



Computer Lab Management Solution

## Quick-Start Guide

- 1) [Installation](#)
  - [Server Installation](#)
  - [Client Installation](#)
  - [Client Deployment](#)
- 2) [Getting Started](#)
- 3) [Creating Groups](#)
  - [Adding users or computers to new groups](#)
  - [Removing users or computers from groups](#)
  - [Removing users or computers after a period of time automatically](#)
- 4) [Monitoring](#)
  - [Viewing Live Thumbnails](#)
  - [Checking recent computer usage history](#)
- 5) [Giving assistance / Remote Control](#)
  - [Reducing CPU Usage/increasing Remote Control Speed](#)
- 6) [Screen Broadcasting](#)
- 7) [Locking Screens](#)
- 8) [Disabling the Internet](#)
- 9) [Add a new Policy](#)
  - [Block Policy Item screen](#)
- 10) [URL Filtering](#)
- 11) [Content Filtering](#)
- 12) [MIME Filtering](#)
- 13) [Restrict all websites except... \(allow-only\)](#)
- 14) [Client-Side Firewall](#)
- 15) [Application Filtering](#)
- 16) [Restrict all applications except... \(allow-only\)](#)
- 17) [White-listing](#)
- 18) [Scheduling Actions](#)
- 19) [Sending Files](#)
- 20) [Running Applications and Websites](#)

## 1. Installation

Minimum System Requirements:

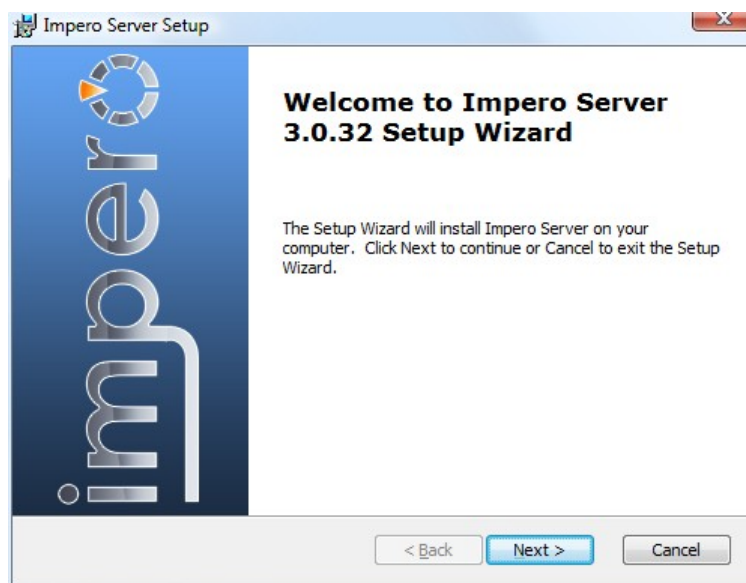
- Microsoft Windows 2000 sp4, XP sp2, Vista, Windows 7, Windows 2008, Citrix, N-Computing, Virtualization
- Microsoft .Net Framework 2.0 sp2
- Windows Installer 3.5
- Intel Pentium processor @ 633mhz
- 256mb RAM
- TCP/IP connection.
- Internet Connection required to register Impero Server
- At least 10mb HDD space

### 1.1 Server Installation

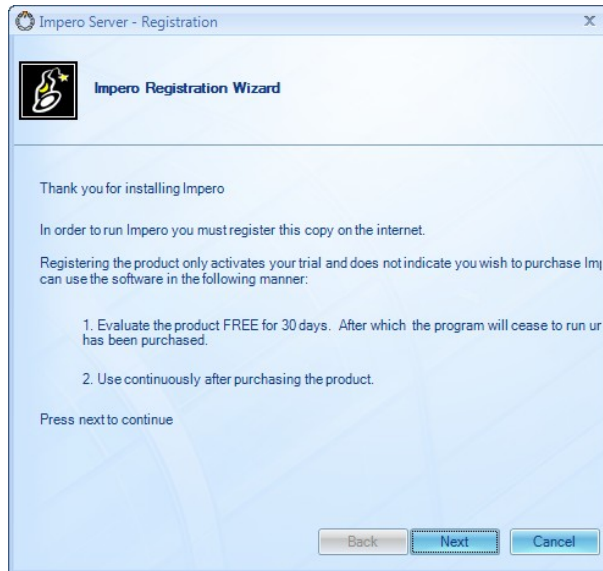
Installing Impero is quite straightforward and we have endeavoured to make the process quick and easy.

After you download the Setup files on to a Server or a computer that will remain powered on during Impero use, please extract the zip file to a local folder then locate the ImperoServerSetup file and run this file.

The Impero Server installation will begin and you must simply follow the on-screen instructions, clicking Next where applicable.



After the Impero Server installation, the Impero Server application will automatically start, presenting you with a Registration Wizard:



Click Next to each screen on the Registration Wizard, filling in the details where applicable. If you use a Proxy Server to access the Internet, the wizard will automatically use the Internet Explorer proxy settings, and you can therefore leave the Proxy Settings empty. If the wizard fails to register, please try again first filling in the Proxy Details.

Once the Registration Wizard is Complete, the Impero Server application will start.

The first screen you see is the Licence Tab where you can see details of your trial or full licence. Please browse through the various Tabs and enter any settings you believe are necessary.

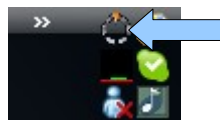
## 1.2 Client Installation

After you have installed the Impero Server as explained in section 1.1, you must install one or more Impero Clients.

To do this, please run the ImperoClientSetup installation file on the same computer you installed the Impero Server to.

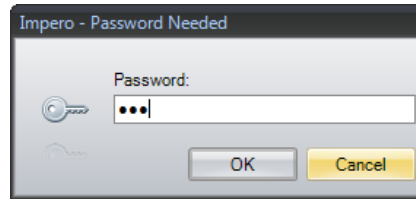
After you run the Installation File, Impero Client will automatically install the required files and start.

You will then see the Client icon appear in the System Tray, near the computer clock.



Click the tray icon once to see the Shortcut menu where you can now run the Impero Console software, alternatively you can run the Console using the shortcut icon on the desktop or start menu.

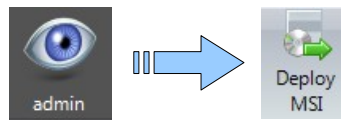
You will be presented with a Password box where you can enter the Console Access Password (this can be changed on the Impero Server>Settings Tab>Console Access Rights):



Please enter the default password of StaffOnly (case sensitive) to see the Impero Console interface.

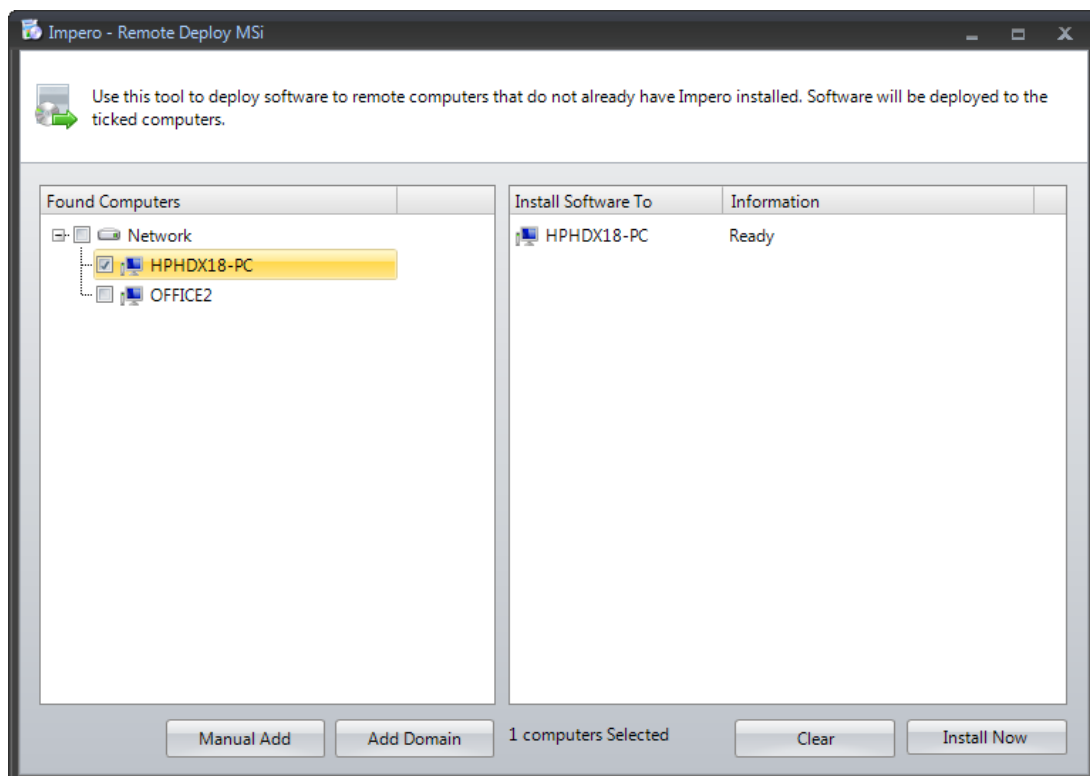
### 1.3 Client Deployment

a) Open the Impero Console Interface as described above or in section 2. (Getting Started), select the main menu icon 'Admin' and select 'Deploy MSI'.



A new application will start called 'Impero – Remote Deploy Msi'. From this application, you can deploy more Impero Clients to your Network Computers.

b) On the first Window, you should see a list of computers on your network, alternatively you can click 'Manual Add' to manually enter a computer name or IP Address or 'Add Domain' buttons to add more computers to the list if you wish.

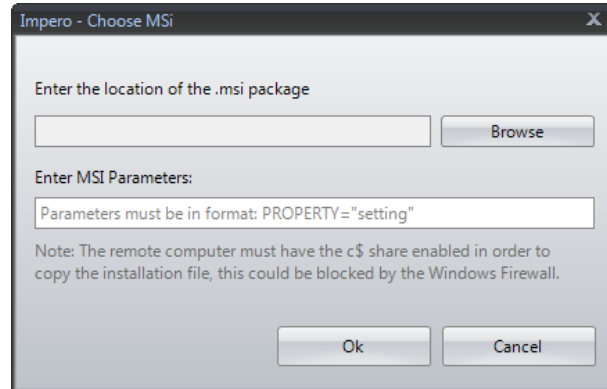


c) From the main Remote Deploy MSI window, please tick any computers on the left that you wish to deploy Impero Client to.

The ticked computers will automatically be displayed on the right.

d) When you are ready, please click 'Install Now'.

You will then be presented with the following window:

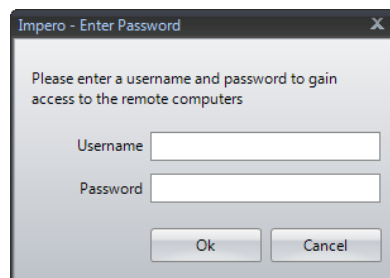


e) Please click Browse and locate the ImperoClientSetupxxx.msi installation file. This must physically reside on the same computer that is running the Remote Deploy MSI tool and not from a remote Share.

Leave the MSI Parameters box empty since the installation is Silent anyway.

f) Click OK.

g) The 'Enter Password' box will appear where you must enter a username and password that has write access permission to the remot computers C: drive:



h) The Remote Deploy MSI tool will detect that you are attempting to deploy Impero Client and subsequently display the Enter Server IP box. Please enter the IP Address of the Impero Server computer... this will enable the Client, once installed on the remote PC to instantly connect to the Impero Server rather than letting the Impero Client attempt to locate the Server itself using a UDP broadcast.

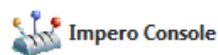
i) Follow the rest of the instructions on screen and the installation, including progress, will be displayed on screen.

If you receive any error messages during installation, there will be a link to see the meaning of the MSI error, however, the most common deployment errors are due to:

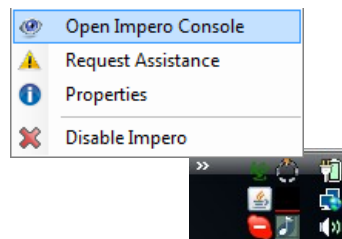
- Remote Computer Windows Firewall being enabled
- Remote Computer is powered off
- Remote WMI service/RPC Server is not installed/enabled
- Remote PC does not meet the [minimum system requirements](#)
- Anti-Virus/Anti-Spyware may be blocking the installation
- Remote DCOM may be disabled which allows connection to WMI

## 2. Getting Started

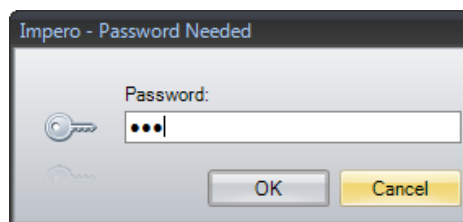
To begin using Impero, please locate the Impero Console shortcut icon on the desktop or start menu and double click.



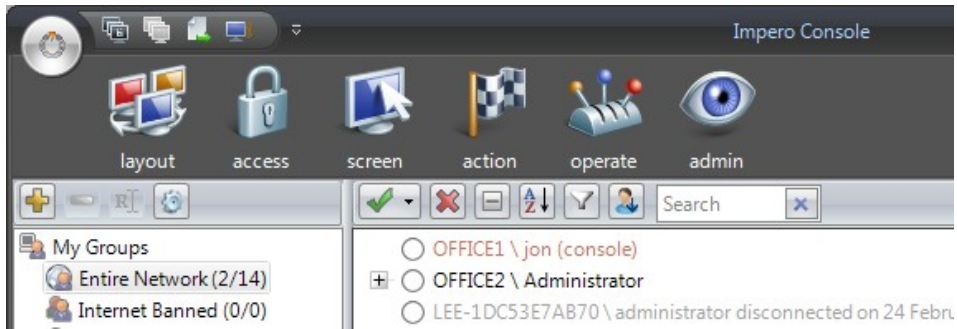
Alternatively, locate the Task Tray icon, near the System Clock and click once to see the following menu:



After clicking the icon to open the Impero Console, you will normally see the Password entry box, unless the Impero Server has been set-up to give your username or computer access to Impero without a password.



Upon opening the Impero Console, you will instantly be presented with a list of users and from this point, you are ready to begin using Impero.

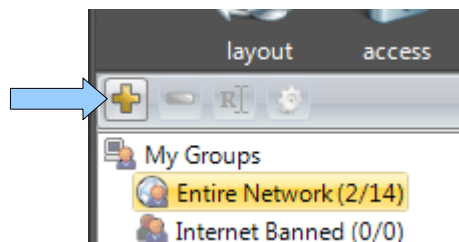


### 3. Creating Groups

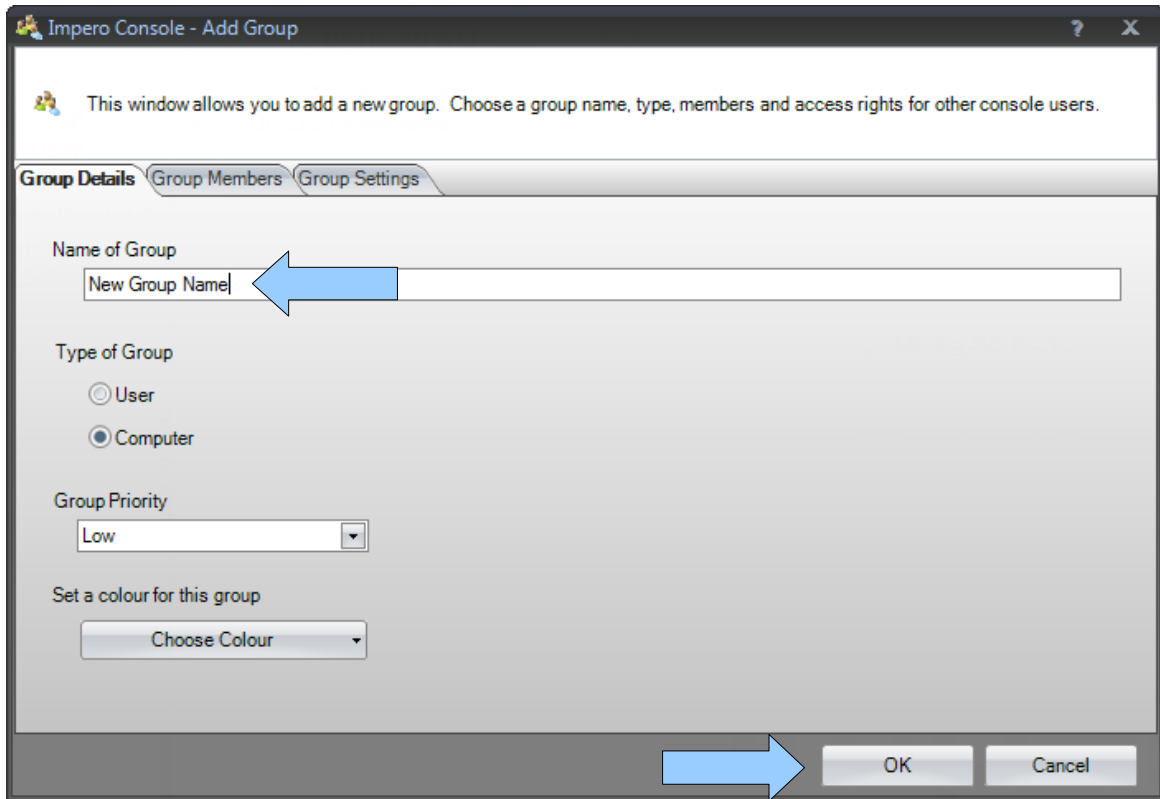
You may want to segregate your network into several groups, maybe one group for each IT Suite for example.

To do this, simply follow the following steps:

a) From the main Console, click the Add New Group button as shown in the image below:

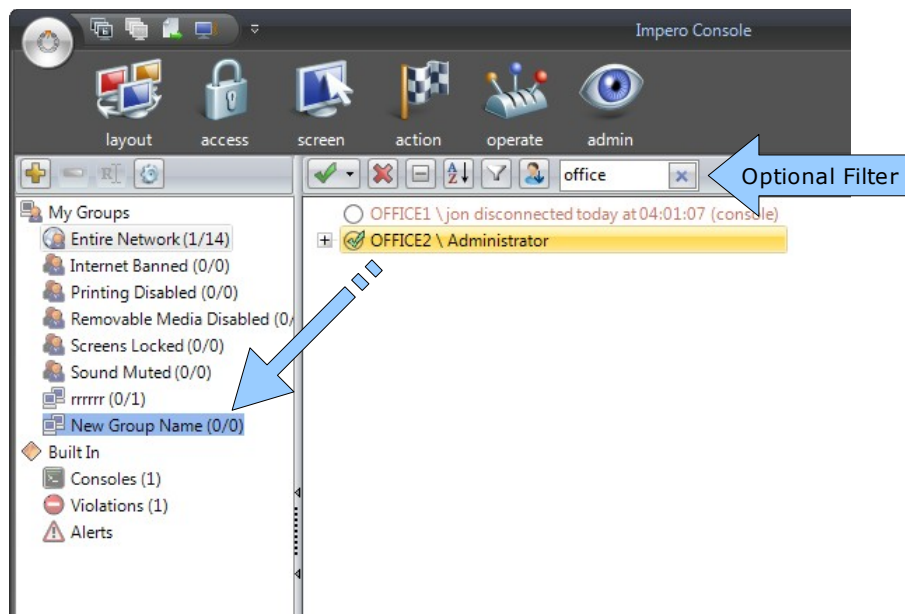


b) In the window that opens, type a name for the group you want to create. If you will be adding computers to this group leave the 'Type of Group: Computer' selected, if you want to add users to this new group, change the 'Type of Group' to User. Once you have named your group, simply press OK.



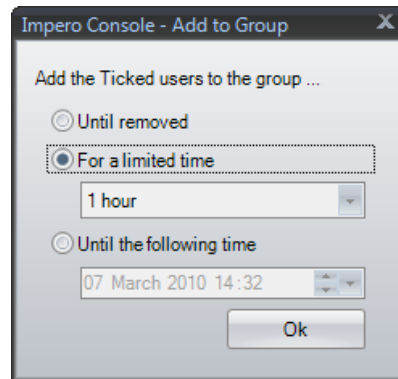
## 2.1 Adding users or computers to new groups

a) All groups are in the 'My Groups' list on the left of the main Console window. To add computers to a group, simply tick the computers on the right panel and drag 1 or more onto the newly created group. The users or computers you ticked will then be added to the group you drag on to:



You can filter the above user list using the search box above the list, this will filter the list by the search criteria you specify.

b) Once you drop the ticked users into the group, you will be presented with the following window, where you can specify when you want the computers or users to be automatically removed from the group:



To make the computer a member of the group permanently, select 'Until removed' and press OK.

You can now switch to the new group by clicking the group on the left of the main Console.

## 2.2 Removing users or computers from groups

- a) Select the group you wish to remove users from
- b) Tick the users you wish to remove from the current group
- c) Right click any one of the ticked users and select 'Remove from this group' or drag and drop onto the Entire Network group.

## 2.3 Removing users or computers after a period of time automatically

- a) Right click the group you wish to remove users from and select 'Properties'
- b) Click the 'Group Members' tab
- c) Find the user in the list and find the column representing 'Removal Date' and tick the checkbox
- d) The drop-down box will become enabled where you can select a date and time of removal or you can manually click the date or time values and edit them

# 4. Monitoring

Impero is a powerful monitoring tool, giving you a high level of control over what happens on

your network.

### 3.1 Viewing Live Thumbnails

To view Live Thumbnails, simply select the 'Layout' button on the main Console window and select 'Live Thumbnails'.

This will display the current group you are viewing in a 'thumbnail' view.



The various controls above the thumbnail view give you greater control of the thumbnails, for example, to resize the thumbnails or take remote control of them.

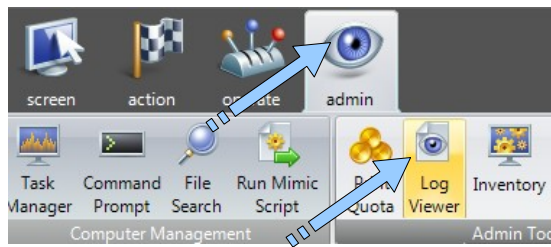
### 3.2 Checking recent computer usage history

If the user is still logged on:

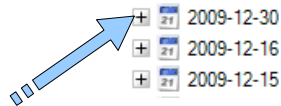
- a) Change Layout to Treeview by selecting the 'Layout' button at the top of the Console then choosing 'Tree View'.
- b) Find the user you wish to see history for and click the + button to the left of list entry, this will expand the user, showing a preview thumbnail to the right
- c) Find the node that says 'Recent History' and click the + button to its left to expand this node
- d) You will be presented with several history nodes, representing Windows, Websites, Applications, Printed documents and Deleted Files. Expand the appropriate node to see the history for that category.

If the user is no longer logged on or you wish to review usage history for previous days:

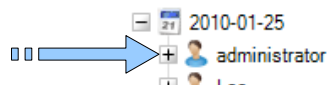
- a) Click the 'Admin' button on the main Console window
- b) Choose 'Log Viewer' and the log viewer should open



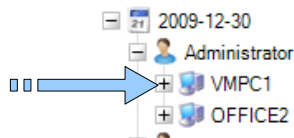
c) Click the + (expand) the Date you wish to see history logs for



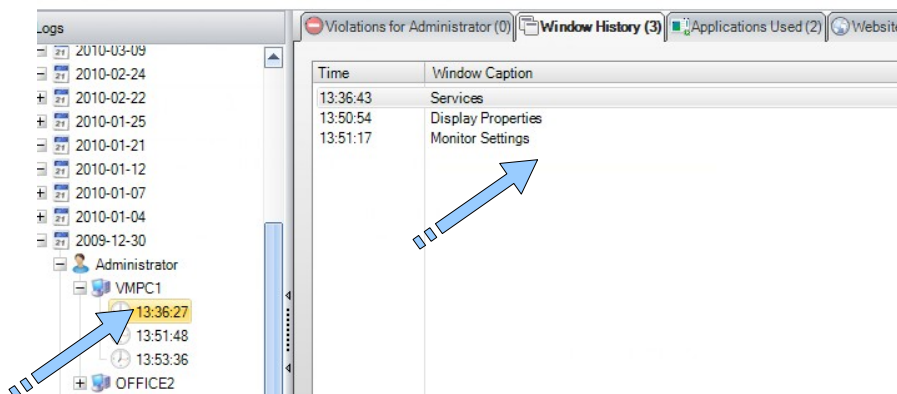
d) You will see various usernames who were logged on that day, expand the node of the username you wish to see logs for



e) You will now be presented with all the computers this user logged onto that day, expand the computer that the user was using which you wish to see logs for



f) Now you will see all the times this user logged onto this computer during the day you are interested in, click one of these times/sessions to see computer usage logs

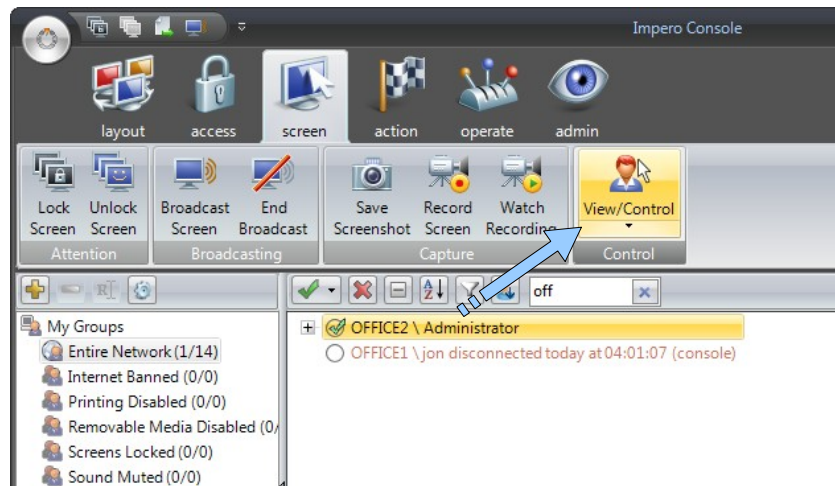


g) Various tabs will be populated with computer usage history and the first tab will show any violations that this user raised

## 5. Giving assistance / Remote Control

To give a user assistance:

a) Find the user in the main list (tree-view) and either double click, right click and select 'Remote Control' or highlight the user, select the 'Screen' button from the main toolbar and choose 'View/Control'



b) A window will open showing the remote screen. To take control, click the 'Control' button once.



c) To see a larger view, click the 'Full Screen' or 'Size' button once.

d) To end the Remote Control session, simply close the window or click the 'quit' button.

### 4.1 Reducing CPU Usage/increasing Remote Control Speed

On certain computers you may see the CPU usage increase to what appears to be quite a high level. Please be assured that the CPU that Impero uses is User-Mode CPU and should not affect the operation of the computer.

However, if the CPU rises above 50% or you wish to speed up the remote control speed, you may find the following useful:

- On the remote control window, click the Settings button and choose Enable Driver. If the remote computer uses an Nvidia or ATI graphics card the Kernel driver will be used.
- Try disabling Hardware Acceleration on the remote computer
- Remove colorful wallpaper on the remote computer and any complex animations

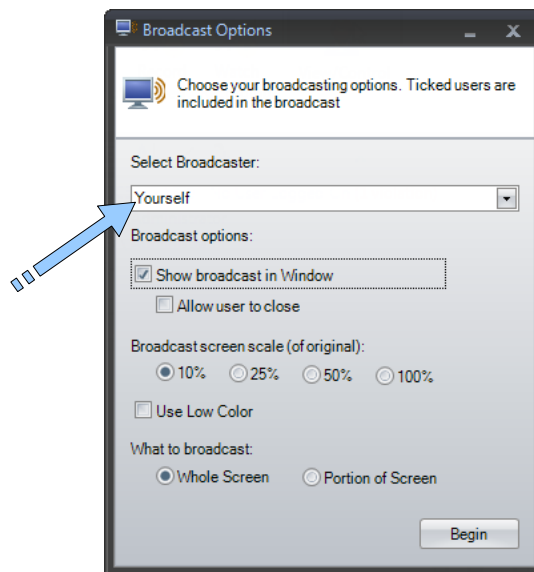
## 6. Screen Broadcasting

To broadcast your screen or another screen to one or more users, please follow the below instructions:

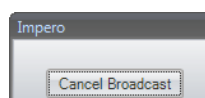
- a) Tick the users in the tree-view list who will receive the broadcast
- b) Click the 'Screen' button on the main Console toolbar
- c) Choose 'Broadcast Screen' option



- d) Select which screen you wish to broadcast from the drop-down box, the default is 'Yourself' to broadcast your own screen.



- e) Amend the various options for the broadcast such as the ratio and colors then press 'begin'.
- f) To cancel the broadcast, press the 'Cancel Broadcast' button on the window in the top right of your screen, or open the Console and click 'Screen' menu option, then select 'Cancel Broadcast'.



## 7. Locking Screens

You can lock 1 or more computer screens to stop the remote user from using their computer. Even after restarting the computer, they will be re-locked due to the policy that is applied.

To lock an individual screen, follow the below instructions to add 1 or more users to the 'Screens locked' group:

1. Tick the users who's screens you wish to lock
2. Click the Screen button from the main toolbar and choose Lock Screen.



3. The users you ticked will now appear in the 'Screens Locked' group on the group selection list to the left of the Console
4. You can click the 'Screens Locked' group to see who's screened are locked
5. To remove users from this group, tick those who you wish to remove and either drag them to the Entire Network group, right click and 'remove from group' or click the Screen menu item and click Unlock Screen

Alternatively: Tick the desired users and drag them into the 'Screens Locked' group

To lock the screens of the whole group, follow these instructions:

1. Select the group from the group list on the left of the Console
2. Click the Access button from the main toolbar and choose Lock Screen



3. This operation will lock the screens of any user or computer in the group you selected  
NOTE: if the group is a computer-group the computer will stay locked even if noone is logged onto the computer.
4. To Unlock screens, follow steps 1 and 2 but choosing 'Unlock Screen' instead

## 8. Disabling the Internet

To disable the Internet for **an individual**:

1. Tick 1 or more users from the main Treeview list
2. Drag the users into the 'Internet Banned' Group

To enable the Internet for an individual:

1. Select the 'Internet Banned' group on the left of the Console
2. Tick the users you wish to give access to the Internet
3. Drag the users to the Entire Network group or Right click any of the users and choose 'Remove from group'

To disable the Internet for a **whole group**:

1. Select the desired group from the group selection list on the left of the Console
2. Click the 'Access' button from the main toolbar
3. Click the 'Lock Internet' button



To enable the Internet for a group:

1. Select the desired group from the group selection list on the left of the Console
2. Click the 'Access' button from the main toolbar
3. Click the 'Unlock Internet' button

## 9. Add a new Policy

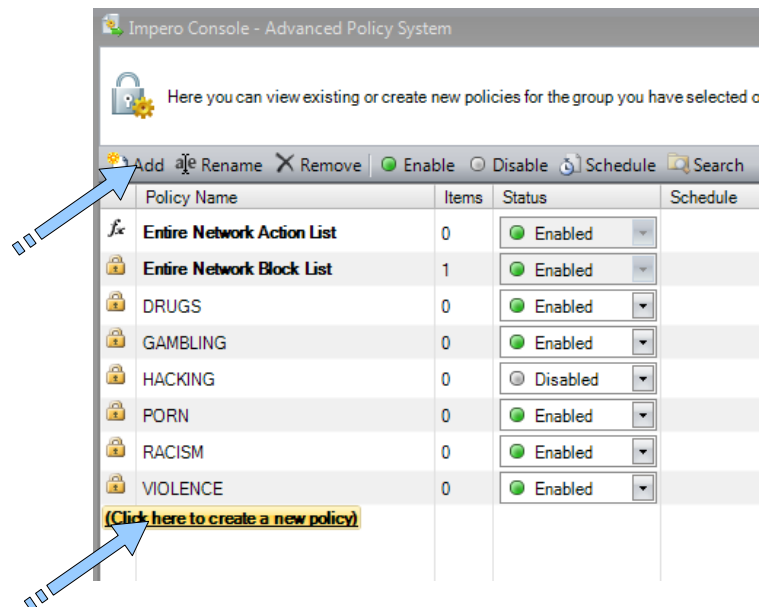
Impero has a very advanced Policy system, allowing you to perform numerous functions according to a schedule.

To add a new Policy to Impero:

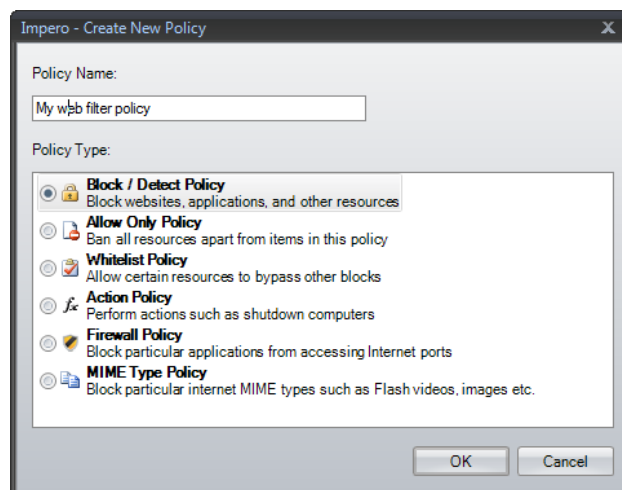
1. Select 'Access' from the main toolbar and choose 'Advanced Policies':



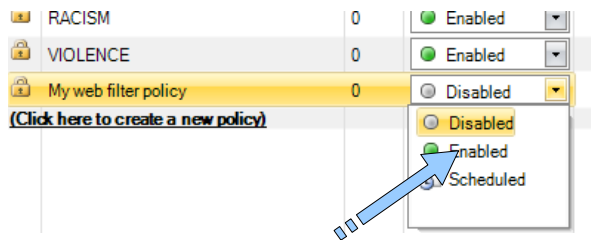
2. In the Advanced Policy window, please select 'Add' or click the link in the list to Create a new policy:



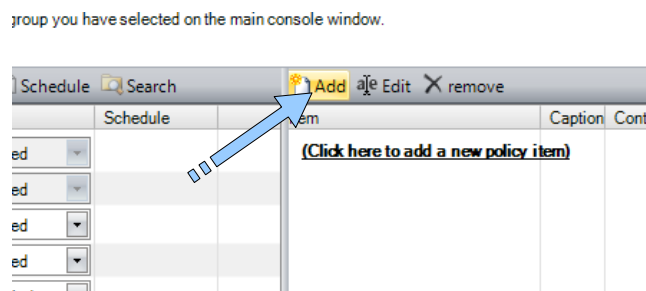
3. Type a name for the new policy and select the appropriate type of policy then click OK:



4. The new policy will appear in the main policy list, but disabled, so we must enable it:



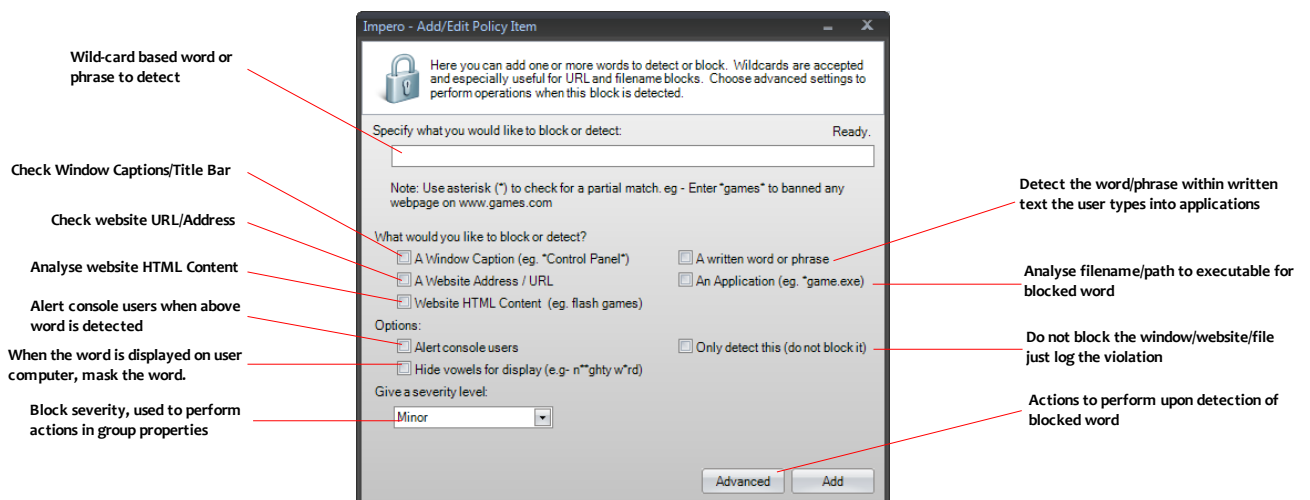
5. Once it is enabled it will change position in the list but still in alphabetical order. You can now add new items to this policy. Select your new policy on the left and choose 'Add new policy item' on the right side of the Advanced Policy window or click the link in the list:



6. The Add/Edit policy item window will appear, where you can add banned resources and the appropriate detection context. This window will change in appearance depending on the type of policy you selected, as explained in subsequent sections.

### 9.1 Block Policy Item screen

The block policy type is the most common type of blocked resource and the screen is shown below:



## 10. URL Filtering

After you have followed the steps in section '[Add a new policy](#)', you are ready to add a resource to be banned. The image below shows how to block a website URL (assuming you have followed the above steps).

1. From the policy selection screen, select 'Block/Detect Policy'
2. Enable or schedule the policy and choose 'Add Policy Item'
3. The following screen will appear where you can fill in the details as shown

Impero - Add/Edit Policy Item

Here you can add one or more words to detect or block. Wildcards are accepted and especially useful for URL and filename blocks. Choose advanced settings to perform operations when this block is detected.

Specify what you would like to block or detect: Ready.

www.websiteurl.com

Note: Use asterisk (\*) to check for a partial match. eg - Enter \*games\* to banned any webpage on www.games.com

What would you like to block or detect?

A Window Caption (eg. \*Control Panel\*)  A written word or phrase

A Website Address / URL  An Application (eg. \*game.exe)

Website HTML Content (eg. flash games)

Options:

Alert console users  Only detect this (do not block it)

Hide vowels for display (e.g. n\*\*ghty w\*rd)

Give a severity level:

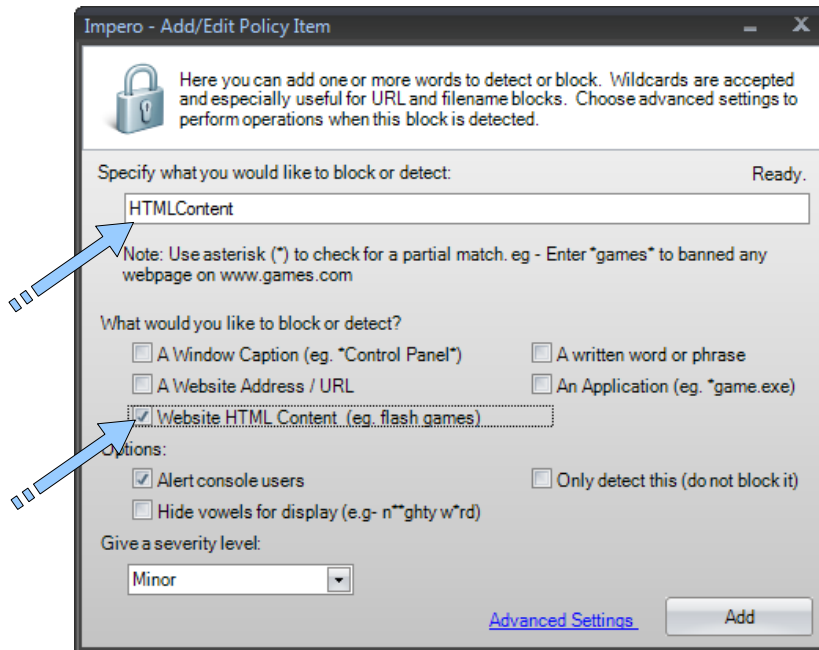
Minor

[Advanced Settings](#) Add

Please note the URL can contain Wild-cards. For example, \*games\* to block any url containing the word games – this can block hundreds of websites with just 1 block item.

# 11. Content Filtering

An example website content filter is shown below.

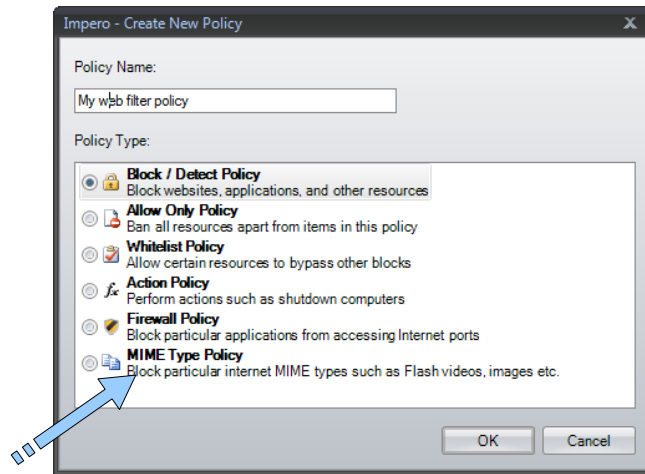


- HTMLContent must be enclosed in \* (asterisks) to be effective.

## 12. MIME Filtering

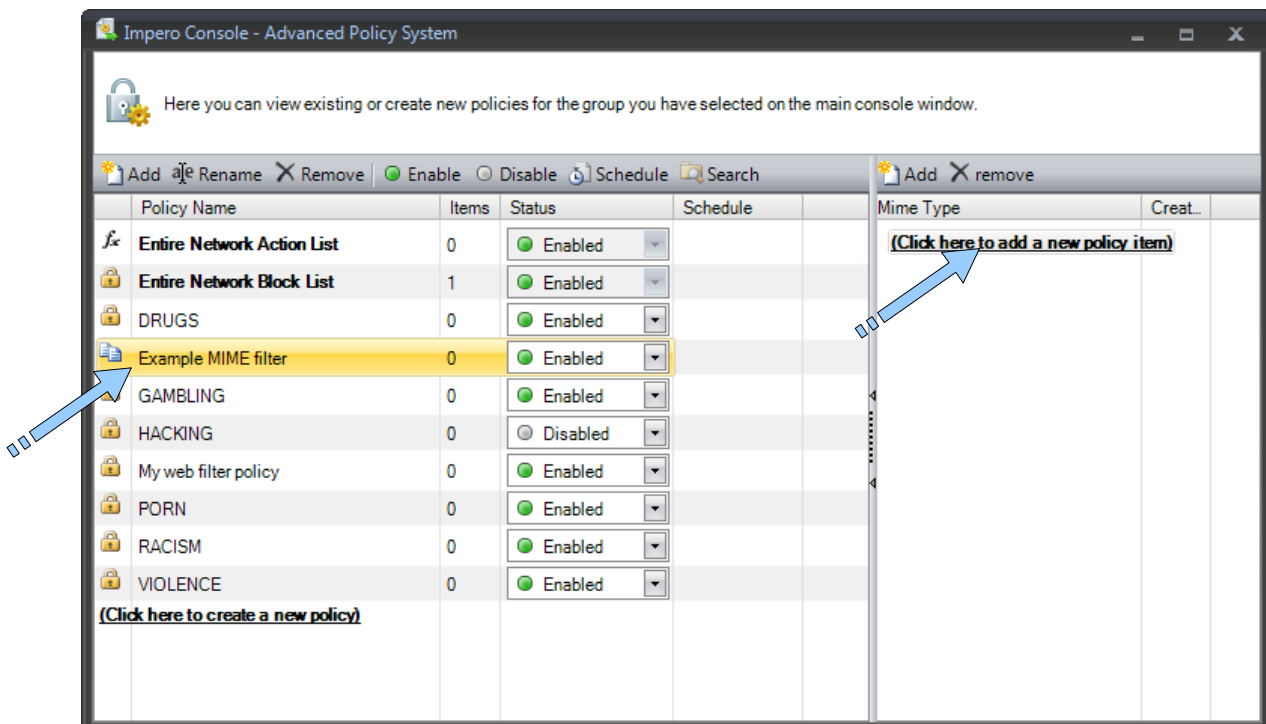
A MIME Filter allows you to block certain types of resources from being used while web browsing, for example, Flash Objects or Video files in web pages.

To add a MIME filter, you must select the MIME Filter type from the Policy Selection screen:

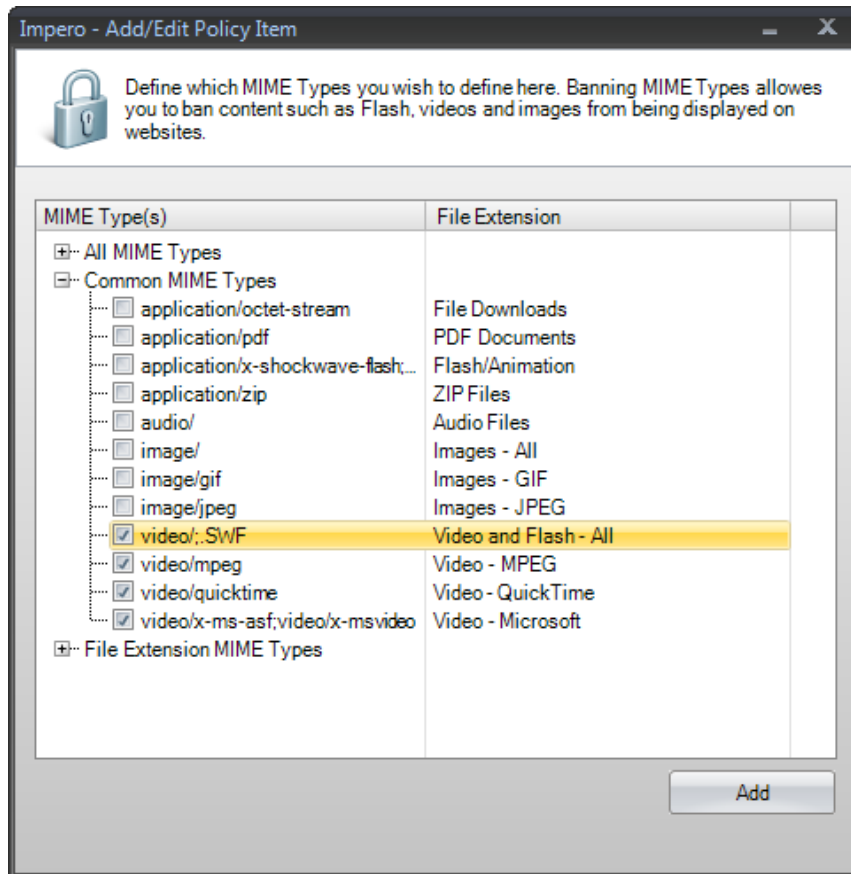


Once you have created a MIME policy, you can add a MIME item to the policy as shown below:

1. Select your enabled or scheduled MIME filter from the Policy list
2. Click 'Add new policy item' on the right



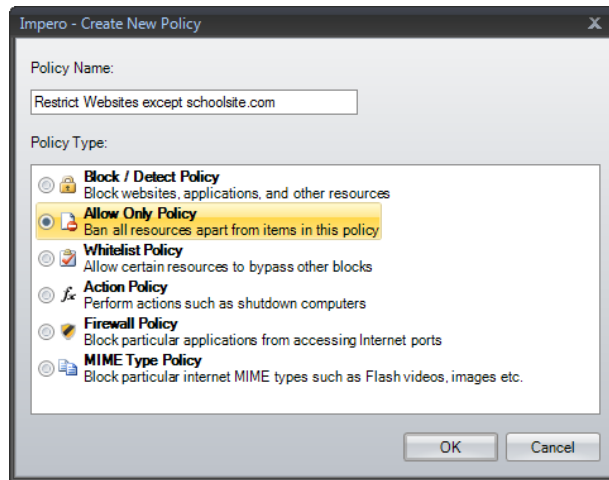
3. Select the MIME type from the list, and click ok, as shown below:



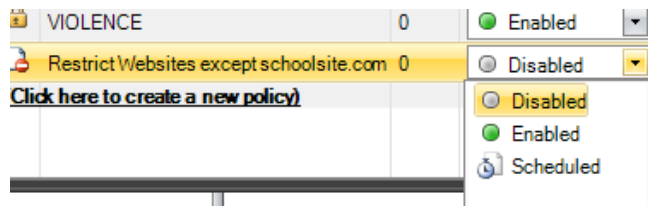
### 13. Restrict all websites except... (allow-only)

To restrict all websites, except a few, please follow the instructions below:

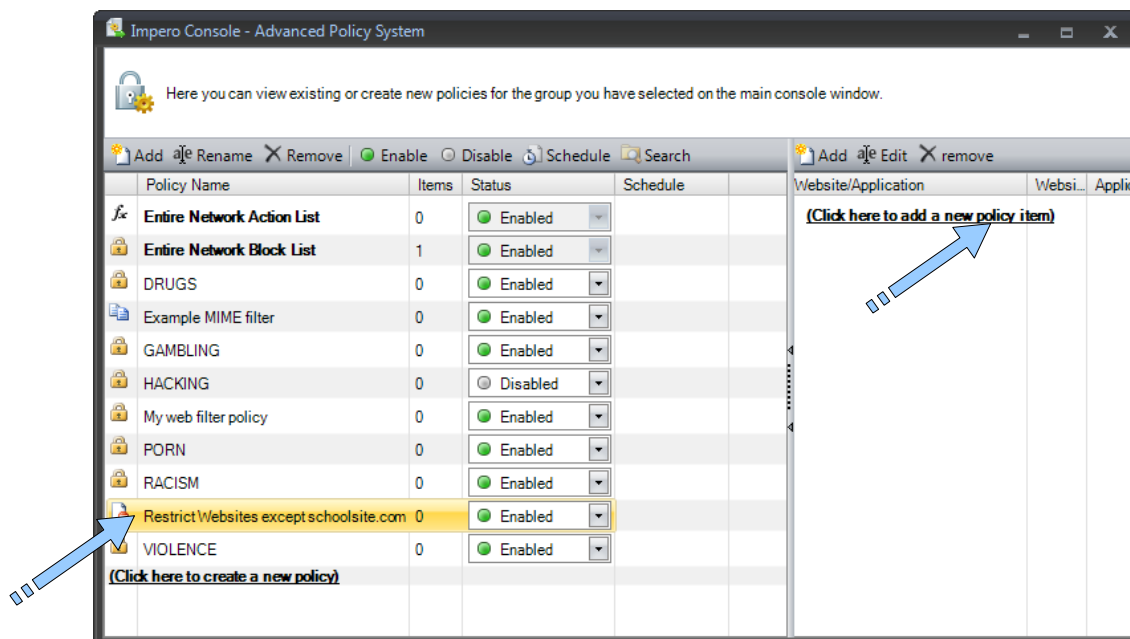
- 4. From the policy selection screen, select 'Allow Only Policy'



- 5. Select the new policy from the list and make sure it is enabled




- 6. Now select 'Add new policy item'



- 4. Select 'a website address/URL' and enter the URL in the box provided

Impero - Add/Edit Policy Item

 Any items you add to a White List will be allowed even if they happen to be blocked in another group policy.

What would you like to white list?

- A Window (e.g- Control Panel)
- A website address / URL
- An Application (e.g - game.exe)
- A written word or phrase (e.g-hack impero)
- Website Content (e.g-flash games)

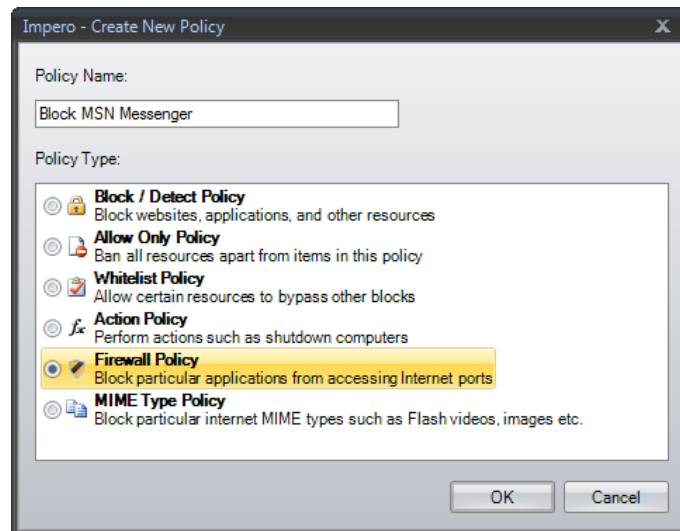
Specify what you would like to white list:

Note: Use asterisk (\*) to check for a partial match. eg - Enter \*games\* to always allow any webpage on www.games.com even if it has been banned by another policy

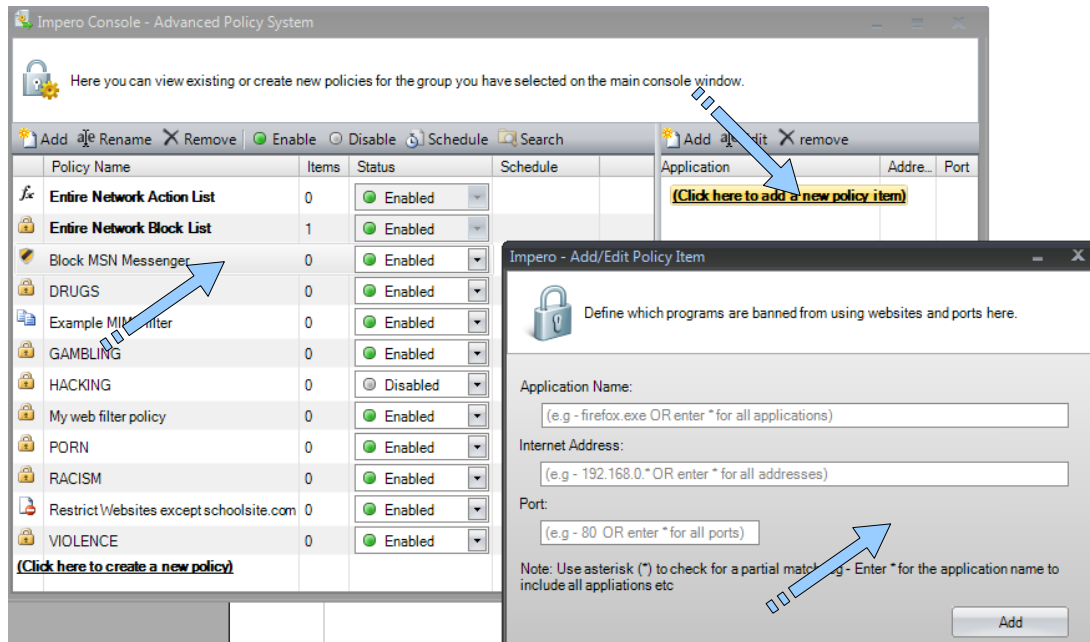
## 14. Client-Side Firewall

Impero has a built in Firewall that can block certain applications from accessing certain ports and IP Addresses.

To add a Firewall policy, follow the 'Add a New Policy' instructions above, but selecting the Firewall Policy type:



Once you have added a Firewall Policy, you can select 'Add new policy item' on the right of the main Policy screen to see the Add/Edit Policy Item screen:



On the Add/Edit Policy Item screen, you can enter an Application Name / Path or use \* for all applications, Internet Address (IP Address) or \* for all, and finally you can choose a TCP Port to block for the named application and IP Address or use \* for all TCP Ports.

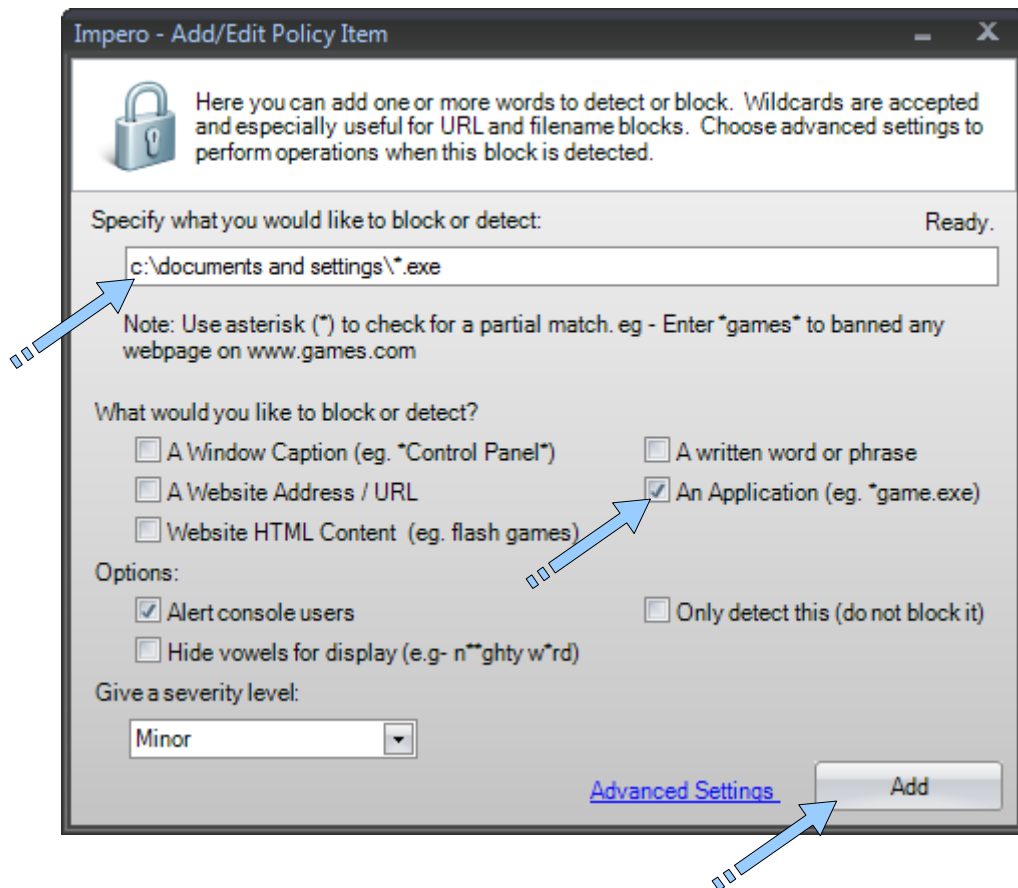
If for example you wish to block MSN Messenger from accessing the Internet, you can specify \*msnmsgr.exe\* as the application name, then use \* for Internet Address and \* for Port.

## 15. Application Filtering

Impero's policy system allows you to block access to Applications/executable files running from hard drives, flash disks or cdroms.

To block access to an application, please follow the below instructions:

1. Create a new Block policy (see section 'Add a new policy')
2. In the Add/Edit Policy Item screen enter the filename you wish to block. You can use wildcards in this field:



3. Once you have added the filename, please select the checkbox 'An Application'
4. Now click Add to add the blocked item

The above image gives an example of blocking all .exe programs from running from the documents and settings folder.

You can easily block all applications from running by blocking \*.exe and white-listing [c:\\\*.exe](#) .. alternatively you can simply make a white-list of applications, see white-listing.



## 17. White Listing

If a website or application is banned for any reason, and it is legitimately required to run or open, you can exempt it from detection by adding the resource to a 'White-list'. Any resource added to a white-list will not be blocked by any other lower or equal priority policy – websites however, will still be banned if you ban the internet in a higher or equal priority policy.

To add a new White-list Policy, follow the steps in section 'Add a new policy'.

1. Once you have a White-list policy in place, you can add policy items to it by selecting the White-list policy and clicking the 'Add new policy item'.

The screenshot shows the Impero Console interface. A table lists various policies, including 'Entire Network Action List', 'Entire Network Block List', and several specific filters like 'All legitimate websites' and 'Block MSN Messenger'. A blue arrow points to the 'All legitimate websites' policy. Another blue arrow points to the 'Add new policy item' link in the table's header. A third blue arrow points to the 'Add/Edit Policy Item' dialog box, which is open over the table. The dialog box has a title bar 'Impero - Add/Edit Policy Item' and a lock icon. It contains the text: 'Any items you add to a White List will be allowed even if they happen to be blocked in another group policy.' Below this, there is a section 'What would you like to white list?' with several radio button options: 'A Window (e.g. Control Panel)', 'A website address / URL' (which is selected), 'An Application (e.g. game.exe)', 'A written word or phrase (e.g. hack impero)', and 'Website Content (e.g. flash games)'. Below the options is a text box labeled 'Specify what you would like to white list:' containing the text '\*good-website.com\*'. A note at the bottom of the dialog box says: 'Note: Use asterisks (\*) to check for a partial match. eg - Enter \*games\* to always allow webpage on www.games.com even if it has been banned by another policy'. An 'Add' button is at the bottom right of the dialog box.

Policy Name	Items	Status	Schedule	Item	Caption	Content
Entire Network Action List	0	Enabled				
Entire Network Block List	1	Enabled				
All legitimate websites	0	Enabled				
Allow only known applications	0	Enabled				
Block MSN Messenger	0	Enabled				
DRUGS	0	Enabled				
Example MIME filter	0	Enabled				
GAMBLING	0	Enabled				
HACKING	0	Disabled				
My web filter policy	0	Enabled				
PORN	0	Enabled				
RACISM	0	Enabled				
Restrict Websites except schoolsite.com	0	Enabled				
VIOLENCE	0	Enabled				

2. The Add/Edit Policy item window will appear where you can choose the White-list Criteria. For a website, choose 'a website address'
3. Enter the website into the text-box below, using wild-cards where necessary.

## 18. Scheduling Actions

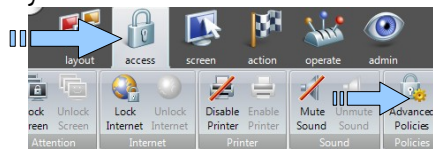
Impero allows you to schedule any policy type. So for example you can schedule block policies to run at certain times of the day.

This becomes more powerful when you apply these schedules to 'Action Policies'.

An 'action' can range from powering off a group of computers to banning the internet.

To schedule an action policy, you must first create an action policy:

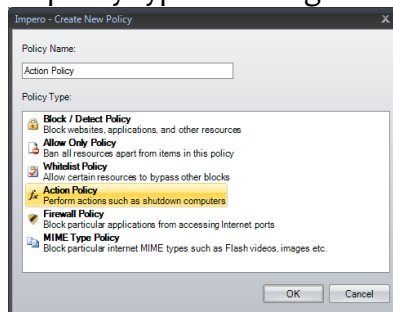
1. Open the Advanced Policy screen



2. Click 'Add' to add a new policy



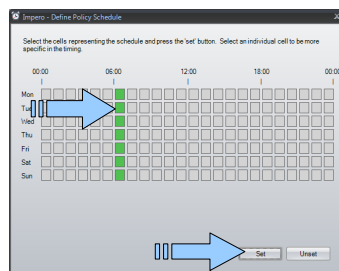
3. Choose 'Action Policy' in the policy type list and give the policy a name



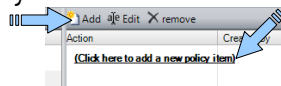
4. Schedule the Policy



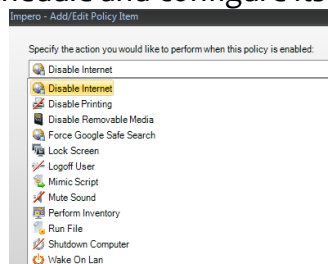
5. Click the 'New Schedule' button that appears to the right of the policy
6. Set the schedule by highlighting the appropriate boxes then press the 'Set' Button and close the window



7. Now you can add a new policy item



8. The add action window will be shown where you can select the action you wish to perform according to the schedule and configure its options

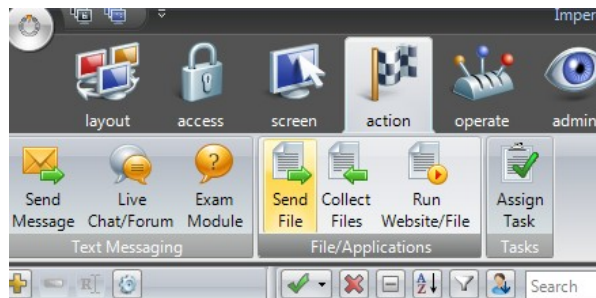


## 19. Sending Files

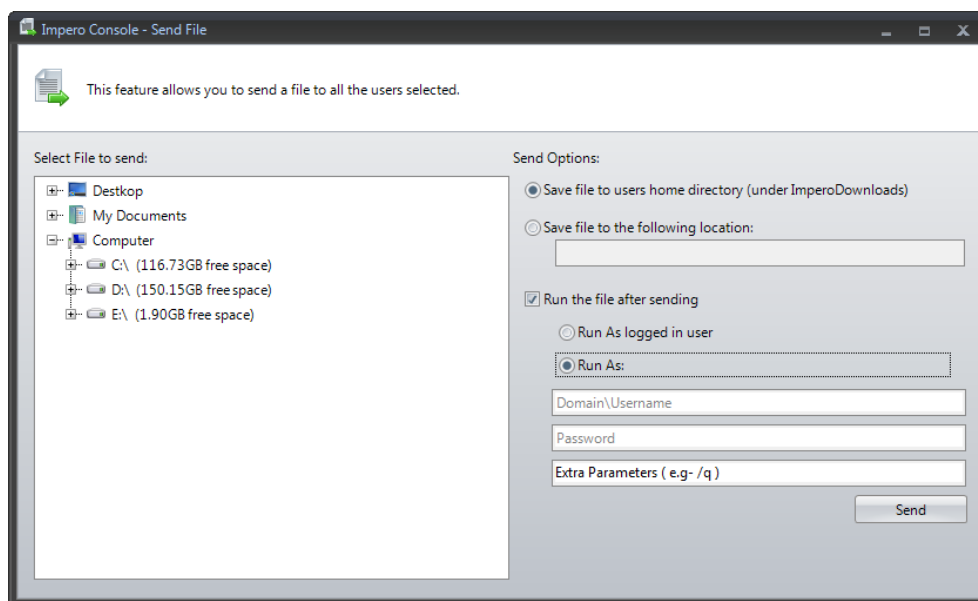
You can send files of any file size to 1 or more clients on the network, with multiple options.

Please follow the instructions below for more information.

1. Tick the users or computers you wish to send a file to
2. Click the Action button from the main toolbar and choose Send File:



3. After you select the Send File option, you will be presented with the Send File window where you can choose a file to send:

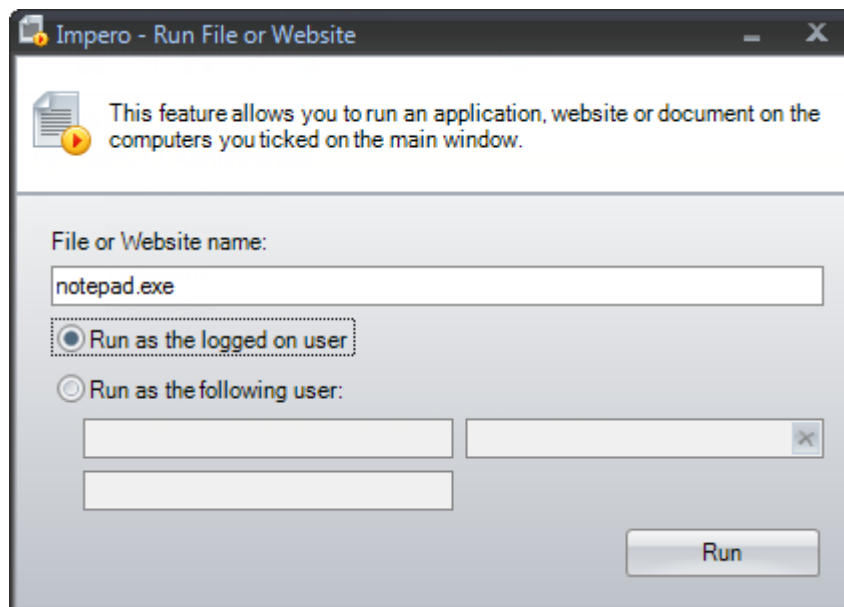


4. Once you select a file to send in the browse box on the right, you can choose various options on the right. The first option is to Save the file to the users Home Directory or Save to a specific location on the remote computer hard disk drive
5. There is also a Check-box that if checked will automatically run the file when the remote computer has received the file.
  1. Choose Run As logged in user to run the file using the remote users credentials or choose Run As: to run with different credentials – security warning!

## 20. Running Applications and Websites

Much like the ability to send files and run them, the Run File/Website option allows you to run a file or website on multiple remote computers.

1. Tick the users you wish to perform this action on
2. Click Action and select Run Website/File:



3. You can now choose whether to run the file as the logged in user or using different credentials – security warning.
4. When you are ready, click Run and the website or file you specified will run on all the remote computers you ticked – the remote computers must be logged in.