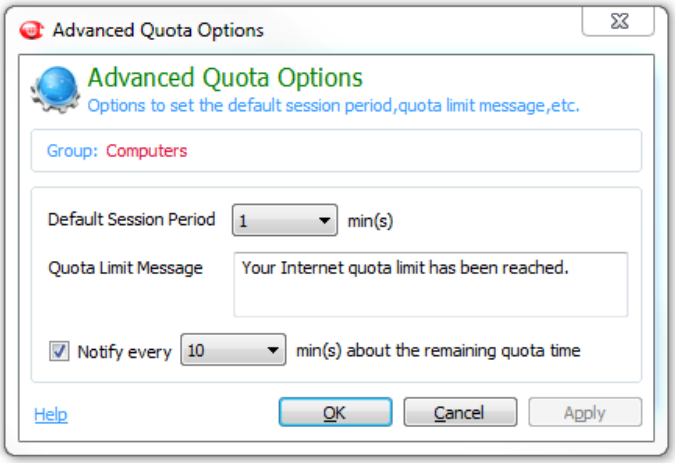
With the Internet Quota Limit, the administrator can control how often users have access to the Internet on a daily basis. The Internet Quota limit is defined by the administrator and will start counting down as soon as the quota is enabled. The users will get notification messages on their computers about how much remaining time they have for their Internet quota.



Limit the Internet browsing time of your users by setting an Internet Quota Limit.

7.3.1 Internet Quota Limit - Advanced Quota Options

Advanced quota options allow you to configure the Internet Quota Limit with default session period, quota limit message and the notification period.



Default Session Period: Each time a user's computer accesses the Internet, BrowseControl records the activity as a default session. The default session is a measurement that is used to accumulate the Internet Quota Limit. Any other

activities during the default session period will not be added to the Internet quota. By default, the default session period is set to 1 minute.

Quota Limit Message: A custom message to notify the user that the Internet Quota Limit has been reached.

Notification Period: An alert message that appears in the system tray to notify the user of their remaining Internet quota. The administrator can define how often the alert message will be shown on the user's computer.

8.0 Download Filter

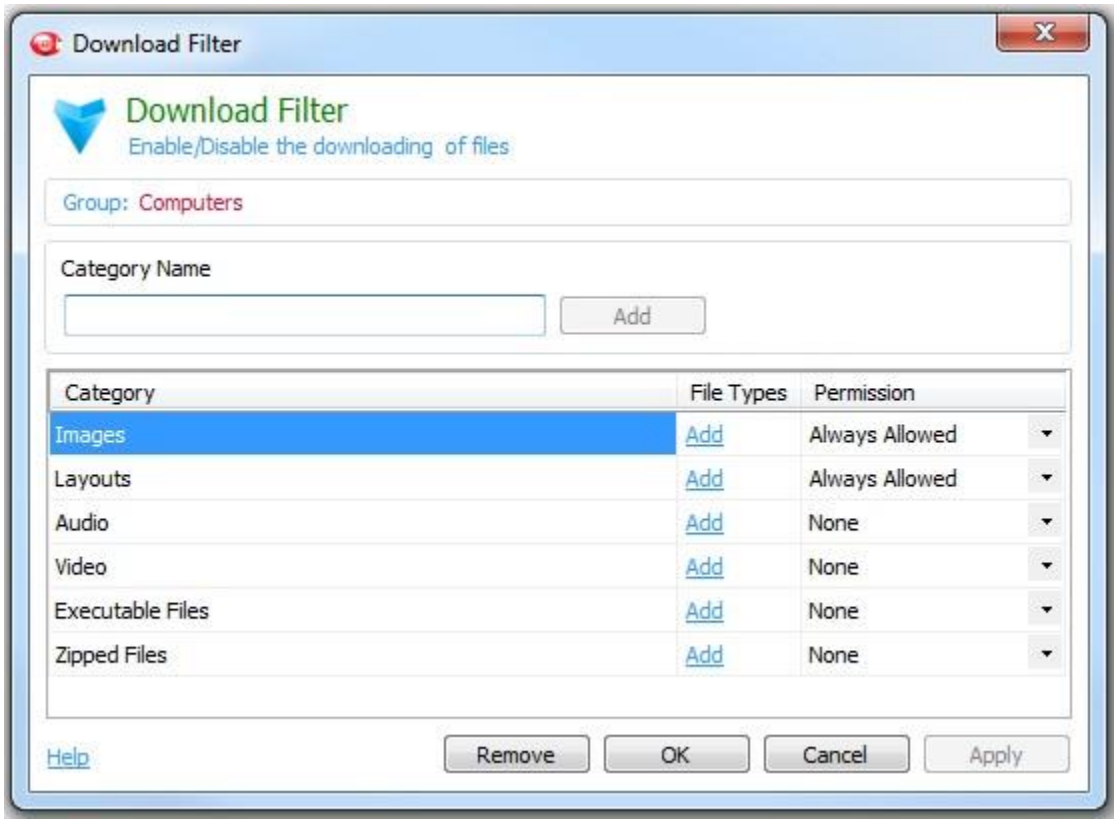
The Download Filter is a list of file extensions that the administrator can allow or deny the users from accessing while they are surfing the Internet. It applies to HTTP websites only.

By default, the Download Filter contains the categories of images and layouts. The reason for this is that some websites retrieve image files and layout files from external websites or servers. In order for the website to look properly, the Download Filter will allow the images and layout files on the website to be loaded without being blocked even though the files are not on the Allowed list.

In contrast, you can put files extension on the Download Filter that may be a threat to your network. By adding .exe, .zip, .tar and etc. files on the Download Filter, you are preventing users from downloading those files.

The streaming of audio and video files can also be blocked by putting in the appropriate file extension, such as .mp3, .swf and .mpeg.

There are three permission types. When “Allowed” is selected, the file extensions in the category will be allowed. When “Blocked” is selected, the file extensions in the category will be blocked. When “None” is selected, the file extensions in the category are not active and will be ignored.



Download filter will prevent specific file extensions from running on the user's Internet browser.

How to add a Download Filter

1. Under the BrowseControl menu on the right-hand side of the CurrentWare console, select **Download Filter.**
2. In the Category Name text box, add a name for the Download Filter and click on the **Add** button.
3. Click on the **Add** link under the File Type column for the category that you just created.
4. A new window will open.
5. Add the file extensions that you want to Allow or Block.
6. After your file extensions have been added to the list, click **Ok**.
7. In this window, under the **permission** column, select Allowed or Blocked to define the permission you want to set for the category that you just created.

9.0 Port Filter

BrowseControl has the ability to control ports. The administrator can disable the access to specific ports by adding them to the Port Filter list.

There are three options in the Port Filter:

- **Port Number:** this is the port number that the computers on your network use to communicate with other computers or over the Internet.
- **Port Type**: this is a description field that allows you to add a name or an alias to the port number that you are adding.
- **Filter Type:** there are two filter types in the Port Filter. The “HTTP” filter is used to control the Internet. It is primarily used for HTTP, HTTPS and the Proxy environment. The “Blocked” type will completely block all incoming and outgoing traffic from the defined port.

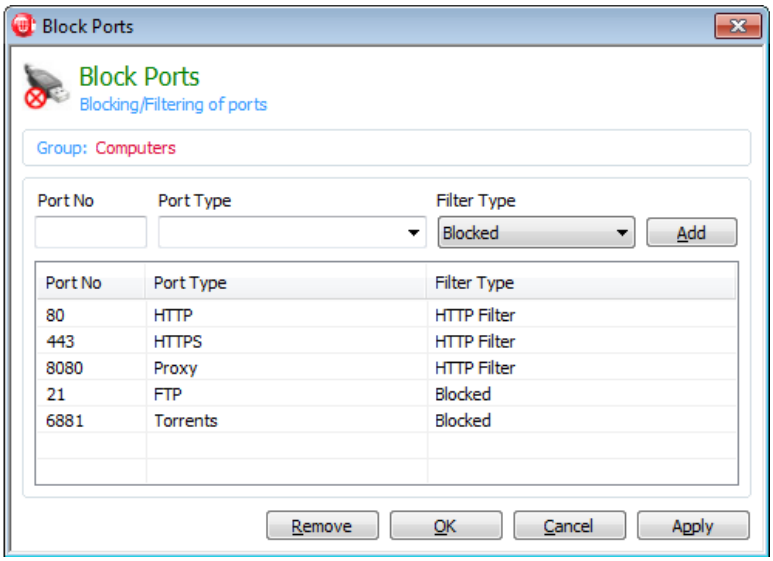
By default, the following ports are added to the Port Filter as HTTP filter:

Port 80 / HTTP / HTTP Filter

Port 443 / HTTPS / HTTP Filter

Port 8080 / Proxy / HTTP Filter

For organizations with a Proxy Server: the company's proxy server port must be added to the Port Filter list with the Filter type set to HTTP Filter. This is required in order for BrowseControl to control the Internet activities of your computers.



Port Filter will stop communication on specified network ports.

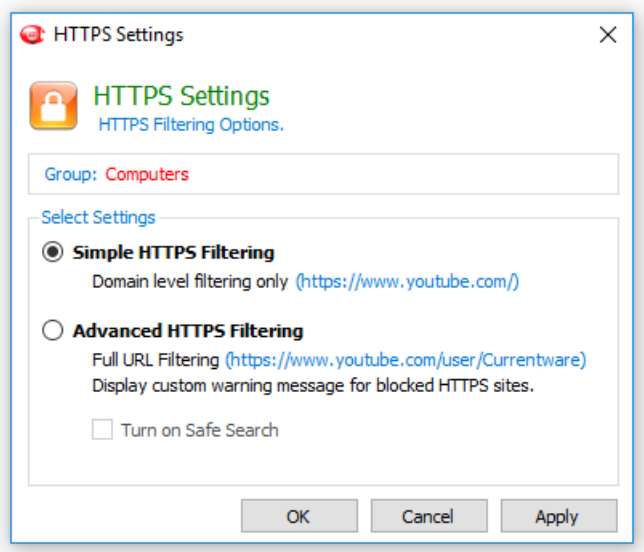
10.0 HTTPS Setting

The HTTPS setting allows the administrator to choose between simple and advanced mode of filtering HTTPS sites. This setting only applies to HTTPS websites and does not apply to HTTP websites.

Simple HTTPS Filtering: this mode allows the administrator to control Internet access to HTTPS websites at the domain level.

Advanced HTTPS Filtering: this mode allows the administrator to control Internet access to HTTPS websites at the domain level and full URL. It also enables Display warning messages.

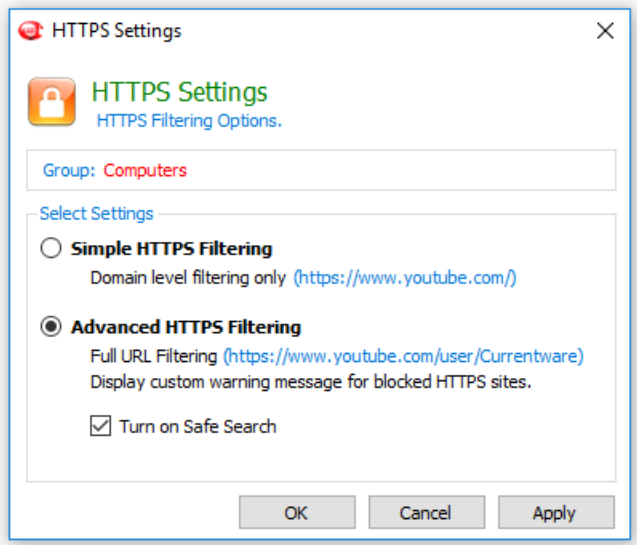
Modes	**Top domain** *(www.currentware.com)*	**Full URL** *(www.currentware.com/subpages)*
Simple	Block or allow access	Must block or allow the entire domain
Advanced	Block or allow access	Block or allow access to specific URL



Use advanced mode to control HTTPS websites with full URL.

10.1 Turn on Safe Search

When you turn on safe search, BrowseControl will filter explicit search results, images and videos, like pornography, from your Google searches.



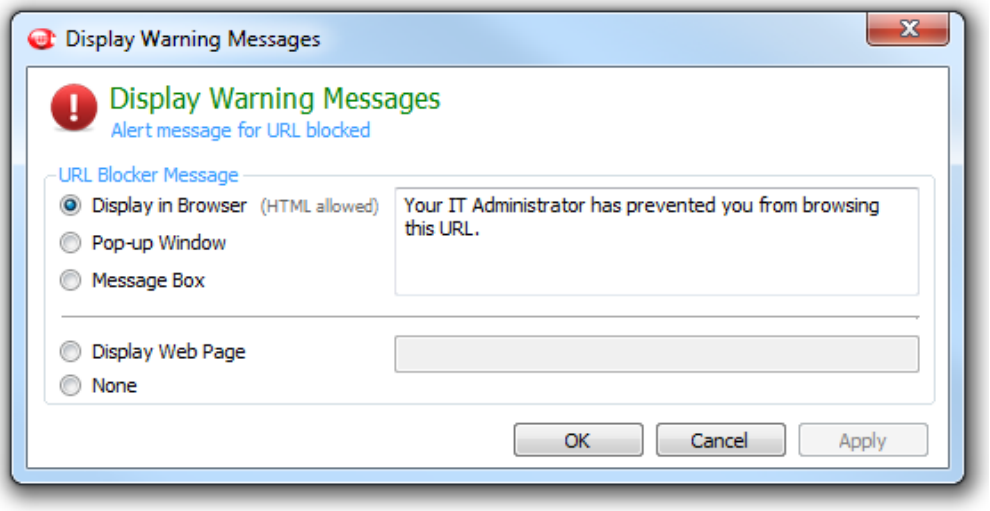
Advanced HTTPS Filtering with Safe Search Enabled.

11.0 Display Warning Message

The alert received by the users when accessing unauthorized websites can be customized in the Display Warning Message option. Only works with HTTPS Setting > Advanced.

The URL Message is fully customizable. There are five different methods to display the warning message.

- **Display in Browser:** The warning message is displayed directly on the Internet browser on the user's current page. HTML code is allowed.
- **Pop-up Window:** A pop-up window in web form will appear every time a user is accessing an unauthorized URL.
- **Message Box:** A Windows message box will display an alert for every URL that is denied.
- **Display Web Page:** The user will be redirected to a special website defined by the administrator.
- **None:** The user will receive the generic Windows error when a website is not available.



Customize the alert message displayed on the users' screen when they access an unauthorized website.

12.0 Application Blocker

The Application Blocker prevents users from launching unauthorized programs on their computers.

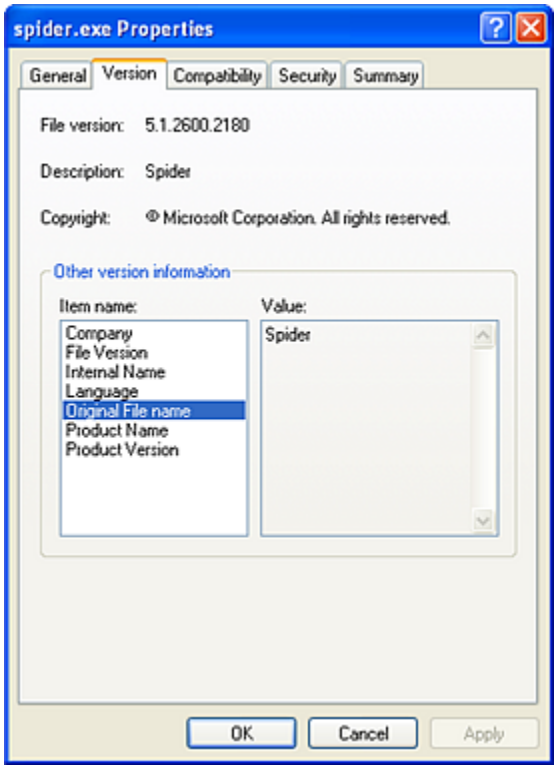
This feature is Group specific. As a result, you can block certain applications to computers and users within one group, and specify a different blocked list for other groups

How to Block Your Users from Launching an Unauthorized Application

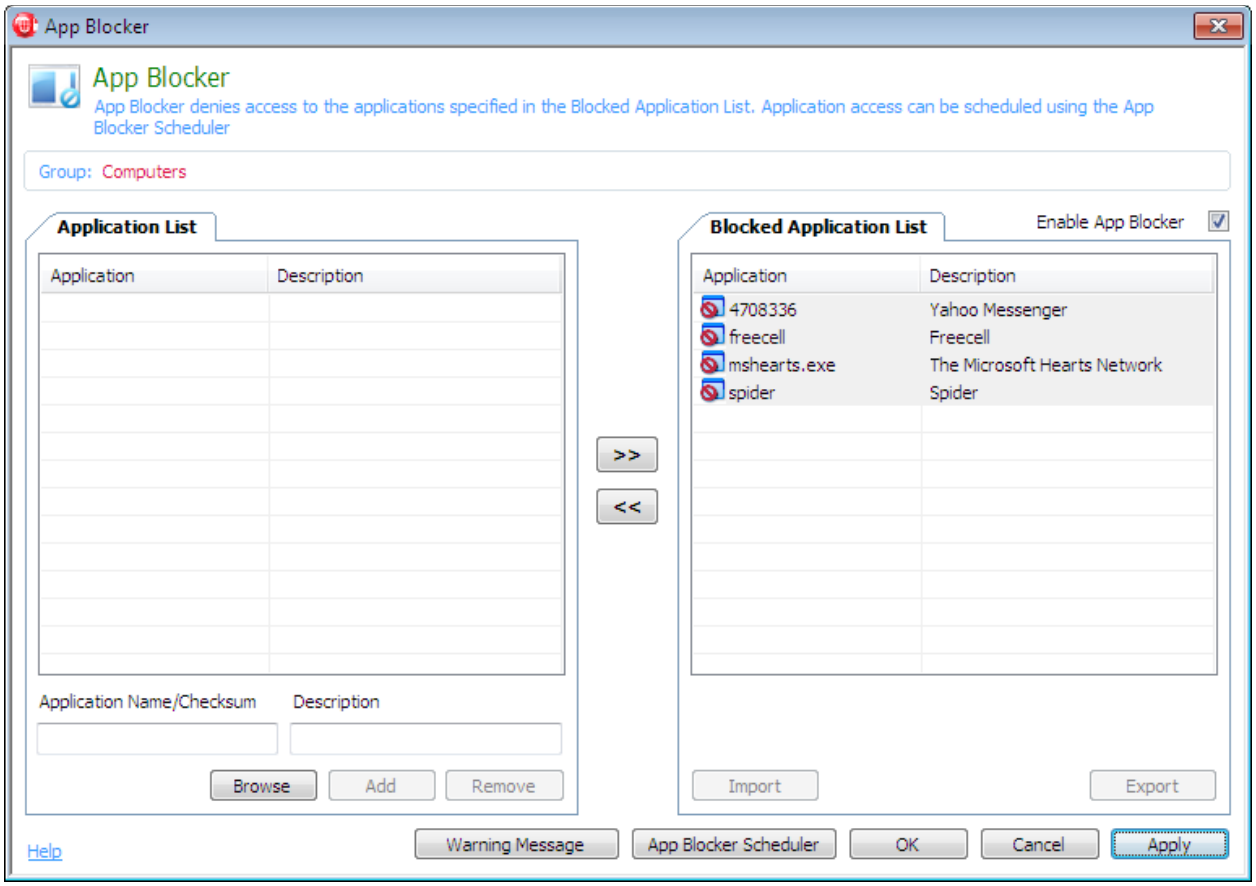
1. Select the group for which you want to apply the App Blocker.
2. Under the BrowseControl tab, click on the **App Blocker** option.
3. Before an application can be blocked, it must be added to the Application List. Enter the Original Filename of the application to be blocked in the **Application Name** textbox. A description can also be entered for convenience.

> **NOTE:** To manually locate the Original Filename of an application, right click on the exe file in Windows Explorer and select **Properties**. Select the **Version tab** and click **on Original Filename** in the Item Name box. The original filename is located in the adjacent Value box. The figure below gives an example for locating the Original Filename of Spider. Not all Original File names have the .exe suffix extension. e.g. FreeCell has no extension so just enter "FreeCell".

4. Alternatively, click on the Browse button and locate the .exe file of the application to be blocked. The Original Filename of the application will automatically be populated in the Application List**.** In case the application does not have an Original Filename, the application will automatically populate the Application list with the File's checksum.



5. To add applications to the App Blocker list, select the applications to be blocked from the list of applications on the left pane and move them to the right pane by clicking on the **>>** button. These applications will now be blocked for the computers and users under the specific Group. The App Blocker list can accommodate up to 200 applications.



The Application Blocker prevents programs from launching on the users' workstations.

12.1 Application Blocker Scheduler

Schedules can be created to allow access to the blocked applications at specific times. This is a Group specific setting. To assign a schedule:

1. Select the group that you want to apply the Application Blocker Scheduler to.
2. Under the BrowseControl tab, click on the **App Blocker Scheduler.**
3. Click on the **Add** button.
4. Choose the **start time** and the **end time** for your App Blocker schedule. The schedule time will allow the application to run during within the chosen period. The application will be denied from launching outside of the scheduled time.
5. Choose the **Schedule frequency** of daily, weekly or monthly.
6. Click on the **Add Schedule** button to add the defined time schedule.
7. Click on the **Enable Scheduler** button.
8. Click on **Apply to Clients**.
9. Up to 20 schedules can be set per group.

At the scheduled time, the users will be able to access the blocked applications. Access to the blocked applications will be terminated immediately, when the stop time is reached.

12.2 App Blocker Warning Message

When a user tries to launch a blocked application, a customized message can be presented to notify the user that access is denied for this application.

1. The message can be changed by clicking on the Warning Message button in the App Blocker Window.
2. Enter your message in the App Blocker Message textbox.
3. Click on the Apply button to save the message.

12.3 Importing Applications to the Blocked Application List by Text File

1. Under the BrowseControl tab, click on **App Blocker.**
2. Click on the **Import button** and browse to the text file that contains your applications. Within the text file that you are able to import, each application should be listed on a new line.
3. Click **Apply to Clients.**

12.4 Exporting Applications from the Blocked Application List by Text File

1. Under the BrowseControl tab, click on **App Blocker.**
2. Click on the **Export button** and browse to the text file that contains your applications. Within the text file that you are able to export, each application should be listed on a new line.
3. Click **Apply to Clients.**

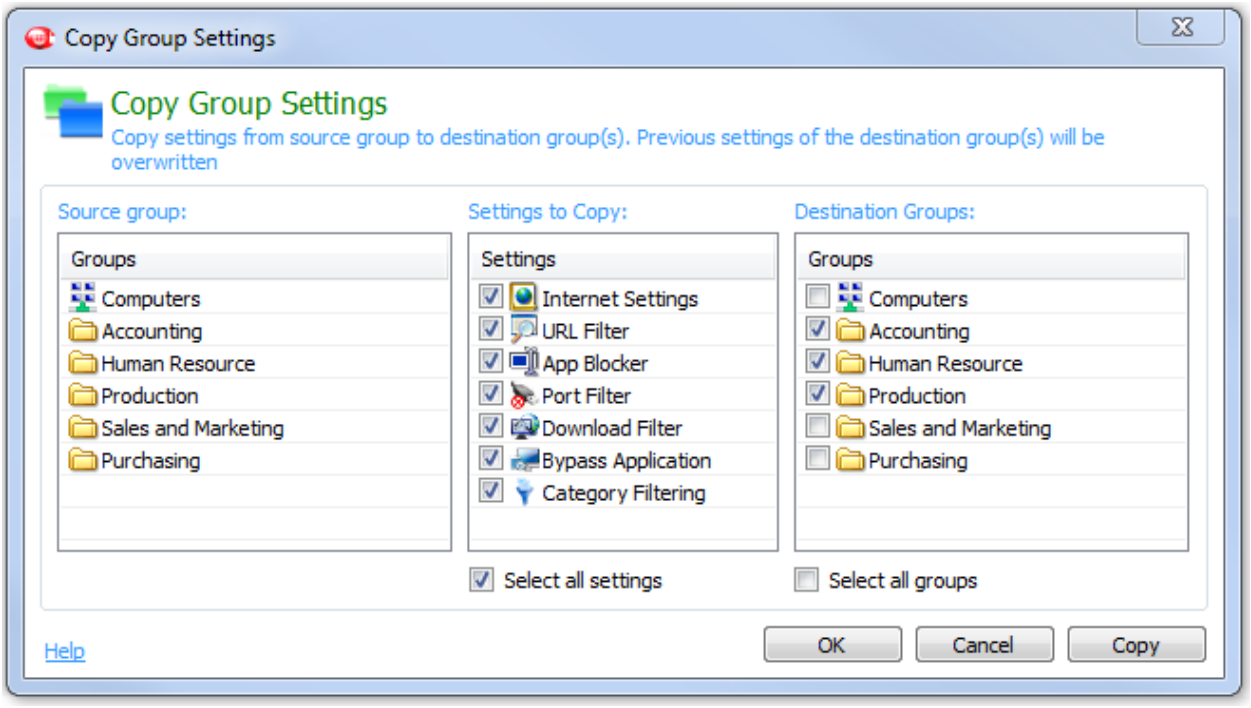
13.0 Copy Group Settings

The Copy Group Settings function allows you to easily transfer the group settings from one group to another group.

Source Group: This is the group you want to copy the group settings from**.**

Settings to Copy: The detail of the group settings that you want to copy.

Destination Group: This is the group(s) you want to copy the group settings to.



Copy the group settings from one group to another folder.

14.0 BrowseControl Client Settings

BrowseControl settings are retained on the client computer when the CurrentWare Server is unavailable or when the client computer disconnects from the CurrentWare Server. You can configure the web filtering settings on the users' computers when the CurrentWare Server becomes unavailable.

14.1 Offsite Management

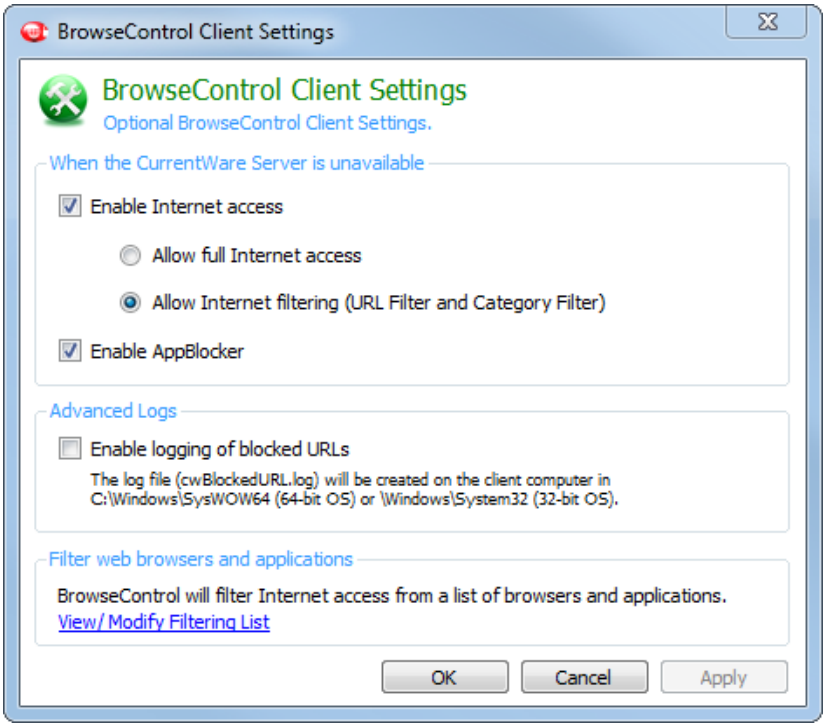
Enable Internet Access When the CurrentWare Server is Unavailable

Toggle the option to activate the Internet access when the CurrentWare Client is not connected to the CurrentWare Server.

When the CurrentWare Server is unavailable, you can pick to allow the workstation to have **Full Internet** access or **apply the existing Allowed List and Block List**.

Enable AppBlocker When the CurrentWare Server is Unavailable

Toggle the option to activate the AppBlocker when the CurrentWare Client is not connected to the CurrentWare Server.



When the CurrentWare Server is not available, the CurrentWare clients can access the Allowed and Blocked list from the local database.

14.2 cwBlockedURL Log

There are situations when your users are blocked from accessing an allowed website because the data is being loaded from an external URL.

Use the Advanced Logs and enable the logging of blocked URLs to help identify the external URL to be added to the Allowed List.

Remember to disable the logging after you are done troubleshooting the affected websites.

Enable Logging of Blocked URLs

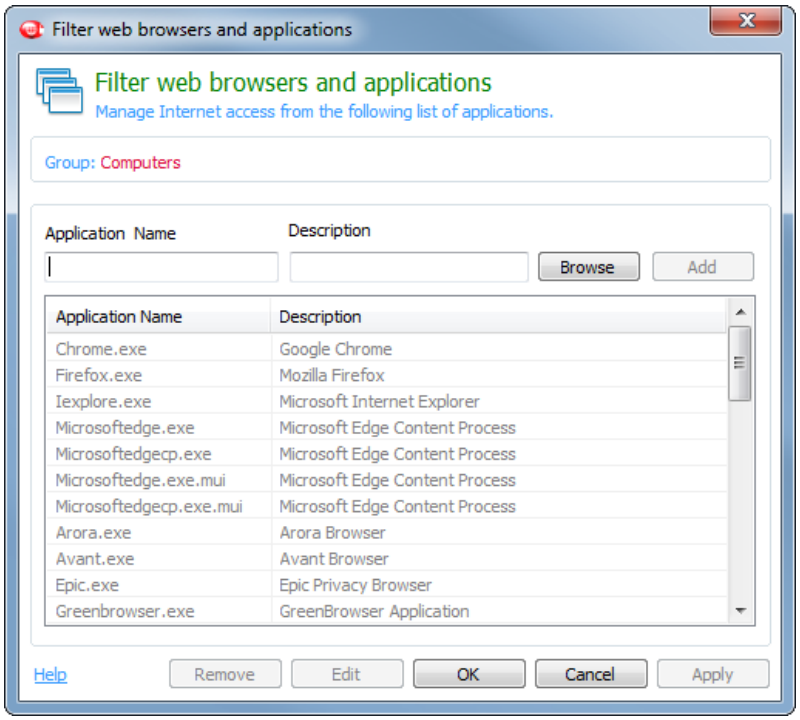
A log file called cwBlockedURL.log will be created on the client computer under C:\Windows\SysWOW64 or C:\Windows\System32.

Browse to the affected website where BrowseControl is blocking it. Open this log file to see which URL was blocked. Add the URL to the Allowed list.

14.3 Filter Web Browsers and Applications

By default, BrowseControl will block Internet access from the most commonly used Internet browsers.

If you want to add more applications to BrowseControl's filter list, this is where you would add it.



15.0 Mode

Switch between PC or User mode.

PC mode: Control Internet by computers. All users logged into the computer will have the same Internet restriction policy.

User mode: Control Internet by users. Each user logged into the computer will have their own Internet restriction policy.

16.0 CurrentWare Server Manager

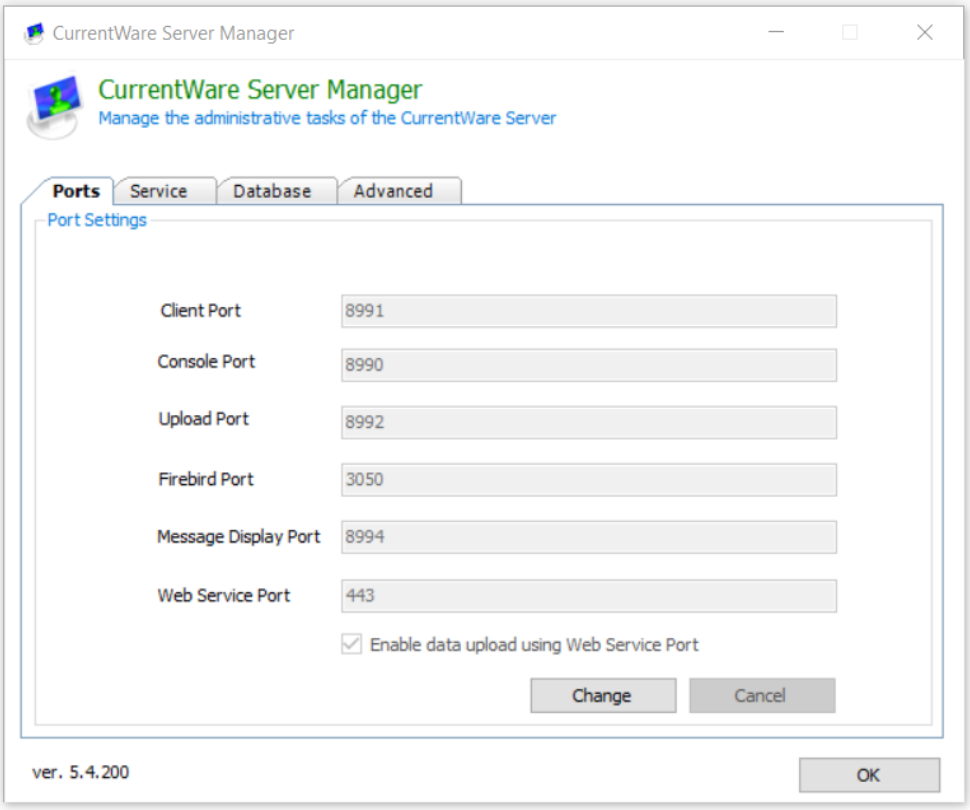
The CurrentWare Server Manager is used to manage the administrative tasks of the CurrentWare Server.

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

16.1 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.

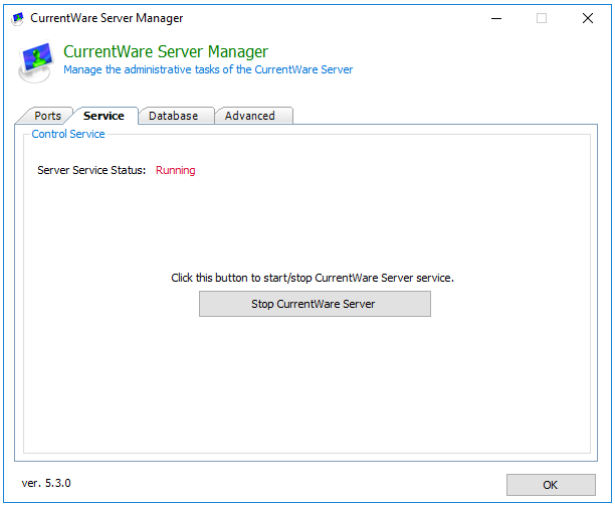


CurrentWare Server Manager.

- **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.

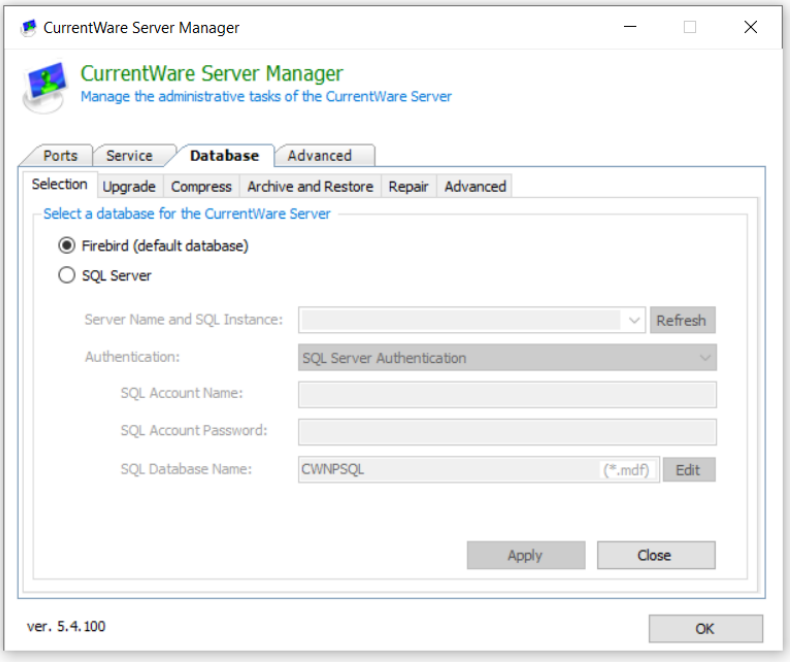
16.2 Stopping the CurrentWare Server Service

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



16.3 CurrentWare Database Selection

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



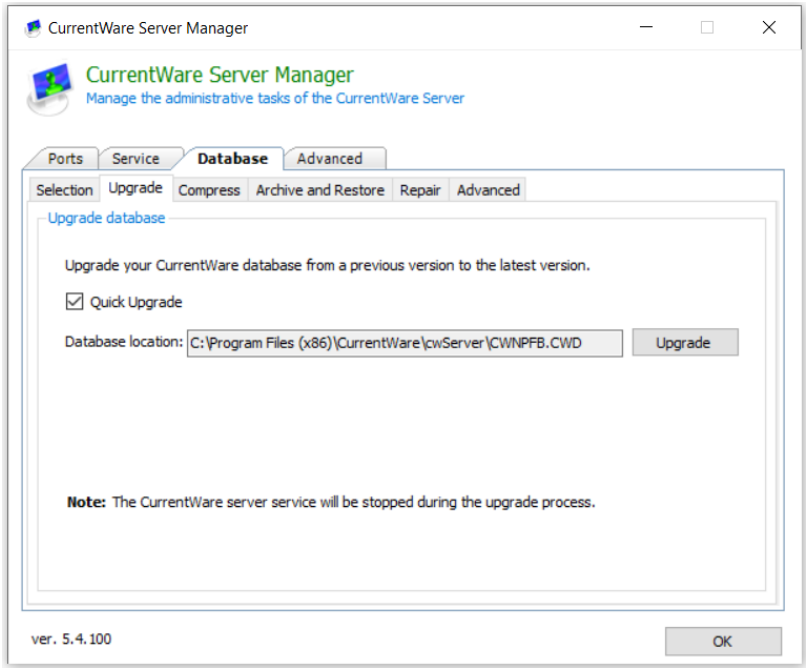
16.4 Upgrading the CurrentWare Database

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.

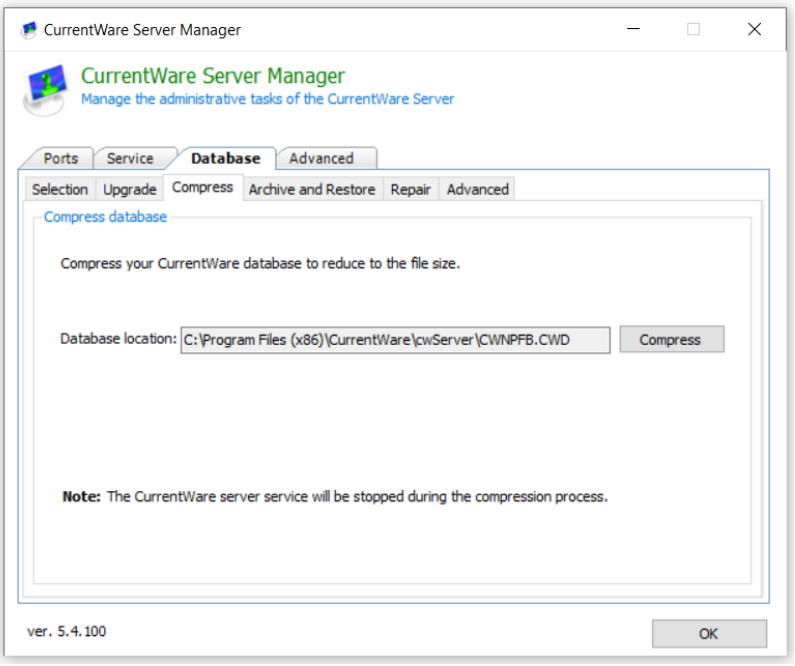


16.5 Compress the CurrentWare Database

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.



16.6 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.

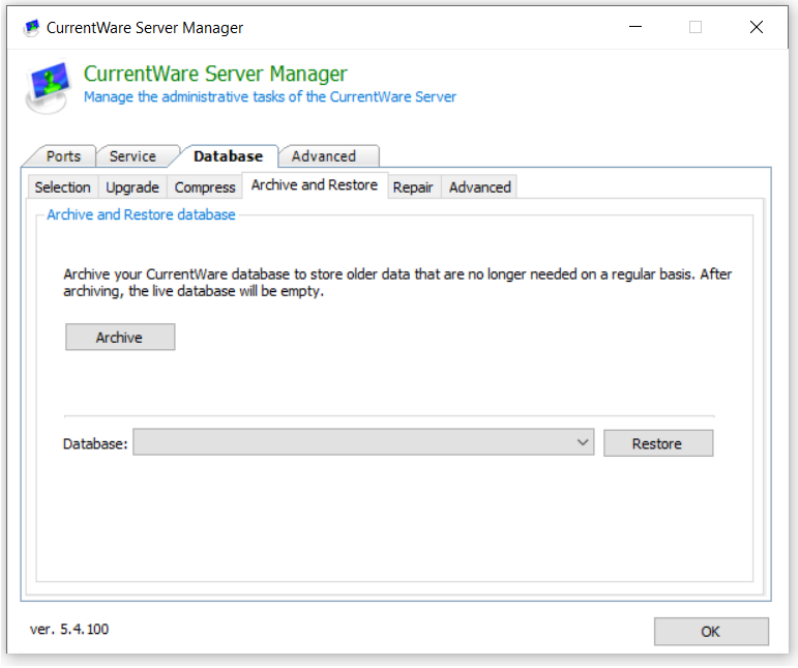
To Archive your CurrentWare Database:

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.

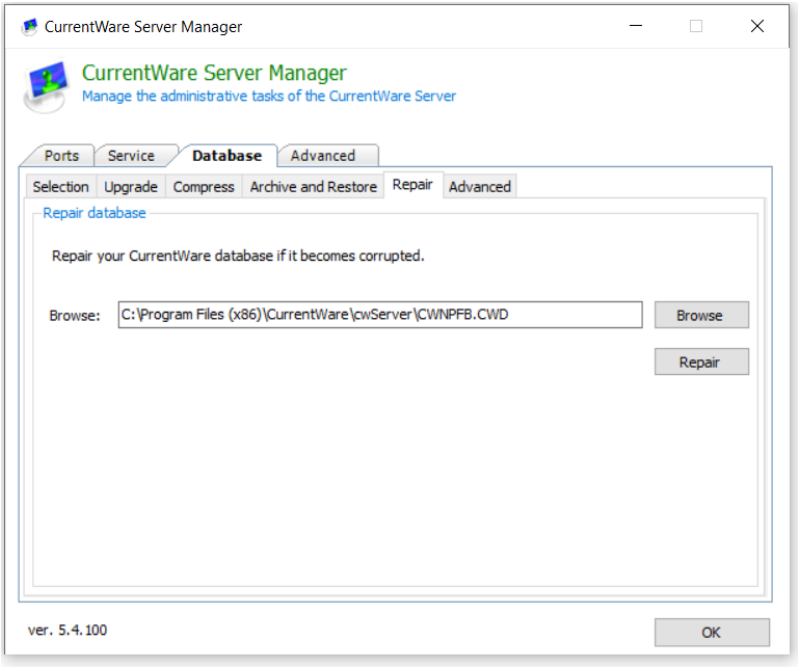
Restoring an Archived Database:

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.



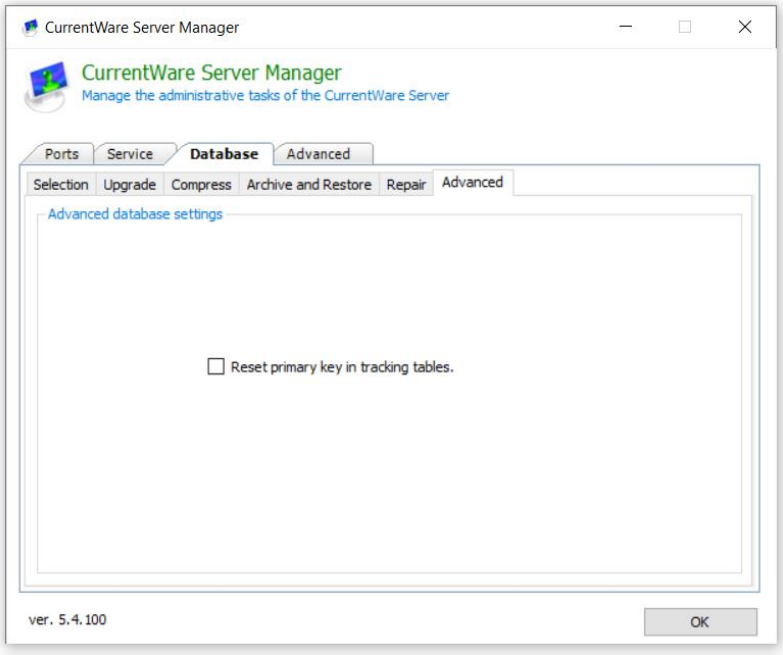
16.7 Repairing the CurrentWare Database

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



16.8 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.



16.9 Advanced

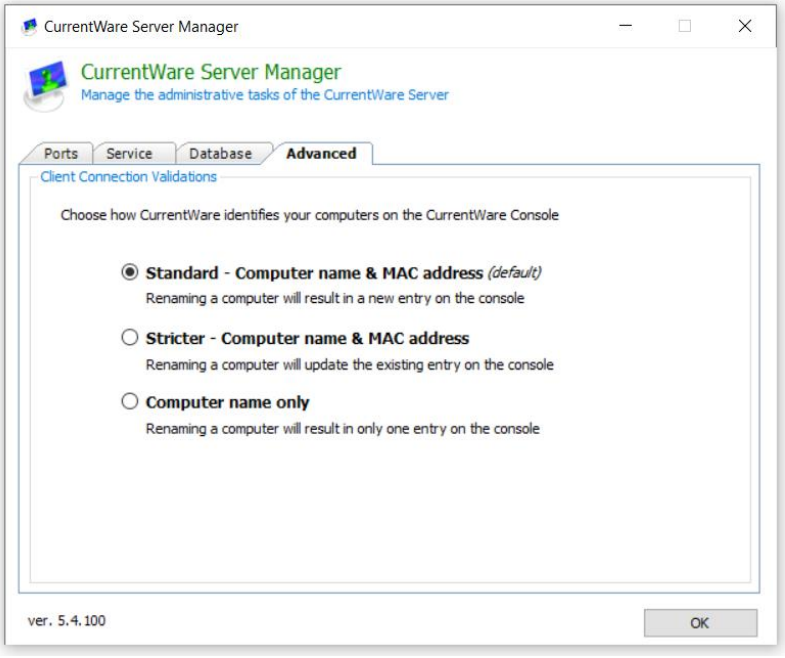
Enabling Stricter client connection handshake will add another layer of validation to the client connection process.

- **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.


CurrentWare Server Manager
CurrentWare Server Manager
Manage the administrative tasks of the CurrentWare Server
Ports
Service
Database
Advanced
Client Connection Validations
Choose how CurrentWare identifies your computers on the CurrentWare Console
Standard - Computer name & MAC address (default)
Renaming a computer will result in a new entry on the console
Stricter - Computer name & MAC address
Renaming a computer will update the existing entry on the console
Computer name only
Renaming a computer will result in only one entry on the console
ver. 5.4.100
OK

17.0 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.

17.1 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.

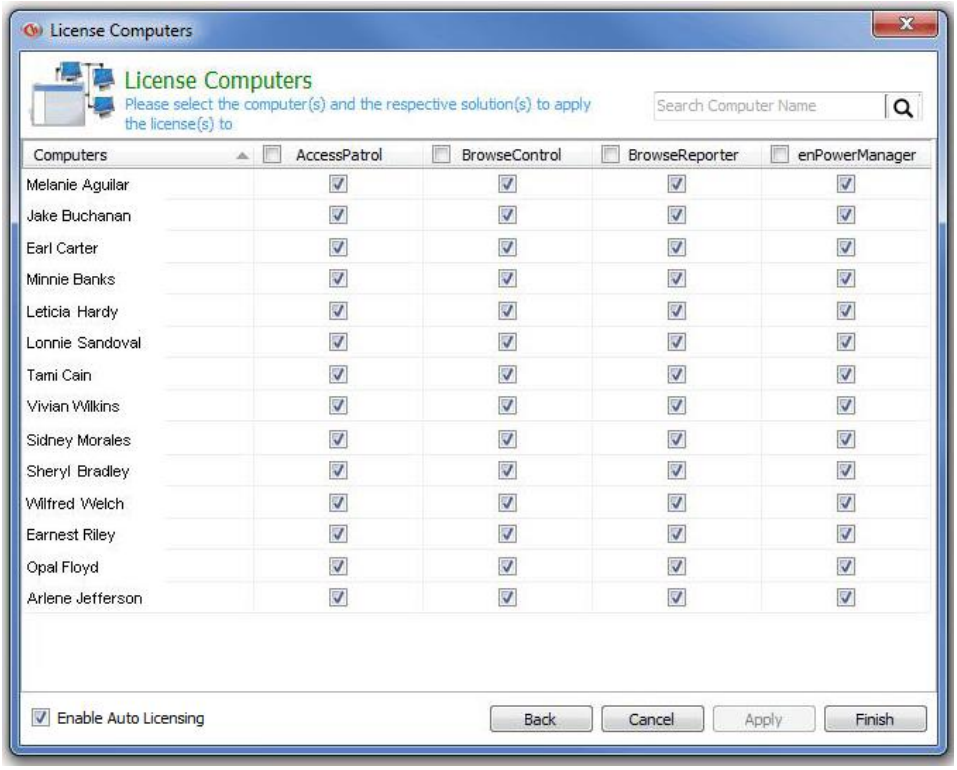
17.2 License Management

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.

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.

18.0 Uninstall CurrentWare Server, Console and Solutions

18.1 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.

18.2 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.

19.0 Uninstall CurrentWare Client

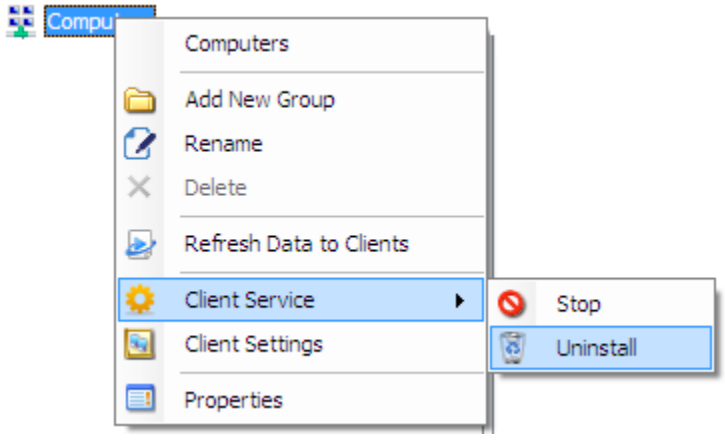
The CurrentWare Client can be uninstalled by three different methods:

1. **Uninstall CurrentWare Client from the Console.**
2. **Uninstall CurrentWare Client on the workstation by command line.**
3. **Uninstall CurrentWare Client on the workstation from the Client Configuration Window.**

19.1 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.



19.2 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 password field. 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.

19.3 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.

20.0 Technical Support

There are several ways to reach our technical support team.

By Email: Send us an email at 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.

21.0 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

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

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

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.