User Guide

Revised in Sept, 2016

CurrentWare Gateway

Version 2.0

Internet Gateway

Table of Content

1.0 Introduction to CurrentWare Gateway 4

1.1 CurrentWare Gateway Features 5

2.0 Installing the CurrentWare Gateway 7

2.1 System Requirements 7

2.2 Configuring your Network for Gateway 9

2.3 Software Installation 12

3.0 Console Overview 18

4.0 Manage Page 19

4.1 The Root Group 20

4.2 Device Discovery 20

5.0 Policies Page 22

5.1 Overview 22

5.2 Add Policy 23

5.3 Using the Scheduler 27

6.0 Reports Page 29

6.1 Overview 29

6.2 Dashboard 30

6.2.1 Header Options - Dashboard 32

6.3 Reports 33

6.3.1 Header Options - Reports 36

6.3.2 Create Custom Reports 39

7.0 Settings Page 40

7.1 General Settings 40

7.2 Internet Filter 43

7.3 Internet Monitor 45

1.0 Introduction to CurrentWare Gateway

The CurrentWare Gateway is a server based solution which provides effective Internet filtering and monitoring functionalities for managing multiplatform devices. It can control and track Internet access on desktop computers, laptops, smartphones (i.e. iPhone, Windows and Android) and tablets (i.e. iPad, Galaxy and Surface).

The CurrentWare Gateway is based on an agentless architecture that does not require any installation on the client devices.

It includes an intuitive web based centralized console for the deployment of web access policies and reporting of real time browsing activities.

1.1 CurrentWare Gateway Features

Multiplatform Management

The CurrentWare Gateway can control and monitor the traffic of any computing device that connects to the Internet through the Gateway. The compatibility list includes but is not limited to the following devices:

- Desktops: Windows, Mac, Linux
- Mobile/Tablets: Android, iOS, Blackberry, Windows Phone
- Laptops: Windows, MacBook, ChromeBook

No Agent Installation

The installation and configuration of the CurrentWare Gateway is straightforward since it does not require any installation or configuration on client devices. This agentless infrastructure provides for a more flexible solution for managing both in house and guest devices, connecting to the company's Internet.

URL Category Filtering

CurrentWare's extensive URL Category database includes over 100 categories, encompassing millions of URLs. Category Filtering is an accurate way of instantly controlling the websites that can be accessed across your organization. Block malicious and non-productive sites easily by restricting unauthorized URL categories.

Custom Allow and Block Lists

The URL Allow and Block lists, enable you to add additional websites to complement the URL Category Filtering. The Allow List permits access to websites that would normally be

restricted if it is part of a blocked category. Conversely the Blocked List will restrict access to a site. The Allow and Block lists can also be used to create your own custom lists independently of Category Filtering.

File Type Blocking

Managing URL traffic based on file types provides an additional dimension to securing your network. Block the downloading of files that would hog the bandwidth such as video and audio files or block the downloading of potentially malicious files. For example, you can allow Sports sites, but block video and audio media through File Type Blocking. File type blocking complements Category Filtering and Allow/Block Lists. Blocking of files can be implemented using the CurrentWare predefined file types or you can create new file types.

Web Monitoring

Comprehensive report generation of the network traffic provides heightened visibility of employee browsing. Reports in the form of tables and charts provide real time data of user browsing activity.

2.0 Installing the CurrentWare Gateway

This section describes the system requirements, the network configuration and the installation steps for the CurrentWare Gateway.

2.1 System Requirements

Hardware Requirement

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

Networking

- **Network Card:** 2 Network Interface Cards.
- **Network Switch or Router:** For bridging the connection between the CurrentWare Gateway and your LAN.

Computer

- **Processor:** Minimum Core i3 with 2.0 GHz and above.
- **Memory:** At least 4GB of RAM.
- **Disk Space:** 5GB of available disk space.

Software Requirements

The CurrentWare Gateway is compatible with the following Operating Systems

- **Windows 8, 8.1 Professional and Enterprise (32 and 64 bit)**
- **Windows 10 Professional and Enterprise (32 and 64 bit)**

- **Windows Server 2012 R2**

  Note:

  Windows 2012 R2 engages NAT (Network Address Translation) or RRAS for Internet sharing.
  Other supported operating systems, utilize ICS (Internet Connection Sharing)

Recommended Internet browsers for CurrentWare Gateway console include:

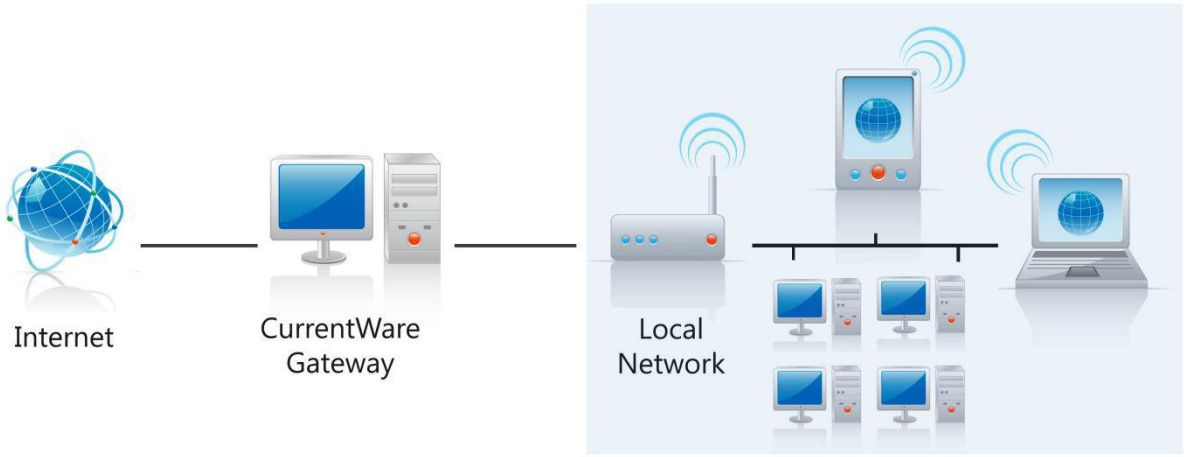
- **Internet Explorer 10 and above**
- **Microsoft Edge**
- **Mozilla Firefox 30 and above**
- **Google Chrome 35 and above**

2.2 Configuring your Network for Gateway

The CurrentWare Gateway filters incoming and outgoing Internet traffic on your network without the installation of any client applications on your devices.

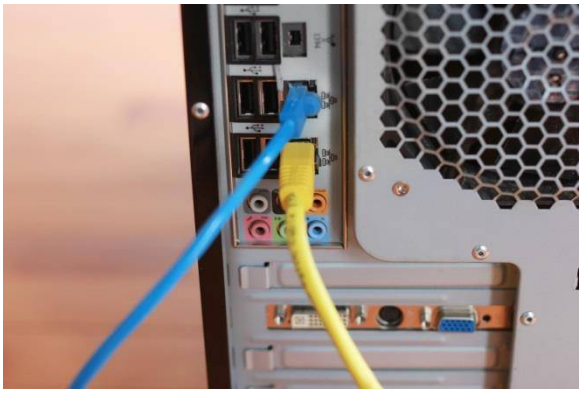
A Typical Network Configuration

This diagram shows the network architecture with the CurrentWare Gateway on your network.

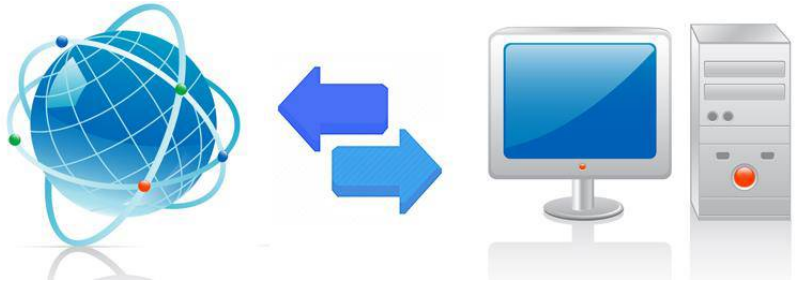


The CurrentWare Gateway must be placed between your Internet modem or router and the computers you wish to control.

Note: You must have two Ethernet ports available on your Gateway computer.

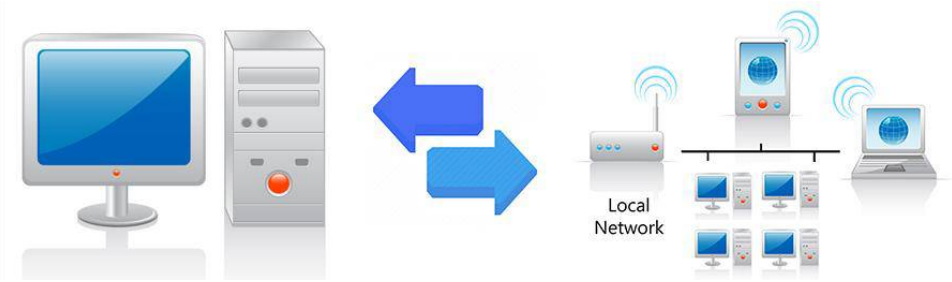


Connect the first Ethernet port to the Internet



The first Ethernet port must be connected to a modem or a router that provides Internet connection.

Connect the second Ethernet port to your LAN



The second Ethernet port should be connected to one of the following routing devices:

1. A network switch

   or
2. A router

If you are using a router, then please follow the below steps:

1. **Disable DHCP Server service on the router**

   The DHCP Server service must be disabled on the router before connecting to the Gateway. The devices connected to the router will be obtaining their IP Addresses from the Gateway Sever.

   a. If DHCP Server service is enabled on the router, then the clients connected to that Router will be getting IP Address from the router's DHCP Server. In that case, the CurrentWare Gateway can only detect the router.
2. **Connect the Ethernet cable to the LAN port of the router**

   The Ethernet connection from the Gateway computer must be connected to one of the LAN ports of the router. Do not connect it to the WAN port.

   a.

2.3 Software Installation

Follow the instructions below to install the CurrentWare Gateway.

Before you begin your installation:

- Log in with an **Administrator account**.
- Turn off the Antivirus\Security applications during the installation to ensure the successful completion.
- We recommend using a dedicated server grade Operating System to ensure the proper functioning of the CurrentWare Gateway.
- The CurrentWare Gateway computer must have **two Ethernet ports.**
- The two Ethernet ports must be connected to the appropriate routing devices:
    - **First network card**: connected to a modem or a router with Internet access.
    - **Second network card**: connected to a network switch or router bridged to your LAN.

For Operating Systems

- **Windows Server 2012 R2:** make sure the RRAS (Routing and Remote Access Services) role and NAT (Network Address Translation) feature is not enabled.
- **Windows 8 and 10:** make sure the Internet Connection Sharing (ICS) is not enabled

CurrentWare Gateway Installation Steps

1. Running the Installer

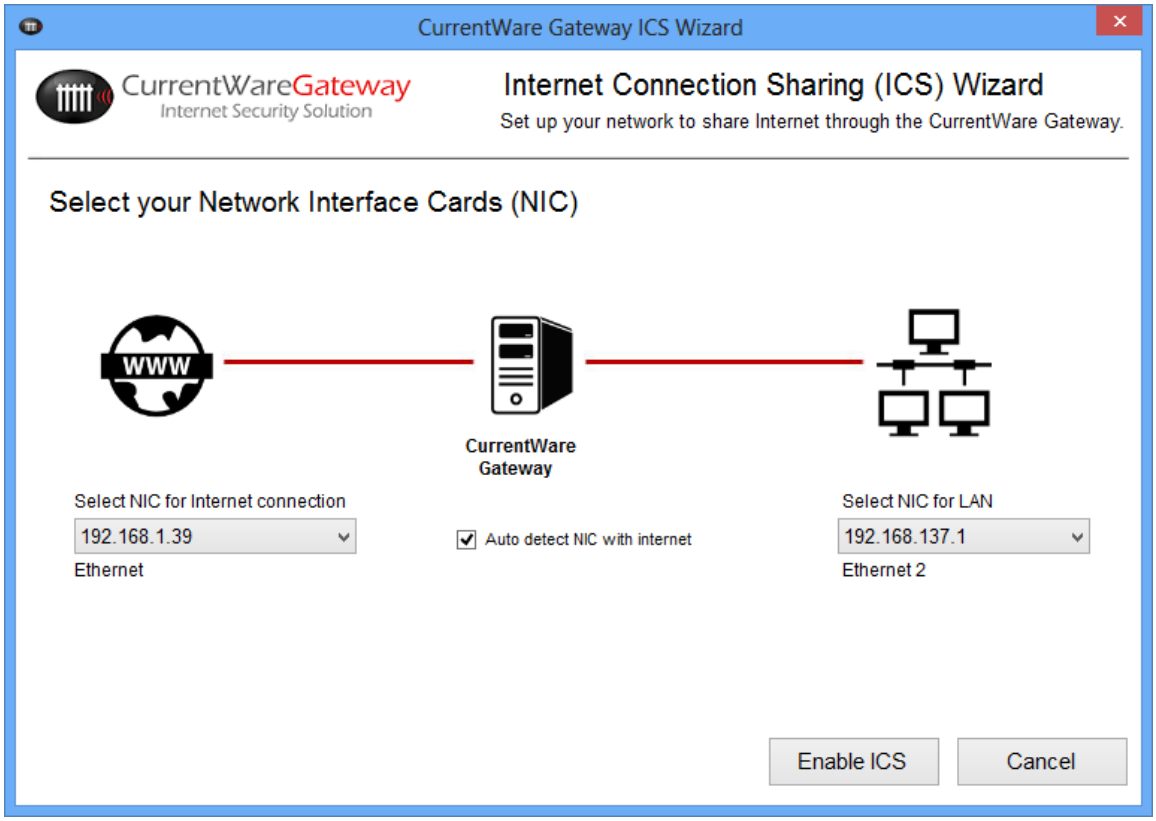
1. Run the **CurrentWareGateway.exe** file
2. The installer checks if the pre-requisite components are installed and will automatically install the missing components.
3. Click **Install** to start the installation of the **CurrentWare Gateway**.
4. The CurrentWare Gateway will take 5 to 15 minutes to install.

2. Running the Gateway Network Setup Wizard

After the CurrentWare Gateway is installed, the Internet Connection Sharing Wizard will pop up automatically to help you set up for the first time. The Gateway network Setup Wizard steps through the process of allowing Internet traffic to the clients using ICS or NAT technology.

Gateway Network Setup Wizard for ICS technology

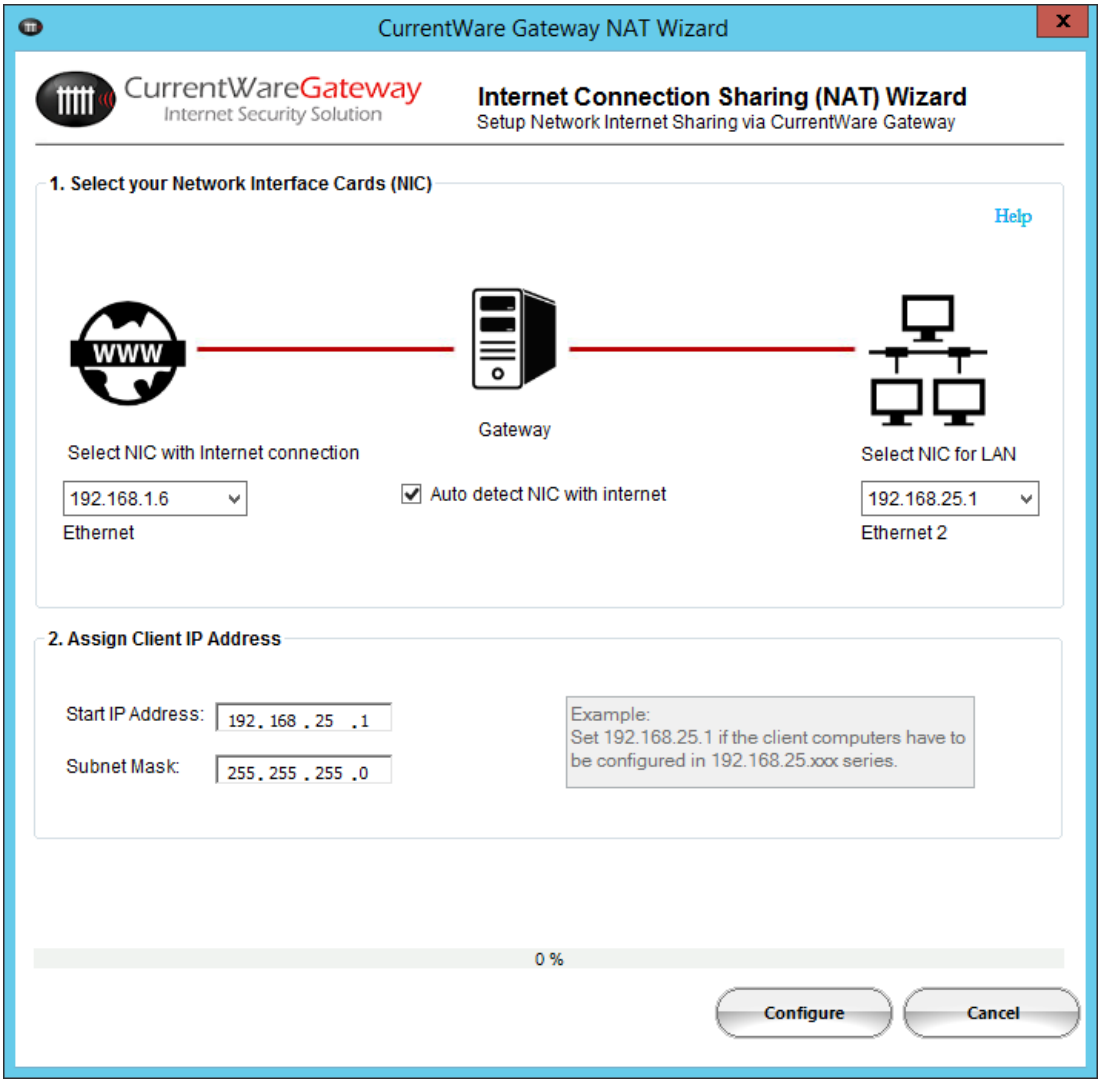
For Windows 8, 8.1 and 10



1. On the drop-down list to the left, select the network card that is connected to the Internet.
2. Or use the check box (Auto Detect NIC with Internet) to automatically select the network card with Internet connection.
3. On the drop-down list to the right, select the network card that is connected to the **Local Area Network (LAN)**.
4. Click on **Enable ICS** button.
5. The status will change to Sharing completed successfully.

Gateway Network Setup Wizard for NAT technology

For Windows Server 2012 R2



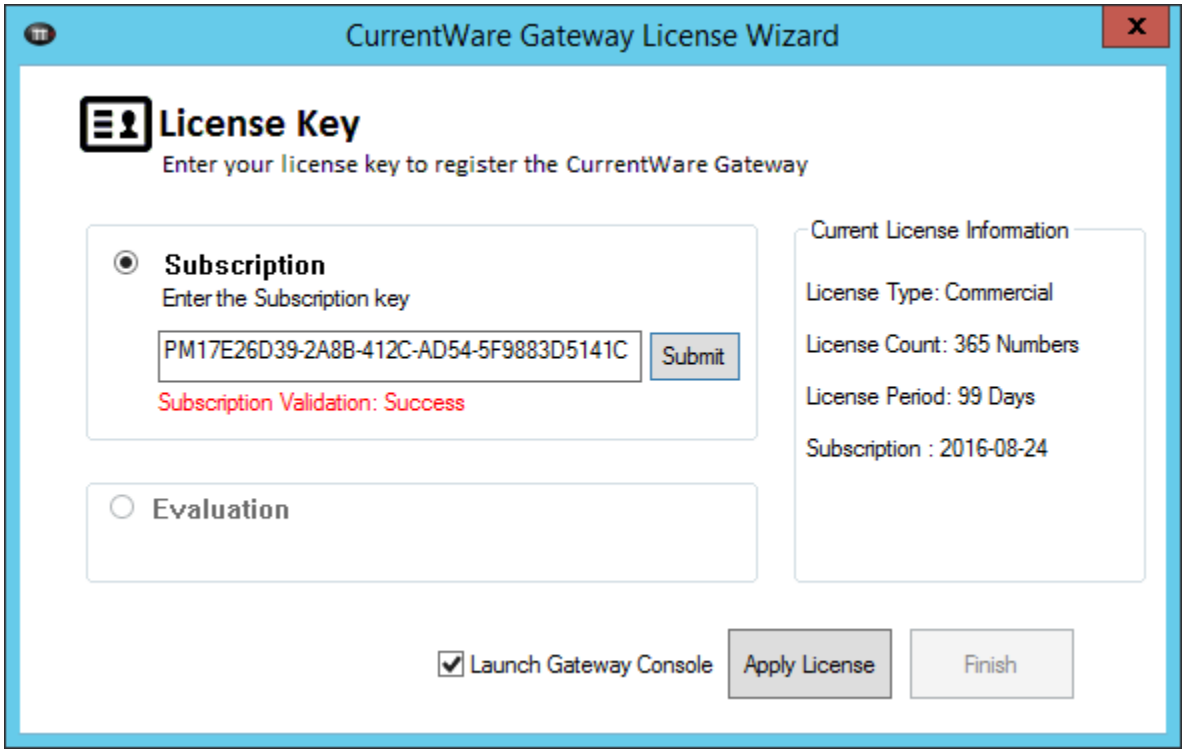
1. On the drop-down list to the left, select the network card that is connected to the **Internet**.
2. Or use the check box (**Auto Detect NIC with Internet**) to automatically select the network card with Internet connection.
3. On the drop-down list to the right, select the network card that is connected to the **Local Area Network (LAN).**

4. Verify the **Default IP Address range** (192.168.1.25) on the 'Assign Client IP Address'. Enter a valid IP Address range if you would like to change the default range.
5. Click on **Configure** button.
6. The wizard will be closed after successful completion.

3. Running the License Wizard

Before you use the CurrentWare Gateway, you must enter a subscription key or select the Evaluation radio button to start the Gateway in evaluation mode.

The subscription key is sent to you by our licensing department after you have completed your purchase of the software.



1. Enter your **subscription key.**
2. Click on the **Submit** button to register your key with our licensing server.

3. Once the registration is completed, your licensing information will be displayed on the right hand side.
4. Click **Apply License** to complete the licensing process.

To evaluation CurrentWare Gateway

Select Evaluation radio button and click Apply License. The evaluation mode lets you try the CurrentWare Gateway with 10 devices for 14 days.

3.0 Console Overview

The CurrentWare Gateway Console is a web based application allowing the Administrator to configure the Gateway settings, deploy web access polices and run monitoring reports.

Starting the CurrentWare Gateway Console

- To start the Gateway Console, double click on the CurrentWare Gateway Console shortcut on your desktop.
- The Gateway Console can also be accessed, by entering http://localhost:8001 on the Internet browser from the Server computer.
- Remotely, the Gateway Console can be accessed by entering http://*GatewayServerIP*:8001 on the Internet Browser from any client devices. (*Please enter the Gateway server machine's IP address on the URL*)

Logging into the CurrentWare Gateway

Every time the Gateway Console is launched, you will be prompted to enter the username and password.

Note: To access the Gateway Console for the first time, you must use the default user name and password.

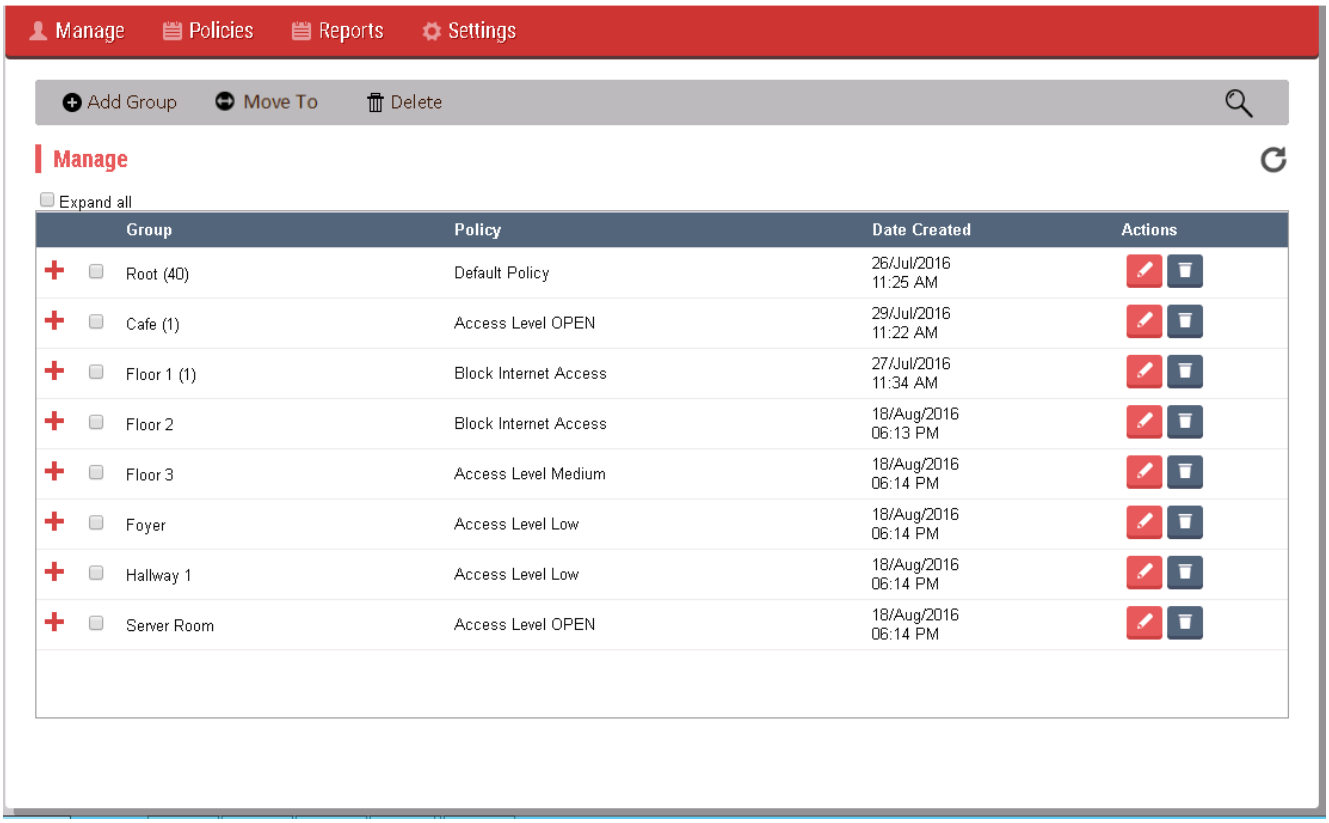
You can change the password by clicking on the **Change Password** link.

Default Username: **Admin**

Default Password: **Admin**

4.0 Manage Page

The Manage page allows the administrator to organize the devices on your network. This page allows you to add groups, assign devices to the groups and edit/delete groups.



- **Add Group:** Add a new group to assign a new Internet policy to it. You can assign policy to a group during the Add Group window. You can also assign a policy to the group in the Policies Page.
- **Move To:** By default, a newly discovered network device will be added to the Root group. The Move To option moves the client device to a different group.
- **Delete:** Use the Delete button to remove a group/device from the list.
- **Search:** Click on the search button to expand the search bar. Search by group, device, IP address, policy, MAC Address or Date created.

- **Edit:** Edit the group name by clicking on the Edit button under the Actions column.

4.1 The Root Group

A default group called **Root** is automatically created when the CurrentWare Gateway is installed. When a new device connects to the Gateway, it will be assigned to the Root group. The Root group cannot be deleted or renamed.

4.2 Device Discovery

How does the CurrentWare Gateway identify your devices?

Devices Connected to a Switch

When a device is connected to the CurrentWare Gateway, via a switch, it will be identified on the Gateway console independently according to its device name.

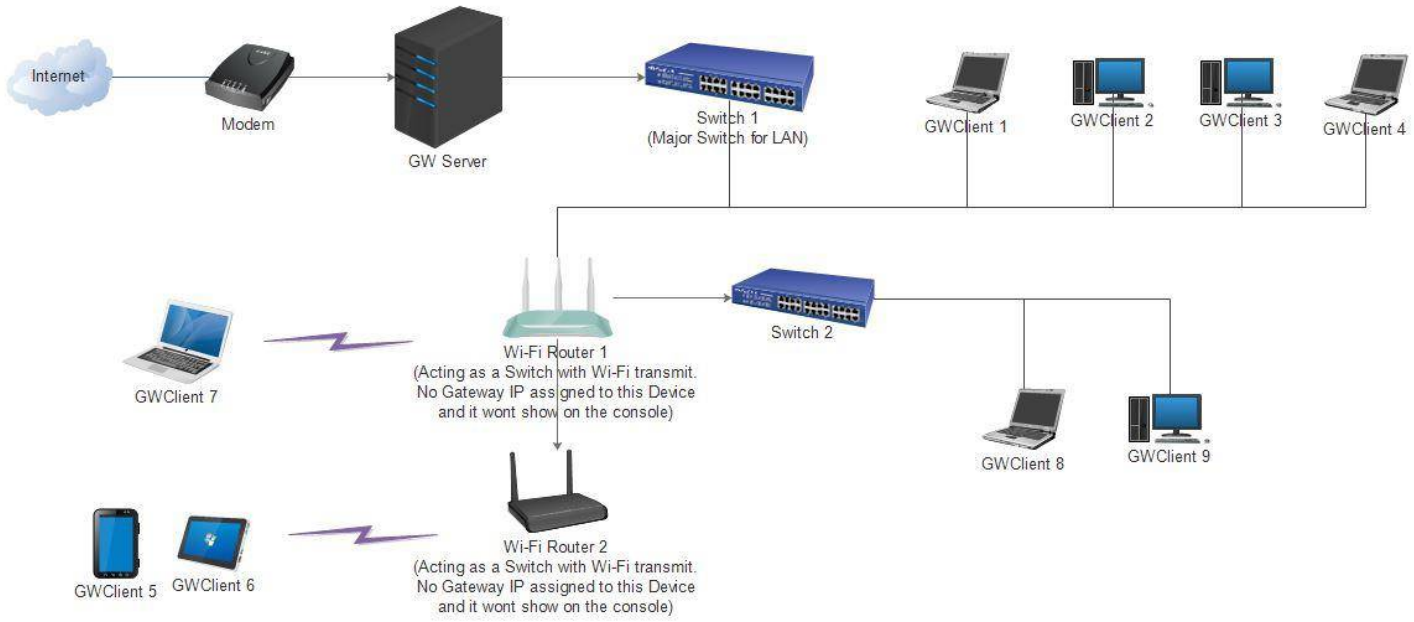
Devices Connected to a Router

The router can be connected to the Gateway in two different methods.

1. **Connect the Gateway network cable to one of the LAN ports of the Router with DHCP Server disabled (*recommended*).**
    - In this case, each device will be listed individually on the console, according to its device name. The Router will not be listed on the console.

2. **Connect the Gateway network cable to the WAN port of the Router with DHCP Server enabled.**

- In this setup, the router will mask the traffic from the CurrentWare Gateway. As a result, the Gateway will only able to identify the router and not the devices that are connected to it. The name of the router will be displayed on the Console. When assigning a policy to the router, all the devices connected to it will share the same policy.
- For example, if you assign a policy to a router named “CW-Router-1900” and 10 computers are connected to it. All 10 computers will share the same Internet policy assigned to the Router.



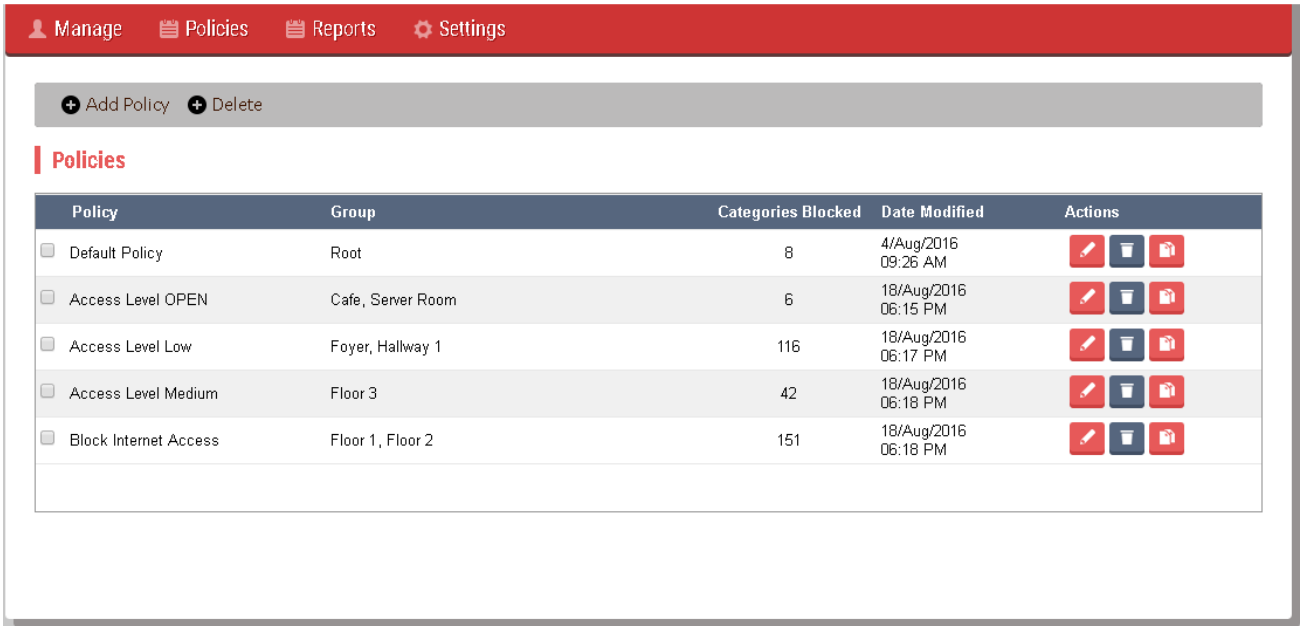
Showing the Devices on the Gateway Console

Connect your device through a switch or router managed by the CurrentWare Gateway. As soon as there is browsing activity on the device, it will be displayed on the Gateway Console.

5.0 Policies Page

The Internet restriction policies are created and managed on the Policies Page. Each policy contains its own Internet restriction rule. Assign one policy per group of devices.

5.1 Overview



Note: The Default Policy will be the only policy assigned to the Root Group. No other policy can be assigned to the Root Group.

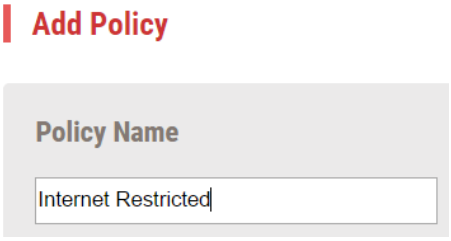
- **Add Policy**: add a new policy and assign it to a group of devices.
- **Delete**: use the Delete button to remove a policy from the list.

5.2 Add Policy

Create an Internet restriction policy and assign it to a group.

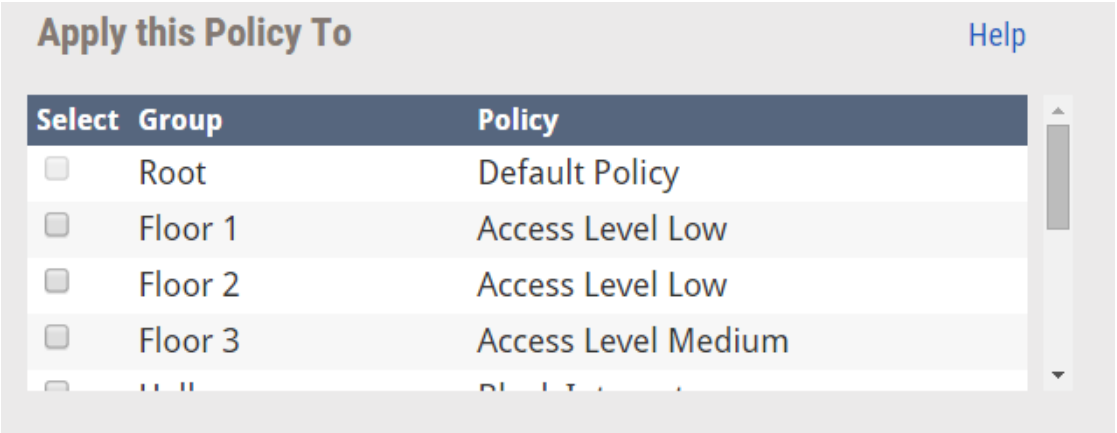
Policy Name

Input a name for the policy.



Apply this Policy to

Select the group to apply this policy to. A Policy can be applied to multiple groups. Each group can have only one policy.

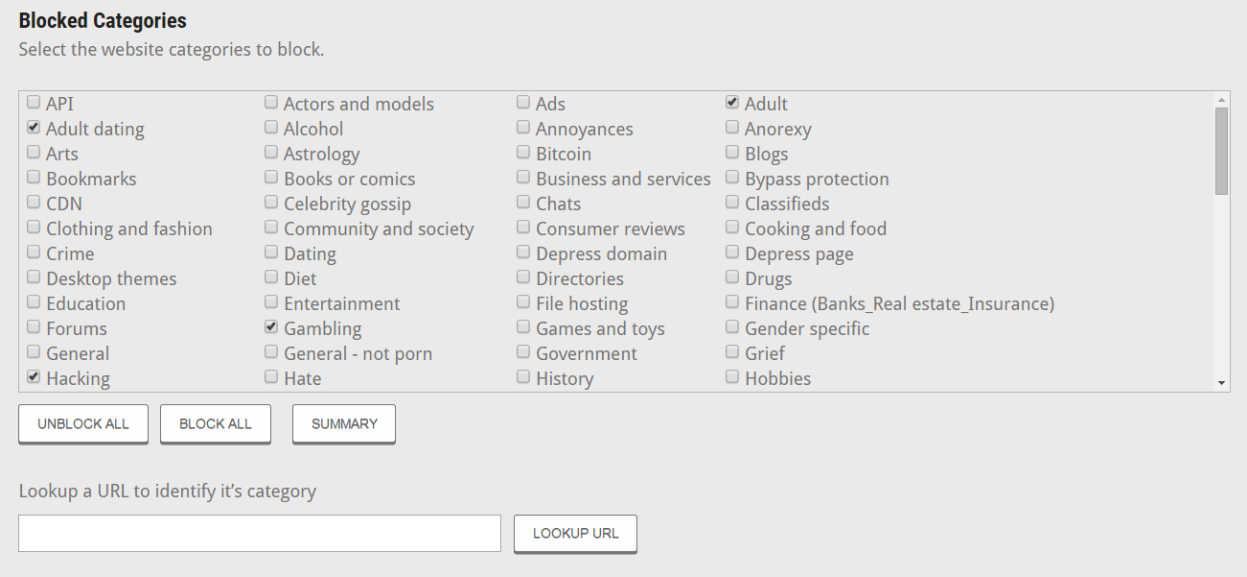


Block Categories

Select the URL categories to be blocked, in order to restrict users from accessing unauthorized sites. A selection of over 150 URL categories is available.

Click on the **Summary** button to display a list of selected categories.

The **Look up URL** option allows you to identify the category that a specific URL belongs to.



Exceptions – Web Sites

Always Allow

Add URLs to the **Always Allow** list to allow users to access specific websites. Even if a URL is part of a blocked category, it will be excluded from being blocked if it is on the Always Allow list.

> For example, to block access to the entire Social Media category, except for LinkedIn: block the Social Media category, then add linkedin.com URL to the Always Allow list.

Always Block

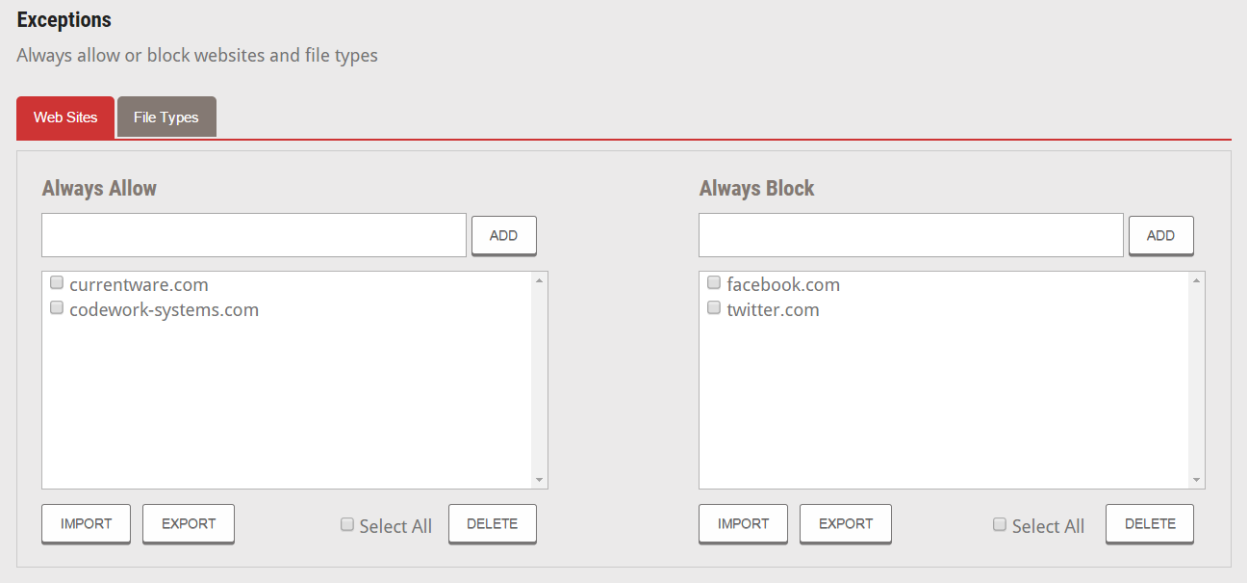
Add URLs to the **Always Block** list to block users from accessing specific websites.

Export

Use the **Export** button to export your Always Allow list and Always Block list to a text file.

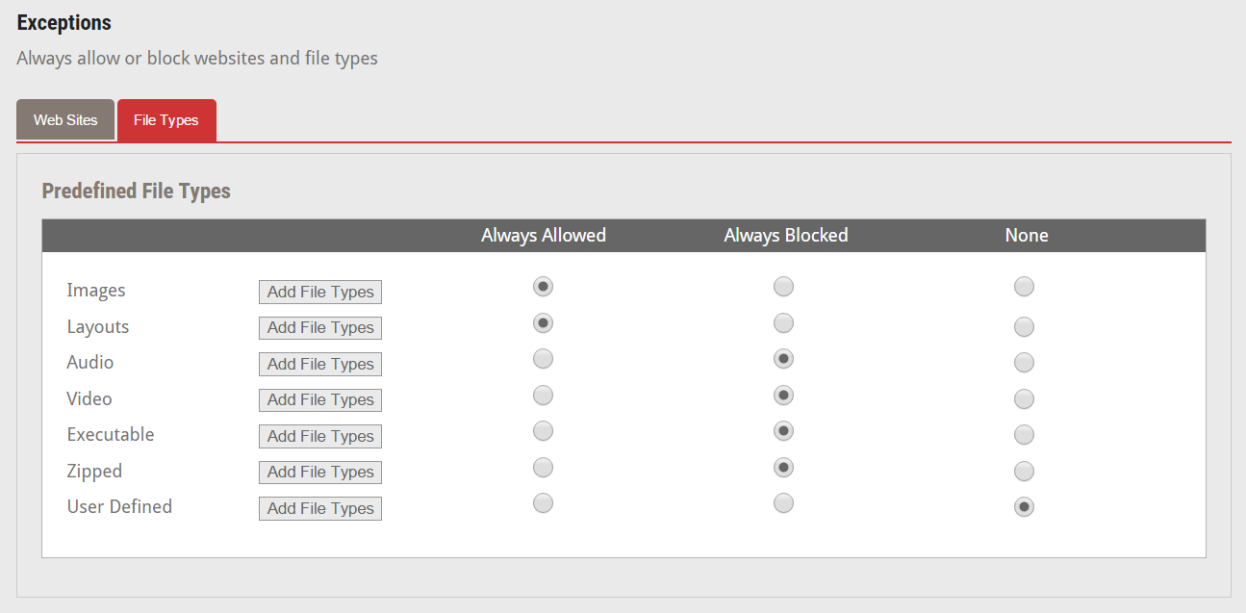
Import

Use the **Import** button to import a text file to your existing Always Allow list and Always Block list.



Exceptions – File Types

Set your file type permissions to **Always Allowed** or **Always Blocked** for specific file types that can be downloaded from the Internet.



There are 6 Predefined File types:

- Images
- Layouts
- Audio
- Video
- Executable
- Zipped

Add additional file types by clicking on the **Add File Types** button. There are three different file type permissions that can be set for each File type:

- **Always allowed:** the file type will always be allowed even if the Category is blocked or if the website is blocked from the Always Block list.

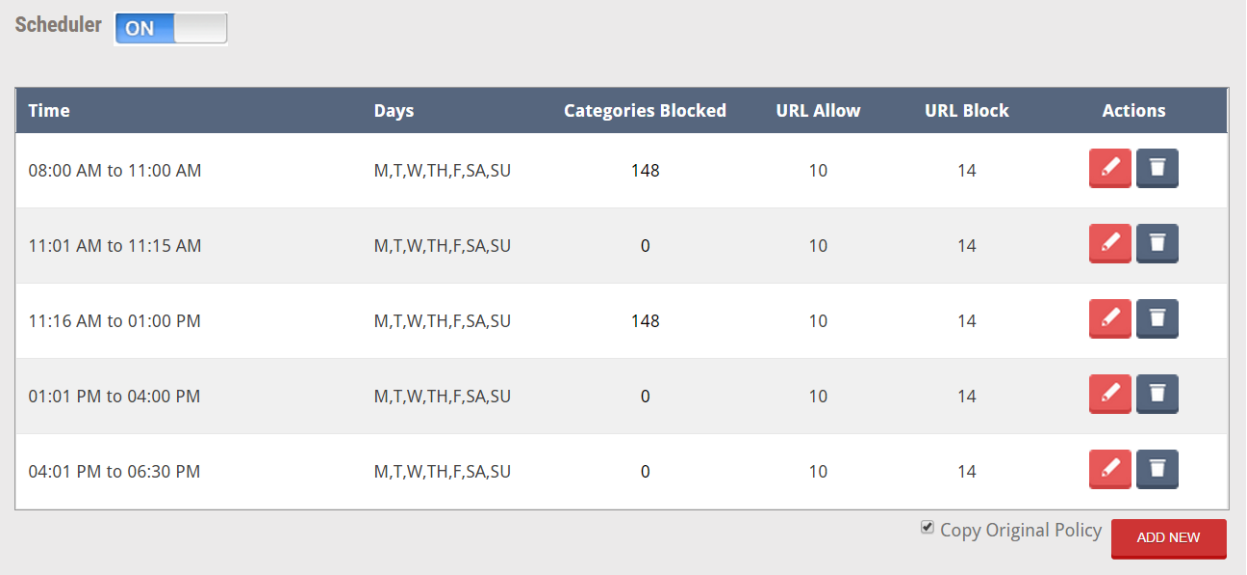
- **Always blocked:** the file type will always be blocked even if the website is allowed from the Always Allow list.
- **None:** the permission is not set to allow or block. The access of the file type will be based on the Block Categories list, the Always Allow list and the Always Block list.

Use the **User Defined** File type to create a new list of file types.

5.3 Using the Scheduler

With the scheduler enabled, multiple Internet restrictions can be assigned at different times and days.

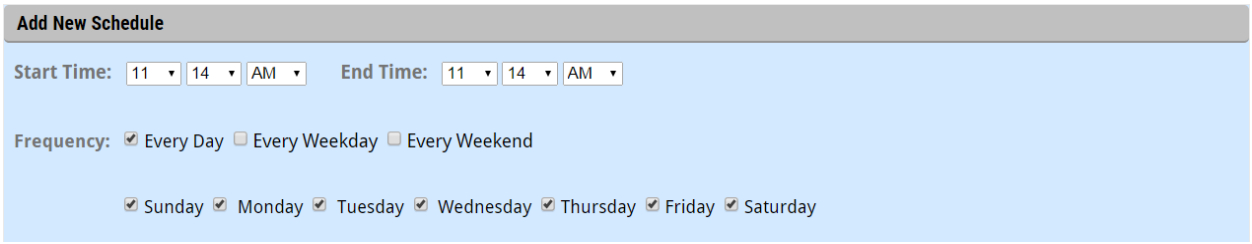
During unscheduled times, the Internet restriction from the respective policy will apply.



Add New Schedule

Select the **Start time** and **the End time** of the schedule.

Select the **Days** you want the schedule to repeat on a weekly basis.



Block Categories (Scheduler)

Select the categories to block user access to these sites.

See section 5.2 - Add Policy for more details.

Exceptions – Web Sites (Scheduler)

Add URLs to the **Always Allow** list to allow your users from accessing specific websites. Add URLs to the **Always Block** list to block your users from accessing specific websites.

See section 5.2 - Add Policy for more details

Exceptions – File Types (Scheduler)

Set your file type permissions to **Always Allowed** or **Always Blocked for** specific file types that can be downloaded from the Internet.

*See section 5.2 - **Add Policy** for more details*

6.0 Reports Page

CurrentWare Gateway allows administrators to monitor their users' Internet browsing activities.

It provides the facility to generate Internet browsing usage reports at the device level. In depth information of the sites visited and the time spent at these sites are presented. Detailed reports and summary level reports can be generated.

6.1 Overview

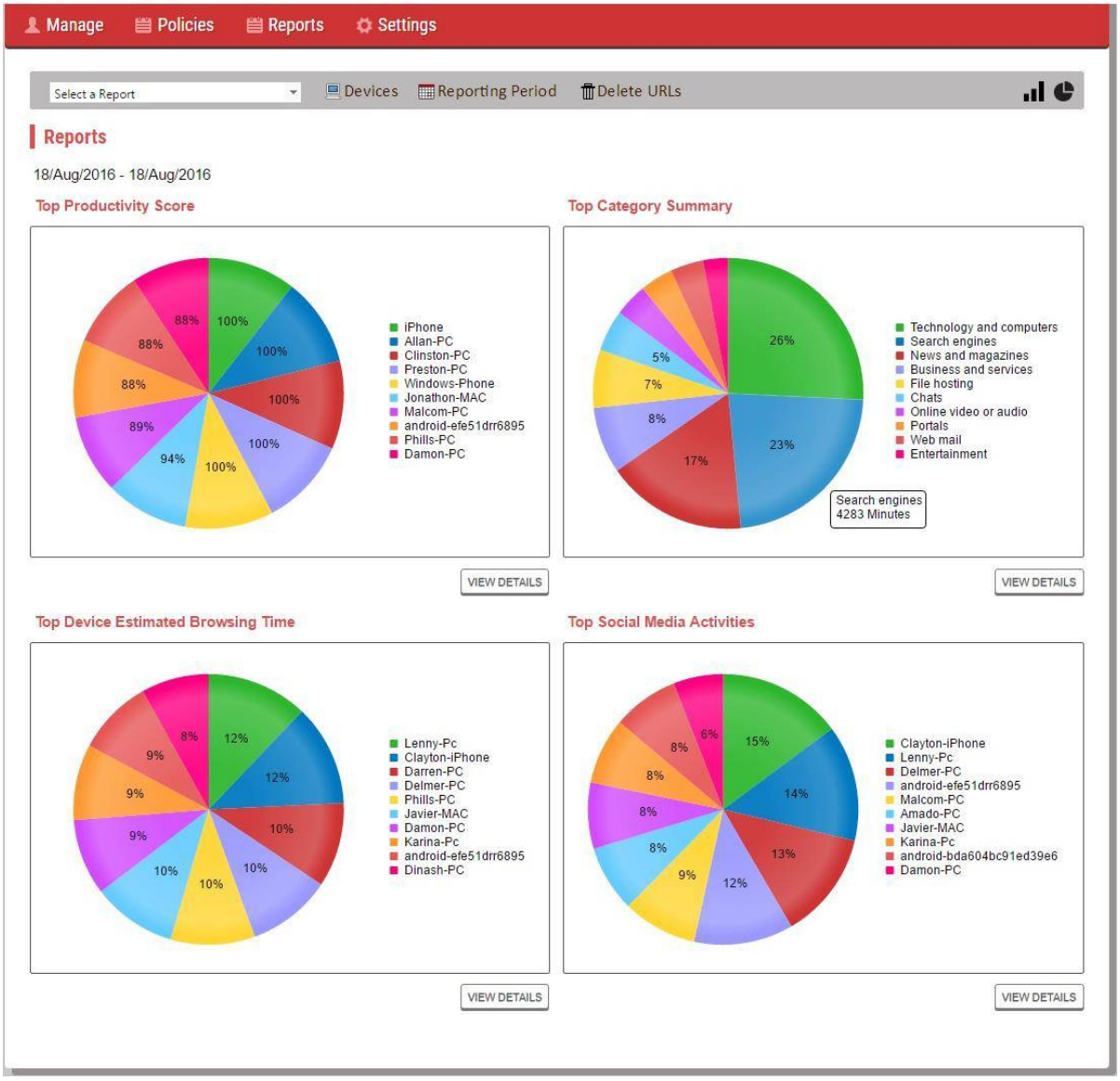
The Reports page consists of the following:

- Dashboard
- Reports
- Report Options

6.2 Dashboard

The dashboard view provides the administrator with a quick glance of 4 charts:

1. Top Productivity Score
2. Top Category Summary
3. Top Device Estimated Browsing Time
4. Top Social Media Activities



The default view of each chart is a pie chart. To change the view from a pie chart to a bar graph, click on the bar graph icon on the top right hand corner.

The default device selection is for **all devices**. The default reporting period is set to **today**.

To view the details of each pie chart, click on the View Details button.

1. Dashboard - Top Productivity Score

This chart shows the top 10 devices with the highest productivity scores.

2. Dashboard - Top Category Summary

This chart shows the top 10 URL categories accessed by all the users on your network.

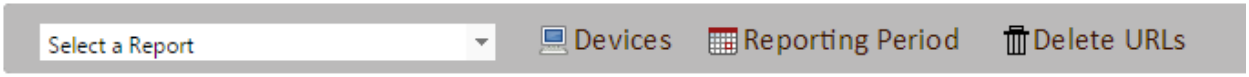
3. Dashboard - Top Device Estimated Browsing Time

This chart shows the top 10 devices with the highest estimated browsing time.

4. Dashboard - Top Social media Activities

This chart shows the top 10 devices with the most time spent on social media websites.

6.2.1 Header Options - Dashboard



Select a Report

The dropdown menu consists of the available built in reports. Select the report of your choice to view its details. Any custom reports that are created, will also be listed on this menu below a separation line.

Devices

The Devices icon, will display a list of devices connected to the Gateway Select your choice of devices from this list, to run reports on their browsing activities.

Reporting Period

Select the period for report generation. Choose from the following reporting periods: today, yesterday, last 7 days, last 30 days, last x day(s) and custom range.

Delete URLs

For database maintenance, it is recommended that redundant data be deleted periodically. To remove old data from the Gateway database, select the devices and the corresponding time period through this icon.

6.3 Reports

The default reports include a range of charts and tables based on the domains visited and the estimated time of browsing.

The reports can be further customized and saved to isolate and display the data according to the administrator's requirements.

The following are the default reports:

1. **Category Summary**

   This report is a summary of the categories of URLs accessed by the devices on your Gateway network. It accumulates the activities from all the devices. Estimated usage time and the number of allowed and blocked requests for each category will be shown in this report.

2. **Category Activity by Devices**

   This is the Category Summary report grouped by devices.

3. **Domain Summary**

   This report is a summary of the website domains accessed by the devices on your Gateway network. It accumulates the activities from all the devices. The report includes estimated usage time and the number of allowed and blocked requests for each domain.

4. **Domain Activity by Devices**

   This is the Domain Summary report grouped by devices.

5. **Social Media by Devices**

   This report is a summary of the social media domains accessed by the devices on your Gateway network. It accumulates the activities from all the devices. Estimated usage time and the number of allowed and blocked requests for each domain are included.

6. **Productivity**

   This report calculates a productivity score for each user. It helps to isolate employees who are abusing company policies and time. The Productivity score is calculated based on the Estimated Productive Time over the total Estimated Time.

   The categories are pre-defined as “productive” or “unproductive”. This grouping can be further customized to meet your company standards.

7. **Detailed Activity**

   A vast amount of network requests get passed through the Gateway before they are stored in the Gateway’s database. To optimize the performance, Gateway only stores the domain name of the network request.

   If the need arises to investigate the individual URL data, this information can be triggered to be captured via the **Enable URL Logging** feature on **Settings > Internet Monitor > Enable URL Logging.**

   URL data for 2 devices can be recorded over a maximum period of 3 days.

   The Detailed Activity report lists the individual URLs accessed on these devices along with the corresponding category, the status of the website, the accessed time and date.

8. **Detailed Activity (Specific URLs)**

   This report displays the browsing data of specific URLs only, as requested by the administrator.

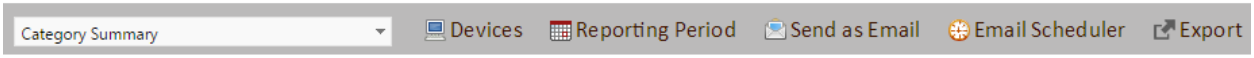
9. **Browsing Time by Domain**

   This report includes the estimated time spent per domain visited by each device. Each domain is tagged by a category. The report is grouped by device per day.

10. **Total Internet Usage by Device**

    This report consists of the estimated browsing time by device, along with the corresponding allowed and blocked requests.

6.3.1 Header Options - Reports



Select a Report

The dropdown menu lists all the Gateway reports, both built in and custom types. Select the desired report from the list to view its details. Any custom reports that have been created, will be listed on this menu below a separation line.

Devices

A list of devices connected to the Gateway will be displayed. Select the required devices from the list to view its reports.

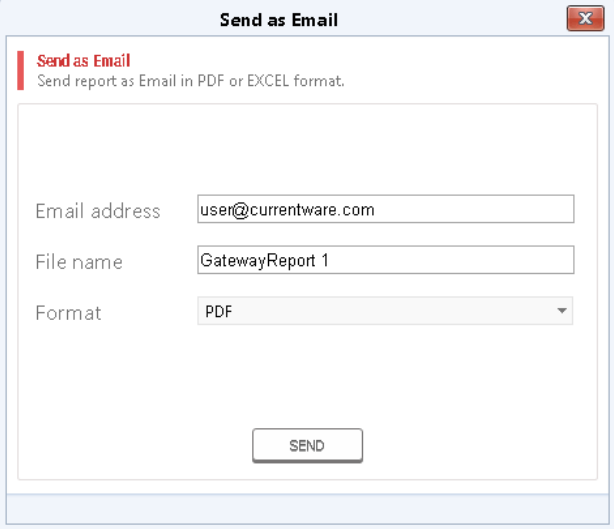
Reporting Period

Select the period for report generation. Choose from the following reporting periods: today, yesterday, last 7 days, last 30 days, last x day(s) and custom range.

Send as Email

Send a report directly to an email address using this option. For file type, choose between .PDF or .XLS (Excel)

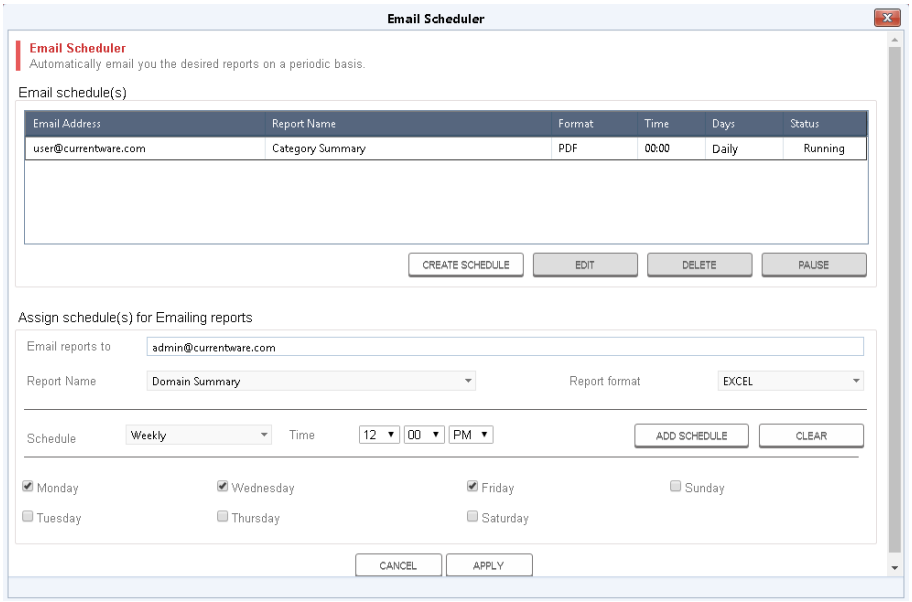
Note: the email settings will need to be configured prior to sending any emails. The configuration can be accessed from the **Settings page: Settings > General > Email Settings**.



Email Scheduler

Automatically email reports on a periodic basis. Set up your email scheduler to send out an email at a scheduled time, with a reoccurrence of daily, weekly or monthly.

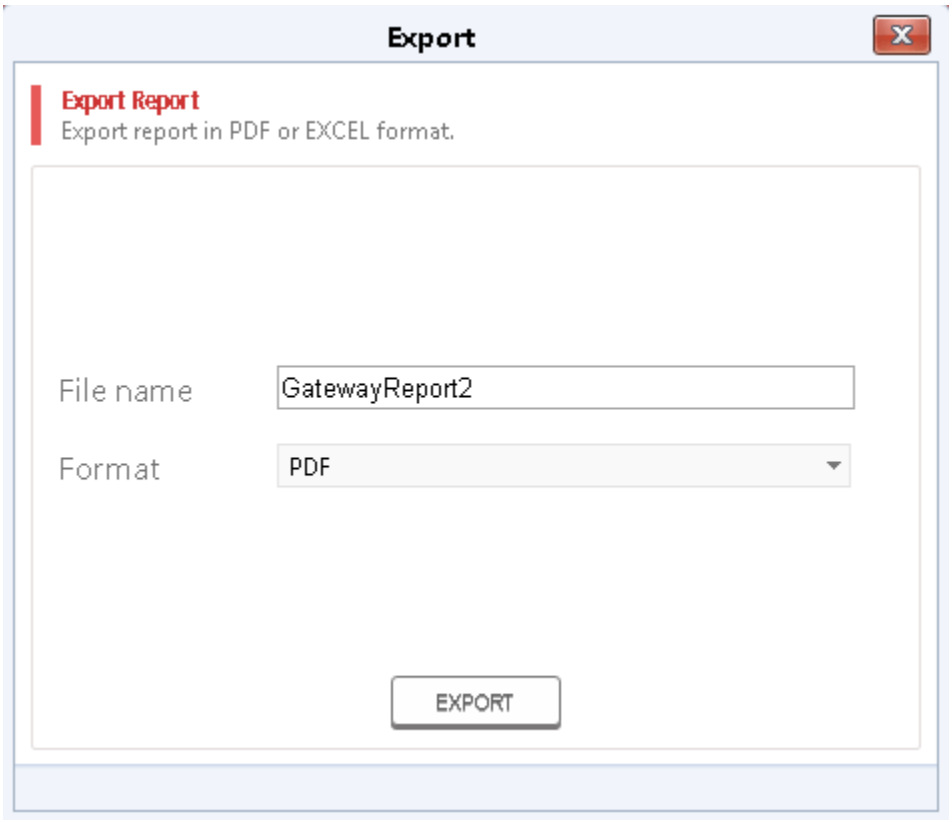
Prior to scheduling email delivery, please ensure that the email settings are configured from the **Settings page**: **Settings > General > Email Settings.**



Export

Reports can be exported in .PDF or .XLS (Excel) format.

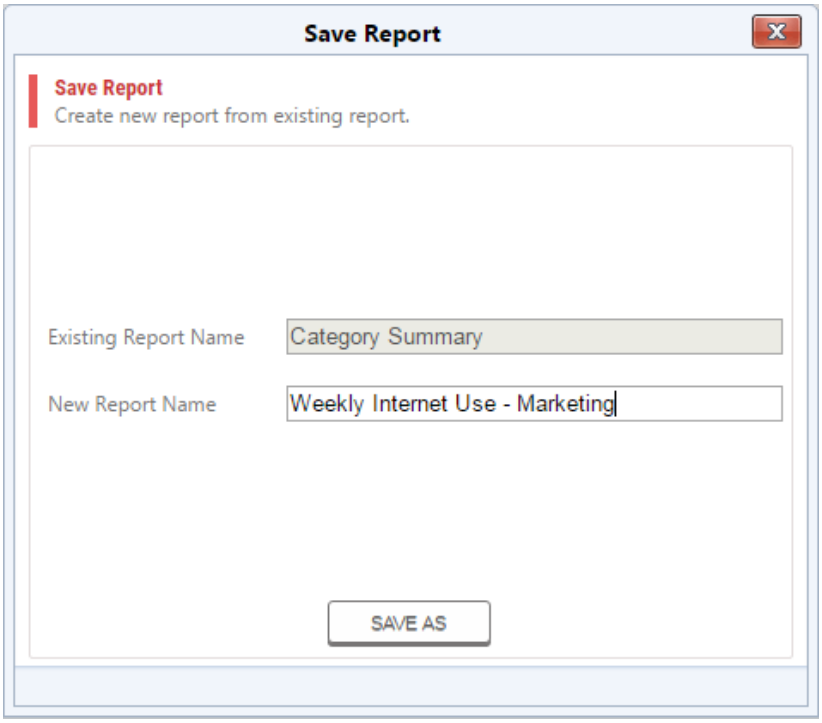
The export option is available for all the reports except for the Detailed Activity and Detailed Activity (Specific URLs) reports.



6.3.2 Create Custom Reports

Custom Reports

To create a custom report, select a built in report of your choice to serve as a template. Select the devices and reporting period. Remove any unneeded columns and assign sort orders to existing columns, Click on the **Save** button the bottom of the reports page. The will be displayed on the Select Report dropdown list preceded by a separation line with the default reports.



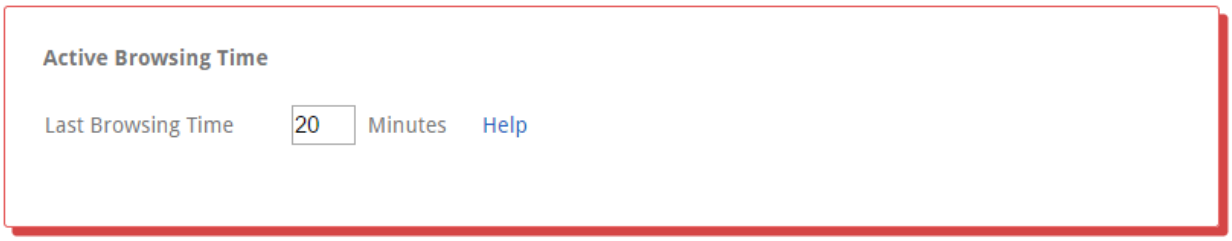
7.0 Settings Page

The Settings page provides customization and configuration of various Gateway features.

7.1 General Settings

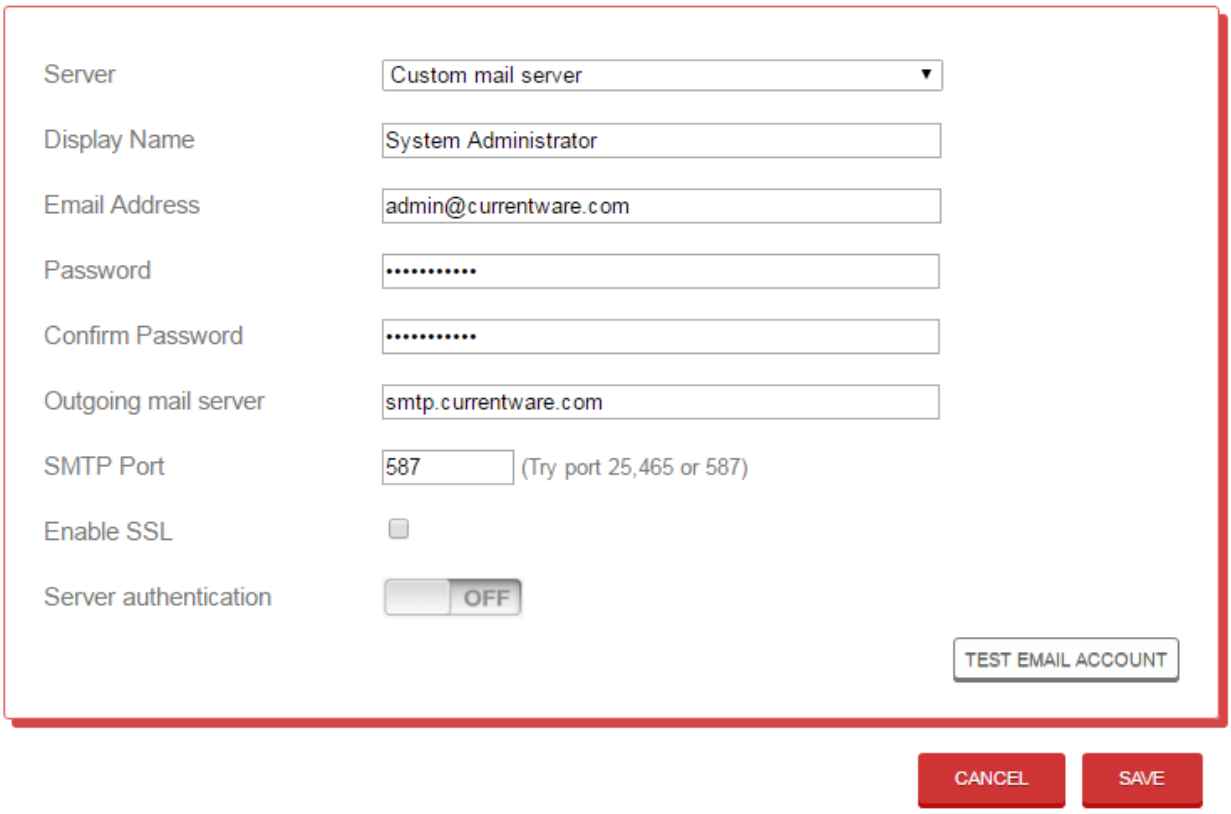
Server Settings

The active browsing time is the minimum browsing time to identify if a device is active. If there is no activity on the device for more than the active browsing time, then the device will be displayed as Idle on the Gateway console. The default value for the last browsing time is 20 minutes.



Email Settings

Setup your email configuration for emailing the Internet monitoring reports. It is required to set up your email settings to use the Email Scheduler. The reports will be sent from the outgoing email address.



- **Server:** Choose from Custom mail server, Gmail, Yahoo and Hotmail.
- **Display Name**: enter the sender's name
- **Email Address:** enter the sender's email address
- **Password:** enter the password for this email account on the mail server
- **Outgoing Mail Server:** enter the URL of your outgoing mail server
- **SMTP Port:** enter the port used to send email from your mail server
- **Enable SSL (optional):** if you mail server requires SSL, you can enable this.
- **Server authentication:** enable this option if your mail server requires authentication.

Service Status

Monitor your CurrentWare Gateway services to see if they are running or not.

License Information

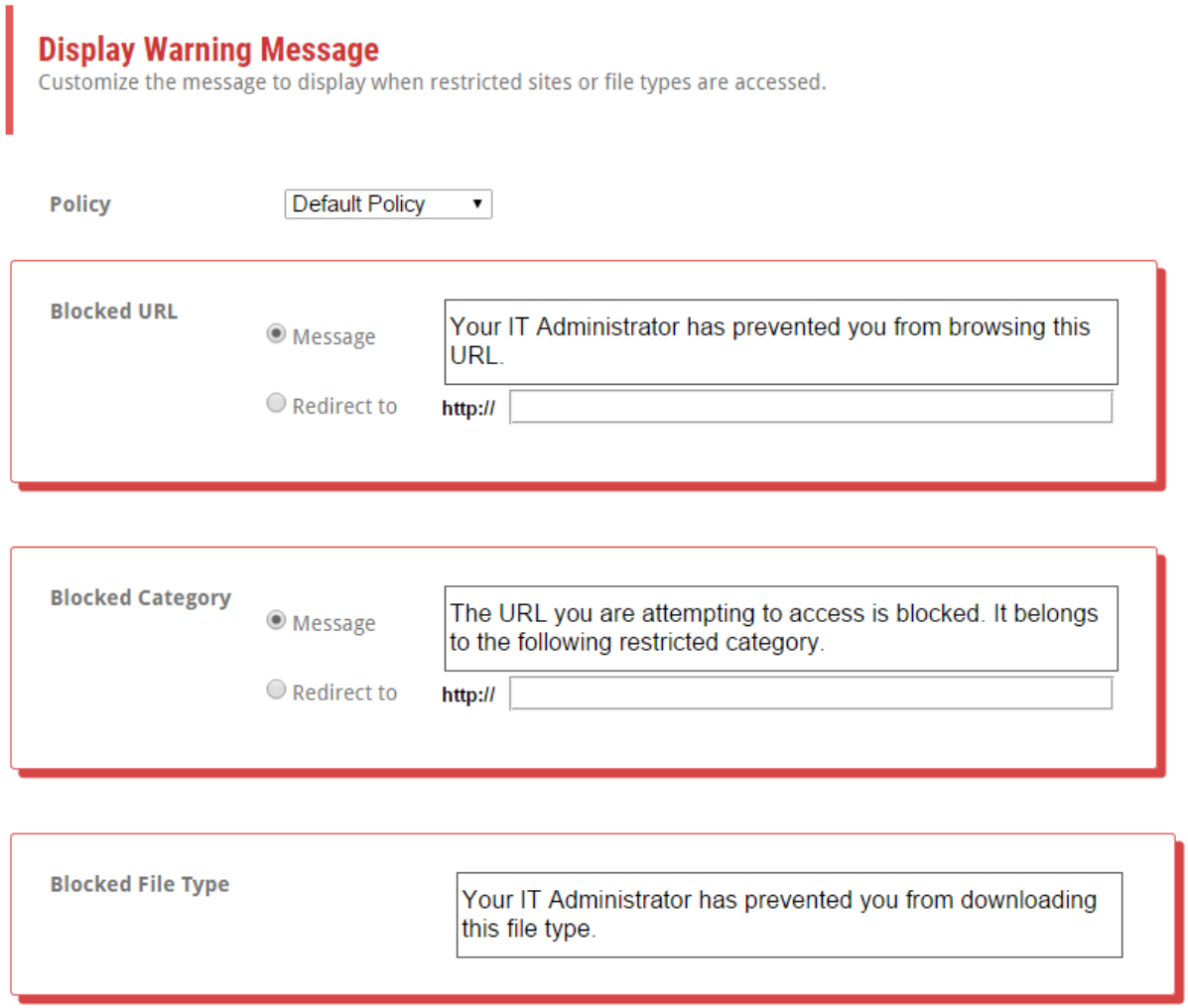
The license info displays the details of your registered license key. This information includes the total number of licenses, number of the used licenses and the expiry date of the license.

7.2 Internet Filter

Display Warning Message

Customize the warning message to alert users when they access an unauthorized website, category or file type.

1. Select the Internet filtering policy to assign the customized warning message.
2. Create a custom message for blocked URL, category and/or file type. Users can also be redirected to a website.



Refresh URL Categories

The URL categories in the Gateway database can be synchronized with the CurrentWare cloud database regularly at specified intervals

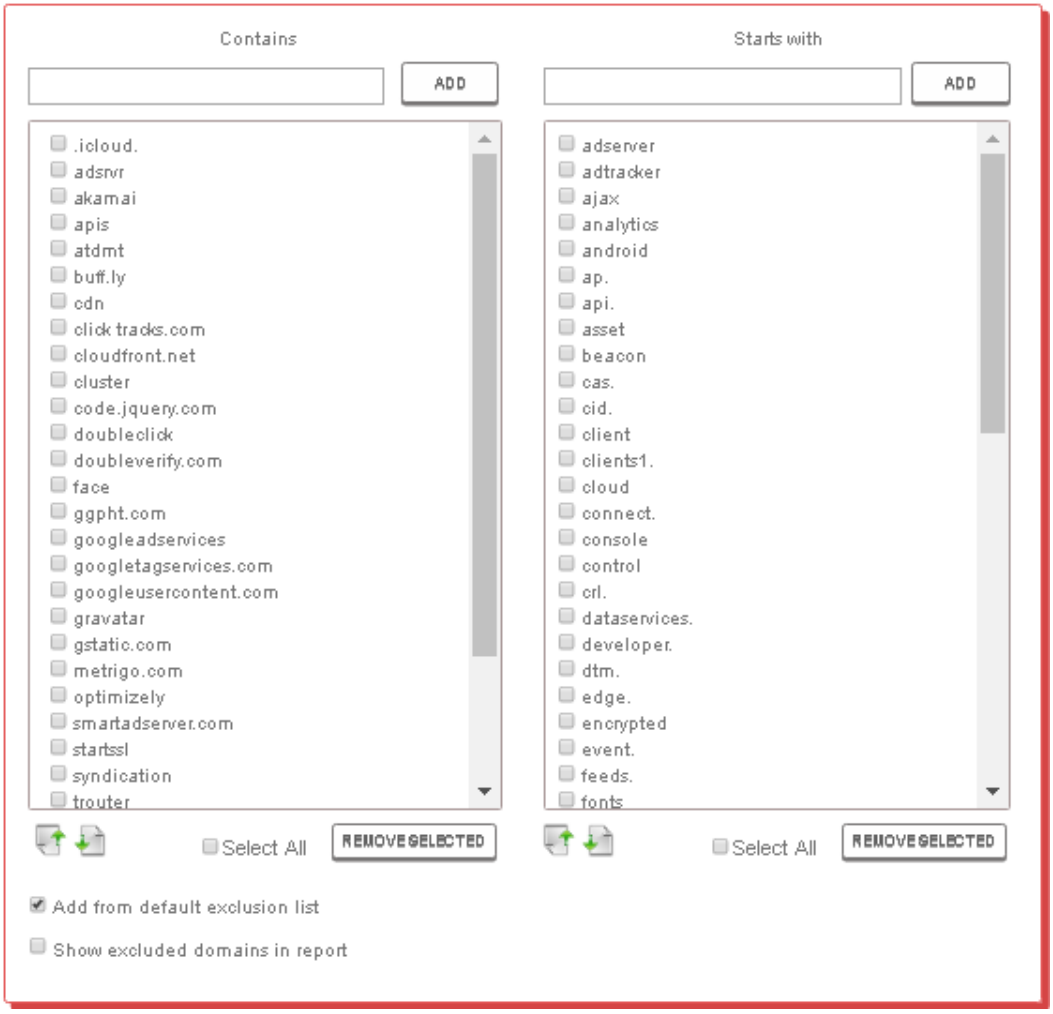
The default period of synchronization is 7 days.

The **Refresh Now** button will initiate the synchronization process immediately, without waiting for the next automatic refresh.

7.3 Internet Monitor

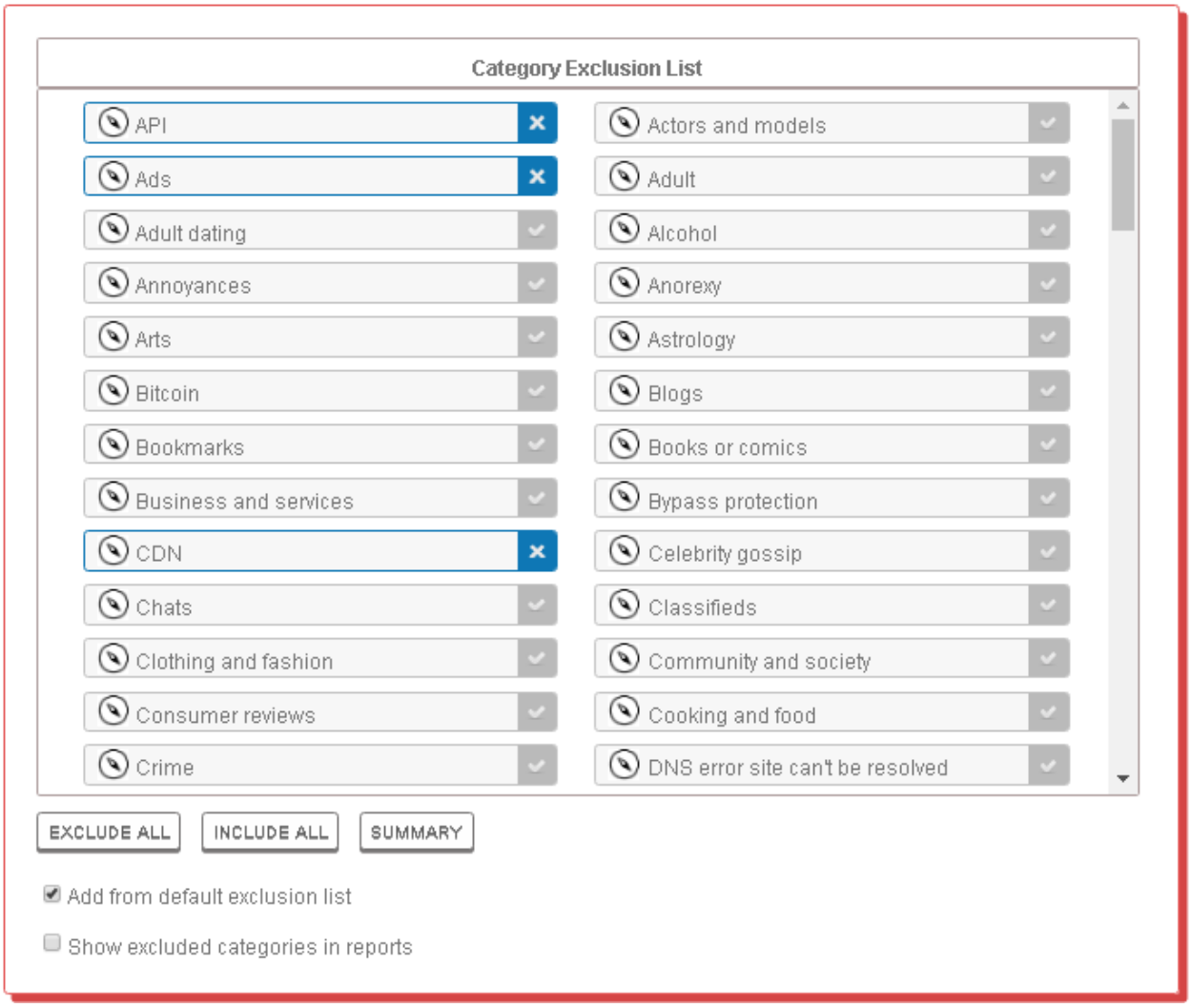
Domain Exclusion

Select the domains to be excluded from the Gateway reports. The excluded domains will not be tracked.



Category Exclusions

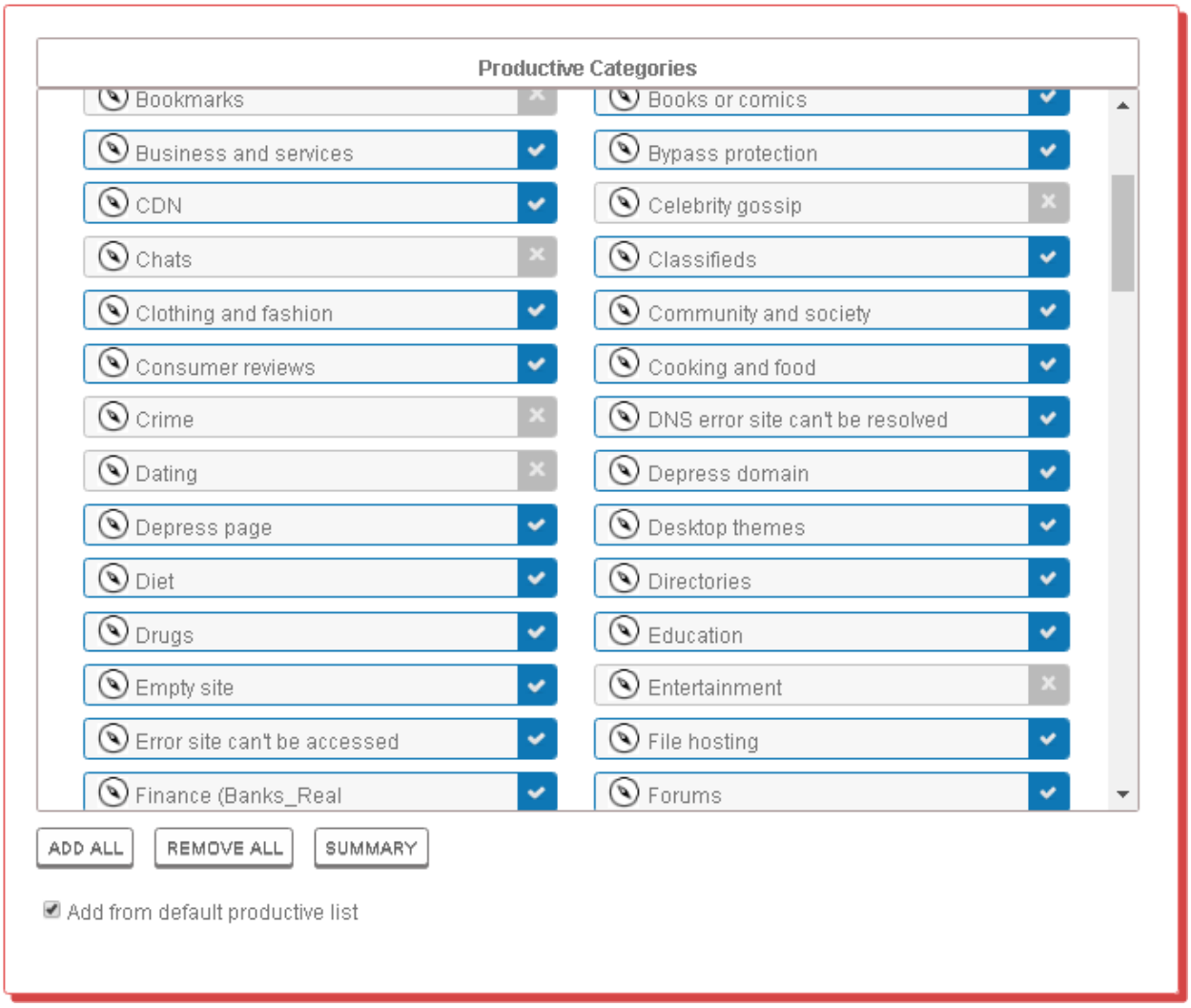
Select the categories to be excluded from the Gateway reports from the Category Exclusion List. The excluded categories will not be tracked.



Productivity Report

Customize the productivity grade for each category to better identify productive and unproductive workers. Adjust the categories that your workplace considers productive and unproductive.

The productivity score on the Productivity report is calculated based on your custom adjustments.

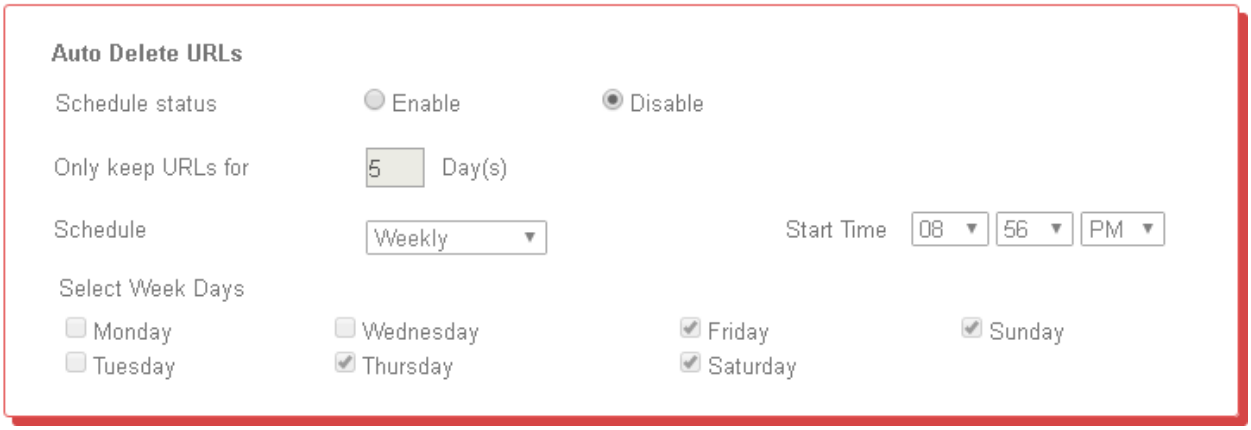


Database Archive

Database maintenance is important if your data grows exponentially. Set up a scheduler to automatically delete older URLs.

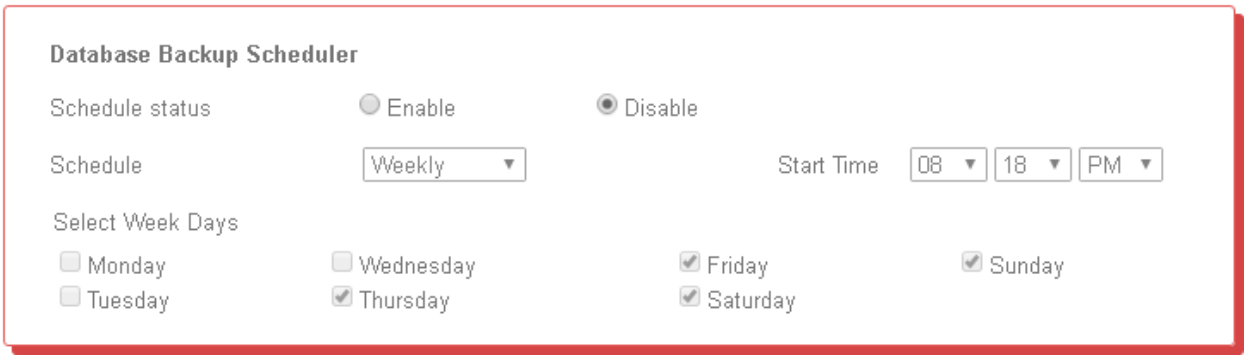
Auto Delete URLs

When enabled, older data will be purged from the existing database.



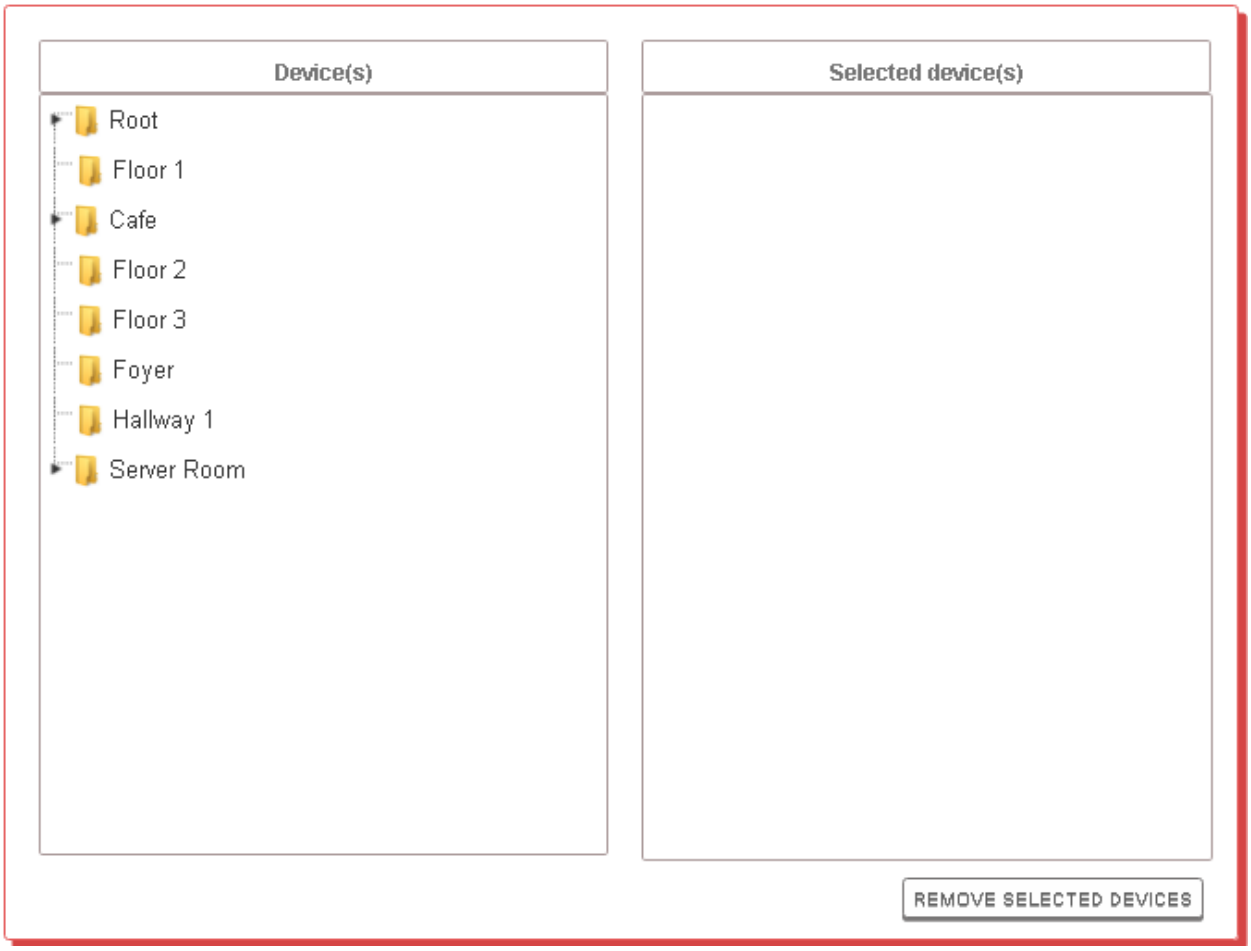
Database Backup Scheduler

Create daily or weekly schedules to back up the Gateway database.

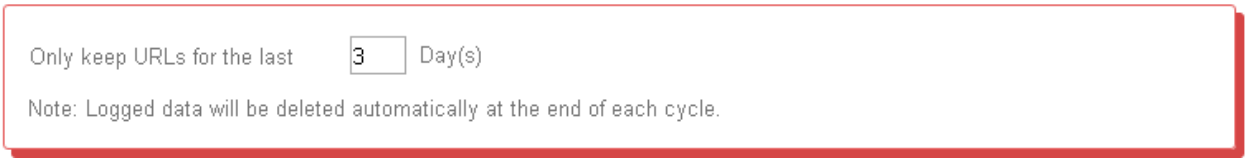


Enable URL Logging

Select up to 2 devices for detailed URL logging. When a device is under detailed URL logging, Gateway will record the device's network requests in full URLs (including sub-domains and sub-directories).

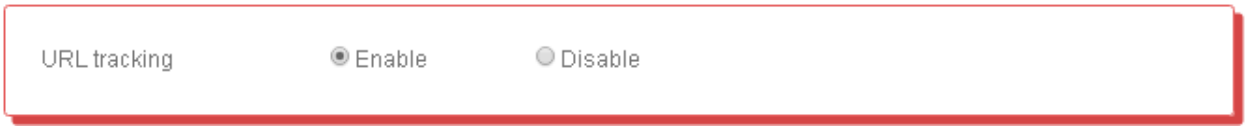


Only keep URLs for N days – The default and maximum value will be 3 days and the logged data will be deleted automatically at the end of each cycle.



URL Tracking

Enable or disable tracking of Internet activity by Gateway.



8.0 Uninstall

To uninstall the CurrentWare Gateway, go to **Control Panel > Programs and Features > Uninstall a program**. Select CurrentWare Gateway and click Uninstall.

Once the CurrentWare Gateway is uninstalled from Windows 8, 8.1, or 10 operating systems, the Internet Connection Sharing will be disabled.

At this point, the computers on your network will lose Internet connection. Remember to reconnect your router back to your LAN.

If you are using Gateway with NAT on server 2012 R2 operating system, the Internet sharing using NAT will not be disabled upon uninstalling. Your devices will still have Internet access.

9.0 Contact

USA

CurrentWare (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

EUROPE

Distology CurrentWare
Emerson Business Centre
Regent House, Heaton Lane
Stockport, UK SK4 1BS

- Tel: 613-368-4300
- Fax: 866-929-9808
- Email: info@currentware.com

CANADA

CurrentWare (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.