

User Guide

Revised in March, 2017



BrowseControl

Version 5.1.4

Internet Restriction Software

BrowseControl User Guide - Table of Contents

1.0 Introduction to BrowseControl.....	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 BrowseControl Functions	33
4.0 Controlling Internet Access	34

4.1 Turning the Internet ON/OFF	34
4.2 Internet Scheduler	35
4.3 Timer	39
4.4 Internet Quota Limit.....	39
4.4.1 Internet Quota Limit - Advanced Quota Options	41
5.0 URL Filter	42
5.1 Allowed List	42
5.2 Blocked List	44
5.3 Importing URLs to the Allowed List or Blocked List by text file.....	45
5.4 Exporting URLs from the Allowed List or Blocked List by text file	46
6.0 Category Filtering	47
6.1 Category Filtering Advanced Settings.....	49
7.0 Download Filter	50
8.0 Bypass Applications.....	53
9.0 Display Warning Message	54
10.0 Application Blocker	55
10.1 Application Blocker Scheduler	56
10.2 App Blocker Warning Message.....	57
10.3 Importing Applications to the Blocked Application List by text file.....	57
10.4 Exporting Applications from the Blocked Application List by text file	57
11.0 Port Filter	58
11.1 HTTPS Filtering.....	59
12.0 Copy Group Settings	60
13.0 BrowseControl Client Settings.....	61
14.0 CurrentWare Server Manager	63
14.1 Changing the CurrentWare Client and Console Port.....	63
14.2 Stopping the CurrentWare Server Service	64
14.3 Compress the CurrentWare Database.....	64
14.4 Archive and Restore the CurrentWare Database	65
15.0 CurrentWare and Terminal Server	66
16.0 Licensing	67
16.1 Register your Permanent License key	67
16.2 License Management.....	68
17.0 Uninstall CurrentWare Server, Console and Solutions	69
17.1 Uninstalling the CurrentWare Solutions	69
17.2 Uninstalling the CurrentWare Server and Console.....	69
18.0 Uninstall CurrentWare Client.....	70

18.1 Uninstall CurrentWare Client from the Console.....	70
18.2 Uninstall CurrentWare Client on the workstation by command line	71
18.3 Uninstall CurrentWare Client on the workstation from the Client Configuration Window.....	71
19.0 Technical Support.....	72
20.0 Contacts.....	73
USA.....	73
CANADA	73
EUROPE	73
ASIA	73
OTHER COUNTRIES	73

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 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 Windows 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

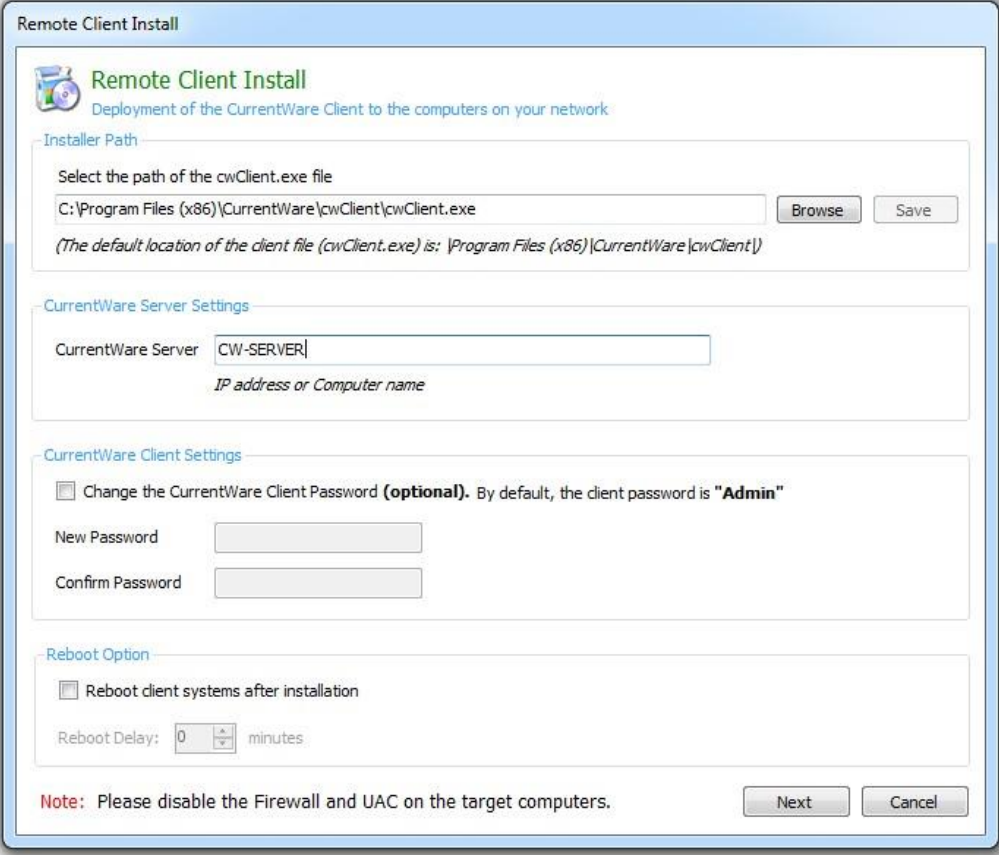
CurrentWare Clients can be remotely installed from the Console. The remote installer can be found on the console under the menu **Install > Remote Client Install**.

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)' and fields for 'New Password' and 'Confirm Password'; and 'Reboot Option' with a checkbox for 'Reboot client systems after installation' 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 titled 'CurrentWare Client configuration' and features the CurrentWare logo on the left. The configuration fields include: 'Enter the IP address / Computer Name where the CurrentWare Server is installed.' with the value '205.145.10.133'; 'Enter the CurrentWare Client password. The default password is 'Admin' (case sensitive).' with a masked password '.....'; 'OPTIONAL - To change the default password, please enter the new password max 15 characters.' with an empty field; and 'Please confirm the password.' with an empty field. At the bottom, there is a 'Version: 5.1' label and three buttons: '< Back', 'Next >', and 'Cancel'.

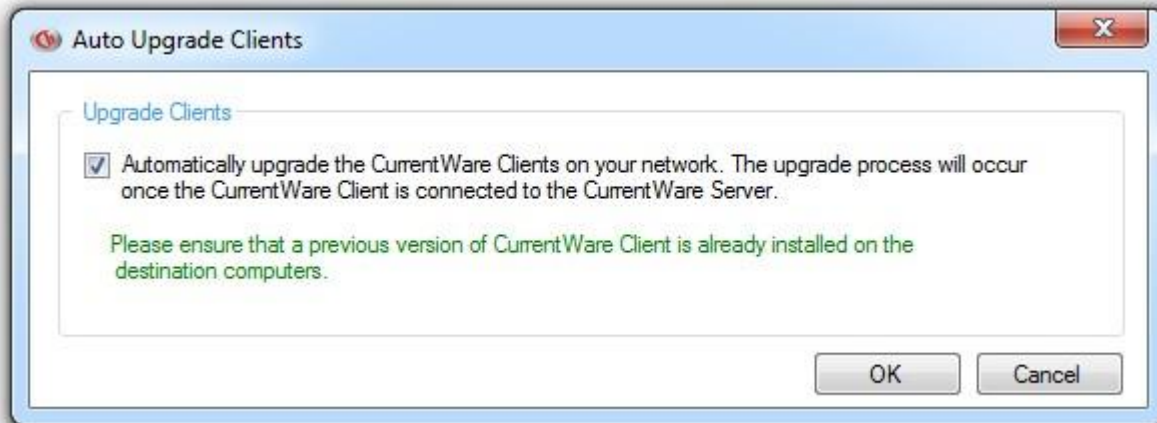
1.6 Upgrading the CurrentWare Clients

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.

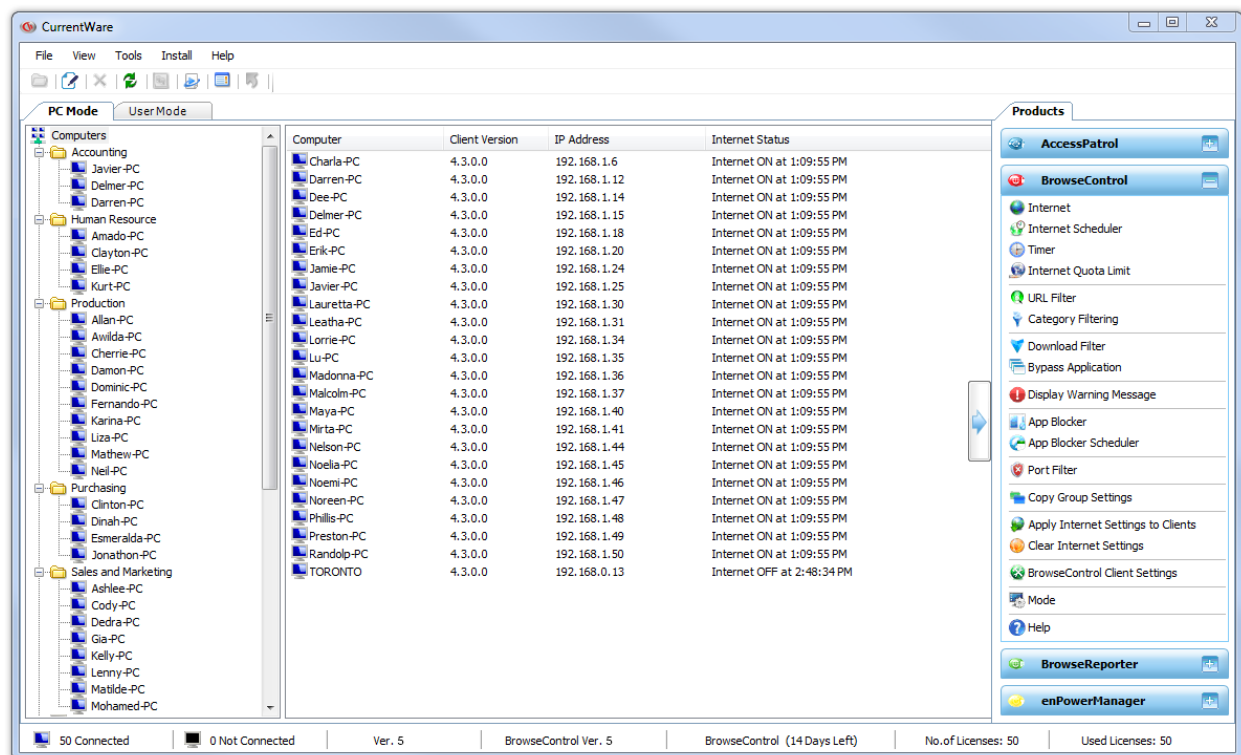
Once you are in user mode, your Terminal Server users will be listed under the User Mode tab automatically after they log onto the terminal server for the first time.

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.

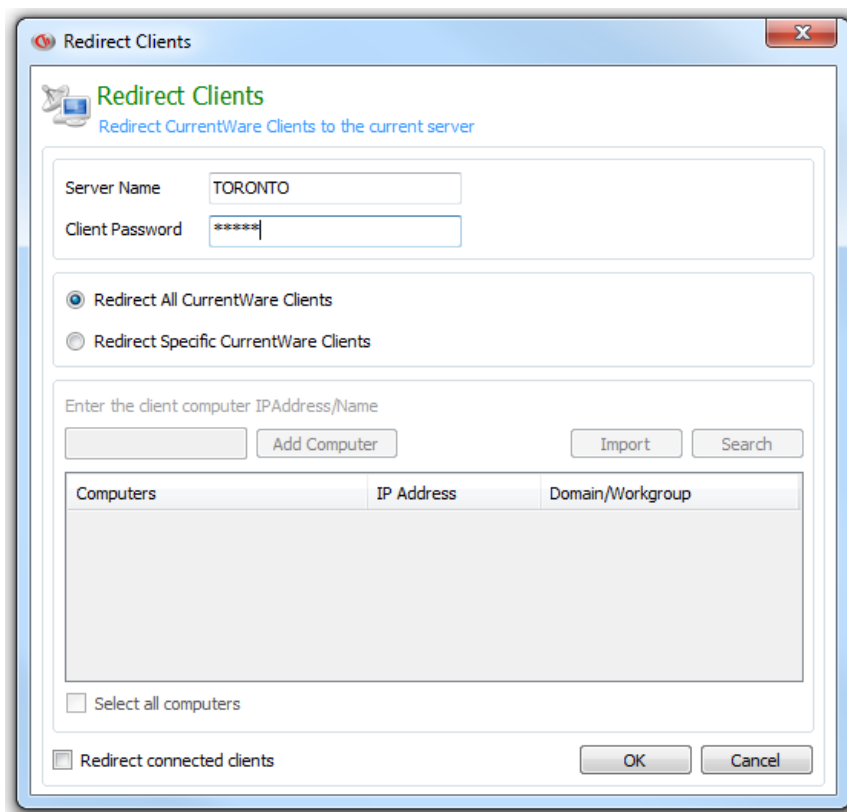
On the CurrentWare Console menu, select **File > Move Computer/Users**. The left hand side contains the source folder and the right hand side contains the destination folder. Select the computer(s) you want to move from the source folder, and then select the destination folder. Click on the >> button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

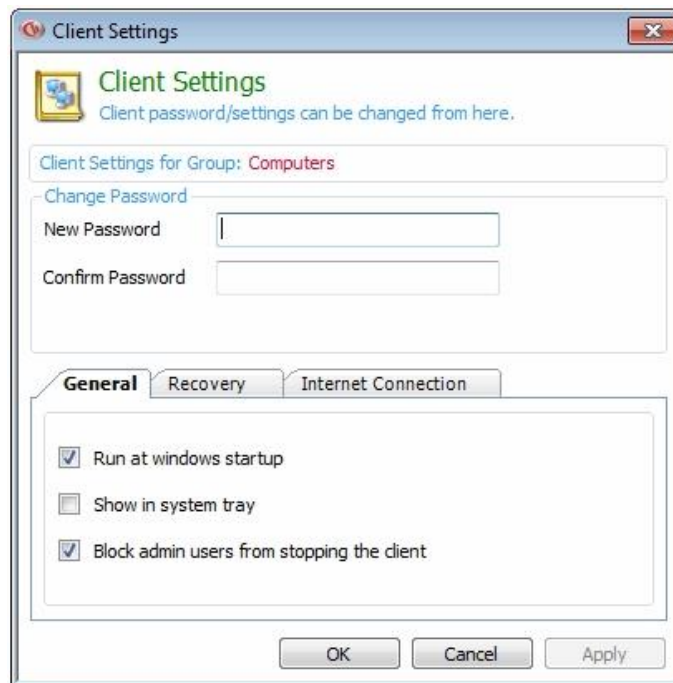
The CurrentWare Client settings can be modified in the CurrentWare Console under **Tools > Client Settings**. You can also right click on a group to find the Client Settings.

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**.

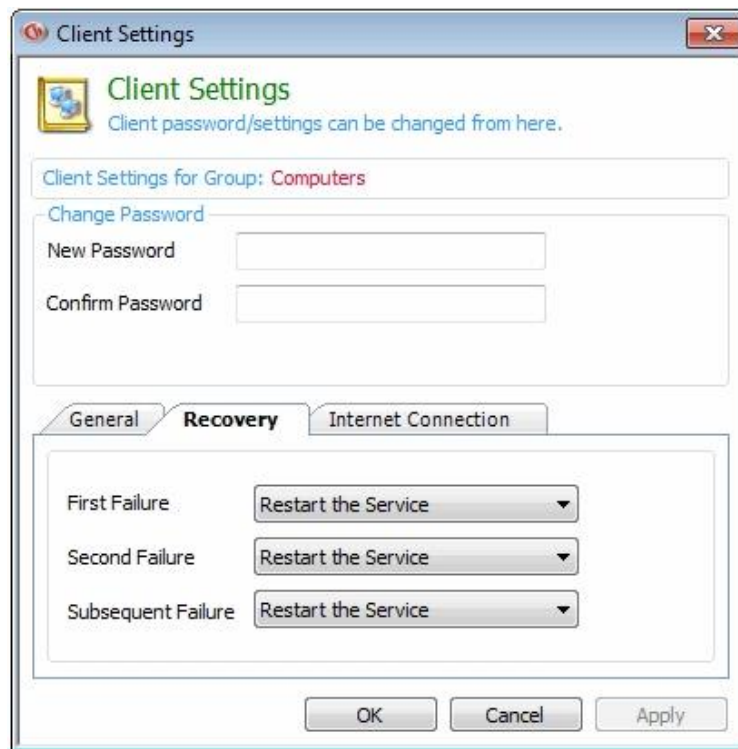
General

- **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.



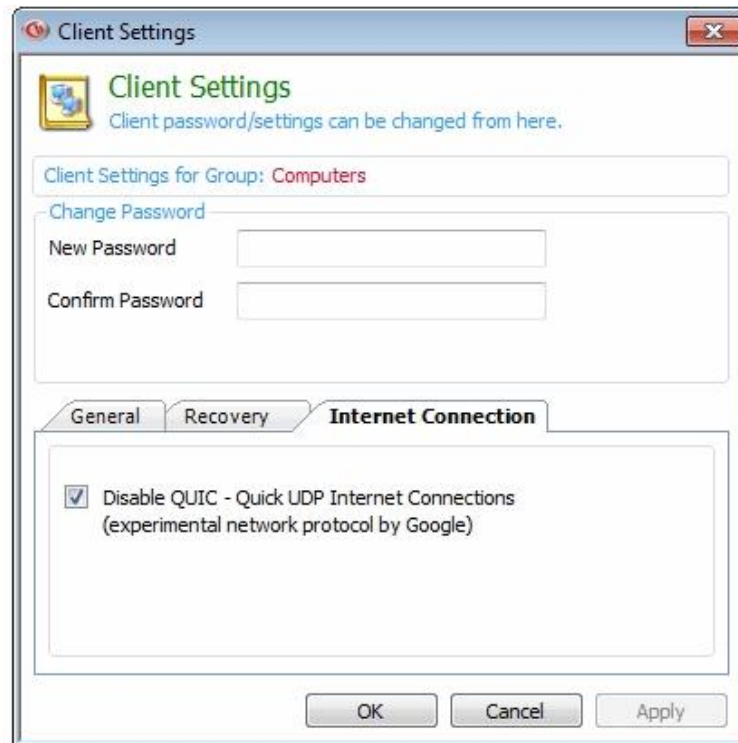
Recovery

- 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.

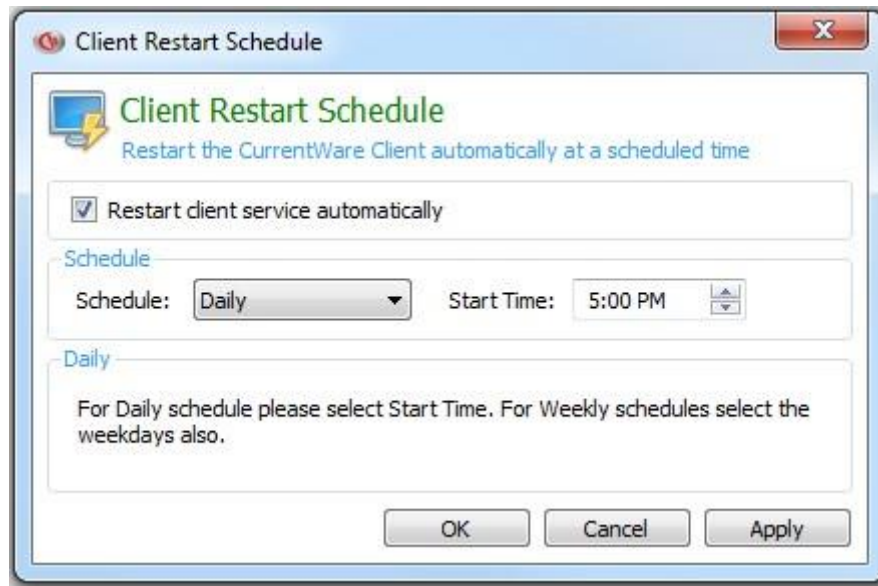


2.4 Troubleshooting

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.

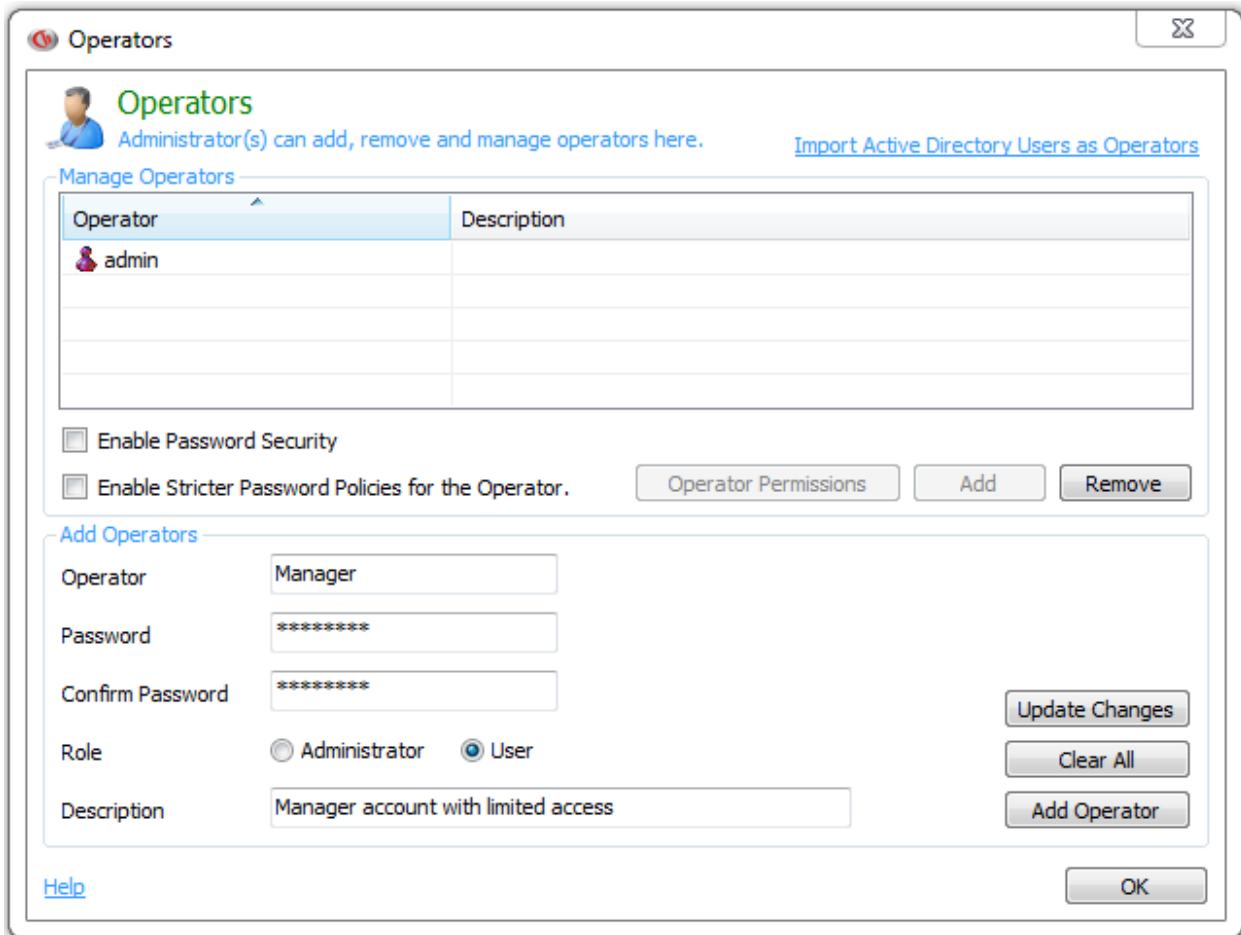
Creating an Operator:

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 Remove

Add Operators

Operator: Manager

Password: *****

Confirm Password: *****

Role: ☐ Administrator ☒ User

Description: Manager account with limited access

Update Changes Clear All Add Operator

[Help](#) OK

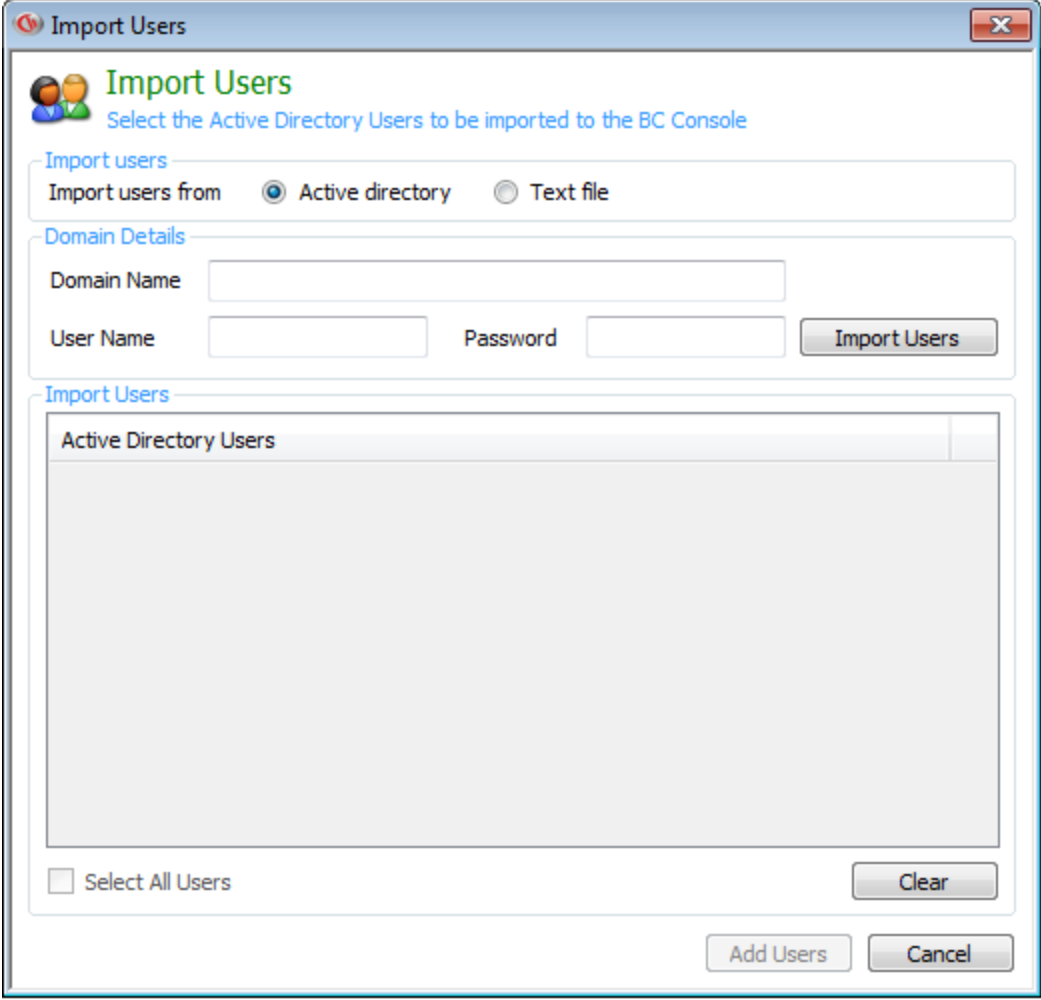
Administrators have unlimited control. Users have limited controls

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

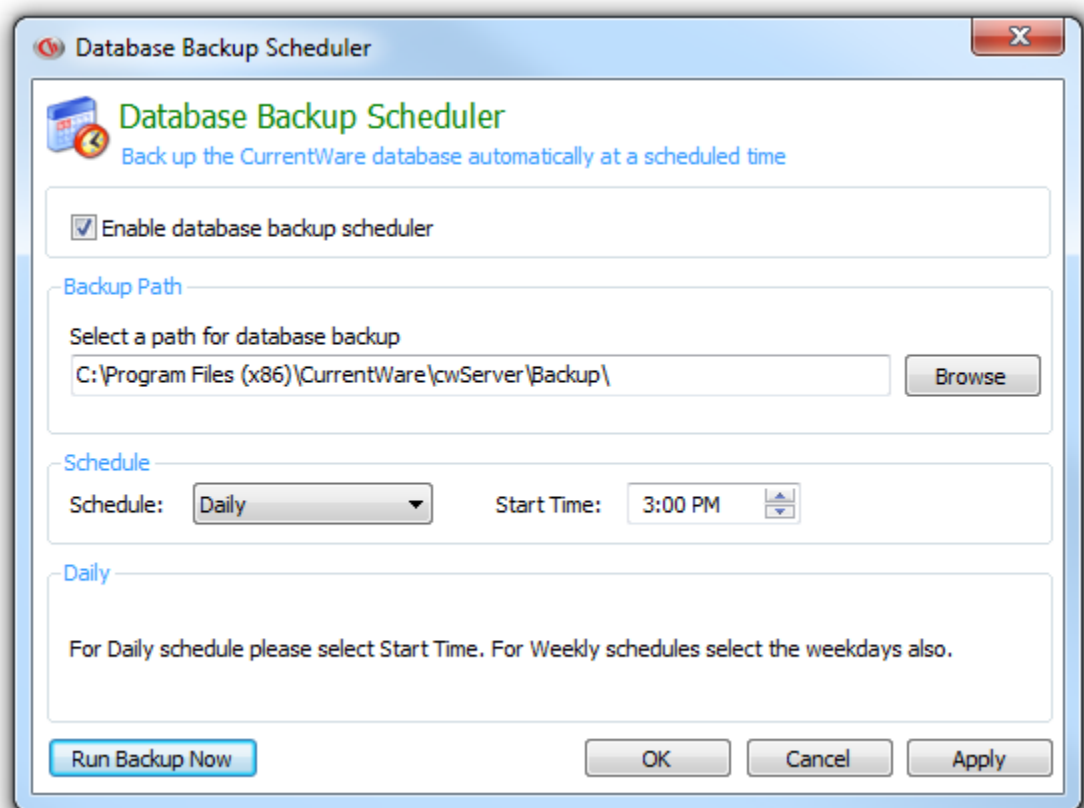
The Database Backup Scheduler automatically backs up the CurrentWare database (CWNPF.B.CWD) at a scheduled time.

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.

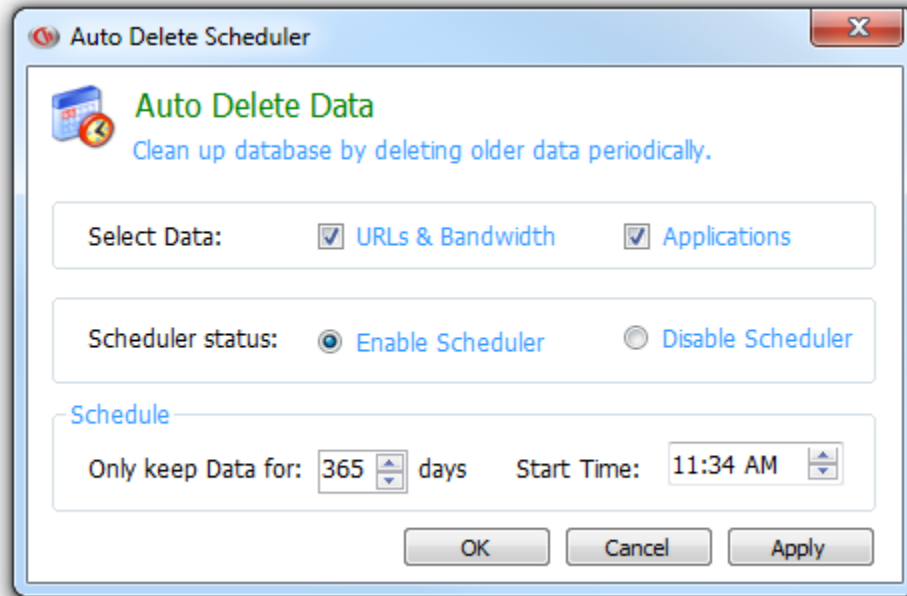
You can perform a one-time back up by clicking on the “Run Backup Now” button.



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.

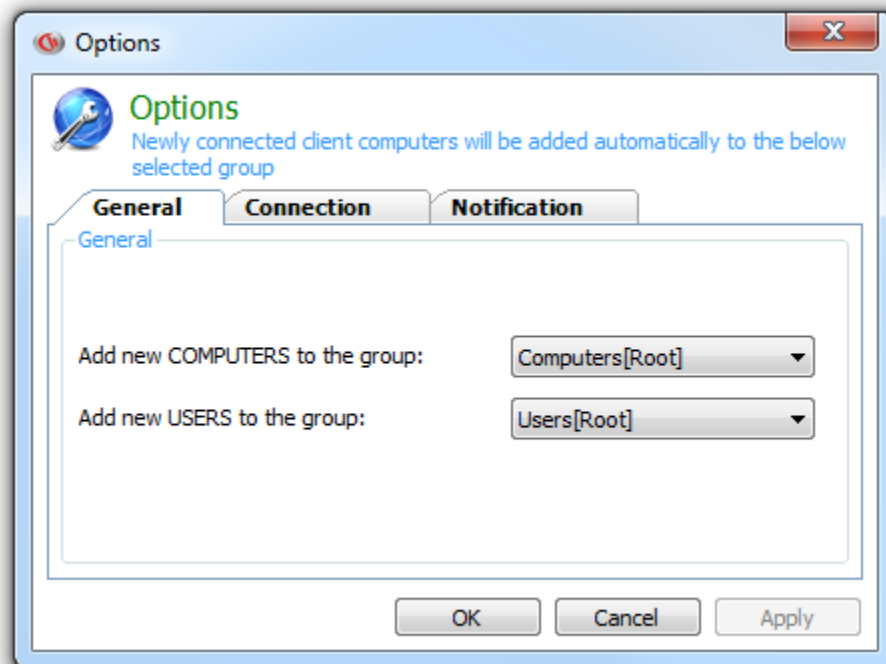
2.9 Options

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.

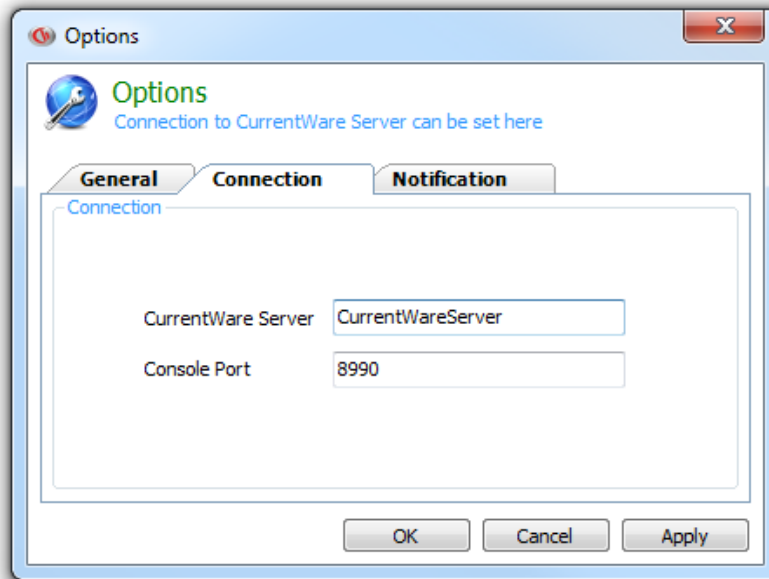
Add new Users to the group: define the group that a new user will automatically be assigned to once it is populated to the CurrentWare Server for the first time.



Connection

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

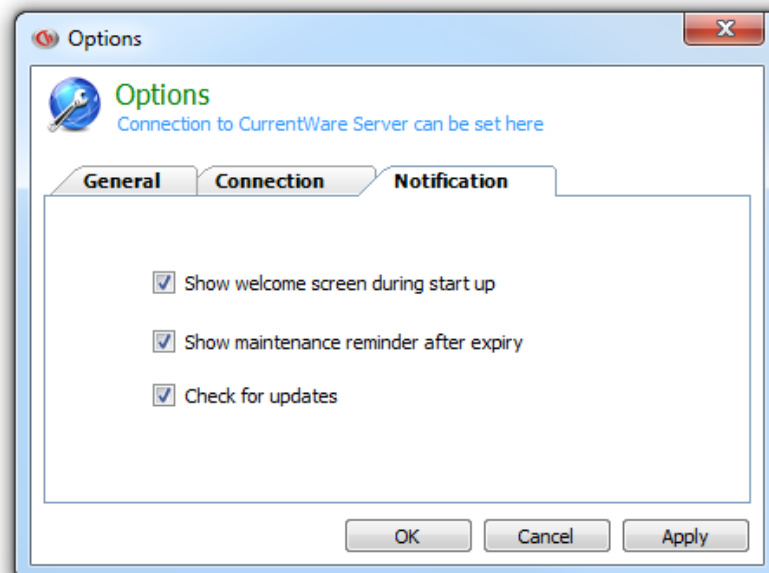
Console Port: The port that CurrentWare Console uses to connect to the CurrentWare Server. The default Console port is 8990.



Notification

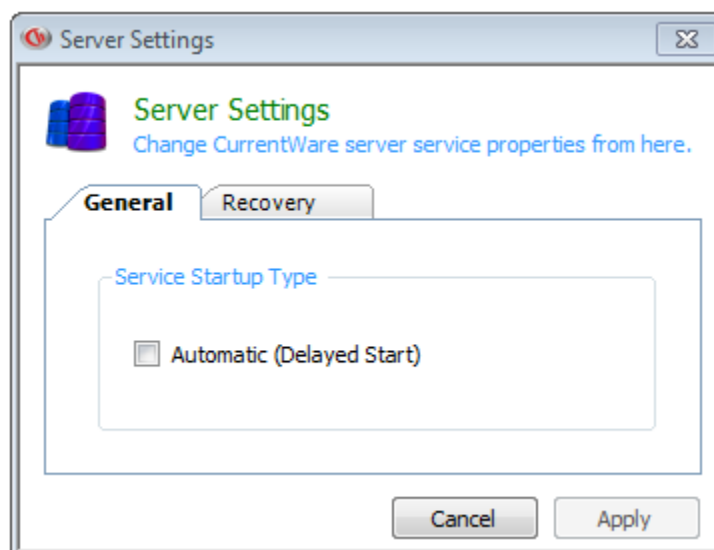
Enable/disable the following notifications:

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



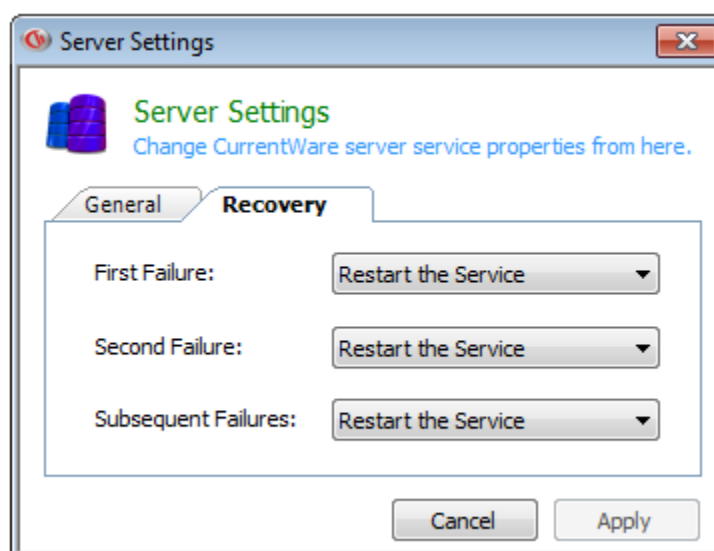
2.10 Server Settings

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

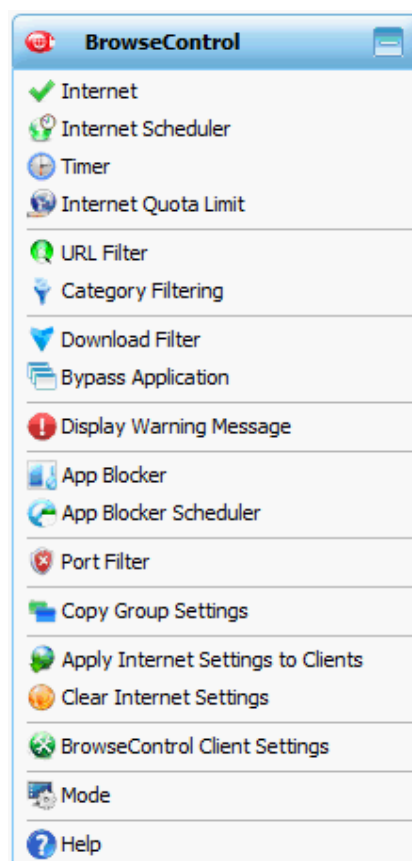
Log Out can be used to re-log into the Console with a different user name and password. This feature can be found under the menu **File → Logout**.

3.0 Overview of 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**
- **URL Filtering**
- **Blocking Users from Downloading Files**
- **Bypass Applications**
- **Application Blocker**
- **Port and Proxy Settings**



BrowseControl Solution Features

4.0 Controlling Internet Access

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

- **Internet ON/OFF**
- **Scheduler**
- **Timer**
- **Internet Quota Limit**

All four settings can be applied at a group level. The Internet ON/OFF feature and the Timer 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.

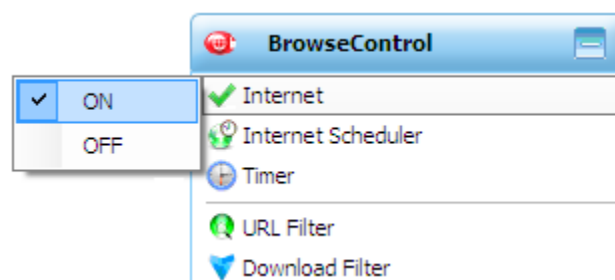
If Internet is set to ON, clients will have complete access to the Internet. (The Blocked list will be activated, see URL filtering for more details)

If Internet is set to OFF, access to any Internet websites will be denied. (The Allowed list will be activated, see URL filtering for more details)

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 tab on the right hand side of the CurrentWare Console, click on Internet and select on or off.

In the CurrentWare console, groups do not inherit settings from their parent groups. The groups stores the CurrentWare settings independently.

The Client settings get priority over its Group settings. For example, if the Internet setting for a Group is set to OFF, you can temporarily override this setting for a specific computer or user and set the Internet to ON for that computer or user. The Client settings will take priority over the Group settings.



4.2 Internet Scheduler

Schedules can be created to allow Internet access at specific times. This is a Group specific setting. Groups can be assigned to three levels of Internet accesses:

1. **Internet ON:** Full access to the Internet and deny access to the URLs listed in the Blocked list.
2. **Custom Allowed List:** Allow access to specific websites. For example, during lunch time you may want to allow users access to additional websites such as facebook.com and myspace.com. This can be achieved by specifying the URLs in the “Custom Allowed URLs” option. When “Custom Allowed URLs” is activated, users can access websites from the “Custom Allowed URLs” list and the global Allowed list from the “URL Filter”. Upon reaching the scheduled end time, the user will only be allowed to browse the authorized websites from the URL Filter’s Allowed list.
3. **Custom Blocked List:** Deny access to unauthorized sites. Users will be denied access to websites listed in the Custom Blocked list during the scheduled time.

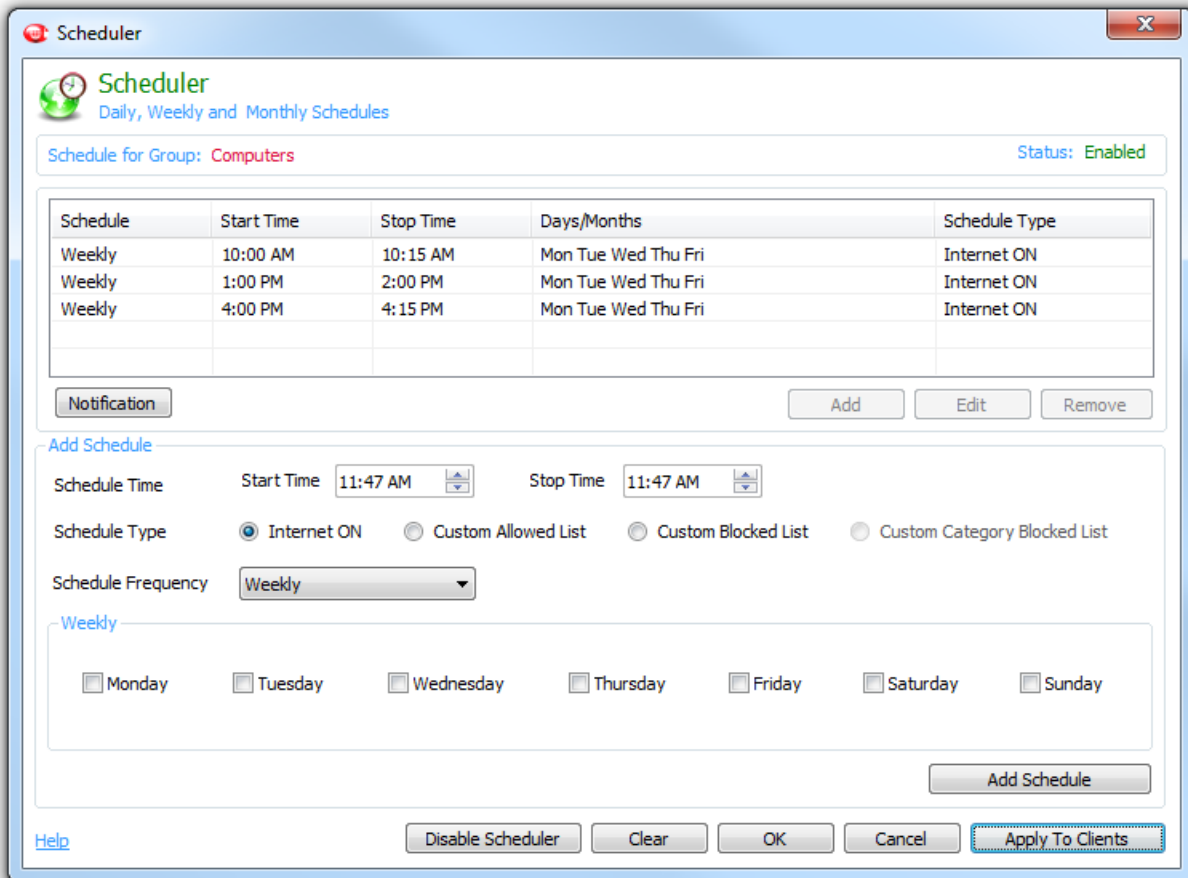
Creating an Internet Schedule

1. Highlight the group you want to assign a scheduler to and select **Internet Scheduler** under the BrowseControl tab 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**



Scheduler
Daily, Weekly and Monthly Schedules

Schedule for Group: **Computers** Status: **Enabled**

Schedule	Start Time	Stop Time	Days/Months	Schedule Type
Weekly	10:00 AM	10:15 AM	Mon Tue Wed Thu Fri	Internet ON
Weekly	1:00 PM	2:00 PM	Mon Tue Wed Thu Fri	Internet ON
Weekly	4:00 PM	4:15 PM	Mon Tue Wed Thu Fri	Internet ON

Notification Add Edit Remove

Add Schedule

Schedule Time Start Time: 11:47 AM Stop Time: 11:47 AM

Schedule Type ☒ Internet ON ☐ Custom Allowed List ☐ Custom Blocked List ☐ Custom Category Blocked List

Schedule Frequency: Weekly

Weekly

☐ Monday ☐ Tuesday ☐ Wednesday ☐ Thursday ☐ Friday ☐ Saturday ☐ Sunday

Add Schedule

Help Disable Scheduler Clear OK Cancel **Apply To Clients**

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

Internet Scheduler Scenarios

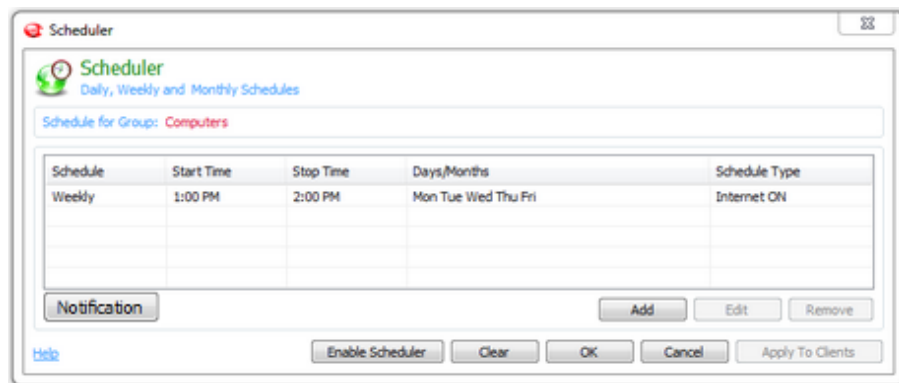
Companies enforce different Internet policies during different times of the day. Below are a few examples that you can use to set up the Internet scheduler suitable for your network.

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.*)



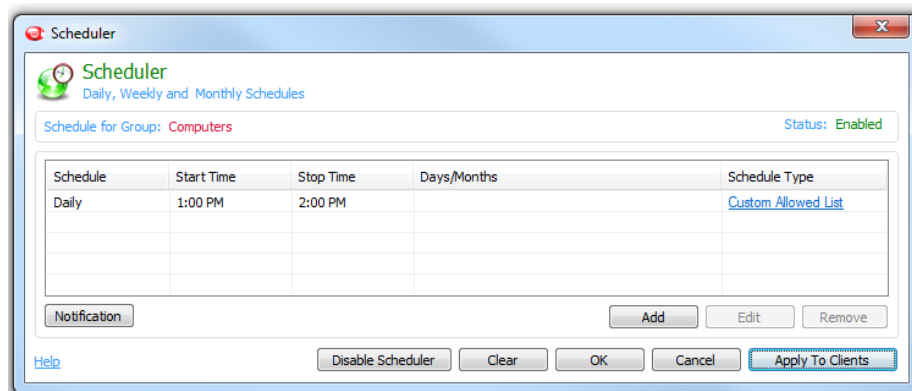
The Internet is set to ON during lunch. All other times, the Internet is OFF.

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.



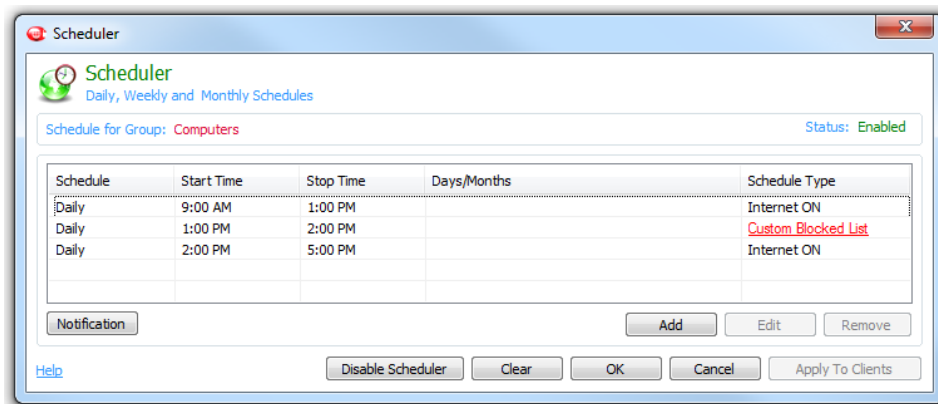
Custom Allowed list is used during lunch hour to add additional websites to the Allowed list

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:

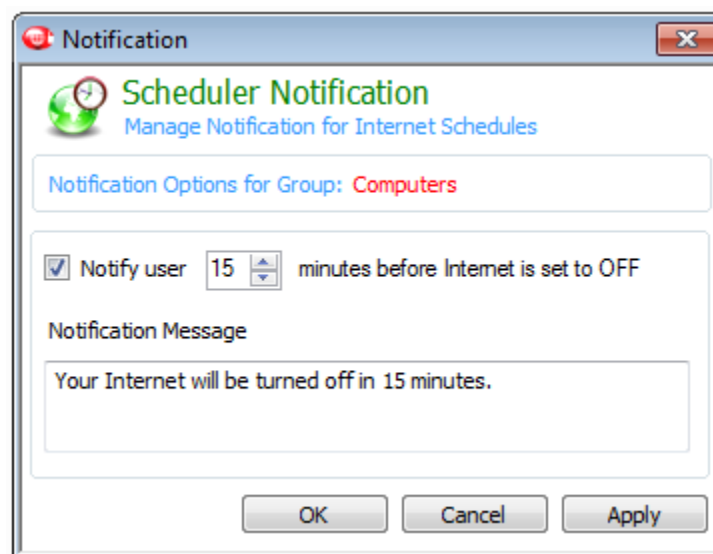
- During standard hours (*9:00 A.M. to 1:00 P.M. and 2:00 P.M. to 5:00 P.M.*), the user will not have access to the websites from the original Blocked list under the URL filter
- During lunch hours (*1:00 P.M. to 2:00 P.M.*), the user will not have access to the websites from the Custom Blocked list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

Notification

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

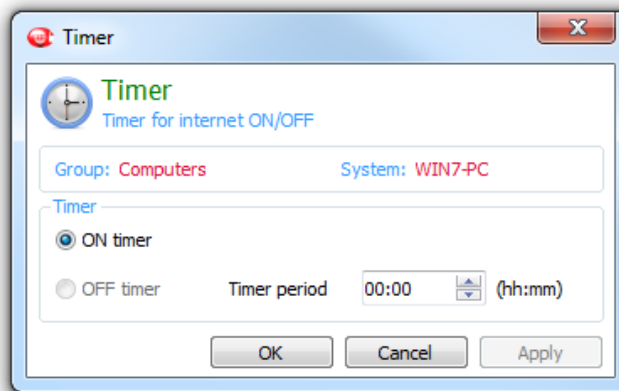


4.3 Timer

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 tab 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.

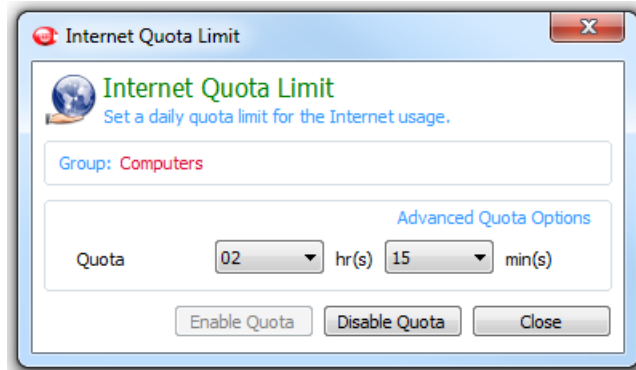


The Timer will temporary allow Internet access to the user for a predefined period of time.

4.4 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

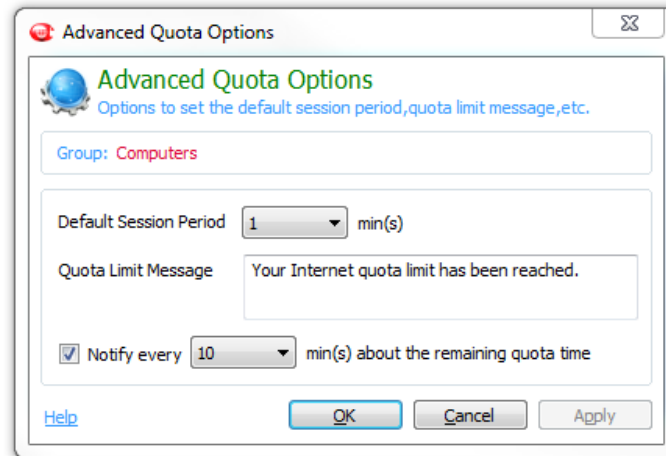
counting down as soon as the quota is enabled. The users will get notification messages on their computers about how much remaining time they have for their Internet quota.



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

4.4.1 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.

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.

The Allowed List and Blocked List are activated based on the Internet settings that you have selected. The scenarios below show when the Allowed List or the Blocked List is activated.

If Internet is OFF, Allowed List is activated. The users will only be able to access the websites that are on the Allowed List.

If Internet is ON, Blocked List is activated. The users will be able to access any websites except for the websites that are on the Blocked List.

5.1 Allowed List

BrowseControl has the functionality to allow access to certain web sites when the Internet connection has been turned OFF. This feature, referred to as the Allowed List, is available to Groups only. That is, the Allowed List is Group specific and cannot be applied to individual computers or users. Since this functionality is group specific, you can have certain URLs available to Clients within one group and deny access to Clients in other groups. Outlined below are the steps for applying the Allowed List.


How to Create an Allowed list for your group

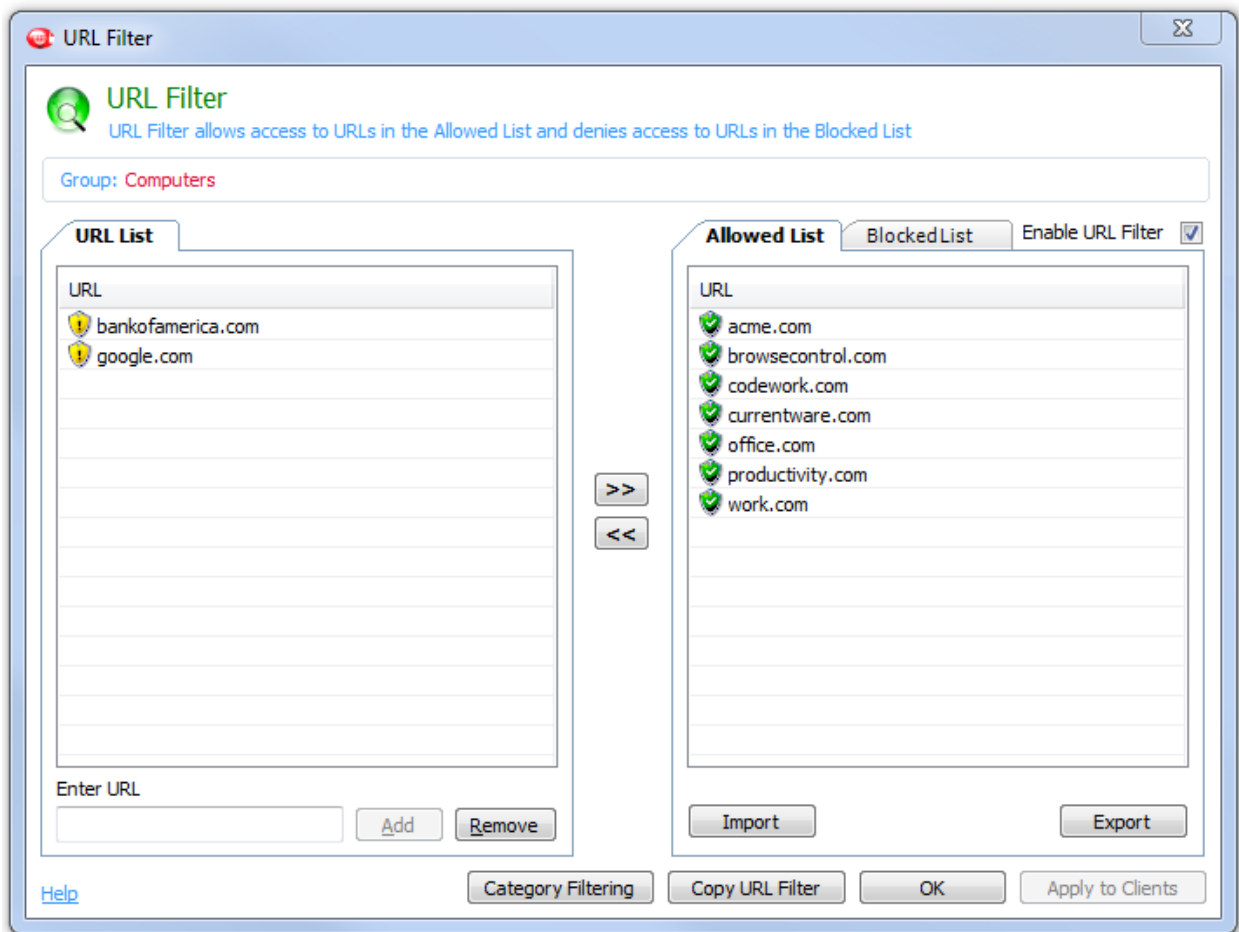
1. Select the group for which you want to create the Allowed list for.
2. Under the BrowseControl tab on the right hand side of the CurrentWare Console, click on **Internet** and select **OFF**. This will disable their Internet access completely.
3. Under the BrowseControl tab, click on **URL Filter** 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.

NOTE: When entering URL addresses, **do not enter <http://> or <https://> before your website**. The <http://> prefix will cause BrowseControl to ignore that website altogether and the website will not be allowed in this scenario if it has the <http://> prefix.

For example, if you would like to give access to <http://www.currentware.com>, on the Allowed list, put in www.currentware.com without the <http://>. To give access

to the entire domain of www.currentware.com, simply add **currentware** to the Allowed List.

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. This feature, referred to as the Blocked List, is available to Groups only. That is, the Blocked List is Group specific and cannot be applied to an individual computer or user.

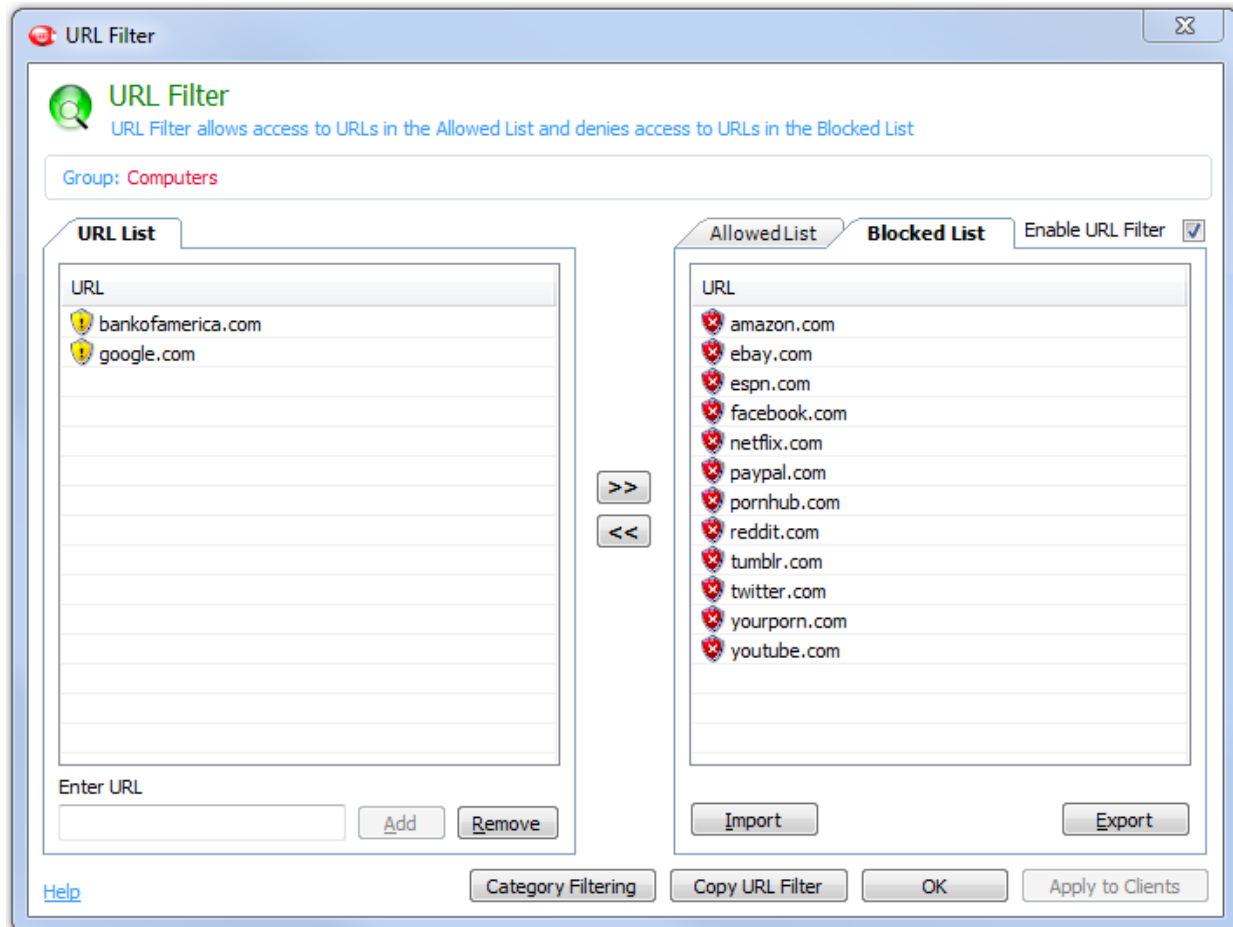
How to Create a Blocked list for your group

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

NOTE: When entering URL addresses, **do not enter http:// or https:// before your website**. The http:// prefix will cause BrowseControl to ignore that website altogether and the website will not be blocked in this scenario if it has the http:// prefix.

For example, if you would like to block access to <http://www.facebook.com>, on the Allowed list, put in www.facebook.com without the http://. To block access to the entire domain of www.facebook.com, simply add **facebook** to the Blocked List

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

5.3 Importing URLs to the Allowed List or Blocked List by text file

1. Under the BrowseControl tab, 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**

5.4 Exporting URLs from the Allowed List or Blocked List by text file

1. Under the BrowseControl tab, 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 import, each URL should be listed on a new line
4. Click **Apply to Clients**

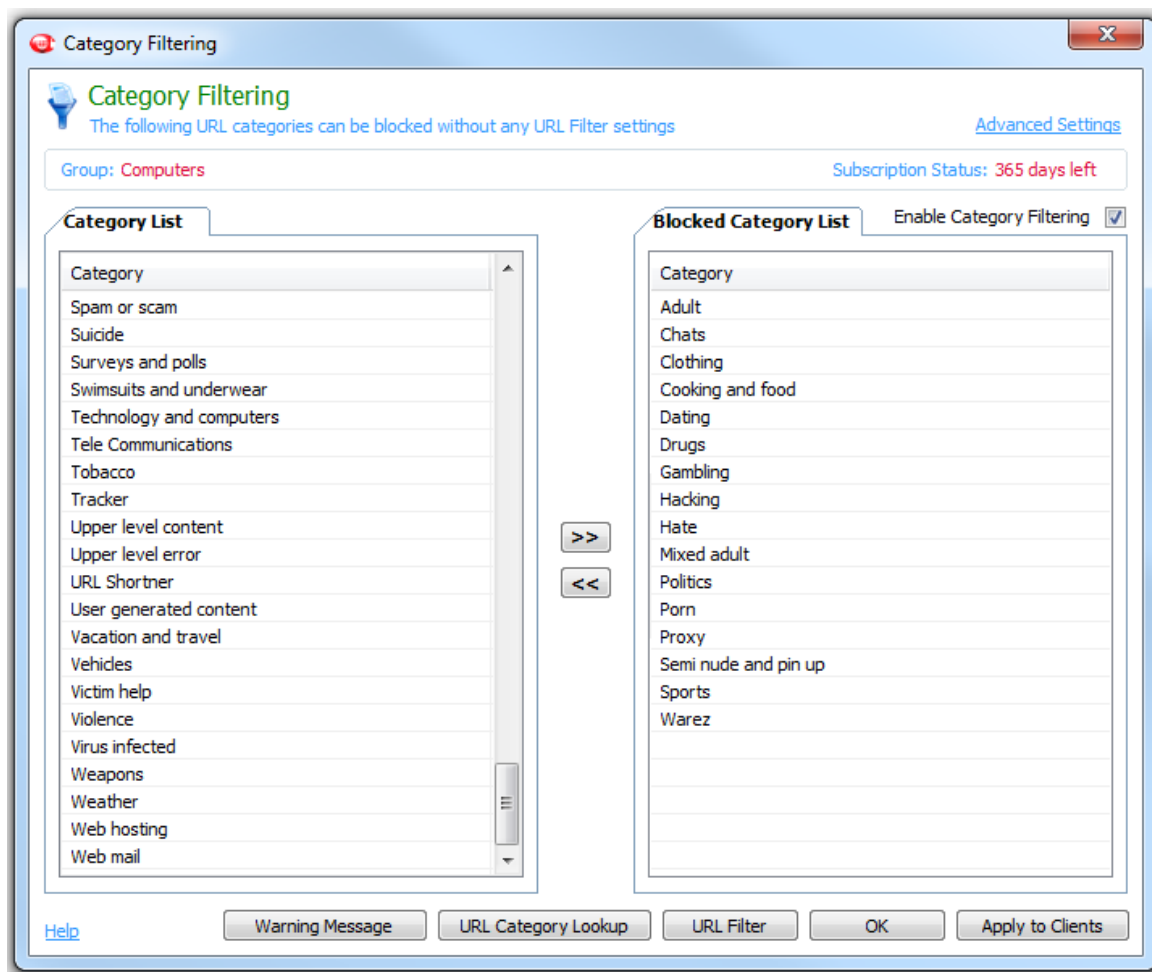
6.0 Category Filtering

CurrentWare's extensive Category Filtering, comprising of a diverse listing of more than 108 URL categories provides the added control of managing website accessibility beyond the simple list of URLs.

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 web sites is instantly facilitated by simply selecting categories to be blocked from a range of 108 URL Category filters.

You can choose from 108 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.

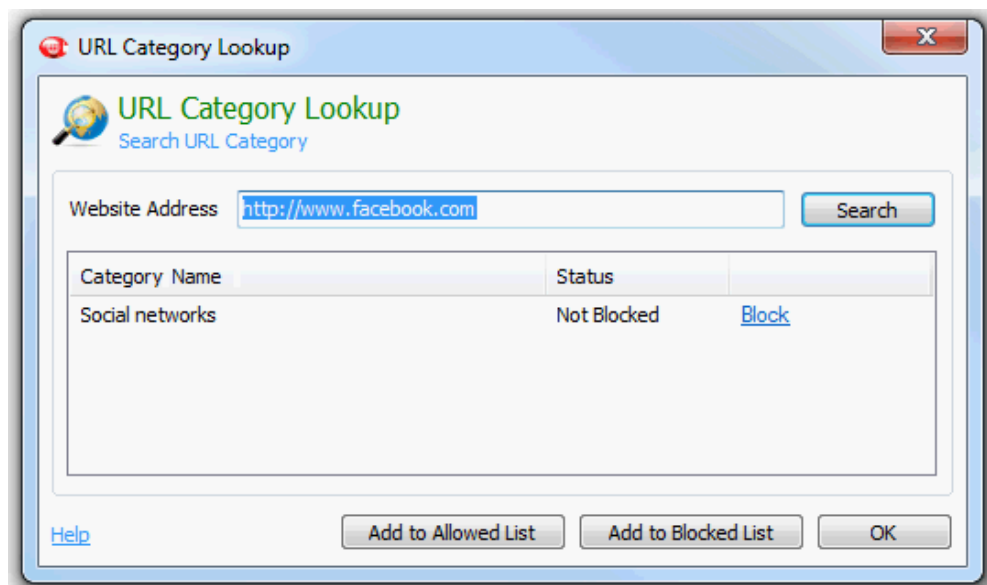


How to Block Websites using Category Filtering

1. Under the BrowseControl tab 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 select 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.

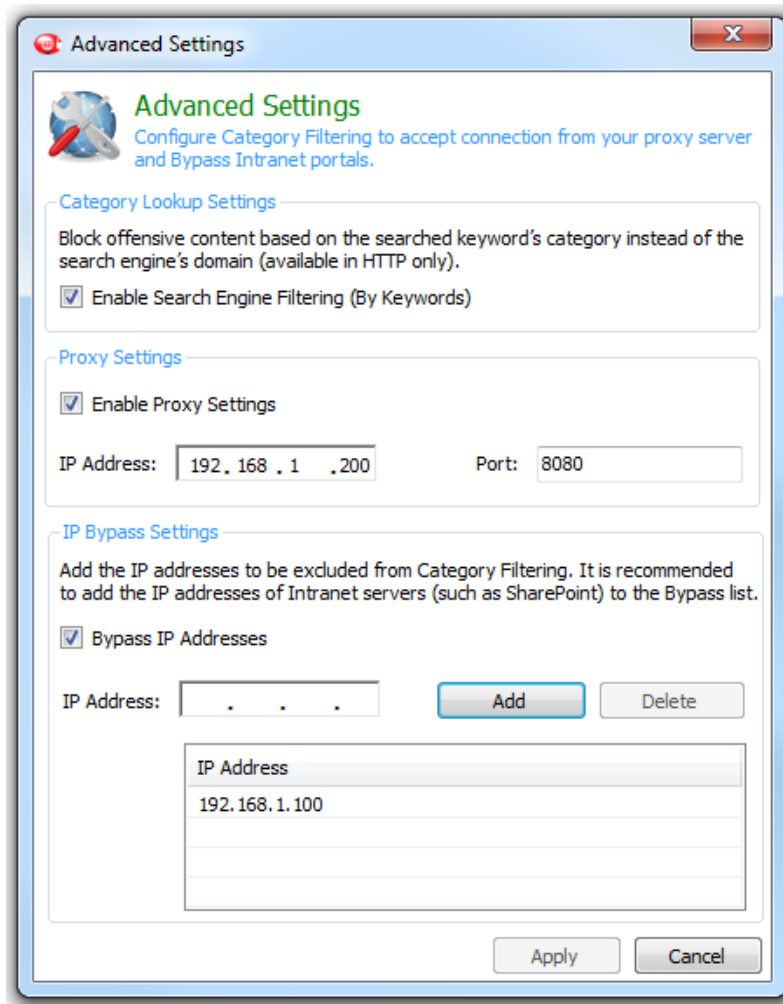
How to lookup websites and their corresponding category listing

1. Under the BrowseControl tab 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 engine 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 Download Filter

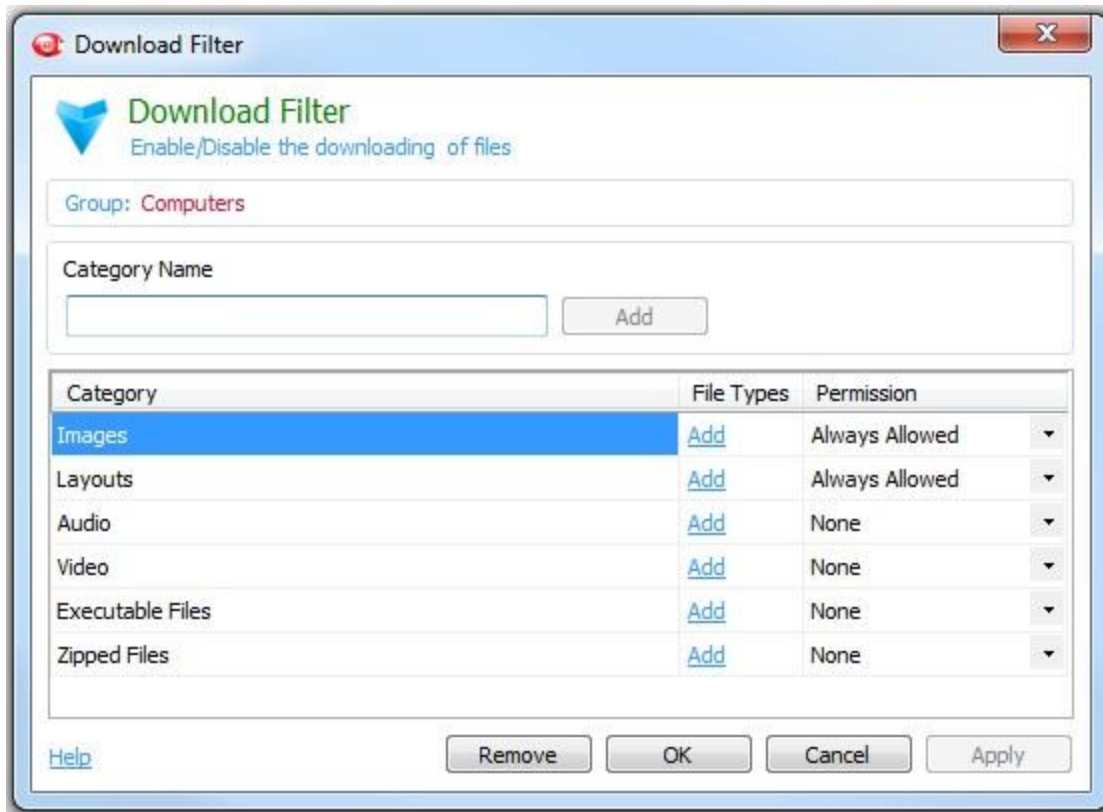
The Download Filter is a list of file extensions that the administrator can allow or deny the users from accessing while they are surfing the Internet.

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

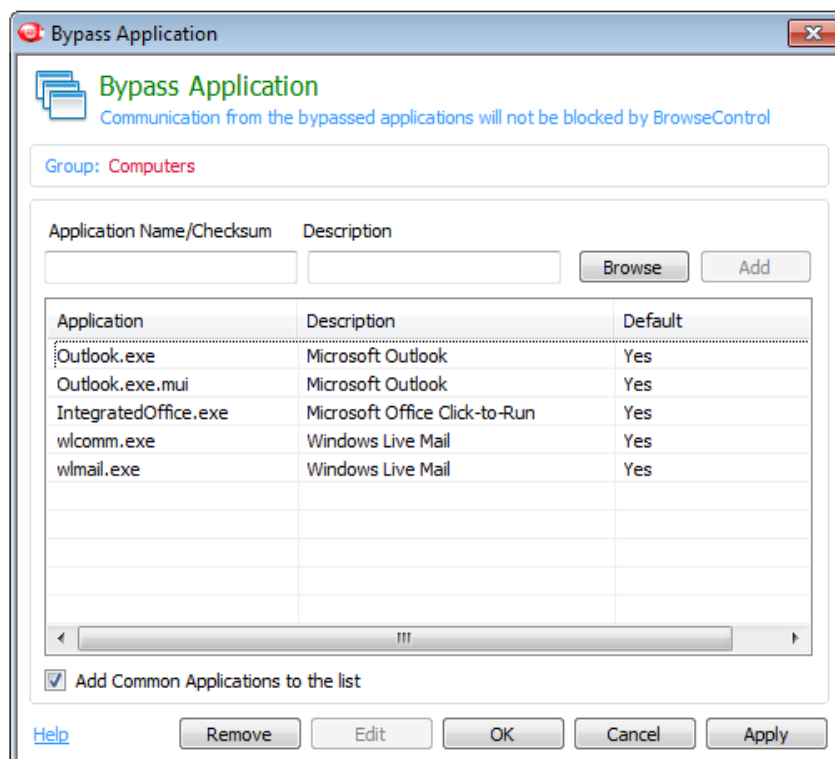
1. Under the BrowseControl tab on the right hand side of the CurrentWare console, select **Download Filter**
2. In the Category Name text box, add a name for the Download Filter and click on the **Add** button.
3. Click on the **Add** link under the File Type column for the category that you just created
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.

8.0 Bypass Applications

When BrowseControl is activated, it monitors the incoming and outgoing traffic from HTTP (port 80). Most of the time, only Internet browsers use port 80 to display websites. However, some networks have software that may use port 80 to transmit packets over the network. For example, some software needs to retrieve update information through port 80. For this type of a situation, you need to add the software that is using port 80 to BrowseControl's Bypass Application List.

Applications added to this list will be unaffected by BrowseControl's Internet ON/OFF settings. This is useful for legitimate applications that require access over HTTP. They can be added as follows:

1. Under the BrowseControl tab, click on **Bypass Application**
2. Under the "Application List," enter the Original Filename of the application to be bypassed, in the "Application Name" textbox.
3. Alternatively, click on the Browse button and locate the .exe file of the application to be bypassed. The Original Filename of the application will automatically be populated in the list. In case the application does not have an Original Filename the application will automatically populate the Application list with the File's Checksum value.



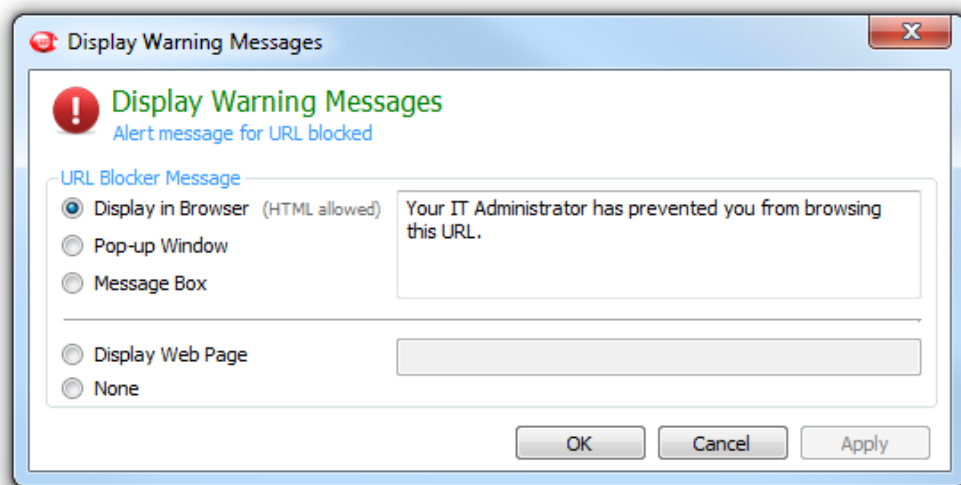
Add applications to the Bypass list to allow complete network access for the defined applications

9.0 Display Warning Message

The alert received by the users when accessing unauthorized websites can be customized in the Display Warning Message option.

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 for when a website is not available.



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

10.0 Application Blocker

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

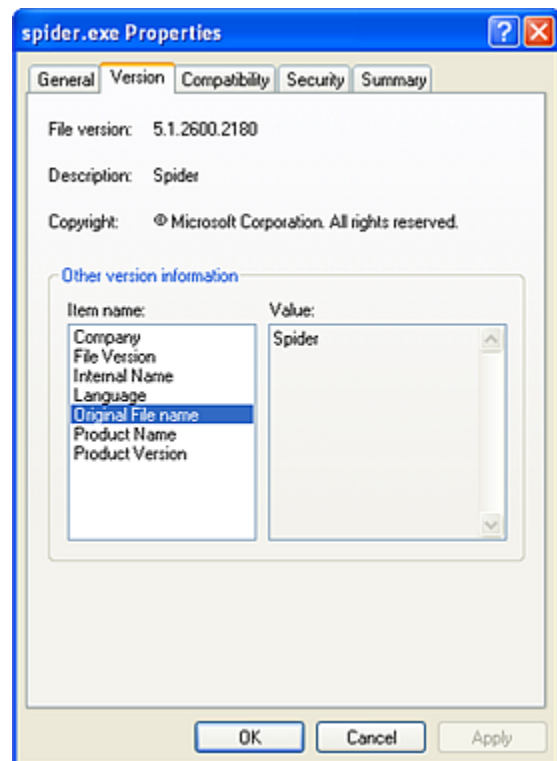
This feature is Group specific. As a result you can block certain applications to computers and users within one group, and specify a different blocked list for other groups

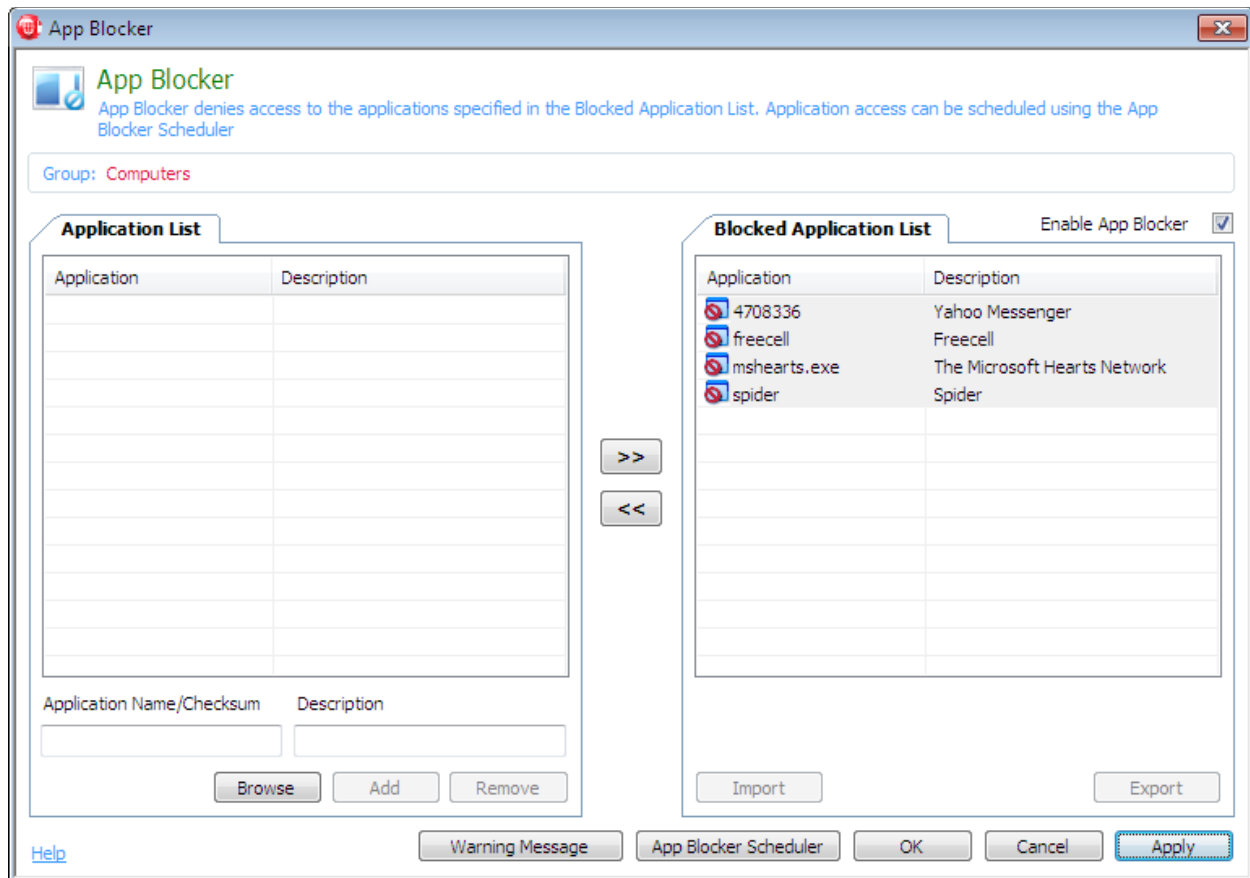
How to block your users from launching an unauthorized application

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 >> 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

10.1 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.

10.2 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.

10.3 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 you are able to import, each applications should be listed on a new line
3. Click **Apply to Clients**

10.4 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 you are able to import, each applications should be listed on a new line
3. Click **Apply to Clients**

11.0 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.

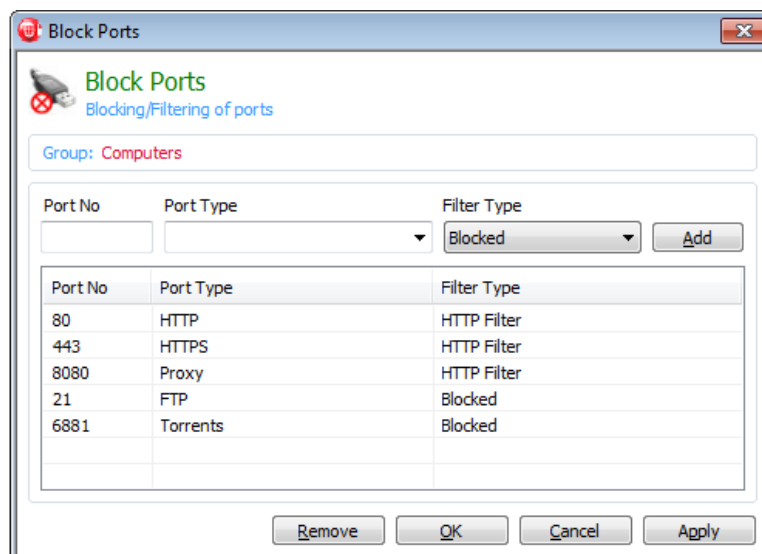
By default, the following ports are added to the Port Filter as HTTP filter:

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

11.1 HTTPS Filtering

The HTTPS filtering function for BrowseControl is compatible with all of the popular Internet browsers.

HTTPS websites can only be controlled in the domain level. You can only allow or block HTTPS websites by the domain. If a domain is allowed or blocked, all of the subdirectories are also allowed or blocked. However, you cannot allow or block a single subdirectory under a domain.

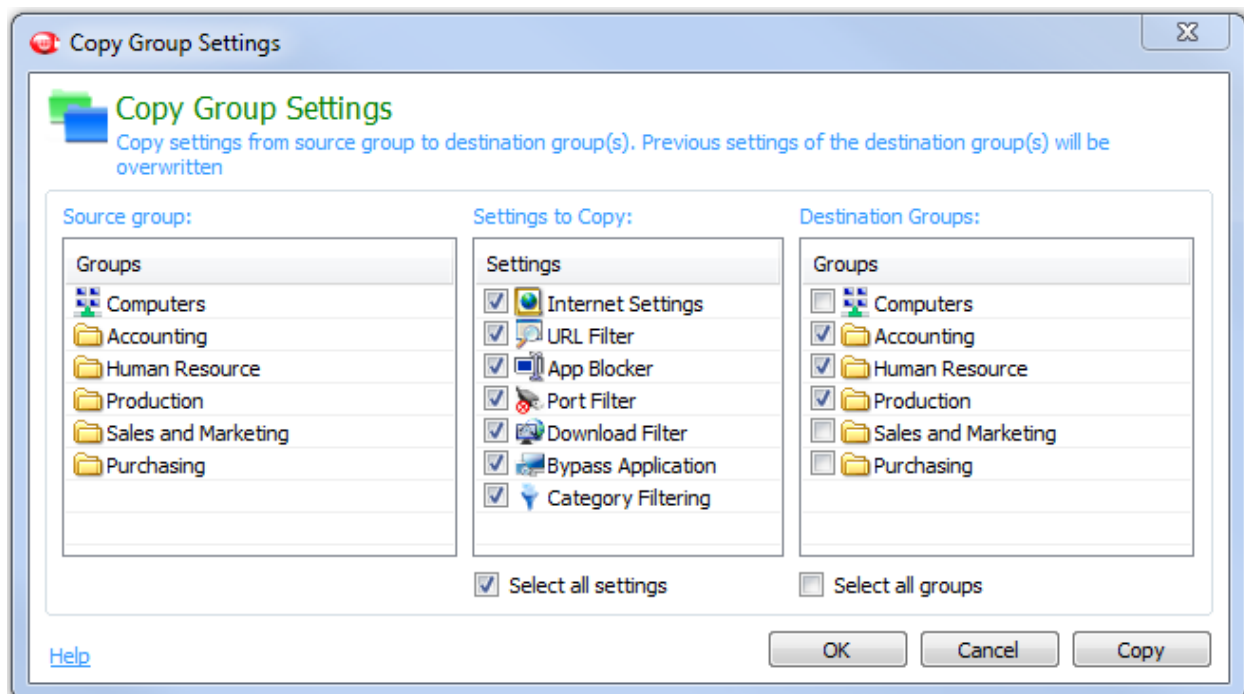
12.0 Copy Group Settings

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

13.0 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.

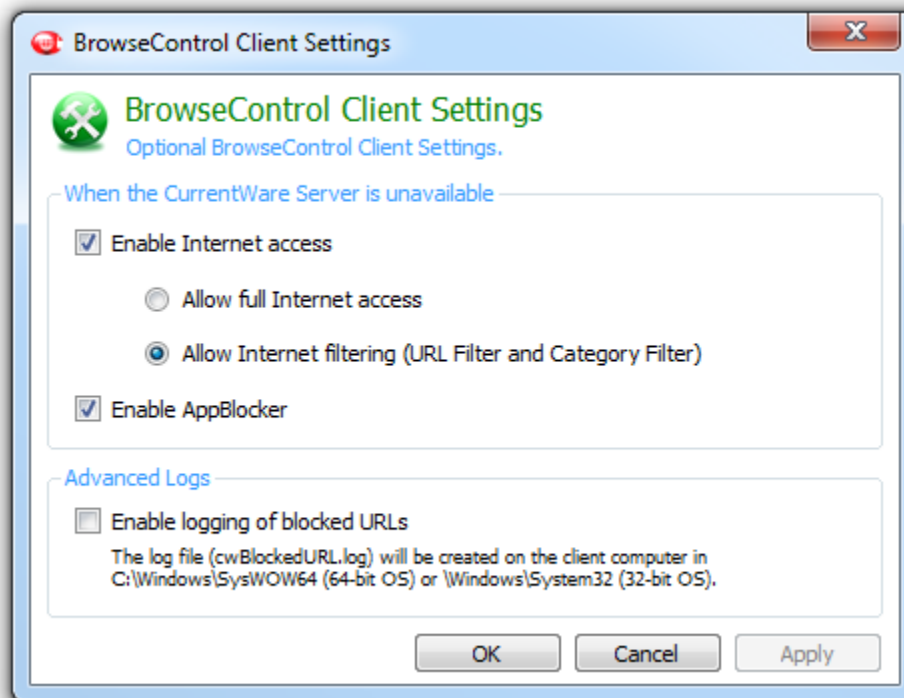
Enable Internet Access when the CurrentWare Server is unavailable

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.

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.

14.0 CurrentWare Server Manager

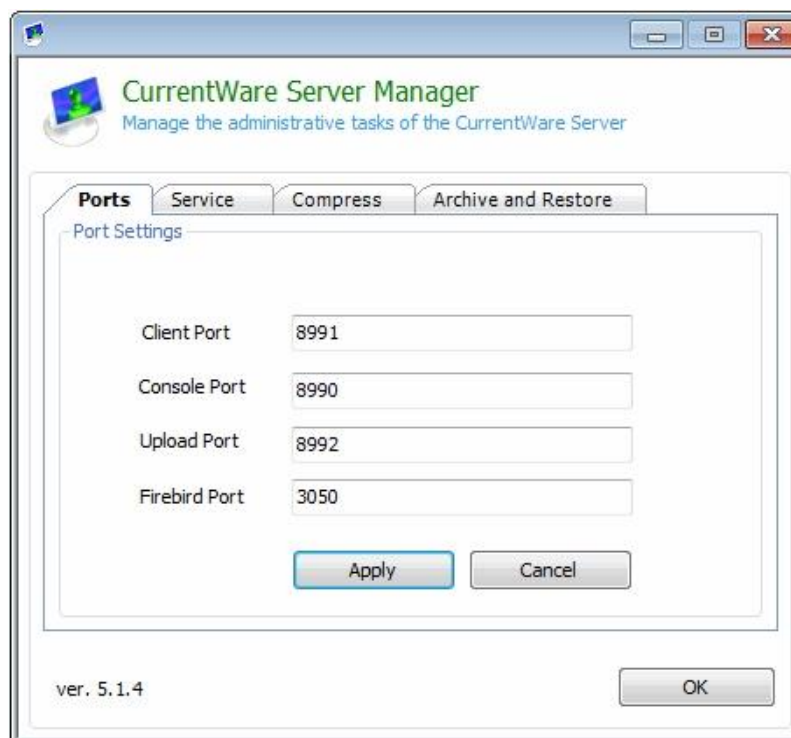
The CurrentWare Server Manager is used to manage the administrative tasks of the CurrentWare Server.

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

14.1 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.

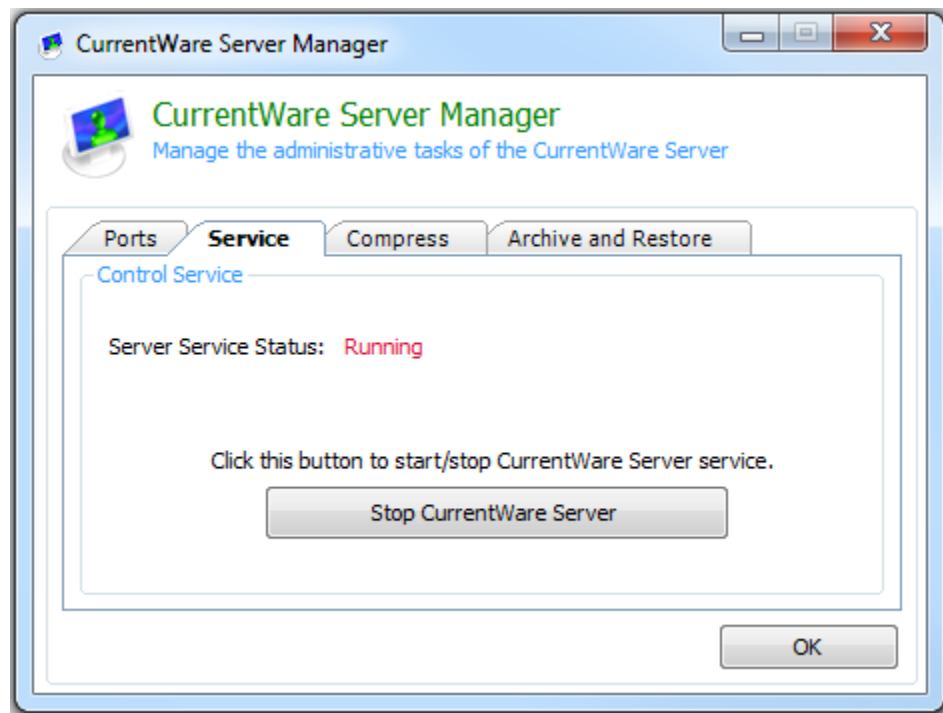
The default ports are listed in the screenshot below.



CurrentWare Server Manager

14.2 Stopping the CurrentWare Server Service

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



14.3 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.

14.4 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.

15.0 CurrentWare and Terminal Server

The CurrentWare Console is supported on a Windows Terminal Server.

The CurrentWare Console for a terminal server is compatible for up to 65 concurrent connections. Beyond this maximum number of connection, some of the CurrentWare functionalities may not work properly. It is advised that you do not have more than 65 users connected to the Terminal Server simultaneously.

The terminal server license is based on a per-user basis. Only one CurrentWare client can be installed on the terminal server computer.

16.0 Licensing

CurrentWare Solutions are licensed on a per-computer basis for client management, while Terminal Server clients are licensed on a per-user basis.

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.

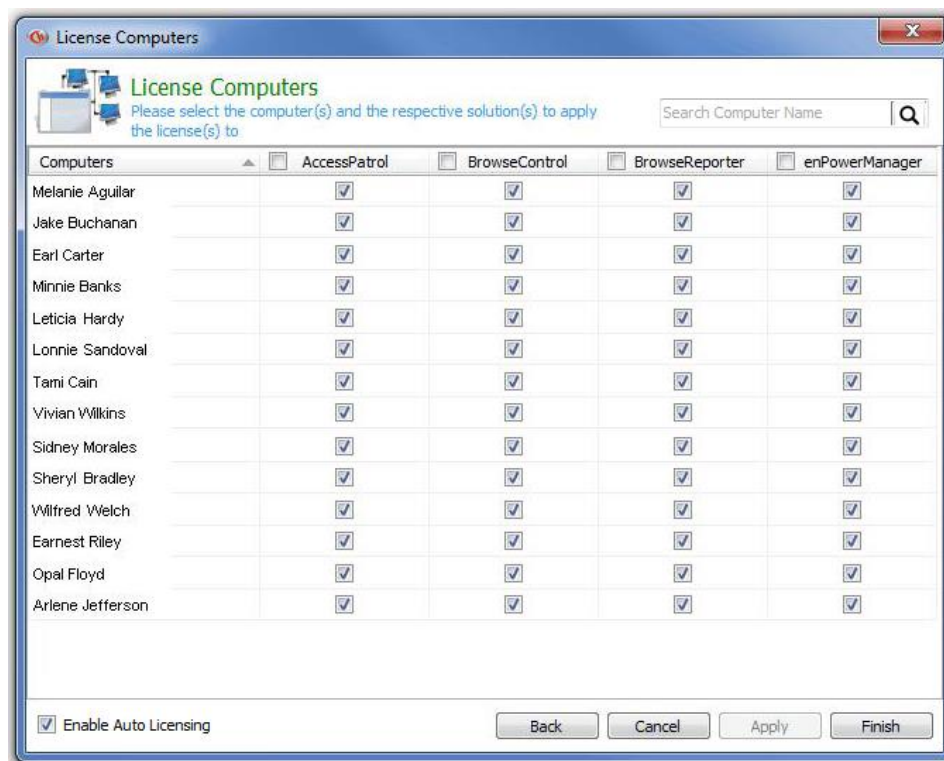
16.2 License Management

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.

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:

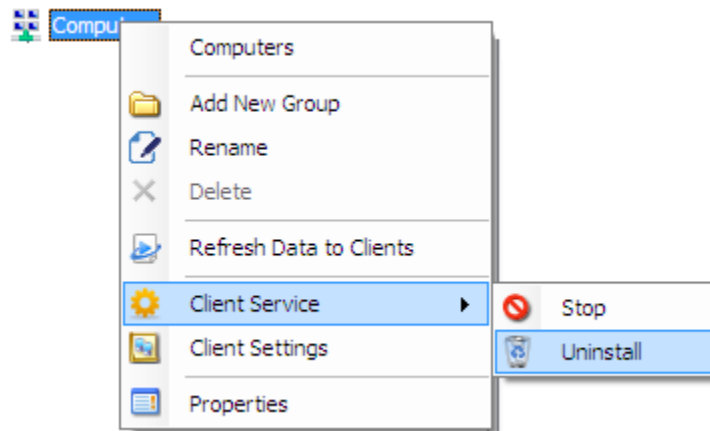
1. **Uninstall CurrentWare Client from the Console**
2. **Uninstall CurrentWare Client on the workstation by command line**
3. **Uninstall CurrentWare Client on the workstation from the Client**

Configuration Window

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 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.

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.