SitW Network User Guide

v3\_after\_Lei\_additions\_March2014 – ANONYMISED BY STEVE 2016

Authors:

Holger Schnädelbach

Holger.Schnadelbach@nottingham.ac.uk

Lei Ye

L.Ye@nottingham.ac.uk

Steve North

Steve.North@nottingham.ac.uk

Mixed Reality Laboratory (MRL), Department of Computer Science, University of Nottingham

[Basic System Description (natural language and diagram)](#h.c785dhvfv8jq)

[Day-to-day operation of the screens network](#h.j7n1kc5z4kat)

[How do I schedule web-based content to run on the screens network?](#h.x2i9gbaafgu6)

[Schedule file location](#h.qrk1kh1j6q7z)

[Backing up and editing the schedule file](#h.e6twmihk4ums)

[Schedule file syntax guide](#h.eqmkucy7ag6b)

[How do I host web-based content to run on the screens network?](#h.cqy96zcg21bm)

[How can I override the schedule file and manually control content?](#h.1u2bl22k2cda)

[Manual Content Selection with the SitW Client Scheduler Remote Control web app.](#h.vk76kmbd7vce)

[Keyboard switching to a local copy of the schedule file](#h.yyzda261w5ql)

[How do I remotely monitor/administer the screens network?](#h.1agsztwnw56u)

[Maintenance via TeamViewer](#h.l7xwveg4ayxu)

[How to enable remote keyboard shortcuts](#h.852u1d8lchhp)

[How to transfer files to a node PC](#h.dj4p4q92bn0a)

[How to use text chat with a colleague on-site](#h.joh56vr1m2gg)

[Screen Remote Control via NEC PC Control Utility PD1 tool](#h.n4emdrflz9md)

[UNION Server remote administration via the Web](#h.9af4cg82qfcv)

[UNION Server - the ‘interaction server’](#h.yt1clbgncmb9)

[How to quickly check if our UNION Server is running, without credentials](#h.kr5247e7j490)

[How to remotely administer UNION server](#h.s6066wolt07a)

[Stopping and restarting UNION Server when installed as a Windows Service using Remote Desktop](#h.8q3bovq2504z)

[Regular maintenance tasks](#h.zdigngu3jztg)

[Regular screens check via Team Viewer](#h.wwa17v2rnhvt)

[Reviewing user added content for suitability (Moment Machine etc)](#h.at8ifwqzzapu)

[On-site screen checks](#h.vlgxkis3q2xv)

[Video Server maintenance](#h.s38xp5szactc)

[A suggested timetable for checks](#h.37uyim5v24ai)

[Troubleshooting and problem solving](#h.uhldjhqr43ll)

[How do I disable security features to fault find on a node PC?](#h.ivdha0ghaot8)

[Secure Lockdown](#h.hjgvgbarfzsk)

[Firefox Kiosk Mode plugin](#h.7rbrowok2c9u)

[Where do I find the log files?](#h.4qielvd6k97x)

[UNION Server logging](#h.89qbcbs6rwmi)

[SitW Client logging](#h.1ifpr1jhunby)

[Known issues and solutions](#h.lx7k114iohc3)

[Windows User account corruption at The Mill and how to recover](#h.z9gna7y0jusz)

[How to manually close the iSpy video panel (grey frame)](#h.tf5qokln5en5)

[How fix iSpy when the stream from the local USB camera (via YawCam) has frozen](#h.252fm37c68vs)

[Keyboard shortcuts for closing crashed Firefox kiosk mode browser windows.](#h.veupku1by7l9)

[What can I do if a screen node is unreachable via TeamViewer?](#h.j9v52pxxdezo)

[Node PC recovery via Windows Remote Desktop](#h.w30xstcaif2u)

[Contacting a venue to request manual reboot of a node PC](#h.pawvel9jagyt)

[Where do I find important configuration settings?](#h.tkk8oz9fsk7j)

[SitW Client](#h.8xsdp9fdjdxy)

[SitwScheduler.ini](#h.5eljyf318115)

[iSpy video panel](#h.oshvi9uew4v7)

[iSpy video stream configuration](#h.f69aadfnerjl)

[UNION Server](#h.6vsy953ntvqc)

[Touch Foil configuration and calibration](#h.rqgcv92zwu1a)

[Phidgets Interface configuration and calibration](#h.22ajp7prgtzy)

[LAN and WAN configuration for nodes (router, IP addresses, port forwarding)](#h.45edeqwu0dma)

[Port Forwarding summary for a node](#h.ket5r014p95f)

[Testing Correct Port Forwarding with the NetCat tool](#h.2n67ai5rbryw)

[Node PC configuration](#h.dah7ox7talft)

[List of software to install on a new node PC](#h.9isvnjc6nc16)

[Firefox configuration (plugin updates disabled etc)](#h.54a8yqwbaox0)

[Windows configuration (resolution, update disabled, pop-ups etc)](#h.3rs1hxb3nxw0)

[Yawcam configuration](#h.fd29t69kyi4r)

[Node hardware configuration](#h.vrhqw4u2vkp6)

[Enable/disable audio system](#h.ak55r4jjr9q4)

[Schedule audio mute and unmute in Windows 7](#h.b7zvpfli2dax)

[Maintenance of Foscam IP cameras](#h.5mo3002dae02)

[UNION Server configuration](#h.kduckzq6jryn)

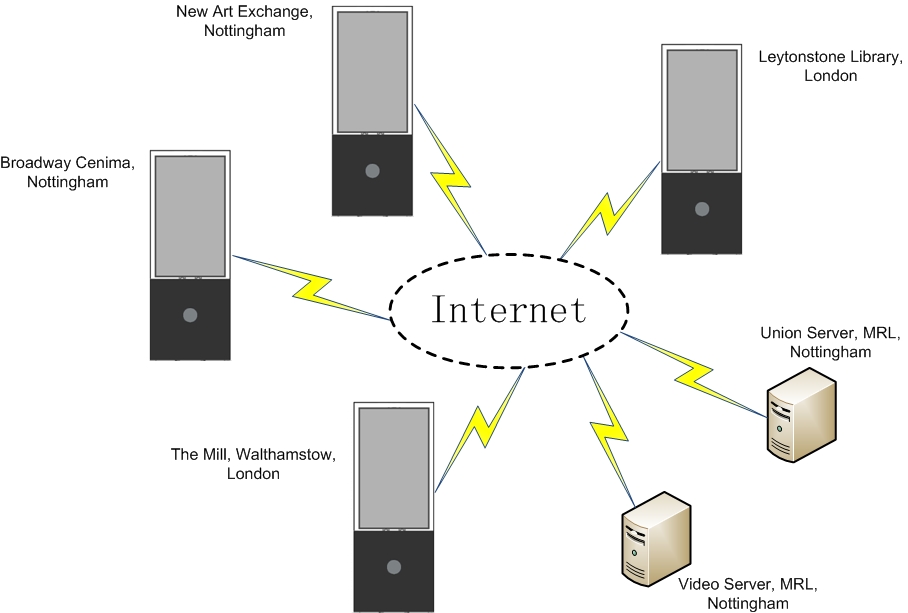
[How to setup UNION Server as a Windows Service - will run without a user logged in](#h.1dzn6c64otuf)

[Important Configuration Summary (IP addresses, video stream URLs, Windows accounts, port forwarding etc) - NO PASSWORDS](#h.gv23q0x579i8)

## Basic System Description (natural language and diagram)

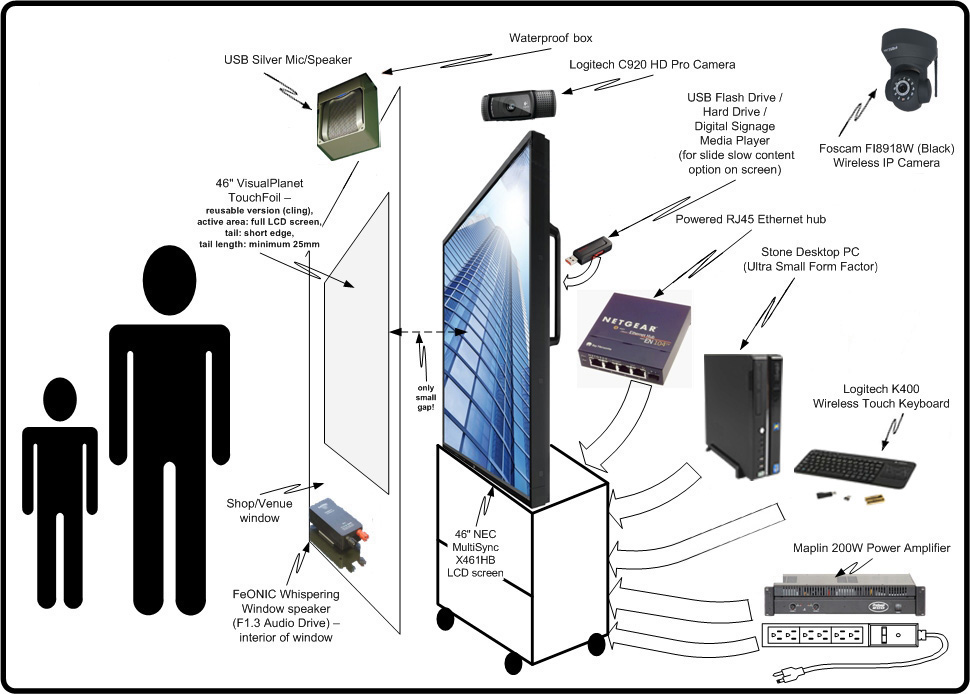
The SitW Network was implemented as a deliverable from the research project, ‘Exploring the potential of networked urban screens for communities and culture’ (EPSRC Reference:EP/I031839/1).

The SitW Network consists of a network of urban screen nodes (currently there are four), based in two UK cities. The screens are publicly facing, located inside partner venues.



Each node consists of:

* A networked Windows PC (running Windows 7 Professional), which is remotely administered.
* A 46” screen (mounted vertically in portrait mode) inside a partner venue, i.e. behind a glass window.
* A mechanism to enable interaction with the screen, through the glass window (varies from node-to-node, according to the glass specification).
* A camera and speaker (both available 'off-the-shelf') operate through the glass, making the installation interactive.
* A secondary camera, recording interactions 24/7 to protect the system and to ensure ethical research principles.
* An optional multi-way video link between the screens via a customised version of an Open Source product.
* Custom client software written to enable communication with a web-based schedule file, switching a program of applications, as required for one or more screens. This application also communicates with a server to share ‘interaction events’ between the screens in the network. Note: real-time manual override of the schedule is also possible (for demos, testing etc), via a custom web interface.
* Software tools for securing the scheduled content from user-tampering and retaining browser ‘kiosk-mode’.
* A physical case to contain/protect the hardware elements.
* Decals and visual branding around the screen - design varies between nodes.



The software system uses an off-the-shelf client/server infrastructure to provide real-time multi-user functionality for applications across the screen network (the ‘interaction server’).

To date, most of the applications implemented have been written in HTML5/Javascript, running in the Firefox browser (full-screen mode) and hosted on a web server. However, content need not follow this model. For example, it might be a stand-alone client application running on each node and (if required) making use of the interaction server.

## Day-to-day operation of the screens network

### How do I schedule web-based content to run on the screens network?

#### Schedule file location

* The schedule is controlled by a plain text file, currently located (and web visible) at:

<http://www.cs.nott.ac.uk/sitw/autoschedule/schedule.txt>

* Remote access and relevant web server permissions will be required to update this file, via an SFTP tool (such as SSH).
* This file is manually created, using the correct syntax, unless automatically generated by the SitW Client Scheduler Remote Control web app.
* In order to relocate this file, configuration changes would be required to SitW Server (TO DO: Lei, is this currently possible?).
* For the SitW Client Scheduler Remote Control web app to work, schedule.txt must have Permission Mode 777. If you are replacing the existing schedule.txt, it will inherit mode 777. If you delete/rename the original and upload a new schedule.txt, it is necessary to set the permissions back to 777.

#### Backing up and editing the schedule file

schedule.txt may be edited in any plain text editor (Windows Notepad etc) and then overwritten via an SFTP tool.

#### Schedule file syntax guide

Refer to <http://www.cs.nott.ac.uk/sitw/autoschedule/schedule.txt> for an example.

Summary of format:

<TIME:TTTT>|<APP NAME>|<URL>|<VIDEO SHARE MODE>|<VIDEO LAYOUT MODE>|<ATTRACTOR MODE>

Example:

1600|App\_Firefox|http://www.cs.nott.ac.uk/sitw/experiences/soundshape/stable/notouch/|videoOn|2|AttractorOff

* TIME: 24-hour clock in the format: TTTT.
* APP NAME options:

**App\_Firefox**

**App\_Chrome**

Hard-coded apps (without specified URL):

Photo Booth experience: **App\_MM**

No VIDEO SHARE MODE or VIDEO LAYOUT MODE options required.

Example: 1100|App\_MM||||

iSpy video only experience: **App\_iSpy**

No VIDEO SHARE MODE (defaults to option 1 - Full screen (2x2 grid layout)) or VIDEO LAYOUT MODE options required (defaults to videoOn).

Example: 1800|App\_iSpy||||

* URL - as you might expect! Currently, works with App\_Firefox and App\_Chrome.
* VIDEO SHARE MODE options:

YawCam only no iSpy video panel: **Yawcam** (which is case insensitive)

iSpy only no Yawcam: **iSpy** (which is case insensitive)

Both YawCam and iSpy: **videoOn** or **iSpy+Yawcam**

Note: VIDEO SHARE MODE is NOT required for App\_MM and App\_iSpy (see above).

* VIDEO LAYOUT MODE options:

**0** - Hide video panel

**1** - Full screen (2x2 grid layout)

**2** - At the bottom (4 pane/stream standard layout)

**3** - Full screen (1 large local video image + 3 small remote video images at bottom)

Note: VIDEO LAYOUT MODE is NOT required for App\_MM and App\_iSpy (see above).

* ATTRACTOR MODE options are: **AttractorOff** or **AttractorOn**.

When Attractor Mode on is set, inactivity (60 seconds) at a screen will cause SiTW Client to trigger Attractor Mode. This is currently fullscreen, mirrored video provided by iSpy. Local or remote screen interaction will disable Attractor Mode and the scheduled experience will run.

### How do I host web-based content to run on the screens network?

Content can be hosted on any web server.

Currently, the project content is hosted here:

<http://cs.nott.ac.uk/sitw/experiences/>

### How can I override the schedule file and manually control content?

#### Manual Content Selection with the SitW Client Scheduler Remote Control web app.

To use the SitW Client Scheduler Remote Control web app, go to:

<http://www.cs.nott.ac.uk/sitw/controller/stable/>

Password: <removed for security>

* From the drop-down menu below, select either an experience (or \*\* AUTOSCHEDULE \*\* to go back to the automatic schedule).
* There is no SUBMIT button, the request will be sent as soon as you select from the drop-down menu. Note: you won't get any visual feedback on the webpage that a change has been made.
* There may be a delay or up to a minute before the screen network responds (as determined by the check interval for SitW Client). Also, the 4 screens are not time synced. So, the changeover may be a bit staggered.
* Your selection will run on all screens in the SitW Network, it is not currently possible to select the schedule for individual screens.
* If it is an experience that requires different settings (or location specific URLs), the code will do all of this automatically. Then all of the SitW clients will pick up the change within approximately 60 seconds. Please note: there are no "file locks" currently. So, if several people all use the app at once, or if you keep changing experience rapidly, the results might be unpredictable!
* On the drop-down menu, \*\*AUTOSCHEDULE\*\* buts it back on schedule.
* The section at the bottom of the page is for more advanced (development) work It allows you to test new experiences on the network, without needing to understand the schedule file syntax. For example, replace <http://www.cs.nott.ac.uk/sitw/experiences/soundshape/stable/>

with <http://news.bbc.co.uk> to run this page on the screens network.

Note: one limitation here is that you can only run web content on Firefox. We don't have an option to run with Chrome.

* You don't need to add any of the schedule file syntax to control iSpy and YawCam.

The radio buttons allow you to select whether iSpy is running or not.

2-way video = standard 4 video feeds along the bottom.

Transmit video only = run YawCam and stream, but don't display video.

No Video is obvious!

* If you tick "Location aware", the app will add the appropriate arguments to the end of the URL (for exampe: ?loc=BW), putting it in the correct section of schedule.txt.
* Clicking the "Run" button will change all 4 screens, as with the dropdown menu.
* To change back to schedule, use \*\*AUTOSCHEDULE\*\* from the dropdown menu.

How it works:

The server-side code for the app is written in PHP and it's all in the "controller/stable" directory, with the HTML.

What's happening? - if you select an experience by name, on the web server schedule.txt is backed up as schedule.bak.txt in the directory "doNotDeleteForManualMode". Then the PHP code writes a new schedule.txt file, with the selected experience running 24/7.

* If you go to the "autoschedule" directory, containing our schedule.txt, you will see a sub-directory called "doNotDeleteForManualMode". Inside this are two files:
  + manualMode.txt - this is just used by the SitW Client Scheduler Remote Control web app to retain state. It will contain "true" if the app has manually selected an experience. This file should not require any manual intervention.
  + schedule.bak.txt - when the app engages manual mode, this will be a backup of the current auto schedule. It will be used to automatically restore back to schedule, when auto is selected from the app. If there is ever a problem with the app, it should be possible to manually recover the schedule from here.

#### Keyboard switching to a local copy of the schedule file

For testing purposes, it is possible to run a local copy of schedule.txt on a node PC, rather than the online schedule. In SitW Client, the keyboard shortcut for switching between a local and online version of schedule.txt is [Ctr] + [\_] (ctrl and underscore keys).

### How do I remotely monitor/administer the screens network?

#### Maintenance via TeamViewer

We use TeamViewer Host v7.0.17271.

A licenced copy is recommended, as this prevents pop-up screen messages appearing on the node screen, after a remote session.

<http://download.teamviewer.com/download/version_7x/TeamViewer_Host_Setup.exe>

Note: the Host version is required to prevent visible windows, even in a licenced copy.

##### How to enable remote keyboard shortcuts

When working remotely in TeamViewer, it is often useful to use keyboard shortcuts.

For example, [Windows key] to get access to the Windows Start menu,

[Ctrl] + [F5]: refresh browser window

[Ctrl] + [F4]: kill browser window

To enable this, click Actions menu (top of TeamViewer) > Send key combinations.

##### How to transfer files to a node PC

In a TeamViewer remote session, click the icon that looks like documents (top right) and then click File transfer.

##### How to use text chat with a colleague on-site

In a TeamViewer remote session, click Audio/Video > Chat.

This is very useful for remote communication with a team member on site, at a node.

#### Screen Remote Control via NEC PC Control Utility PD1 tool

The 46’ screen models that we use for the network are:

NEC MultiSync X461HB (HD Ready/720p 1360 x 768)

NEC MultiSync X462HB (Full HD/1080p 1920 x 1080)

Note: all screens are standardised to the resolution portrait 768 x 1360 (9:16). So, the X462HB screens are running at less than their potential Full HD.

NEC provide a Windows-based remote control application (NEC PC Control Utility PD1 tool) for these screen models, allowing multiple functions including: power on/off, channel select, input select etc. This tool is available free from here: <http://www.nec-display.com/dl/en/dp_soft/pccu_pd1.html>

At each node, the screen is connected to the network and listens on a fowarded port for incoming connections from an instance of the NEC PC Control Utility PD1 tool.

This software provides a method for maintaining the screens, while they are not public-facing.

To remotely access and control a screen (when first used):

* Run NEC PC Control Utility PD.
* Click Tool > Communication Settings > New Setting
* Enter the public IP address that has been configured at the venue with port 7142 forwarded to the screen (see port-forwarding information elsewhere in this guide).
* Click OK.
* Repeat until each of the screens in the network has been added.

To remotely control a screen (in this example, turn the screen on/off):

* Note: it can take the NEC PC Control Utility PD1 tool a while to refresh and detect the screens after starting. Initially, the screen names are grey and no details (name, status, inputs etc) appear in the bottom left panel. Once connected, the text is black and clicking on a name will display the screen’s details. Right-click on the required screen and then click Control > Power > Power On (or Power Off, as appropriate).

#### UNION Server remote administration via the Web

##### UNION Server - the ‘interaction server’

Interaction between screen applications is provided by the free version of UNION Server: <http://www.unionplatform.com/> This is hosted on our own Windows XP Virtual Machine at: <removed for security>. We use UNION Server v1.x series and the client code in our applications may not be compatible with later/current releases of UNION.

##### How to quickly check if our UNION Server is running, without credentials

Go to - <http://www.unionplatform.com/check/index-1.x.html>.

Enter the server details as:

Host: <removed for security>

Port: 8080

Click Go.

If all is well, you should get back: Connected to [<removed for security>] on port [8080]. Connection type: WEBSOCKET. Ping: [Loading].

If you need to stop, start, debug, check who's using the server, then read on...

##### How to remotely administer UNION server

It can be accessed in two ways: 1. On a web page that I've set up 2. By running a local Shockwave movie/Windows .exe.

# Web access (the easiest way):

Go to:

<http://www.cs.nott.ac.uk/sitw/servers/union/admin/>

Login details below.

# Local client method-

Go here to download one of the admin clients:

<http://www.cs.nott.ac.uk/sitw/servers/union/admin/downloads/>

Either download Windows .exe shockwave projector version and run locally (Flash security settings might need changing)

or download shockwave file and run locally (Flash security settings might need changing)

For all methods, use the following details:

Host: [<removed for security>]

Port: 9110

Password: <removed for security>

Tick remember password

##### Stopping and restarting UNION Server when installed as a Windows Service using Remote Desktop

Note: UNION Server is configured to run as a Windows Service (see later section on UNION Server configuration). This means that you can log in and out using both UoN Computer Science account credentials OR the admin account for the machine itself. In either case, logging out afterwards ensures that others can access the server. UNION Server will continue to run in the background.

Note: UNION Server will also restart with Windows XP. So, following scheduled patching, the server should recover on its own.

When testing changes to UNION Server’s configuration, you will need to stop and then restart it. This is achieved using Remote Deskop and the admin account for the Virtual Machine that hosts UNION Server: [<removed for security>]

* Remote Desktop into [<removed for security>], using the Windows admin a/c for this machine:
  + username: [<removed for security>]
  + pwd: <removed for security>
* Use the UNION Server stop server batch file to kill UNION Server.
* Stop the startserver service.
* Start the startserver service.
* Log out of snnadmin.

### Regular maintenance tasks

#### Regular screens check via Team Viewer

* Using TeamViewer’s Computers & Contacts panel, visually check that all screens and SitWVServer are showing as online.
* Using TeamViewer, connect to each screen in turn and then:
  + Check if currently scheduled experience is displayed.
  + In each screen, if iSpy is running for the current experience, test that ‘mouse event detector’ for Attractor is working. Click somewhere on the browser and check that interaction events are detected in iSpy (yellow frame around feed flashes in response to click).
  + Check for pop-ups, update reminders etc.
  + <Every few checks>Confirm that the TouchFoil driver is running.
* Using TeamViewer, connect to SitWVServer and check that all IP cameras are recording.
* Using NEC PC Control Utility PD1, check that each screen is powered 'on' (rather than accidentally left in standby, after a previous session).
* Using a browser, check that UNION Server is running:
  + [[<removed for security>] /union/admin/](http://www.cs.nott.ac.uk/sitw/servers/union/admin/)
  + Instructions elsewhere in this document.
  + If it connects, it’s working...

#### Reviewing user added content for suitability (Moment Machine etc)

Unmoderated content will require regular monitoring.

For example, Moment Machine has an admin interface for checking images:

[http:// [<removed for security>]:2221/?id=adminPage](http://pdnet.inf.unisi.ch:2221/?id=adminPage)

#### On-site screen checks

At least once a week a visit to each venue is advised.

#### Video Server maintenance

Video Serve is a desktop PC, which is running in MRL for 7/24.

An un-customized iSpy (v4.5.4.0) is running on this PC to record the video streams from 4 onsite IP cameras. In iSpy we can monitor 4 video image windows. Each window connects to an IP camera. By right clicking on the video window, we can do configuration (e.g. set camera address, name, time tag, mirror image, etc), and start/stop recording. The 4 video streams are being recorded in E:\SitwIPCam\_iSpy\video\<Node name>.

Each video file keeps 24-hour period video image. According to agreement, we only keep 7 days video recording. Therefore we need to do cleanup in about every 2 weeks time.

Video Server is also used to record the onscreen actions of each node. All onscreen clicks at each node will be recorded in log files in this format:

Node Name | Date and Time | running app | coordinates of click

These log files are being stored in E:\yl\SitwUsageLog\log\logActions.

Each log file keeps 24-hour period actions.

#### A suggested timetable for checks

It is suggested that you perform the above listed tasks on a daily basis.

## Troubleshooting and problem solving

### How do I disable security features to fault find on a node PC?

#### Secure Lockdown

When Inteset Secure Lockdown is enabled, you will **NOT** be able to browse the web or do anything else, without first disabling lockdown. This requires restarting Windows and will take a few minutes.

As keyboard shortcuts are also disabled, it will not be possible to quickly reload a failed web page.

Some things are still possible in lockdown mode. For example, iSpy’s right-click options are still available BUT it is very difficult to trigger these without a mouse.

What stops users from browsing in Firefox, is the kiosk mode, rather than Secure Lockdown. If a user can break out of kiosk mode (as seems to be possible in Google Presentation slideshows), then it is not totally impossible that they could still browse.

However, even if they manage to close applications down, they can’t start anything new. They will end up with a black desktop, without icons, Task Bar, Start Menu etc.

What Secure Lockdown can do:

* Let only one Master Application start (although this application can start other apps)
* Removes the Windows Taskbar and Start button
* Removes Desktop right-click menu
* Removes Task Manager access
* Removes CTRL-ALT-Delete functions
* Removes System shutdown or logoff
* Removes Windows Ease of Access features
* Removes Windows Help and Support

What Secure Lockdown cannot do:

* Lockdown the features of any program that is started automatically by Windows, or is started by the Master Application that Secure Lockdown starts.
* Prevent the closing of any program, except for the Master Application (and I found that even this isn’t always reliable...ask me for details).

To disable lockdown mode for maintenance or ‘free browsing’ - either onsite with a keyboard or remotely via TeamViewer:

* If you are connecting to a node remotely using TeamViewer, make your connection and then click Actions (on the grey TeamViewer toolbar at the top of the screen) and then tick ‘Send key combinations’ (you will need to do this each time that you connect). You might also need to left-click somewhere in the TeamViewer window, to get focus for the keyboard.
* Press [Alt] + [Shift] + [s] Note: I found in TeamViewer that only the [Shift] key on the right-hand side of the keyboard worked for this!
* In the Secure Lockdown window, enter the password (it should be the same as the Windows user account password for the machine that you are working on).
* Click Apply.
* Untick ‘Disable secure lockdown’.
* Click Apply.
* Click Yes to confirm that you want to disable Secure Lockdown.
* Click OK to restart Windows. You might get an error about closing an application, if so just click OK. Windows will restart. This may take longer than expected. Via TeamViewer you may have to wait up to five minutes before it becomes available to connect again.
* After Windows restarts with lockdown mode disabled (and TeamViewer has reconnected, if you are working remotely), you may see that Firefox and iSpy will automatically start. This is because they automatically start both in lockdown and non-lockdown modes. If you want to make changes, you will need to close this down. As Firefox is in Kiosk mode, you will need to press [F4] to close Firefox (if using TeamViewer, remember to re-enable ‘Send key combinations’ first!).
* Next, close the Scheduler by right-clicking on the Task Bar entry (the yellow Python one, not the console entry) and clicking Close. iSpy should now also shutdown.
* Now you can make your changes!
* If you need to run Firefox not in kiosk mode, hold [Shift] and click (or double-click depending on the location of the icon) on any Firefox icon.
* You will get a window asking if you want to use Firefox Safe Mode.
* Use Firefox! Note: when you are finished, you do not need to re-enable kiosk mode. Just close Firefox and the next time it starts (or is started by the scheduler) it will go back into kiosk mode.

To enable lockdown mode after maintenance or ‘free browsing’ - either onsite with a keyboard or remotely via TeamViewer:

* Click Start and then either click Secure Lockdown (if it is visible on the Start menu) or type “Secure” and then press [Enter] to search for Secure Lockdown.
* You will see a message confirming that Secure Lockdown is running and that you need to press [Alt] + [Shift] + [s] to access it.
* Click OK (?) to dismiss this window.
* Press [Alt] + [Shift] + [s]
* In the Secure Lockdown window, enter the password (it should be the same as the Windows user account password for the machine that you are working on).
* Click Apply.
* Tick ‘Enable secure lockdown’.
* Click Apply.
* Click Yes to confirm that you want to enable Secure Lockdown.
* Click OK to restart Windows.
* Windows will restart. This may take longer than expected. Via TeamViewer you may have to wait up to five minutes before it becomes available to connect again.
* When it restarts, the machine should be in lockdown mode and Firefox and iSpy should automatically start.

#### Firefox Kiosk Mode plugin

R-Kiosk is a Firefox plugin that puts the browser in Kiosk-Mode:

<https://addons.mozilla.org/en-us/firefox/addon/r-kiosk/>

Whereas Secure Lockdown limits what a user can do in Windows, R-Kiosk limits behaviour inside Firefox.

Most keyboard shortcuts are suppressed, but the following will still work:

* Reload current page (inc. refresh cache): press [Ctrl] + [F5]
* Close Firefox: press [Alt] + [F4] (or [Ctrl] + [F4])

If you need manual access to the browser’s address bar and other functions (either on-site or via TeamViewer), you will need to run Firefox in Safe Mode:

Press and hold [Shift] and then click on any Firefox shortcut.

To completely disable R-Kiosk:

Go into Firefox safe mode and then go to Firefox > Addons > Extensions.

Disable is available as an option for R-Kiosk.

### Where do I find the log files?

#### UNION Server logging

Log into the UNION Server VM in Remote Desktop (Computer Science account credentials).

Log files may be found in: C:\union\Union Server\

By default, UNION keeps the last five days’ logs.

The can be modified here:

C:\union\Union Server\lib\log4j.properties

Change this line:

Edit log4j.appender.union.MaxBackupIndex=5

And restart UNION Server.

Reading UNION Server/UPC logs

Identifying individual SiTW nodes in UNION log files:

Broadway: [<removed for security>]

NAE: [<removed for security>]

The Mill: [<removed for security>]

Leytonstone: [<removed for security>]

The remote admin console for UNION server: this is likely to be in the IP range:

[<removed for security>] for example: [<removed for security>]. This is treated as a client by the server, but is only acting as a passive watcher.

Note: Client IDs change on each connection, they do not persist from session to session. Therefore, they are of limited value beyond the scope of each evaluation session.

UNION logging formats:

There are two types of log: Log and UPC Messages.

Both contain the same UPC (Union Procedure Call) message format in XML, but the rest of the formatting differs.

These formats are:

Log format:

<YYYY-MM-DD> <HH:MM:SS>,<ClientID> <LOG LEVEL> - <DESCRIPTION OF EVENT> [<UPC MESSAGE IN XML>]

For example:

2012-10-30 11:31:37,140 DEBUG - Server sending to client [1003] message [<U><M>S2C\_ROOM\_ATTR\_UPDATE(u9)</M><L><A><![CDATA[sitw.music\_1]] ></A><A>1003</A><A><![CDATA[pad\_8]] ></A><A><![CDATA[false]] ></A></L></U>]

UPC Messages format:

Date, Time, Client ID, User ID (only if using user accounts), Address (this is IP address), Queue Duration (ms), Processing Duration (ms), UPC (this is the UPC message)

For example:

10/24/12 19:26:52 UTC+1, 703, , [<removed for security>], 0, 0, <U><M>u5</M><L><A>sitw.music\_1</A><A>pad\_13</A><A>true</A><A>4</A></L></U>

The Union Procedure Call Protocol Specification:

UPC messages represent different events between the UNION server and its client.

<http://unionplatform.com/specs/upc/>

Look at the Native UPC Messages in Tables 1 and 2.

The Internal Message ID column corresponds to the u numbers in the log.

For example, here is a u159 message from the log:

10/24/12 18:30:04 UTC+1, 691, , [<removed for security>], 16, 125, <U><M>u159</M><L></L></U>

In Table 1, you will see that u159 is described as:

WATCH\_FOR\_PROCESSED\_UPCS

"Asks the server to notify the sending client upon processing any UPC message. The server sends the result of the request via a u160. Notifications are transmitted via u161. By default, u159 requires administrator privileges."

The most relevant UPC messages to SiTW experiences (summary):

Summary of relevant UPC message (for current SiTW experiences, such as SoundShape):

u4 JOIN\_ROOM

u6 JOINED\_ROOM

u54 ROOM\_SNAPSHOT

u37 CLIENT\_REMOVED

u131 ROOM\_OCCUPANTCOUNT\_UPDATE

u5 SET\_ROOM\_ATTR

u9 ROOM\_ATTR\_UPDATE

u74 SET\_ROOM\_ATTR\_RESULT

Not used in SoundShape, but sometimes relevant to SitW experiences:

u3 SET\_CLIENT\_ATTR

u8 CLIENT\_ATTR\_UPDATE

u73 SET\_CLIENT\_ATTR\_RESULT

The most relevant UPC messages to SiTW experiences (detail and examples):

Client joining the experience

Client to Server (a request): u4 JOIN\_ROOM

Server to Client (a confirmation): u6 JOINED\_ROOM

Server to Client (to enable persistence of state): u54 ROOM\_SNAPSHOT

Server to Clients (updating all Clients that a Client has joined or left): u131 ROOM\_OCCUPANTCOUNT\_UPDATE

A client requesting to join the experience:

This was Leytonstone contacting the server and requesting to join SoundShape-

10/24/12 19:14:14 UTC+1, 701, , [<removed for security>], 0, 47, <U><M>u4</M><L><A>sitw.music\_1</A></L></U>

It is a u4 message, which means JOIN\_ROOM (a room is an experience, in sitw terms!).

sitw.music\_1 is SoundShape. Remember that SoundShape reloads every 15 minutes (to prevent network problems from leaving a failed web page on screen). So, this doesn't mean that Leytonstone wasn't in SoundShape before 19:14.

Server informing that number of clients in experience has changed:

<U><M>S2C\_ROOM\_OCCUPANTCOUNT\_UPDATE(u131)</M><L><A><![CDATA[sitw.music\_1]] ></A><A>1</A></L></U>

Server confirming that a client has joined the experience:

<U><M>S2C\_JOINED\_ROOM(u6)</M><L><A><![CDATA[sitw.music\_1]] ></A></L></U>

A new client getting an update on the status of all SoundShape pads:

<U><M>S2C\_ROOM\_SNAPSHOT(u54)</M><L><A></A><A><![CDATA[sitw.music\_1]] ></A><A>1</A><A>0</A><A>pad\_19|false|pad\_18|true|pad\_17|true|pad\_16|false|pad\_15|true|pad\_14|true|pad\_13|true|\_MAX\_CLIENTS|-1|pad\_12|true|pad\_11|true|pad\_10|false|pad\_8|true|pad\_9|false|pad\_23|false|pad\_22|true|pad\_25|false|pad\_24|false|pad\_7|false|pad\_6|false|pad\_21|false|pad\_5|false|pad\_20|true|pad\_4|true|pad\_3|false|pad\_2|false|pad\_1|true</A><A>1001</A><A></A><A>0</A><A><![CDATA[\_ROLES|0|68|\_CT|1351596319934|36]] ></A><A><![CDATA[]] ></A></L></U>

Client leaving the experience

Note: Clients don't normally request to leave, they just disappear.

u37 CLIENT\_REMOVED

Updating all Clients that a Client has joined or left:

Server to Clients: u131 ROOM\_OCCUPANTCOUNT\_UPDATE

Example:

2012-10-31 09:14:55,554 DEBUG - Server sending to client [1071] message [<U><M>S2C\_CLIENT\_REMOVED(u37)</M><L><A><![CDATA[sitw.music\_1]] ></A><A>1072</A></L></U>]

One Client changing something in an experience (in the case of SoundShape, this is pressing pads)

Client to Server (a request): u5 SET\_ROOM\_ATTR

Server to All Clients (a confirmation): u9 ROOM\_ATTR\_UPDATE u9

Server to Originating Client (a confirmation): u74 SET\_ROOM\_ATTR\_RESULT

A music pad is turned on (sounding and flashing):

This uses UPC message u5 - SET\_ROOM\_ATTR - "Asks the server to set a room attribute for the specified room."

Steve explains: the UNION server retains the state of each music pad, whether it is true (playing) or false (off). When a new client (screen node) connects to the UNION server, it can then get an immediate update on the status of all music pads. Without this, the screen pads could all be in different states, depending on when the node logged into the experience.

This is someone at The Mill touching and turning on pad 13 -

10/24/12 19:26:52 UTC+1, 703, , [<removed for security>], 0, 0, <U><M>u5</M><L><A>sitw.music\_1</A><A>pad\_13</A><A>true</A><A>4</A></L></U>

There are 25 pads arranged in a 5x5 grid. As pads are numbered from columns (left to right) and then from rows (top to bottom), pad 13 is the third pad from the left on the third row down.

A music pad is turned off (not sounding or flashing):

This is someone at The Mill touching and turning off pad 23 -

10/24/12 19:26:40 UTC+1, 703, , [<removed for security>], 0, 0, <U><M>u5</M><L><A>sitw.music\_1</A><A>pad\_23</A><A>false</A><A>4</A></L></U>

There are 25 pads arranged in a 5x5 grid. As pads are numbered from columns (left to right) and then from rows (top to bottom), pad 23 is the third pad from the bottom right.

The Server checking clients are still connected

Approximately every 5 seconds.

Server to Client (a request - tell me if you're still there!): u3 \_PING

Client to Server (a confirmation - I'm here!): u2 CLIENT\_HEARTBEAT

This is the Server asking Broadway Cinema if it’s still there:

10/24/12 19:26:47 UTC+1, 702, , [<removed for security>], 0, 0, <U><M>u3</M><L><A>702</A><A></A><A>\_PING</A><A>14</A><A></A><A>0</A><A>false</A></L></U>

This is Broadway Cinema confirming to the Server that it’s still there:

0/24/12 19:26:57 UTC+1, 702, , [<removed for security>], 0, 0, <U><M>u2</M><L><A>CLIENT\_HEARTBEAT</A><A>702</A><A></A><A>67</A></L></U>

#### SitW Client logging

For monitoring system behavior and for debugging purpose, important events at each node are being recorded locally into log files. Generally the log includes information below:

Date and time

System start up / shutdown / restart

System initialization

App start up and parameters

Onscreen mouse action

Enter / Quit attractor mode

Error messages

For example:

*2014-03-15 11:30:39 ------------ SitW Scheduler v9.0 ------------*

*2014-03-15 11:30:39 ////////////////////*

*2014-03-15 11:30:39 \*\*\*\*\*\* NAE(NA) \*\*\*\*\*\**

*2014-03-15 11:30:39 ////////////////////*

*2014-03-15 11:30:39 \*\*\*\*\*\* Web Schedule Mode \*\*\*\*\*\**

*2014-03-15 11:30:39 \*\*\*\*\*\* Day Schedule Changed \*\*\*\*\*\**

*2014-03-15 11:30:40 Run Program 9 - ['1130', 'app\_ispy', '', '', '', 'attractoron', '', '', '', '']*

*2014-03-15 11:30:40 (((((( Mouse click @ (20, 20) ))))))*

*2014-03-15 11:30:41 (((((( Mouse click @ (460, 1062) ))))))*

*2014-03-15 11:30:45 (((((( Mouse click @ (451, 1066) ))))))*

*2014-03-15 11:30:46 (((((( Mouse click @ (1113, 494) ))))))*

*2014-03-15 11:31:47 <<< Enter ATTRACTOR Mode >>>*

*2014-03-15 11:31:55 <<< Quit ATTRACTOR Mode >>>*

*2014-03-15 11:32:02 ------------ Quit Scheduler ------------*

Log files are being stored into

NAE and Broadway - D:\yl\SitwScheduler\log\logEvent

Leytonstone and Mill - C:\yl\SitwScheduler\log\logEvent

Each log file keeps 24-hour period information.

### Known issues and solutions

#### Windows User account corruption at The Mill and how to recover

Symptoms:

* Unable to reach The Mill in TeamViewer.
* No IPcam stream from The Mill.
* When you connect with Remote Desktop, you see a version of the Windows user account which appears not to have any of our applications (iSpy, YawCam, Firefox, TeamViewer, scheduler: all missing). It looks like a brand new user account.

Solution 1: in Remote Desktop, press [CTRL]+[ALT]+[END].

Click LogOff and Remote Desktop shuts down.

Now, try connecting with TeamViewer, you should be back in the correct version of the user account.

Note: after using Remote Desktop, the iSpy panel is always in the wrong position. Run the OLD\_isy.exe version in c:\program files\ispy\ispy to reposition the panel and then close it.

Run the scheduler and ispy should now be in the correct position

Solution 2: use System Restore and restore back to last know good restore point: this works, but you might lose any changes made since the last restore point.

#### How to manually close the iSpy video panel (grey frame)

Right-click on the grey strip at the right-hand edge of iSpy and then click Exit.

#### How fix iSpy when the stream from the local USB camera (via YawCam) has frozen

Is it necessary to disable Inteset Secure Lockdown to do this? NO

Is it necessary to reboot Windows from TeamViewer (with Secure Lockdown left enabled)? YES

This happens when YawCam continues to stream a single frame, without updating from the USB camera. It happens occasionally, after the system has been running for several days.

Using Team Viewer, it can be fixed by rebooting the computer, without disabling Secure Lockdown. If you are at a node and can’t use TeamViewer, then you WILL need to disable Secure Lockdown, as reboot is not possible.

If you are connecting to a node remotely using TeamViewer, make your connection and then click Actions (on the grey TeamViewer toolbar at the top of the screen) and then click Remote Reboot > Reboot.

If prompted by TeamViewer if you want to wait for partner to reconnect, say yes.

When Windows restarts, YawCam should be streaming correctly

#### Keyboard shortcuts for closing crashed Firefox kiosk mode browser windows.

Press [Alt] + [F4] (or [Ctrl] + [F4]).

### What can I do if a screen node is unreachable via TeamViewer?

#### Node PC recovery via Windows Remote Desktop

Using Windows remote Desktop, connect to the Node PC, using the appropriate Windows account.

#### Contacting a venue to request manual reboot of a node PC

<TO DO: basic training for venue staff?>

#### Where do I find important configuration settings?

##### SitW Client

###### SitwScheduler.ini

NAE and Broadway - D:\yl\SitwScheduler\cfg\SitwScheduler.ini

Leytonstone and Mill - C:\yl\SitwScheduler\cfg\SitwScheduler.ini

##### iSpy video panel

###### iSpy video stream configuration

Stream data can be found here on each node:

C:\Users\<user name>\AppData\Roaming\iSpy\XML\config.xml

##### UNION Server

Most of the configuration files can be found on [<removed for security>] at: C:\union\Union Server\lib\

##### Touch Foil configuration and calibration

More information about Touch Foil device driver and user guide can be downloaded from:

<http://www.visualplanet.biz/support/download.php>

It is using driver MA7 at Broadway and driver MA9 at Leytonstone and the Mill.

Here we use driver version MA7 as a sample:

* Starting the Driver Control Program

To start the driver, double click on the shortcut MA7\_Control on the desktop

* Configuring USB Communications

Select the Comms tab

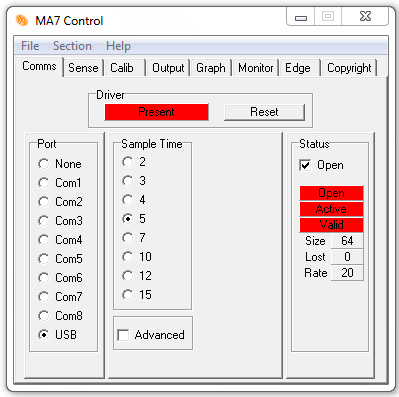
Connect to a free USB port

Select USB option in the PORT section

Tick the Open box in the Status section

Make sure the driver box called Present is red indicating that the driver has loaded When the driver recognizes the touchfoil, the Open, Active and Valid boxes will go red

Sample time adjustment is used to set the touchfoil to work through different thickness of material, for example, sample time of 15 is the highest thickness setting. The default value of 5 should enable the touchfoil to work through glass between 4-12mm thick



* Calibration

Select the Calib tab

Click with the mouse the Start Calibration box

You will see the following on the screen; three targets will appear in turn like the one shown above:

Touch and hold your finger on the centre of each target. Remove your finger only when the next target appears

If the touch calibration is not correct after this procedure, please run the process again and adjust your finger position on the targets to compensate for any misalignment

|  |  |
| --- | --- |
| Untitled-1.jpg | Untitled-1.jpg |

* Adjusting the Touch Sensitivity Level

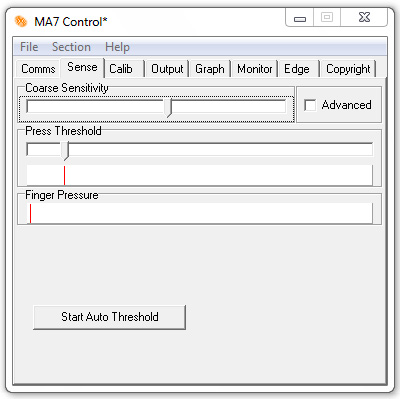
Select the Sense tab:

First set the coarse sensitivity bar to approximately 50% by dragging the bar with your mouse

Set the Press Threshold level so the background movement of the Finger Pressure moving red bar does not go beyond the press threshold level, by dragging the bar with your mouse (it will not move fully to the left hand side)

Touch the screen to see if the Finger Pressure red bar goes above the Press Threshold level. This action creates a touch

If the Finger Pressure bar does not go above the Press Threshold level when you touch the screen then increase coarse sensitivity in small increments only until the Finger Pressure red bar goes above the Press Threshold level

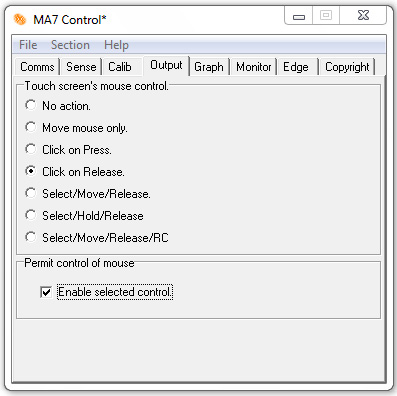


* Setting the Touch Output to suit the Application Requirements

Select the output tab

Select the required mouse control for your application - Click on Release

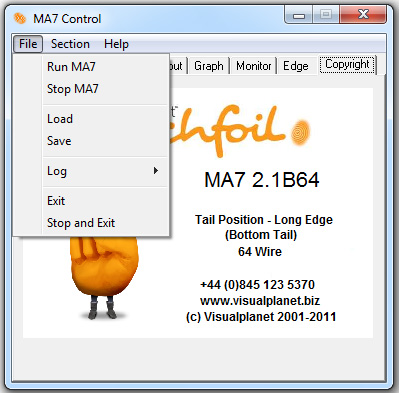
To enable the touch function on the screen check the Enable selected control box



* Saving the Configuration Settings

Select File

Click on Save to save the current settings



##### Phidgets Interface configuration and calibration

Phidgets Interface is used at NAE, where the Touch Foil does not work. Phidgets interface is composed by 5 light sensors and a controller board. It works as a key-pad to control the cursor on the screen.

|  |  |
| --- | --- |
| LightKeypad_2.jpg | Key1+2_v2.jpg |

Phidgets device driver can be downloaded from:

<http://www.phidgets.com/docs/Operating_System_Support>

* Attach Phidgets Interface on the shop window beside the screen and facing outward
* Install Phidgets driver on PC
* Connect USB cable from Phidgets Interface to a free USB port on PC
* Start Phidgets Interface software at D:\yl\SitwPhidgetsKey\run.bat

Phidgets Interface has been well tuned to get best performance. In case users need to customize its behavior, there is a configuration file locates at

D:\yl\SitwPhidgetsKey\cfg\SitwPhidgetsKey.ini

Parameters and current settings:

Sensitivity = 0.70

- Value range from 0 to 1. Higher value gets higher sensitivity

MovingPace = 7

- Cursor moving pace

SampleInterval\_Key = 50

- Sampling interval for checking key press (in milli second)

SampleInterval\_Env = 10000

- Sampling interval for checking environment brightness (in milli second)

Log\_Action = Yes

- Turn on/off action log

Log\_Brightness = Yes

- Turn on/off brightness sensors reading log

#### LAN and WAN configuration for nodes (router, IP addresses, port forwarding)

##### Port Forwarding summary for a node

The port configuration on a node should be similar to this, where xx.xx.xx.xx is the static public IP address of the router:

* Port 3389 forwarded to the node PC for Remote Desktop, for connection to it at:
  + xx.xx.xx.xx
* Port 81 forwarded to the IPcam, so that it can be reached externally on:
  + http://<ipcam user>:<ipcam pass>@xx.xx.xx.xx :81/videostream.cgi
* Port 82 forwarded to the Yawcam application on our PC so that it can be reached externally on:
  + http://xx.xx.xx.xx :82/video.mjpg?q=30&fps=33&id=0.5
* Note: The Mill is configured to port 83, as 82 seemed to be reserved for something else.
* Port 7142 forwarded to the screen's local IP address (should be on it’s default 192.168.0.10). So that the screen can be reached using the PC Control Utility PD1.

Note:

If you are accessing the screens network (for video recording, screen remote control, RDP administration etc) from behind a firewall, you may also have to open the following ports on any machines being used:

IP Camera Access (81), YawCam video stream (82,83), Remote Desktop Protocol (3389) and NEC PC Control Utility PD1 (7142)

##### Testing Correct Port Forwarding with the NetCat tool

You can test a node to check the required ports are open.

NetCat is a great tool for this.

Search for the Windows version (nc111nt.zip) or try:

<https://yesanshare.googlecode.com/files/nc111nt.zip>

Best instructions:

<http://www.catonmat.net/blog/unix-utilities-netcat/>

Using Command Prompt (from the same directory as NetCat):

Node static public IPs:

Broadway: [<removed for security>]

NAE: [<removed for security>]

The Mill [<removed for security>]

Leytonstone: [<removed for security>]

Testing for NEC Utility port:

nc -v -n -z -w 1 <node static public IP> 7142

Pass:

(UNKNOWN) [<node static public IP>] 7142 (?) open

Fail:

(UNKNOWN) [<node static public IP>] 7142 (?): TIMEDOUT

Testing for IPcam port:

nc -v -n -z -w 1 <node static public IP> 81

Pass:

(UNKNOWN) [<node static public IP>] 81 (?) open

Fail:

(UNKNOWN) [<node static public IP>] 81 (?): TIMEDOUT

Testing for Remote Desktop port:

nc -v -n -z -w 1 <node static public IP> 3389

Pass:

(UNKNOWN) [<node static public IP>] 3389 (?) open

Fail:

(UNKNOWN) [<node static public IP>] 3389 (?): TIMEDOUT

And ports 82 and 83 for YawCam video streams.

#### Node PC configuration

##### List of software to install on a new node PC

* Firefox
* Chrome
* Java 7
* Adobe Flash Player
* Adobe Shockwave Player
* Python & Tools

Python: python-2.7.3.msi

wxPython: wxPython2.9-win32-2.9.4.0-py27.exe

NumPy: numpy-1.6.1-win32-superpack-python2.7.exe

SciPy: scipy-0.9.0-win32-superpack-python2.7.exe

Win32API: pywin32-217.win32-py2.7.exe

* TeamViewer Host v7.0.57223 (doesn’t need licence for host, only connecting client) - NOTE: versions of host above v7 (v8+) may not work with our licence clients! Get it here: <http://www.cs.nott.ac.uk/sitw/software/TeamViewer_Host_7_0_57223_THIS_IS_THE_ONE_FOR_OUR_LICENCES.exe>
* TouchFoil driver (if using TouchFoil) – MA7 / MA9
* NEC PC Control Utility PD 1 (if using NEC screen)
* SiTW Client
* Phidgets mouse driver thingy (if required for non-touch foil location)
* iSpy (SiTW custom build)
* Inteset Secure Lockdown v2 - product key: [<removed for security>]
* R-Kiosk (Firefox addon): <https://addons.mozilla.org/en-us/firefox/addon/r-kiosk/>
* YawCam
* Winrar

##### Firefox configuration (plugin updates disabled etc)

Disable Firefox plugin update reminder:

At the Firefox address line, type: about:config and press [Enter].

Search for: plugins.update

set: plugins.update.notifyUser = false

Disable Firefox plugin deactivated warning:

Seems to prevent this:

"Some plugins have been deactivated for your safety"

At the Firefox address line, type: about:config and press [Enter].

Search for: extensions.blocklist.enabled

set: extensions.blocklist.enabled = false

Disable auto update in FireFox:

Click Tools > Options > Advanced > Update tab

Click "Never check for updates"

Untick: "Use a background service to install updates"

Hide the FireFox plugins infobar (warning about plugins being out of date):

Type - "about:config" into the address bar of the browser, confirm the info dialog, then search for the preference named "plugins.hide\_infobar\_for\_outdated\_plugin" & double-click it in order to toggle it to "true".

##### Windows configuration (resolution, update disabled, pop-ups etc)

Windows resolution:

Set to: 1360 x 768

Flash Player:

Go to Start > Control Panel.

Disable Flash Player automatic updates

Java:

Go to Start > Control Panel.

Disable Java automatic updates

QuickTime:

Go to Start > Control Panel.

Disable Quicktime automatic updates (if it’s installed)

Windows update:

Go to Start and search for Windows Update.

Disable Windows Update’s automatic update features.

Instructions for installing SSL certificate in Chrome to allow camera access:

Certificate is here zipped: [<removed for security>]

1) Copy the unzipped certificate (pdnet.inf.unisi.ch.cer) somewhere on the machine (e.g., desktop).

2) Open Chrome and go to the Settings panel.

3) In the Settings panel click on "Show advanced settings" and scroll to the "HTTPS/SSL Manage certificates". Click and open the "Manage certificates" option.

4) This will open the "Certificates" window. In this window go to the "Trusted Root Certification Authorities" tab and click on the "Import" Button.

Password is the same as the username, i.e.,

password: screensinthewild

Set home pages for Firefox and Chrome.

TeamViewer > options:

Security >

Random password (for spontaneous access) - Disabled (no random password)

Advanced > Advanced settings for connections to this computer

Tick: Automatically minimise local TeamViewer Panel

Note: this is not actually set at Broadway...so maybe not necessary?

Windows power options

Turn the display off: Never

Put the computer to sleep: Never

##### Yawcam configuration

Tested with version 0.3.8 not latest version...

Settings > Output > Stream

Port: 82

Stream type: MJPEG

Scale to: 320 x 240

Image quality: 30%

Additional settings

Maximum connections: 10

ImageProducer rate: 10fps

Settings > Startup

Tick Start Stream ouput

Tick Hide to traybar at start

Untick Check for new versions

Untick Show preview

Untick all others

|  |  |
| --- | --- |
| Untitled-1.jpg | Untitled-2.jpg |

#### Node hardware configuration

##### Enable/disable audio system

###### Schedule audio mute and unmute in Windows 7

How to automatically mute/unmute Windows 7 audio at scheduled times:

* Download nircmd from: <http://www.nirsoft.net/utils/nircmd.html>
* Unzip and run (as admin): nircmd.exe
* Confirm copy into Windows dir.
* Test that Windows 7 can mute and unmute, from Command Line:
  + Mute:
  + nircmd.exe mutesysvolume 1
  + Unmute:
  + nircmd.exe mutesysvolume 0
  + First...to schedule Mute in (WIndows) Task Scheduler:
* Start Task Scheduler by clicking Start and then typing “Task Scheduler”.
* Click Action > Create Task. Note: NOT basic task.
* Under General Tab, add name...”Mute Audio”
* Under Triggers Tab, click New.
* Set the drop down menu Begin the Task to “On a schedule”.
* Set to Weekly and tick: Monday, Tuesday, Wednesday, Thursday, Friday (for weekdays only)
* Click OK.
* Under Actions Tab, click New.
* Set to Start a Program.
* Under Program/Script enter: nircmd.exe
* Under Add arguments (optional) enter: mutesysvolume 1
* Click OK > OK
* Now...to schedule Unmute in (WIndows) Task Scheduler:
* Click Action > Create Task.
* Repeat above...using mutesysvolume 0 for the program argument

##### Maintenance of Foscam IP cameras

A Foscam IP camera is installed at each node. It can be accessed remotely by a web browser.

NAE: http:// [<removed for security>]:81

Name: [<removed for security>]

Password: <REMOVED FOR SECURITY>

Name: [<removed for security>]

Password: [<removed for security>]

Broadway: http:// [<removed for security>]:81

Name: [<removed for security>]

Password: <REMOVED FOR SECURITY>

Name: [<removed for security>]

Password: [<removed for security>]

Leytonstone: http://81.149.250.182:81

Name: [<removed for security>]

Password: <REMOVED FOR SECURITY>

Name: [<removed for security>]

Password: [<removed for security>]

Mill: http:// [<removed for security>]:81

Name: [<removed for security>]

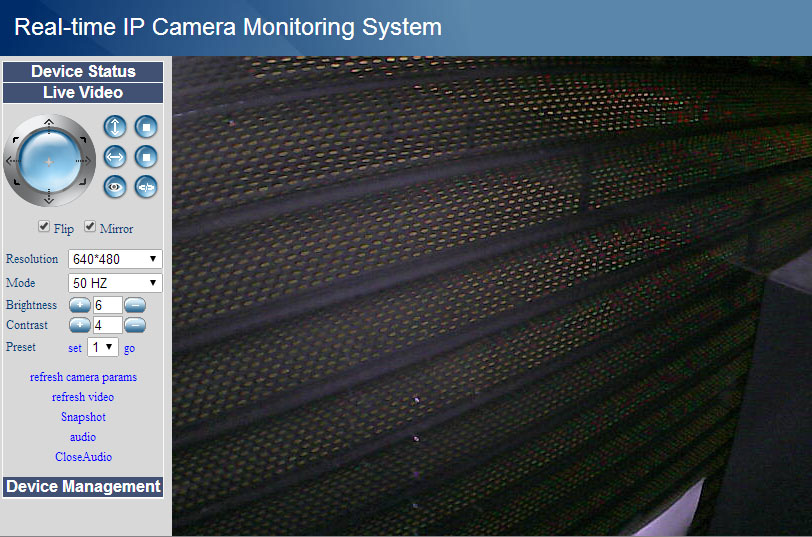
Password: <REMOVED FOR SECURITY>

Name: [<removed for security>]

Password: [<removed for security>]

Please note port number 81 must be forwarded to IP camera at each local network system. This can be done by configuring the port forwarding settings in local network router.

After you log into the IP camera control panel successfully, you may control the viewing angle, resolution, brightness and many other options. More details can be found from <http://foscam.co.uk/>. IP Camera model is Foscam FI8918W Wireless.



#### UNION Server configuration

##### How to setup UNION Server as a Windows Service - will run without a user logged in

Download Windows Server 2003 Resource Kit Tools from here:

<http://www.microsoft.com/en-us/download/details.aspx?id=17657>

The only components required from this are the tools for creating a Windows service:

srvany.exe

instsrv.exe

These can also be found here for future use:

<https://www.dropbox.com/sh/223ejh5ule4xiyh/2_5SSOq2cZ>

* On the VM, put srvany.exe and instsrv.exe into a new folder: c:\rktools\
* Open Command Prompt in C:\union\Union Server\
* In Command Prompt, run: c:\rktools\instsrv "startserver" "c:\rktools\srvany.exe"
* Open the Windows Services Management Console: Start > Control Panel > Administrative Tools > Services.
* Find the new service "startserver".
* Right-click on startserver and then click Properties.
* On the General tab, set "Startup type" = Automatic (Set to "Manual" for manual startup)
* On the Log On tab: select the "Local System account" radio button. Also tick the "Allow Service to Interact with the desktop" tick box.
* Leave the Windows Services Management Console open.
* Go to the Registry Editor: Start > Run > type: regedit and press [Enter].
* Add a new registry key:
  + HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\startserver
* Add another new key inside the previous, so that you have:
  + HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\startserver\Parameters
* Inside HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\startserver\Parameters, create two new string values:
  + Name: AppDirectory Type: REG\_SZ Value: C:\union\Union Server\
  + Name: Application Type: REG\_SZ Value: C:\union\Union Server\startserver.bat
* Back in the Windows Services Management Console, right-click on startserver in the services list and then click Start.

This should have now worked with a standard .exe, but there is a further problem with a Java application, such as UNION Server.

By default, Java apps stop working when a user logs out.

See:

<http://superuser.com/questions/374147/java-services-stop-working-when-user-logs-out>

UNION Server’s original start command in C:\union\Union Server\startserver.bat is:

java -Dfile.encoding=UTF-8 -cp lib\union.jar;lib\stax-api-1.0.1.jar;lib\wstx-asl-3.2.6.jar net.user1.union.core.UnionMain start

Change this to:

java -Xrs -Dfile.encoding=UTF-8 -cp lib\union.jar;lib\stax-api-1.0.1.jar;lib\wstx-asl-3.2.6.jar net.user1.union.core.UnionMain start

The -Xrs flag stops the JVM from terminating on Windows user log off.

## Important Configuration Summary (IP addresses, video stream URLs, Windows accounts, port forwarding etc)

[<removed for security>]