



This section of the manual gives a basic introduction to AB Tutor, and describes some of the concepts, such as network layout and passwords.

- [AB Tutor manual](#)
- **Introduction**
 - [What is AB Tutor?](#)
 - [Basic ABT setup](#)
 - [Advanced setup options](#)
 - [Introduction to passwords](#)
 - [Startup passwords](#)
 - [Connection password](#)
 - [Startup switches](#)

Introduction

What is AB Tutor?

AB Tutor is a networked classroom, instruction, monitoring and teaching tool that lets you train students in a networked classroom or lab, simply, effectively, at a very affordable price. Teachers, trainers and administrators can use the software to easily control, manage, monitor and support their students.

This is a list of the key features of AB Tutor

Cross platform

- Windows central server
- Windows and Mac tutor applications
- Windows and Mac client applications

Computer Monitoring

- Real-time remote screen watch
- Simultaneous watch by multiple tutors
- Network efficient sizeable thumbnail views, with changeable refresh times
- Create different thumbnail arrangements for each group
- Monitor running applications and files
- Identify what site/file the student is working on
- Monitor and log student activity (applications, printing, websites and keystrokes)
- Take time and name-stamped snapshots of student activity
- Record and play back student screen activity
- Live search for users/computers
- Monitor multiple class groups simultaneously

Keyword Notification

- Inform tutor when specific keywords are typed
- Automatically take snapshots of violations
- Trigger remote screen recording upon violation
- View and export all violations with screenshots, user details and context
- All event details held on central server for ease of access

Internet Monitoring and Control/E Safety

- Block ports to prevent any internet activity
- Blacklist or whitelist specified sites
- Filter by keyword/wildcard
- Notify tutor when student visits specified sites

Remote Administration Tools

- Detailed inventory of remote hardware/software
- View and manage remote services and processes
- Administer remote machines via command prompt
- Automated remote client and tutor updates

Remote Control

- Take over remote mouse and keyboard
- Share control of applications with student
- Launch and close down applications remotely
- Automatically launch websites or open files remotely
- Set policy to immediately prevent application from running
- Lock remote computer's keyboard and mouse
- Create customised lock screen messages (eg for lesson plans)

Broadcast and share

- Broadcast tutor screen to students with audio
- Show static, locked, screen to students
- Show a student's screen to others with audio
- Select screen area to broadcast

Classroom Management

- Power up remote machines, manually or on schedule
- Remote logon
- Remote logoff and shutdown
- Schedule shutdown
- Block printing
- Auto-connect to computers
- Auto-connect when connection lost
- Create defined classroom groups of computers and/or users
- Automatically apply different policies to different groups of users
- Sync computers and users from active directory
- Only allow tutors to connect to pre-set groups
- Distribute and collect files from student machines
- Remote file management
- Lock screen if network cable unplugged
- Allow clients to join groups
- Battery status shown on tutor
- Traffic light help system

Application control

- Blacklist or whitelist specific applications
- Launch applications remotely
- Close down inappropriate applications

Communication

- One-to-one and one-to-many text chat
- One-to-one and one-to-many audio chat
- Broadcast text messages

Polling and Assessment

- Create + distribute single-question polls to remote computers
- Results of poll collected in real-time
- Run tests with multiple choice questions
- Export results for further analysis

Optional privacy setting

- Inform users when AB Tutor is running
- Let users know when they are being watched
- Allow user to block remote viewing/control

Licensing Options

- Choose perpetual or subscription licensing
- Option to purchase a site licence to make management of licences simple and remove worry of running out

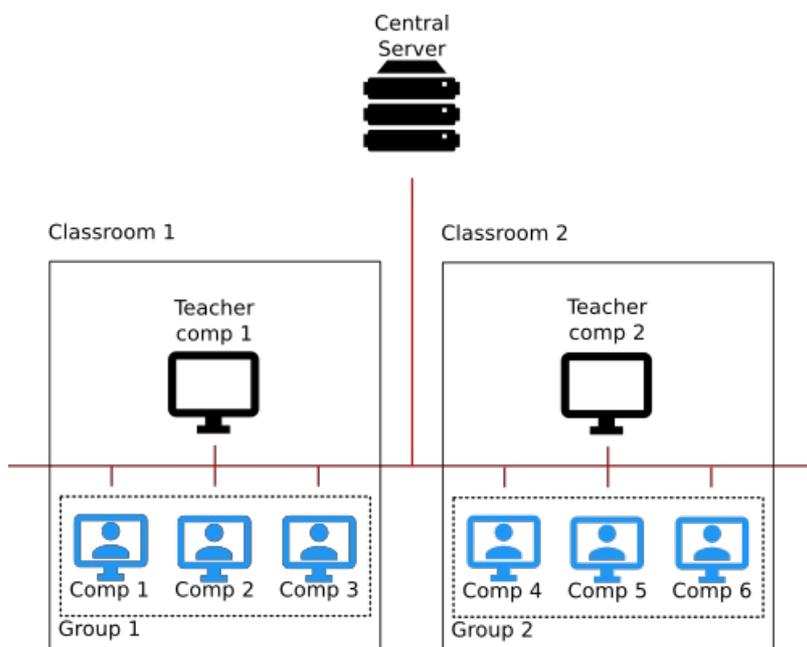
Introduction

Basic Setup

With version 9, AB Tutor works on a central server model, meaning that the Clients and Consoles all connect to the Central Server, which manages all the settings including users, policies, user interface settings and groups.

Groups are configured on the Console and can contain either computers or users. The simple way to set up AB Tutor involves treating the classrooms as separate units, with a single teacher computer at the front, and a number of clients around the room. This level of setup is ideal when all the computers are fixed, and there are a limited number of classrooms with computers in them.

With this setup, any teacher can go into either classroom, log on to the teacher machine in that room and see the clients in the room.



Installation

- Install the AB Tutor Central Server onto a server on your site.
- Download the AB Tutor installer from the Central Server Web Interface.
- Either add a DNS entry for 'abcs' or create a modified msi using the tool from the Central Server Web Interface.
- Use your msi to install your Consoles and Clients. This can be done through Group Policy Software Deployment.
- Approve the clients in the web interface.

Configuration

- Create users, either manually or by syncing with Active Directory. Assign roles to the users.
- Launch the AB Tutor Console on any machine. Log in as a user with the Console Administrator role.
- Create the groups for your classrooms. These can be made by dragging computers from All Items onto All Groups to create the group directly, or by right clicking on All Groups, selecting New device Group and then setting up AD sync on the server.
- Set the group permissions to allow any teachers who use that classroom access to this group. Alternatively, leave it blank to allow access to all users.

Advanced options

More advanced AB Tutor setups may contain additional features:

- **Groups of users** - A group of users allows certain users to be seen no matter what computers they log in on.
- **Default policies** - Policies can be applied to all items and groups which will always affect any items in those categories.
- **String Match groups** - Groups can be created to match usernames or hostnames by string matching, rather than against entries which have been registered on the server.

For more information on any of these steps, see Installation and Creating Groups.

Passwords

⚠️ AB Tutor provides powerful remote monitoring and control functionality. You must therefore take steps to secure your installations of the tutor and client software and prevent un-authorised users from misuse of the system.

There are three types of passwords associated with AB Tutor that protect your security in different ways. These are your website logon password, the user credentials and dynamic group passphrases.

Website Logon Password

Your website username (email address) and password are used to access [your account](#) on www.abtutor.com, allowing you to manage your licences/installations, download the software, get support etc. They can also be used to register your installs of AB Tutor by entering them into the server registration dialogue. This will automatically fetch your licence details from our servers and register the software.

User Credentials

The [user credentials](#) are used to control what level of access the user has and what groups they can open. Users with the **Console Administrator** role have full access, including to "all items" and configuration settings. Users with **Console User** but not **Console Administrator** are restricted to controlling the client machines in specific groups.

Dynamic Group Passphrase

The [Dynamic Groups passphrase](#) is set by a teacher when they create a dynamic group, and used by students who wish to connect to that teacher's group. This passphrase is optional, however it is useful to prevent students joining groups they shouldn't.

Security

Startup Passwords and Levels of Access

There are various levels of access users can be given in AB Tutor:

- **Client User** - This is a user who is to be controlled by AB Tutor. If a user is to be added to a User Group, they need to be added in the web interface first. This role would typically be given to students.
- **Console User** - This gives the user access to run the AB Tutor Console and take control of Client machines. If this access is given, there are additional options available:
 - **Console Administrator** - This role gives the user access to **All Items** and allows them to create groups and configure the Console. This role automatically includes all the other Console User Roles.
 - **Policy User** - This role allows the user to apply policies to groups, clients, users and devices.
 - **Policy Creator** - This role allows the user to create policies, however they will not be able to create shared policies unless they are a Console Administrator.
 - **Private Group Creator** - This role allows the user to create their own private groups from the devices registered on the server. It is intended for use where the setup makes it impractical for the Administrators to create all the required groups.
 - **Dynamic Group Creator** - This role allows the user to create and use Dynamic Groups.
- **Web Administrator** - This role allows the user to log in to the web interface to register users and devices, and to configure the server.

The Administrator access level allows a network manager to control how the Tutor program connects to other workstations through its settings, group management and policy management tools. It also allows an administrator to restrict Tutor level access to pre-set groups and to limit the functions that are available to tutors connecting to those groups. The Administrator has access to some very powerful features and should therefore be limited to users with sufficient technical and networking expertise.

Normal level access controls which users have access to which groups and features, as set by the administrator. Someone with normal user access cannot get to any of the configuration options within the system and cannot connect to workstations outside the classroom groups created by the administrator and assigned to them.

User role permissions

The following table gives an overview of the rights of the Administrator and Tutor.

Feature	User	Admin
Connect to computers within a pre-defined group	✓	✓
List view	?	✓
Icon view	?	✓
Assessments menu	?	✓
Events and log viewer	?	✓
Administrative tools	✗	✓
Connect to All Items	✗	✓
Remote watch and control	?	✓
Send key sequences	?	✓
Demo	?	✓
Chat	?	✓
Audio chat	?	✓
Launch and close programs	?	✓
Create policies	Policy creator	✓
Create shared policies	✗	✓
Apply and remove existing policies	Policy user	✓
Lock/unlock remote machines	?	✓
Logon/logoff/power on/shutdown/reboot remote machines	?	✓
Send/collect files	?	✓
Customise toolbar and context panel	✓	✓
Customise toolbar and context panel defaults/overrides	✗	✓
Groups - set up and manage groups and classrooms	Priv grp Creator	✓
Tutor Console settings	✗	✓
Purge log entries	✗	✓

? All those functions marked with a question mark can be disabled by an administrator, so might therefore not be available to everyone logged in as a tutor. (See [Group Restrictions](#))

Introduction

AB Tutor glossary

An AB Tutor installation involves some understanding of networks and hence a number of technical terms are used in this manual. In this section, you can find simplified descriptions of many of these terms.

AB Tutor terms

AB Tutor components and roles	
Central Server	The Central Server is a component of AB Tutor which is installed on a server on your site. This component manages the entire install, passing data between the Clients and Consoles and holding the settings, logs, policies and so on. The Central Server can be managed through the Web Interface.
Console	The Console is the component of AB Tutor which is used to control the Clients. It has a graphical interface to allow teachers to see the students' computers and allows them to create and apply policies, send actions and view events.
Client	The Client is the component of AB Tutor which allows computers to be controlled. It installs almost invisibly on machines and, via the Central Server, allows the Console User to control the Client computer.
Central Server Web Interface	This interface allows Web Admins to manage the Central Server. From here, they can create users, authorise devices and configure site wide settings.
Console User	A Console User is a role given to a User which allows them to log in to the Console and control clients. They may also be given roles allowing them to create and apply/remove Policies.
Console Admin	A Console Admin automatically has the role of a Console User, but can also configure global settings in the Console, such as Admin Policies, Global Lock Messages and so on.
Web Admin	A Web Admin has access to the Web Interface to create users and so on. This user can't access the Console, unless also given Console roles.
Console features	
Policies	Policies can be thought of as rules for the Clients. These include things like website or application blocking, keyword monitoring and so on. They can be applied to computers or people, can be scheduled or set for specific networks.
Admin Policies	Console Admins can create policies which are available for all users to apply. They can also create policies which can't be applied or removed by Console Users.
Actions	Actions are things which affect the Client immediately, such as launching a program or shutting down. They can be sent by Console Users and Console Admins. Many actions can also be included in policies to allow them to be scheduled.
Groups	Groups are created through the Web Interface and are collections of devices or users. These allow them to be organised sensibly (eg, into classrooms) and to be managed together. Console Users can only interact with Clients through Groups.
Restrictions	Restrictions can be applied to Groups by Console Admins. These remove access to certain features of AB Tutor for Console Users when they are managing that Group.
Console main view tabs	
Users	The users tab shows any registered users in the selected group. The users must have been registered in the Web Interface. If a Device Group is selected, registered users logged on to those devices will be displayed. If a Users group is selected, all users in that group will be shown if Show Offline is selected. If a stringmatch group is selected, nothing will be shown here as this tab only shows registered users. If a Policy is applied to a user, it will affect them and only them on any computer they log in on.
Devices	The Devices tab shows all devices in the selected group. For a Devices group, it will show all devices in the group, if Show Offline is selected. For a users group, it will show all devices which have sessions with the group's users logged in. For a stringmatch group, it will show any devices with host/usernames which match that group. If a Policy is applied to a Device, it will affect any user who logs in on that Device. Be careful applying policies to users logged in on a terminal server - if they are applied to the device, they will affect all users on that server.
Sessions	The sessions tab shows any running sessions relevant to the selected group. For a Devices group, it will show all sessions on the group's devices. For a users group, it will show all sessions with those users logged on. For a string match group, it will show all sessions matching the strings. If a Policy is applied to a session, it will just affect that user until they log off. On logoff, the policy will disappear.

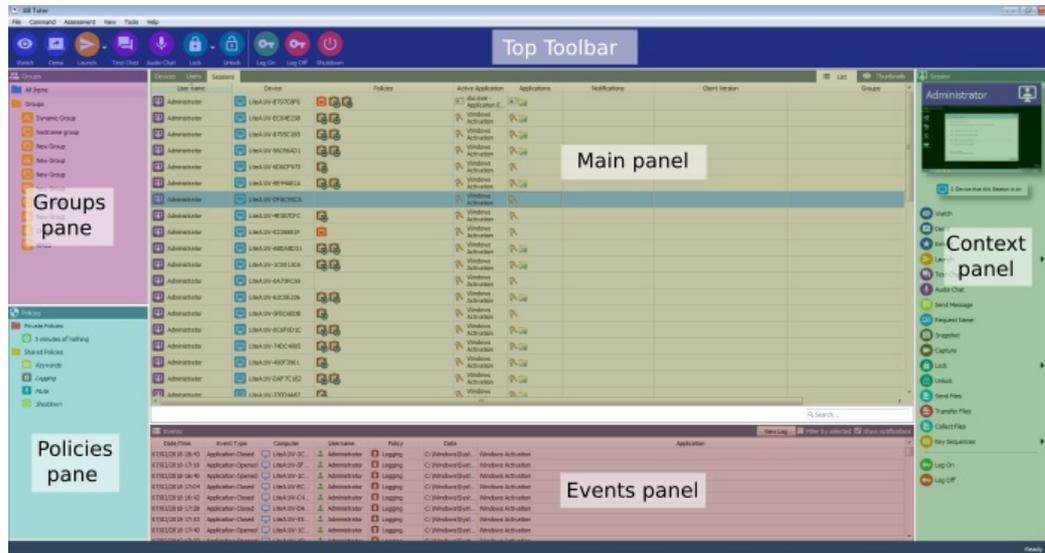
Networking terms

DNS	DNS is like a phone book for computers, allowing hostnames to be translated into IP addresses so a connection can be established. In version 9, the only connection which uses DNS is connections to the Central Server. If possible, we recommend setting up your DNS server so that abcs points to the server with the Central Server installed on it.
Hostname	The hostname is the name of the computer.
Port	Connecting to a specific network port on a server allows the server to know which program on that server the connection is intended for. AB Tutor uses port 5151 on the Central Server for all communication - Consoles, Clients and the Web Interface. This port must be unblocked in any firewalls on that server, and any network hardware between the Clients/Consoles and the Central Server.

The interface

Depending on whether you are logged onto AB Tutor as tutor or administrator, you will be presented with slightly different interfaces:

Administrator Overview



The interface is laid out to give easy access to the more commonly used parts of AB Tutor, however it can be customised to remove controls which rarely get used and to make the more important ones easier to get at. The interface is divided into several sections.

Top Toolbar

The Top Toolbar contains shortcuts to many of the most frequently used actions and policies. This area can be customised by right clicking in the toolbar and selecting **Customise**. From here, any **Action** or **Policy** can be added as a new button. If the software is being run by a Console Admin, they can choose whether the settings should be defaults, enforced or just for themselves.

Left column: Group pane

The group pane shows a list of the available groups for the current user. A Console Admin will see the **All Items** entry as well, which will show all devices registered on the server. The user can select one or more groups from the list, and the computers and/or users in those groups will be displayed in the main panel. If you select the **Groups** folder option then the computers from all available groups will be displayed.

Computers can be added to a group by dragging and dropping. For more information on adding to and configuring groups, please see [Groups](#).

Left column: Policies pane

The policies pane shows all policies which are available for this user. It is split into two sections - **Private Policies** which are policies created by the current user that will only be seen by them and **Shared Policies** which are policies created by admins for all users to see. The right click menu in this pane allows policies to be created, edited and deleted. You can also apply a policy to a computer simply by dragging the policy onto the computer or computers.

For more information on policies, please see [Policies](#).

Centre column: Main panel

This panel shows the devices, users or sessions in the currently selected group(s). From here, the user can see what the computers are doing, what software is being run on them and run commands against them. The main panel has two display options. The first is **list view** which shows columns with information about the computers. This view is generally intended for admins as it allows more computers to be displayed at once, with more information. The second is **thumbnail view** which shows a thumbnail of each computer, and optionally the running applications and applied policies. For more information on either of these views, please see the associated pages. To switch between the views click the buttons in the top right of the main panel.

Across the top of the main panel, you can select how the group members are displayed. There are three possible views - Devices, Users and Sessions. Which ones are shown depends on the type of group selected and the options

ticked in the **View** menu. To filter by computer name or username, type the filter text into the box in the bottom right:

To the left of the filter box is a button to show only connected computers - when this button is blue , only connected items will be shown. When it is grey , all possible entries will appear. Policies can still be applied to disconnected computers or users, however they will not take effect until the computer next connects to the Central Server.

Centre column: Events panel

When a policy violation is triggered by a user, information about the violation will be displayed in this panel. Any event can be clicked on to see more information about it in the right bar, or historical events can be viewed using the **View Log** button. To only show events related to the selected computer(s), tick the **Filter by selected** box.

Right column

The right hand column is context sensitive, meaning that the information displayed there changes depending on what the user selects. Appropriate controls and information will be shown.

Right column: Computers or Groups

When a computer is selected, the right column will show thumbnail of the computer and a list of commands which can be applied to that computer. The commands shown in the list can be customised by right clicking on the column title and selecting **customise**. If a command has an arrow next to it, clicking on the arrow will show a list of options for that command (eg the lock button's arrow will show a list of previously set lock messages), however just clicking on the command will apply it with the default option. Commands which end with ... will trigger a dialogue box before they are applied.

If a group or multiple computers are selected then any commands chosen will be applied to all selected machines, if they online - policies will be applied to all machines. When multiple computers are selected, up to 6 thumbnails will be displayed in a grid and clicking on the thumbnail area will open a watch session for the selected computers in grid mode.

Right column: Policies

When a policy is selected, the right column will show basic information about the selected policy. This will show the type and the policy schedule or duration.

Right column: Events

When an event is selected in the bottom pane, the metadata for that event will be shown. This includes any screenshot or video taken, which can be zoomed in on by clicking, along with the time/date, user, application and any associated data.

Status Bar

The Status Bar is displayed at the bottom of the AB Tutor Window. It is used to show information about selected menu items or buttons, the current group being watched, the number of found workstations, the number of connected workstations and the connection to the server.

View Menu

The view menu allows different components of the interface to be shown or hidden. The left and right panels, the top toolbar, and the events pane can all be turned on or off. You can also force the **Sessions** and **Users** tabs to always be shown, which can be useful if the software is being used with Terminal Servers. Finally, if the **Lock Layout** option is unselected, the individual panes can be moved around the interface, or dragged out, allowing them to be put on a second monitor. If you want to return the view to the default, you can select **Reset Layout**.

Getting to know the interface

Types of Client

There are 3 types of client which can be displayed in AB Tutor - each with their own tab in the main view. The user and session tabs can be turned on and off in the view menu, as in a lot of setups they won't be useful and will only clutter the interface.



Devices

A device is any computer (including laptops and tablets) with the AB Client installed on it. This view is useful for the traditional computer room setup where the Console user will always want to connect to the same set of computers. If a policy is applied in this view, it will affect the specified computer and will stay on it to affect the next user (unless set to expire).

Users

A user is a person who has been registered with AB Tutor in the Web Interface as a Client User. This view is useful for controlling a number of Client users who could be using different computers at different times, for example in a school with a terminal server setup or if there are some problem users who need to be monitored or restricted wherever they are. If a policy is applied in this view, it will affect the specified user and will get automatically applied to any computer they log in on, and be automatically removed when they log off.

Sessions

A session is created when a user logs on and is a temporary "container" for everything they do while they are on the computer. The session is destroyed when the user logs off. If a policy is applied in this view, it will affect that session, but will disappear when the user logs off. This view is also useful with terminal servers as it allows the Console user to see all the sessions on their terminal servers at once.

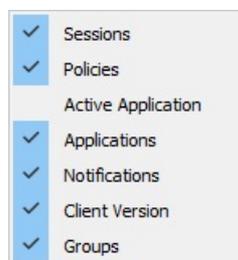
Getting to know the interface

List View

The list view in AB Tutor is intended to give information on a large number of computers at once and make it easy to keep track of them. The displayed computers can be sorted by any column, or filtered by hostname/username.

Device name	Sessions	Policies	Active Application	Applications	Notifications	Client Version	Groups
-------------	----------	----------	--------------------	--------------	---------------	----------------	--------

This view can be customised by right clicking anywhere on the column headers and selecting which columns you would like to display. Columns can be rearranged by dragging.



Device name

This column shows the name of the computer. By default, this will show the hostname, however this can be changed by right clicking on a computer and selecting **Set Alias**. This option is entirely cosmetic and will only change the display name, not anything on the Client device. The icon shows the status of the client, either blue (online) or grey (offline).

Sessions

This column shows the username of the currently logged in user, along with their real name if the client knows what it is. Real names are extracted automatically by Windows from Active Directory but can be overwritten by sending a **Request Name** Action to the Client.

Policies

Policies are displayed as a row of icons. The name and type (private, shared) of a policy can be seen by hovering over it with the mouse. If the policy is temporary, it will display time left - if it's protected, this will be displayed too. Note that policies can still be applied to (and are displayed for) offline devices, however they won't actually take effect until the client comes online again.



Active Application

This column shows the currently focussed window on the client, allowing the Console user to quickly check that all Client users are working on the correct thing. This column is hidden by default as the active application will always be shown on the left in the Applications column, however this can make it easier to see at a glance.

Applications

Applications are displayed as a row of icons. Hover over an application to see its title bar information. The active application will always be shown first in the row. Any application can be closed or temporarily blocked by right clicking on it. The temporary block will last for 30 minutes, but can be removed earlier by removing the policy created by the block.

Notifications

The notifications column will show any alerts or additional information about the client, for example poll results, battery status (on mobile devices), traffic light responses etc.



Client Version

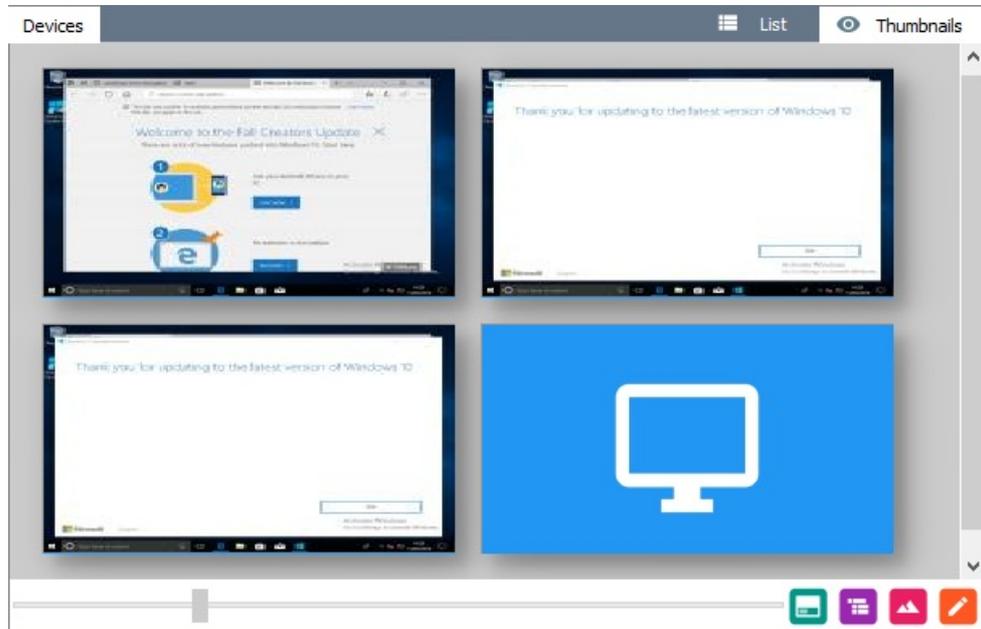
The OS of the client and the current version running on it are shown here. The icons show the OS and also the form factor of the client (desktop, laptop, tablet).

Groups

This column will show any groups that the client appears in. On the Devices tab, only Device Groups will be displayed, on the Sessions tab, only User Groups will be displayed.

Thumbnail View

The icon view displays the selected group(s) as a series of small updating thumbnails. The size of these thumbnails and whether information is displayed under them can be configured. If a Device is offline, it will be replaced with the standard Device icon.



Across the bottom there is a series of controls for the view:

-  Control the zoom level
-  Set whether the details are shown under the thumbnail, or as a popup when you mouseover.
-  Align the thumbnails to a grid.
-  Set a background for the group.
-  Turn edit mode on and off.

In this view, you have the same access and control through the top toolbar and side bars as in the list view. These give you full control over the connected clients and allow you to start programs, apply policies, etc.

 If running as a Console Admin, changes to the layout can be saved as defaults, per user settings or global overrides.

Getting to know the interface

Actions

In AB Tutor, actions are commands which can be sent to a client. These are generally one off triggers to do something to the machine or put it into a state, as opposed to policies which are generally ongoing or repeating. Some actions can be applied through policies to allow them to be applied on a schedule or to be ongoing.

There are 3 places that actions can be found and applied. The right **Context Panel** will show a list of available actions when a device, session or user is selected in the main view. This list can be customised to add or remove entries by right clicking on the heading and selecting customise. If this is done by a Console Administrator, they can select whether they save their changes as:

- **Global Defaults** which will affect all users, but can be overridden (eg, the Admin can give a user a trimmed down set of options, but they can select or hide additional ones if they want).
- **User Settings** which will only be saved for the current user. This is the only option non-admin users have and so will be done automatically without showing the options.
- **Global Overrides** which will force all users to use these settings and will prevent them from changing them.

The second place is the **Top Toolbar**, which by default shows a subset of the options available on the right. These buttons are larger and offer easy access to more commonly used functions. The third place is the **Command Menu** on the menu bar. This will always show all actions which haven't been blocked through **Group Restrictions**.

Any action which appears with an arrow next to it has a menu of saved settings for that action which can be opened by clicking on the arrow instead of the icon or action name.

Watch

Watch allows the Console user to view the screen of the Client user(s) and optionally take control.

Demo

Demo transmits the Console user's screen to the selected Client(s), They can choose to send all or part of their screen, whether to include audio and whether to display it full screen on the Client.

Exhibit

Exhibit allows one Client's screen to be shown to the rest, for example during a presentation.

Launch

Launch allows applications, documents or websites to be opened on the Client. These will be opened as the currently logged in user.

Text Chat

Text Chat opens a chat session between the Console and Client(s). If multiple Clients are selected, there is an option to allow them to talk to each other.

Audio Chat

Audio chat allows the Console user to talk to the Client(s) using microphone and speakers. This can be broadcast or two way chat.

Send Message

Send message allows single messages to be sent to Clients. These do not allow replies to be sent.

Request Name

Request name allows you to ask a Client user what their name is. This can be useful on sites with generic logons or cryptic usernames.

Snapshot

Snapshot takes a screenshot of the Client's screen, optionally with the user's name, device name and time embedded in it, and saves it to the event logs on the Central Server.

Capture

Capture starts a recording of the Client's screen, with duration selected by the Console User. This will be saved to the event logs on the Central Server.

Lock

Lock will lock the Client's session, preventing keyboard or mouse input and putting a message on the screen. Custom messages can be created through the lock screen manager.

Unlock

Unlock will return a previously Locked computer to normal, allowing the Client user to take control again.

Send Files

Send Files allows the console user to send files to Client users, and to specify the target destination. This works with multiple clients simultaneously.

Transfer Files

Transfer Files is a 1:1 file transfer tool, showing a tree view of both computers and allowing files to be copied from one to the other.

Collect Files

Collect files allows the Console user to pull files off Client computers, specifying patterns for the files to collect. The files will be named based on the Client hostname, username and time they were collected.

Key Sequences

Key Sequences allows strings of keystrokes to be sent to Clients. These can include special keys such as Control or Alt.

Log On

Log On allows multiple computers to be logged on at once, as long as they all use the same username and password.

Log Off

Log Off allows a log off command to be sent to all the selected computers.

Reboot

Reboot allows Clients to be restarted. A warning can be displayed with optional override.

Shutdown

Shutdown allows a shutdown command to be sent to clients. A warning can be displayed with optional override. This can also be used to suspend or hibernate a client, optionally logging the user off. If a full shutdown is performed, there is the option to tell Windows to apply updates.

Inventory

Inventory collects information about the computer's hardware and software and saves it into the Event Logs. You can view it from the Events panel, or the Log Viewer.

Services

Services displays a list of the services running on the client, allowing them to be stopped, started or restarted.

Processes

Processes displays a list of the processes running on the client and allows them to be stopped if required.

Command Prompt

Command Prompt allows DOS commands to be sent to Windows machines or Bash commands to Macs. These can be sent to multiple computers simultaneously and will run as the System or root user.

Windows Event Log

Windows Event Log will open the Windows Event Log viewer and try to access the events log on the Client. This will only work with Domain authentication.

Using AB Tutor

Screensharing

AB Tutor has three forms of screen sharing -  [Watch](#) for seeing a Client's screen on the Console,  [Demo](#) for sending the Console's screen to one or more Clients and  [Exhibit](#) for showing one Client to other Clients.

Watch

Watch allows the Console User to view the screen of one or more Clients. To view:

- Select one or more clients to view.
- Press the Watch button or select the Watch option from the right panel, or (for a single client) double click on the client you wish to Watch.

The quality of the video can be lowered (to speed it up on slow connections) from the [Console Settings](#) menu.

Whilst Watching client workstations, the toolbar will be available at the top of the client screen. Click on the handle or a blank part of the bar to hide it and click on the handle at the top of the screen to unhide it.



Shared

When this button is pressed, it enables you to take control of the currently viewed workstation whilst allowing the Client user to also use their mouse and keyboard at the same time.

Lockout

When this button is pressed, it enables you to take control of the currently viewed workstation, disabling the Client user's mouse and keyboard.

Audio

When this option is selected, the Console user will be able to hear the sounds being played on the Client machine.

Ctrl+Alt+Del

This will send a Ctrl+Alt+Del command to the workstation to activate the Windows login or security screen.

Text Chat

Press this button to open a Chat window to send and receive text messages with remote client workstations.

Snapshot

Pressing this button whilst viewing a remote screen will take a screen shot which will be saved to the Event Logs on the Central Server.

Scale

Pressing this button will resize the remote view to fit in the current window size. This is useful if there's a major difference in resolution/DPI between the Console and Client, or if the Console user wants the Watch window to only take up part of their screen. If the window is significantly smaller than the resolution of the student workstation, it can be tricky to read text on the screen. If this is a problem, make the window bigger.

Fullscreen

This button toggles between windowed view and fullscreen view.

Previous/Next client

These buttons will jump to the next or previous computer selected. The **left** and **right** arrow keys will also jump

between computers, provided you are not in any of the **Shared** modes. This option is only available if more than one Client was selected for the Watch session.

Shuffle

This option will pick a Client randomly out of the ones selected in the Watch and display it. This option is only available if more than one Client was selected for the Watch session.

Cycle

This option automatically cycles through the selected computers - it is functionally equivalent to pressing the next button every few seconds. The interval can be set in **Tools, Settings, Watch/Demo**. This option is only available if more than one Client was selected for the Watch session.

Grid

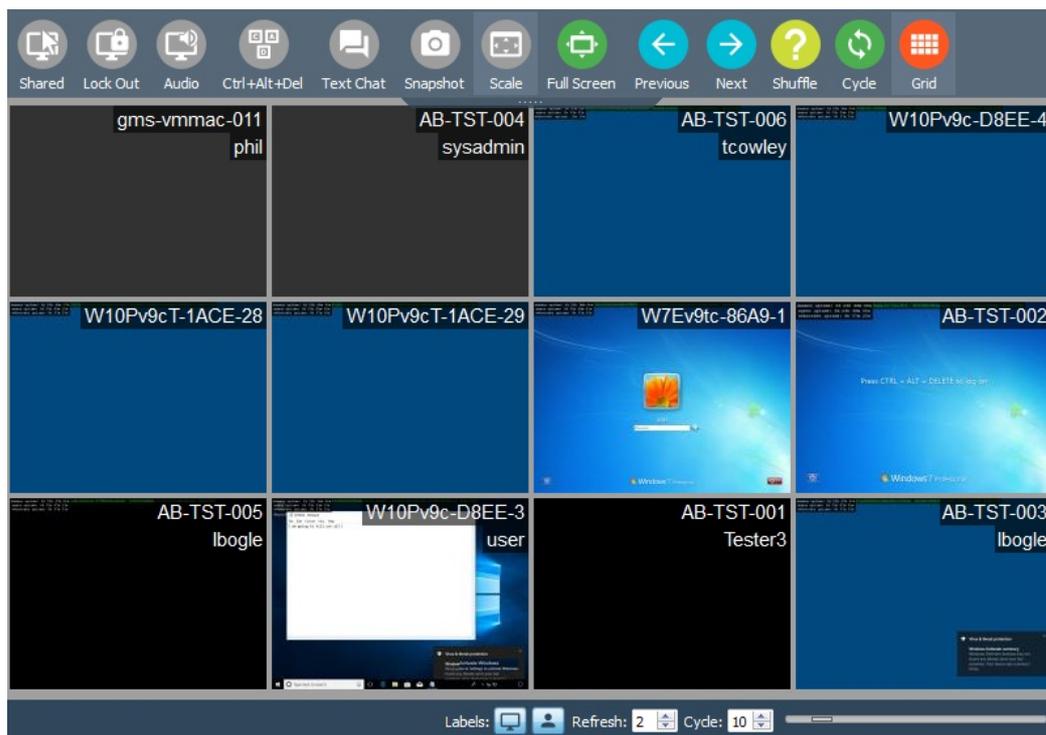
This option will switch the Watch session over to grid mode, as described below. This option is only available if more than one Client was selected for the Watch session.

Close

This button will close the current watch session. It is equivalent to pressing the window's **X** button, but can be accessed from full screen watch mode.

Live Watch - Grid

The **Grid** view allows multiple computers to be viewed simultaneously. To start using the Grid View, select one or more groups or multiple Clients in the main window and then click on **Watch** or on the thumbnails at the top of the Context panel. With multiple Clients selected, it will automatically start in grid mode. Clients can be removed from grid view by right clicking on them and selecting **Remove**.



Full Screen

The **Full Screen** button works in the same way as in a normal watch session and will display the Grid View full screen.

Cycle

The **Cycle** button at the top of the watch window will still work in Grid View, however it will scroll a screen of clients at once. The cycle delay time can be set at the bottom of the window. The **Previous** and **Next** buttons will also jump to the next screen, as will scrolling the mouse wheel.

Labels

The **Labels** options allow the  computer name and  username overlays on the Grid View screens to be turned on and off.

Refresh

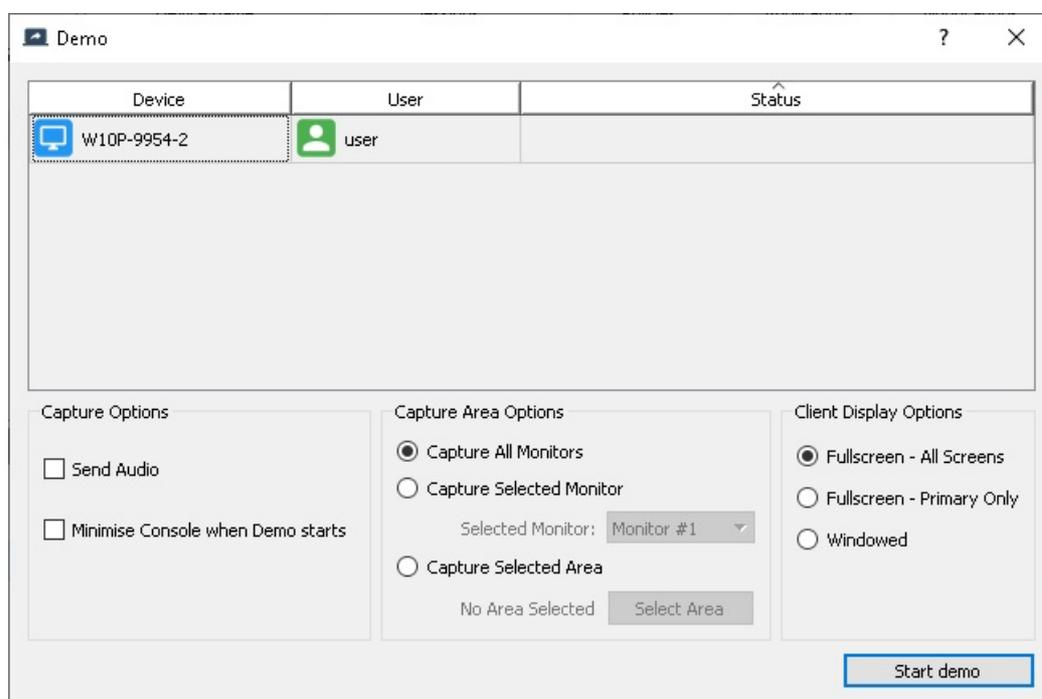
Refresh allows the time between screen refreshes to be adjusted. Lower refresh times will lead to more network load, but a better idea of what's happening on the clients. Computers which are not currently visible will not be refreshed until they are displayed.

Resizing the grid

To change the size the Clients are shown in the grid, move the slider in the bottom right. Moving the slider to the left will make each computer smaller, and hence allow more to be displayed on the screen. Moving the slider to the right will make the computers bigger, and hence reduce the number visible at once. You can also resize the views by holding ctrl and scrolling the mouse wheel.

Demo

This command will show the Console's workstation screen to all selected clients. This can be used when running a presentation or to demonstrate to the entire class how to use the computer or an application etc. When this action is selected, the following window will open, allowing the Console user to set up the Demo as required:



- Capture Options:
 - **Send audio** allows the Console user to set whether their audio is transmitted to the Clients.
 - **Minimise Console when Demo starts** will minimise the AB Tutor window and the Demo dialogue box when the demo starts, so it doesn't get shown to the Clients. If you are Demoing from a different screen, it might be easier to not minimise it.
- Capture Area Options:
 - **Capture All Monitors** will demo all of the Console's screens to the clients.
 - **Capture Selected Monitor** allows the user to select which screen should be sent for the demo. When the dropdown is open ed, the screens will be labelled with their number, allowing easy selection.
 - **Capture Selected Area** allows the Console user to only send part of their screen to the clients, for example to just send part of a window - perhaps to allow slides to be shown whilst leaving the notes only on the Console.
 - **Select Area** allows the Console user to select the area to be sent if **Capture Selected Area** is turned on.
- Client Display Options:
 - **Fullscreen - All Screens** will show the Demo centred across all screens on the Client computers, locking their mouse and keyboard and preventing them from using the computer for anything else.
 - **Fullscreen - Primary Only** will show the demo just on the client's primary screen. This prevents the demo being split if a single screen (or area of screen) is demoed to a multiple monitor client. Again, the mouse and keyboard will be locked.
 - **Windowed** shows the Demo in a smaller, resizable window on the Client and allows them to carry on using the computer. This is useful if the Console user is demonstrating something and wants their Clients to follow along on their own computers.

Clients can be dragged into the list section of the dialogue box to add additional Clients to the demo. Right clicking

on the computers in the list will allow them to be removed.

Once everything is set, press **Start Demo** to begin the Demo. The button will change to saying **Stop Demo**, clicking this will end the Demo. If AB Tutor was minimised to start the demo, you will need to restore the dialogue box to end the Demo, or if you just close it, the Demo will end.

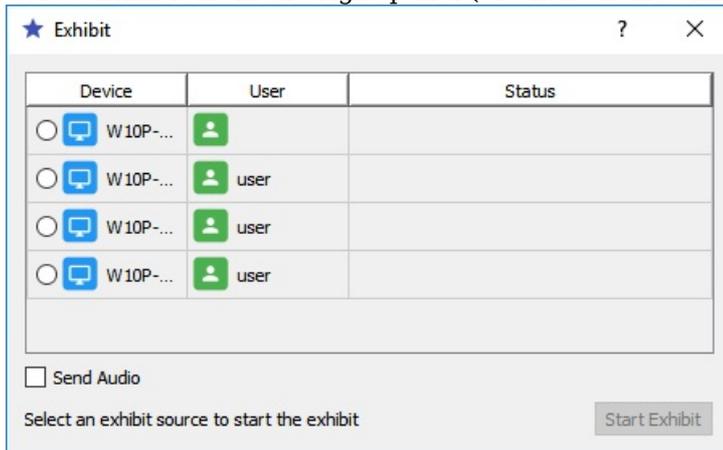
★ Exhibit

This command allows you to display a Client's screen to other Clients.

Please note, this icon is not added to the Top Toolbar by default. You can add it by right clicking on the toolbar and selecting **Customise**.

To Exhibit a remote Client:

- Select all the Clients that you want to involve in the Exhibit - subject and recipients
- Select Exhibit from the right panel (or click on the exhibit icon)

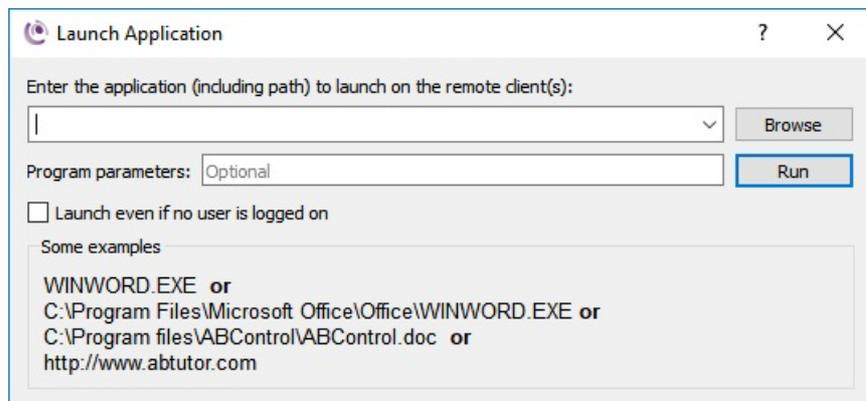


- Select the Client you wish to exhibit to the rest
- If you wish to transmit audio from the exhibited client, select **Send Audio**
- Press **Start Exhibit**. A Watch window will open on the Console, however this can be minimised if you want to use the computer for something else during the Exhibit. You can take control of the Exhibiting machine as normal via the Watch session, if you wish to.
- To end the Exhibit, press **Stop Exhibit**.

Using AB Tutor

>Launch

Launch allows the Console user to run applications, documents or websites on the Clients. For example, the Console user could launch the same document on all student workstations in preparation for the next activity/exercise.



- Select the Clients you wish to run the Launch against, then click the Launch button.
- Enter the application to launch, or select a previously entered application by clicking the down arrow.
- Enter any command line parameters to be passed to the launched application (e.g. a file to open).
- Click the **Run** button.

To remove entries from the drop down list, select them, right click and select **remove**. The whole list can be wiped using **remove all**.

Some applications can be launched without the need to enter a full path as they are in the "system path" on the Client machine (e.g. notepad.exe or winword.exe). If the application doesn't launch without a path then you must add one.

You can also specify document files without giving information about the application needed to open them. (e.g. U:\Personal\StudyGroup.docx) as the client application will attempt to find the launching application associated with the file's extension. In this case the extension is '.docx' and Windows knows that Microsoft Word is the application that uses this extension.

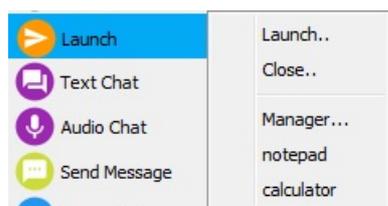
Also note that you must enter the file extension in order to launch a document in its associated application. Windows will hide extensions by default, but they can be shown by opening Windows File Explorer and going to **tools, folder options, view** and unticking **Hide extensions for known file types**.

It is also possible to enter a simple web address or URL (e.g. http://www.mycompany.com) and the default web browser on the remote client machine will launch and show this web page.

To launch Mac apps, use the full path to the app, eg **/Applications/Safari.app**.

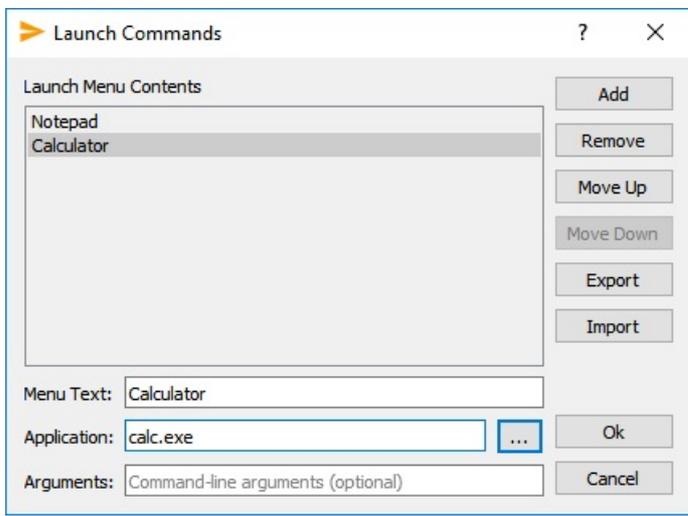
It is also possible to launch applications even if the user is logged off (for example, maintenance tasks), however as this is generally not desirable it needs to be enabled manually by ticking the checkbox in the launch dialogue.

Items can be added to the applications main drop-down menu by using the Launch Manager. These items then appear under the Launch menu or as a drop-down menu when you press the small down arrow to the right of the Launch buttons.



Launch Manager

The Launch Manager allows you to save frequently used applications, allowing them to be run directly from the menu. To access the Launch Manager, select it from the dropdown next to the **Launch** action buttons.



- Press the Add button to create a new entry
- Enter the Menu Text to be shown in the drop down menus
- Manually enter the path and filename or use select to find the application to be launched

i Check that applications on the Client machines are installed in the same location as on the Tutor to ensure successful execution.

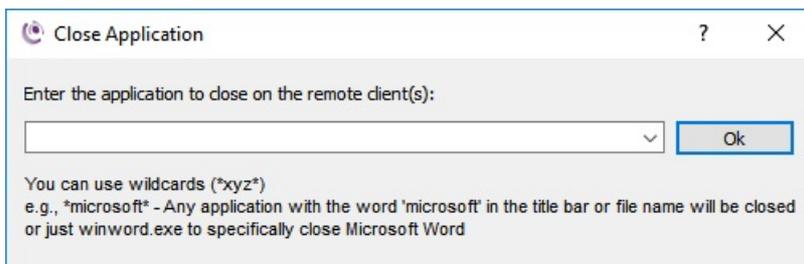
- Add any start-up command line parameters to be passed to the launched application. (e.g. the path/filename of a file to open in Word)
- Repeat the above process to add more applications
- Press OK to save or Cancel to abort the additions

The order of the items in the menu can be changed by using the Move Up and Move Down buttons so the most commonly used applications can be placed at the top of the list.

Close Applications

Menu: **Application - Close...**

Programs can be closed on the student workstations from the tutor workstation. For example, if a tutor has launched an application on all student workstations, they may wish to close that application on all workstations ready for the next activity / exercise.



To specify the application to close you can either:

1. Specify filename of the application to close - case-insensitive (e.g. winword.exe or IEXPLORE.EXE)
2. Specify the applications title text or part text using wildcards (e.g. *Microsoft*) will close all running applications with the text Microsoft in its window title.

i It is possible to close all running applications by simply entering *

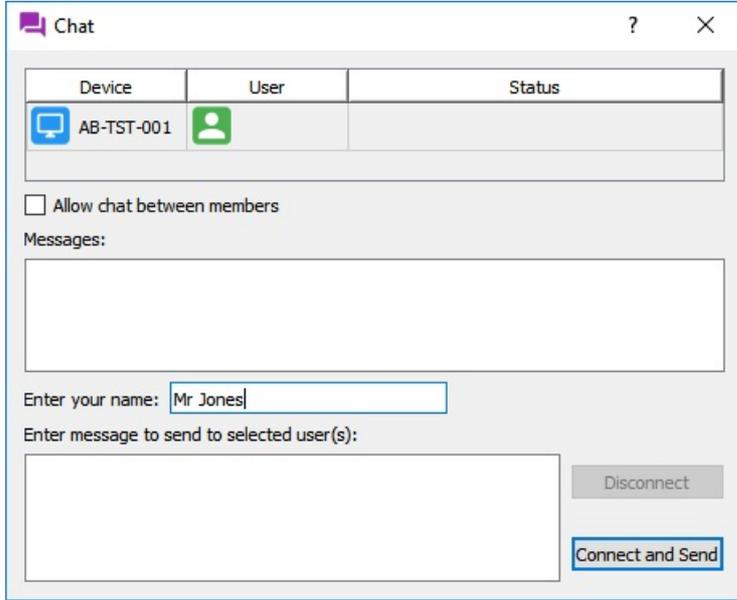
i No warning message will be displayed prior to closing the applications on the remote machines.

Using AB Tutor

Chat actions

Text Chat

This command will open a chat window allowing the Console user to send a text message to all selected Clients. The tutor can then wait for a reply back from the student(s). This is intended for 2 way conversations - if you want to just leave a message on the student's screen, please use the **Send Message** command. The window will open with the selected Clients displayed in the top pane - additional Clients can be dragged in to add them and unwanted clients can be removed by right clicking on them and selecting **remove**.



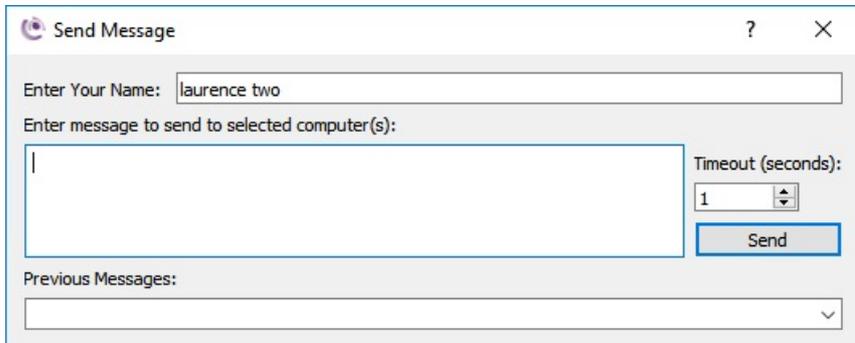
The screenshot shows a window titled "Chat" with a help icon and a close button. It contains a table with columns "Device", "User", and "Status". The first row shows a device icon, "AB-TST-001", a user icon, and an empty status field. Below the table is a checkbox labeled "Allow chat between members" which is unchecked. A "Messages:" label is above a large empty text area. Below that is a text input field with "Mr Jones" entered. Another text input field is labeled "Enter message to send to selected user(s):". To the right of this field are two buttons: "Disconnect" and "Connect and Send".

If you want the Client users in the list to be able to talk to each other, rather than just to the Console user, tick **Allow chat between members**. Your name, as displayed in the chat, can be changed in this window too. When the chat window is closed on the Console, or you click **Disconnect** the chat windows will close on the clients.

 All chats are logged on the server, however they are hidden from the normal log interface. If they are required, they can be extracted by a network admin.

Send Message

This command will display a dialogue box allowing the tutor to send a simple text message to all selected students. The message is displayed on the students' screen in the form of a simple message box with an OK button to clear the message. You can force the remote message box to close after a given number of seconds.



The screenshot shows a dialog box titled "Send Message" with a help icon and a close button. It has an "Enter Your Name:" label and a text input field containing "laurence two". Below that is a label "Enter message to send to selected computer(s):" and a large text input field. To the right of this field is a "Timeout (seconds):" label and a spin box containing the number "1". A "Send" button is located below the spin box. At the bottom, there is a "Previous Messages:" label and a drop-down menu.

To send a message:

- Select the Client(s) to which you want to send the message.
- Select the **Send Message** menu or button on the toolbar.
- Optionally enter your name. This lets the remote user(s) know who the message is from. (This name will be remembered for all subsequent chats/messages).
- Enter the message you want to send.
- Alternatively, select a previously sent message from the drop-down list.
- Enter the number of seconds you want the message box to remain visible. (Enter 0 to disable the timeout feature so the message box won't disappear until the OK button is pressed).
- Press the **Send** button

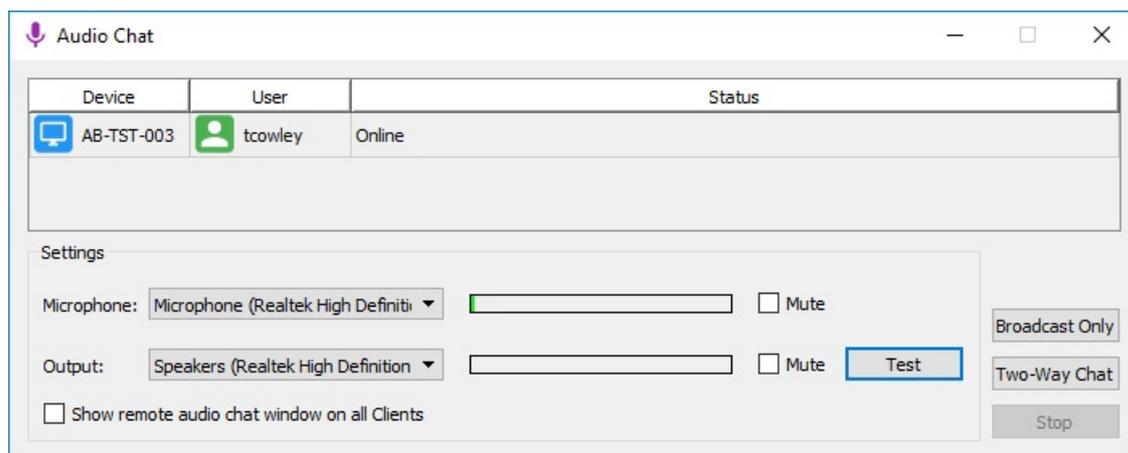
Each time you press the Send button, the system also adds the message to the 'Previous Messages' list for subsequent selection. If you wish to remove an entry, select it from the list then right click in **Previous Messages** and select **Remove**. You can also use **Remove All** to wipe the list completely.

Audio Chat

This command will display a dialogue box allowing the Console user to have an audio conversation with Client user(s) via a microphone and speakers. This function will only work if both the Console and Client have audio capabilities (i.e. a sound card with a microphone and headphones or speakers attached).

Two Audio commands are available:

- **Broadcast Only:** You can select one or more workstations to which you want to send an audio announcement, but the Client user(s) are not able to reply.
- **Two-way Chat:** You can instigate a two-way audio conversation with the remote user(s). In this case, they will not be able to hear each other.



Press the Stop button to end the audio session.

 The Audio dialog box will remain open allowing you to use other features. (E.g. you can have an audio conversation with a remote student at the same time as viewing/controlling their screen.)

Settings:

You can mute the audio input or output at any time by selecting the Mute buttons. This allows you to hear the Clients without them hearing you, or vice versa. You can check your audio is working by watching the microphone volume bar and by pressing the **Test** button to check output.

Audio Chat will initially use the default microphone and output settings from your operating system. You can change which one is used on the Tutor using the dropdown menus. If you need the Clients to be able to select non-default audio options, tick the **Show remote audio chat window on all Clients** to open a box with the same dropdowns on the Client.

Request Name

Request Name allows the Console user to open a dialogue box on the Client asking the user to enter their name. It will then display that name in the Sessions column, with the original username in brackets. This is useful if the Client uses a generic login or the usernames used on your site are cryptic. Names assigned this way can be cleared by right clicking on the Client and selecting **Clear Name**.

Using AB Tutor

Snapshot

This command allows the Console user to take a snapshot of the selected Client's desktops which will be saved to the Event Log on the Central Server. Multiple computers can be selected and snapshots taken simultaneously. The snapshot will show the current user and hostname in the top right if the option in [Console Settings, General](#) is ticked.

Capture

This command records the Client's desktop for the specified time. The Tutor can set the desired record time and frame rate, and whether the user's details are printed on the video. Note that the available frame rates are all low to save space, and that large amounts of recording could fill the server's hard drive.

If the user logs out during the recording process, the video will be split into multiple files, however it will keep recording.

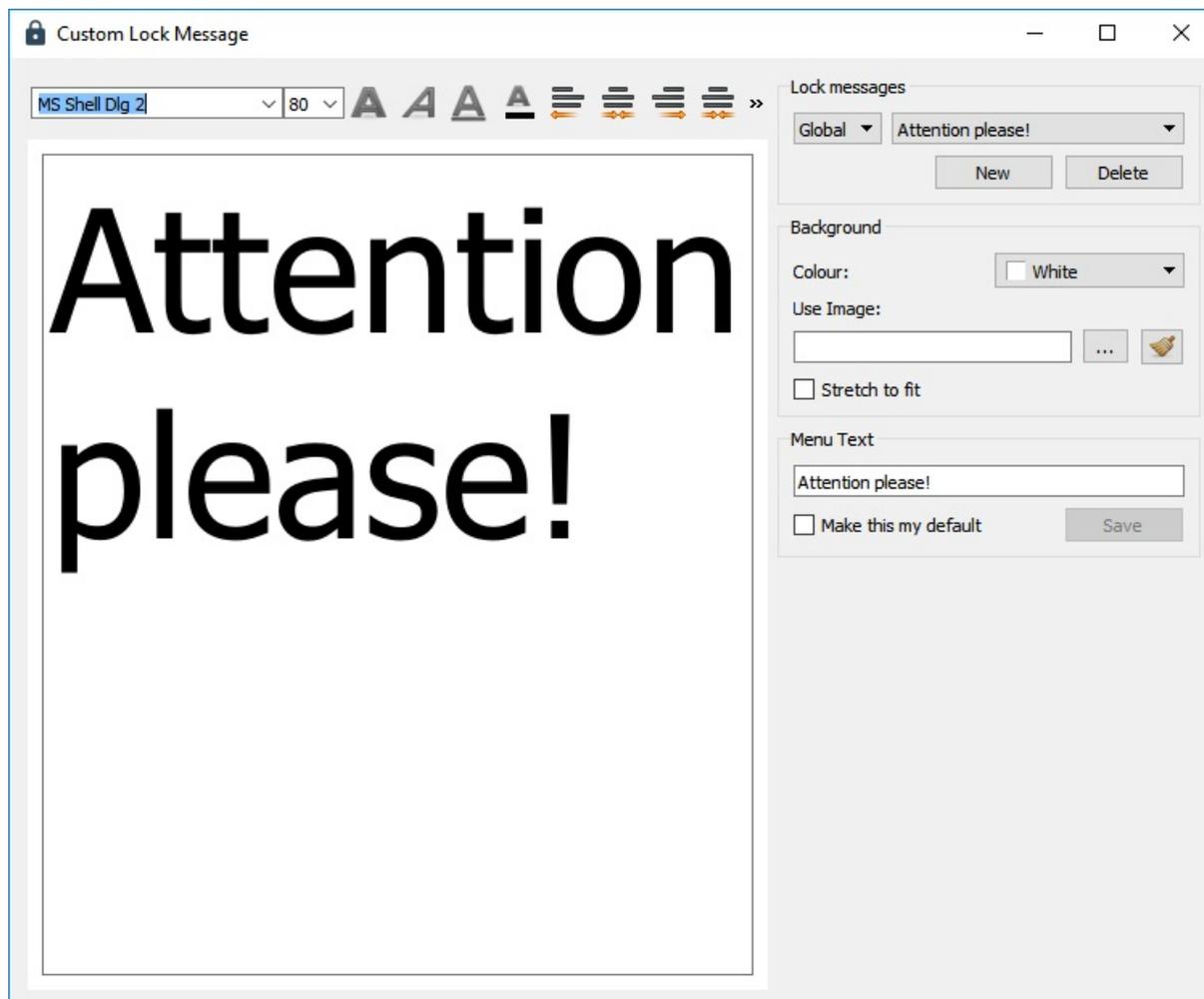
Once created, snapshots and videos will show in the events pane, and if selected will display in the right hand panel. Click on the thumbnail of the video/screenshot to pop it out into its own window, which can then be resized. To view historical events, select **View Log** from the top of the Events pane.

Using AB Tutor

Lock/Unlock

This Action locks the Client computer, preventing mouse/keyboard input and displaying a message, with optional picture. A lock icon will be displayed in the notifications section on the Console. The Client will remain locked until the lock action is removed by clicking the **Unlock** button or right clicking on the notification area icon and selecting **remove**.

When you lock a client, you can either click the button to lock it with the default message or choose a custom lock screen message from the dropdown. To create custom lock messages, open the dropdown and select **Lock Messages**.



The left hand pane allows for the text of the lock message to be edited, including text size, colour and alignment. On the right, you can select the background colour or image and save it to the list shown in the **Lock** dropdown and in the lock policy creation window. You can select previously saved lock screens using the dropdown at the top, and if running as a Console Admin, you can choose whether to save this one as a **Global** (shared) or **User** lockscreen. Other users will have access to the **Global** ones and their personal **User** ones, but not other User's **User** lockscreens.

 A lockscreen can be given a transparent background from the colour dropdown by selecting **more...** and setting the alpha channel appropriately. Be careful with this option as it could lead to an invisible lock screen, which is hard to diagnose.

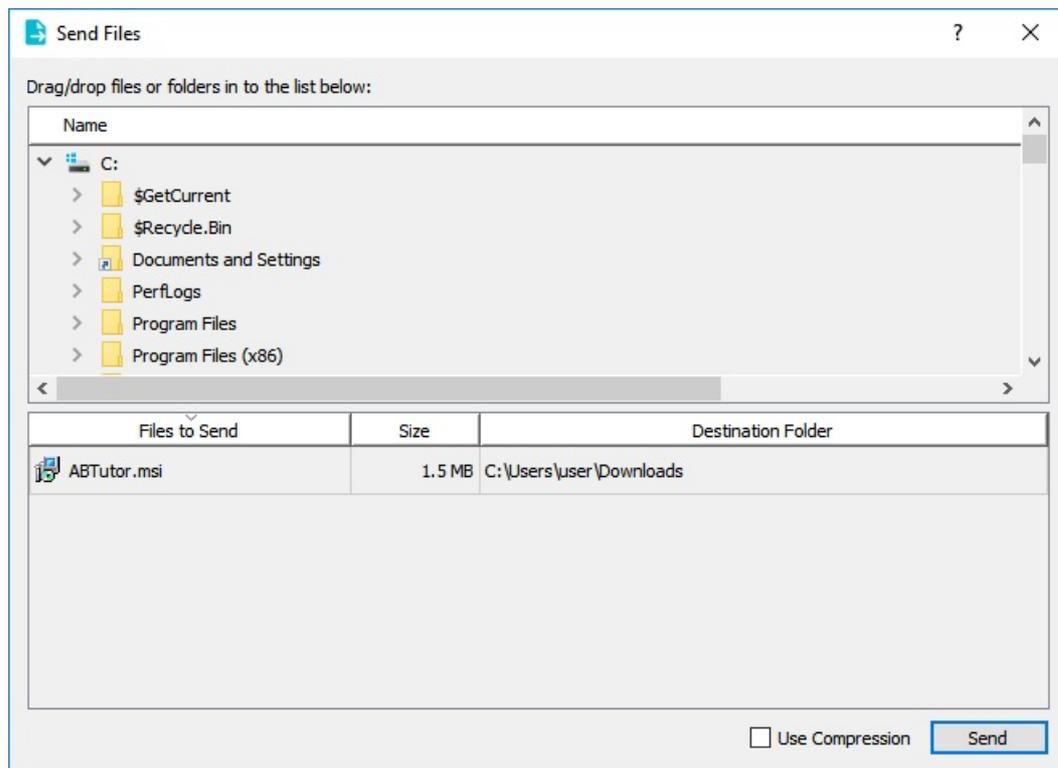
If the student forces the machine to reboot by pulling the power cable, then when the system starts up again this policy will activate and lock the screen, keyboard and mouse again. In case of problems, all action (as opposed to policy) locks can be removed by restarting the Central Server - this will eliminate all saved states and hence allow the clients to unlock, but will not remove any applied policies.

 Use this option with care! It will activate whether or not the user logging on is a full Administrator to the computer. It is also possible to lock your own computer, if the setting **Tools, Settings, General, Block this Hostname from showing in the Clients List** is unselected, or if you apply a lock to a group which you are a member of.

Using AB Tutor

Send Files

This enables the tutor to send one or more files in a directory to all selected student workstations. On selecting this command, the following dialogue box is displayed.



- Use the tree view at the top to browse to the files you want to send.
- Select one or more files from the **files list** on the right.
- Drag and drop them into the **Files to Send** list below.
- To change the Destination folder to which the files will be sent, right-click on the file and select **Change destination folder**.

There are two special locations that AB Tutor will expand appropriately for the logged in user: **%DESKTOP%** will save this file to the remote user desktop and **%MYDOCUMENTS%** will save it in the user's personal folder. These can also be used as part of a path, eg **%DESKTOP%\exams**. Alternatively, if you wish to send it to a specific location, enter this manually.

Repeat this with any other files you wish to send to those clients. This tool will allow you to send files to multiple clients, however you can't send different files to different clients, except by using **Send Files** more than once. Once all files have been added, press the **Send** button to start sending the files to the selected Clients.

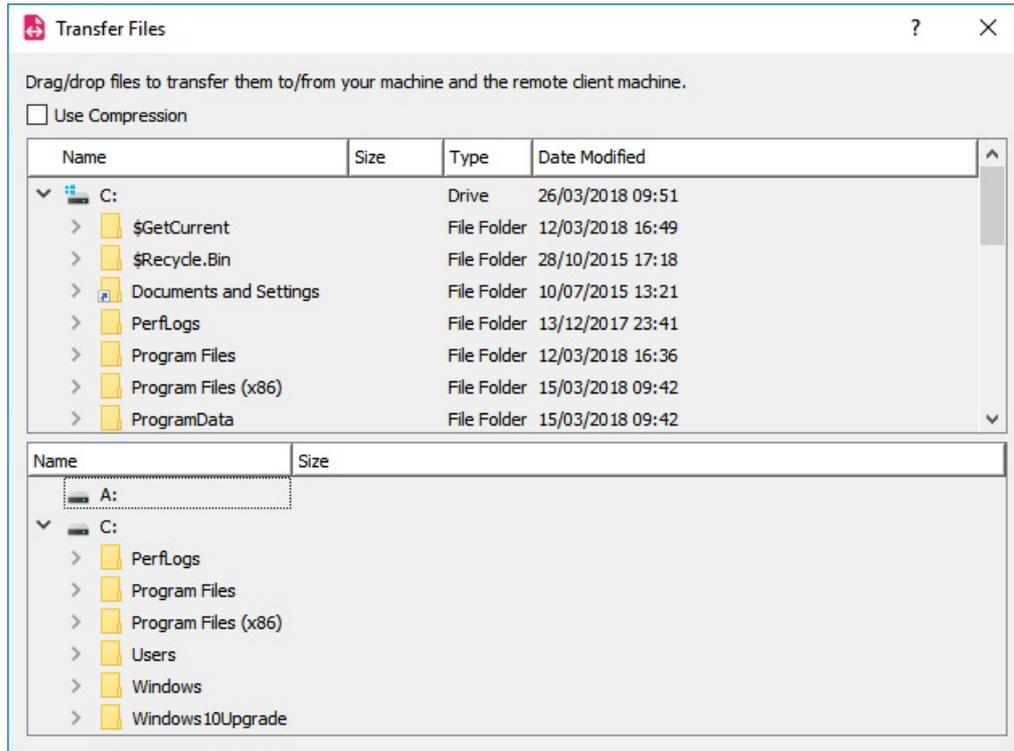
Files can be removed from the Send list by right-clicking the mouse and selecting **Remove from list**.

 By Dragging/dropping a **folder** from the file view, the whole folder will be added to the Send file list, including sub-folders.

 The Send Files dialog window can be re-sized and the panels within the dialogue re-sized to optimise the file/folder views.

Transfer Files

This enables the tutor to send/receive one or more files or folders to a single selected student workstation. On selecting this command, the following dialog box is displayed

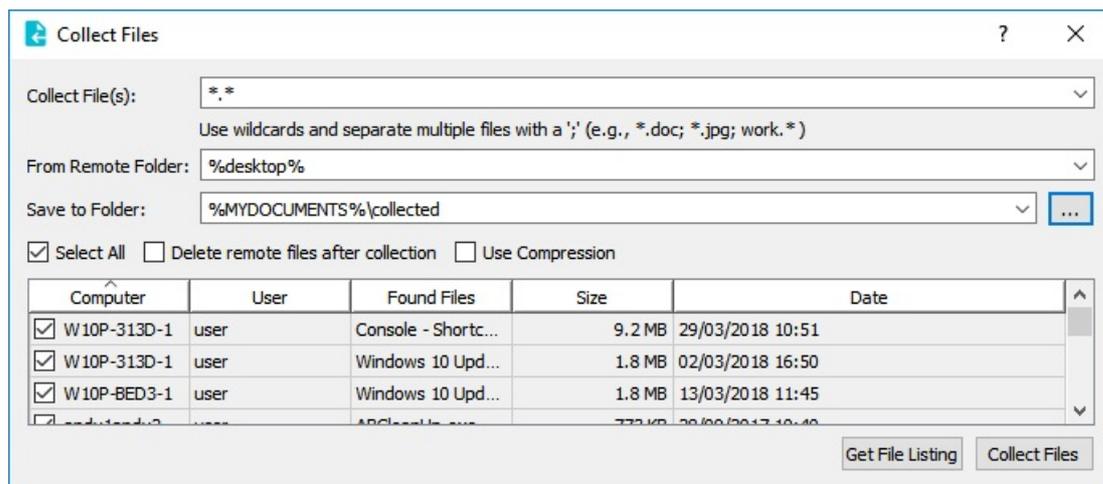


The top half of the dialog box shown the directory and files on your current machine and the bottom half shows the folders and files on the remote workstation.

- Browse to the local folder by using the top panel. When you expand a folder, the files and subfolders within that folder will be displayed.
- Browse to the required remote folder in the lower panel.
- Select one or more files from either the local files list or remote and drag/drop to the other file list window.
- If a file exists, you will be prompted to confirm the overwrite operation.

Collect Files

This command collects specific files from the client computers.



To Collect files:

1. Select the clients you wish to collect files from.
2. Select **Collect Files** from the **Command** menu or from the right click menu.
3. Specify the filename(s) to collect. Use wildcards to obtain all files of a specific type (eg *.doc). You can also enter multiple patterns to match against by separating each one by a semi colon ';' character.
4. Specify the Remote Folder to search for the files. This is where the files are on the Client computer.
5. Specify the local folder to save the collected file to.
6. Press the Get file Listing button to show a list of files found.
7. Un-tick any file you do not want to collect. You can tick or untick **Select All** to select or deselect all files at once.
8. If you wish to delete the files from the remote clients when they have been collected, tick the **Delete remote files after collection** checkbox. You can also turn compression on here - this will speed up transferring some types of files (eg text, doc), but not others (jpg, mp4).
9. Press the Collect Files button to start collecting the remote files and saving them on your machine. A file transfer window will open, showing progress on each file. If any files fail to transfer, their bar will go red and a warning will be displayed.
10. Once the file transfers have finished, the window can be closed. If you want to collect any more files, you can do so, or you can close the **Collect Files** window to finish.

All files are downloaded to the specified local folder; the computer names, user names and date/time are appended to the file name to indicate where and when the file was copied from.

e.g. in the above example the selected files are copied into the local user's "My Documents" folder.

Special Inserts:

When specifying folders, special inserts can be used to access the remote user's personal folders and to organise the collected files.

- To access the user's 'My Documents' folder use %MYDOCUMENTS%
- To access the user's 'Desktop' use %DESKTOP%
- To insert the user's username in the retrieved file path, use %username%
- To insert the user's computername in the retrieved file path, use %computername%
- To insert the current date, use %date%

eg %MYDOCUMENTS%\Course Work - will find all files in a sub folder called 'Course Work' from the users 'My Documents' folder.

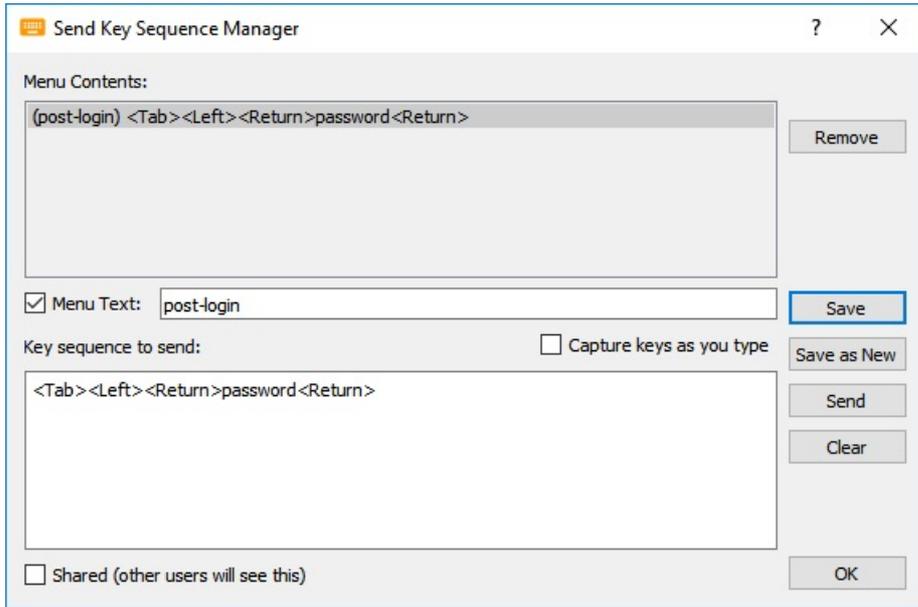
For the local folder, c:\work\%username%\%date%\ would put the file in c:\work\jbloggs\2018-02-19

Absolute paths (eg c:\temp, h:\English\Essays or /home/user/) can also be used.

Using AB Tutor

Key Sequence

This tool allows the Tutor to send a sequence of key presses to be carried out on the client. The **Key Sequence Manager** allows you to pre-define and save these sequences to the menu.



The list at the top shows any previously saved key sequences. These can be rearranged by dragging them in the list, or removed using the button to the right. To add a new entry to the list, simply start typing in the lower box. Normal printable keys will be captured by default, however if you want any special keys, such as alt, ctrl, shift, backspace etc to be picked up, tick the **Capture keys as you type** box. This will capture special keys as well. If you need to remove anything you've typed, untick the box before editing! Once you have finished a key sequence, you can optionally add a menu title text to the **Menu Text** box to make it easier to spot. **Save as New** will create a new menu entry from the current text, **Save** will overwrite the currently selected menu item with the modifications you've made.

If you need a pause during the key sequence (for example, to allow a dialogue box to open) you can do this using `<Wait:1000ms>` where the number is the time to pause for in milliseconds (ie, 1000ms = 1 second).

Modifier keys or combinations of keys can be sent by grouping them in angle brackets, eg: **<Ctrl+S>** for save, **<Alt+F4>** for close, **<Win>** for the Windows key.

If you are a console administrator you can tick the **Shared** box to allow other users to use that Sequence, however non-admin users won't be able to edit it. **Send** will immediately send the current text to the selected client(s), **Clear** will remove all text from the bottom pane.

To send a previously saved Key Sequence, click on the arrow next to the Key Sequences entry on the right pane, or go to **Command, Key Sequences >** and select it from the menu.

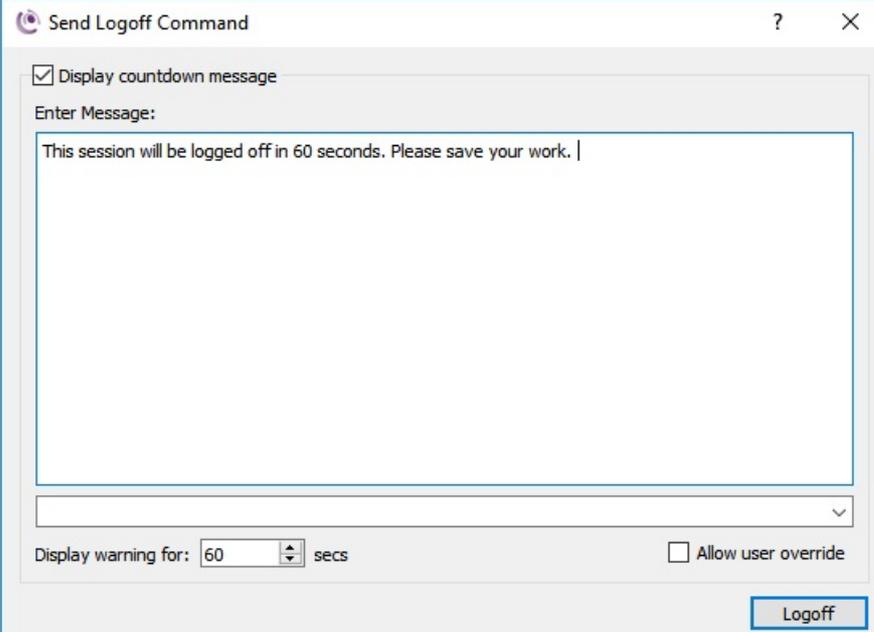
Using AB Tutor

Logon

This action opens a dialogue to fill in username, password and domain which sends a log on command to the selected clients, allowing a Console user to quickly and easily log a large number of computers on to the same account. This is most useful on sites where a generic username is used for all users.

Logoff

This action sends a logoff command to the selected clients. The dialogue which opens allows the Console user to display a warning message if they wish, with a timeout. Additionally, if **Allow user override** is selected, the Client user will be able to cancel the logoff before it happens, in case they are still using the computer. Previously used messages will be saved in the dropdown, but can be removed if required by selecting them, right clicking in the box and selecting **remove**



Send Logoff Command

Display countdown message

Enter Message:

This session will be logged off in 60 seconds. Please save your work. |

Display warning for: 60 secs

Allow user override

Logoff

Power on

Power on sends a wake on lan packet to the selected client(s), telling them to start up. This relies on the bios and operating system being configured correctly for wake on lan - for more information please see the [WoL troubleshooting](#) section.

Reboot

Reboot will tell the selected Client machine(s) to restart. When clicked, a dialogue box will appear with the same options as for **Logoff** above.

Shutdown

Shutdown will tell the selected Client machine(s) to power off. Again, when clicked a dialogue box similar to the **Reboot** and **Logoff** boxes will appear.

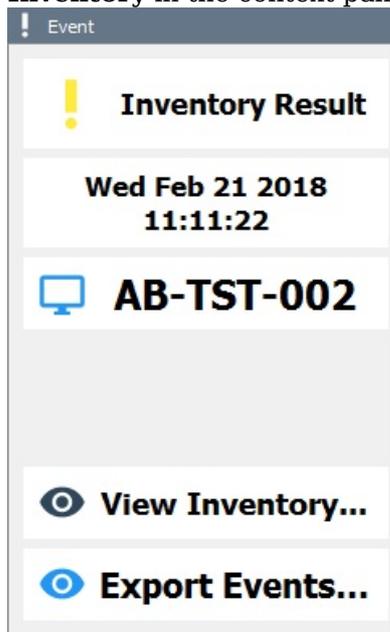
Using AB Tutor

Administrative Tools

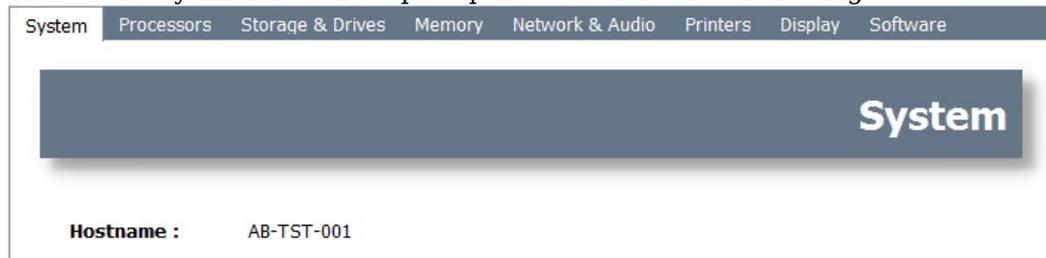
The admin tools give administrators access to some advanced functions for administering the remote machines. Admin tools will run against the currently selected computer(s), however **Services**, **Processes** and **Windows Event Log** can only be used on a single computer at a time. These tools will only show up for Console administrators.

Inventories

It is possible to view a detailed inventory of various hardware/software components for either a single computer or for multiple computers. Select the **Inventory** action to request inventory information from the selected Clients. This will then return as an event. To view the inventory, select the relevant event(s) and then select **View Inventory** in the context panel.



The inventory information is split up into tabs for ease of viewing:



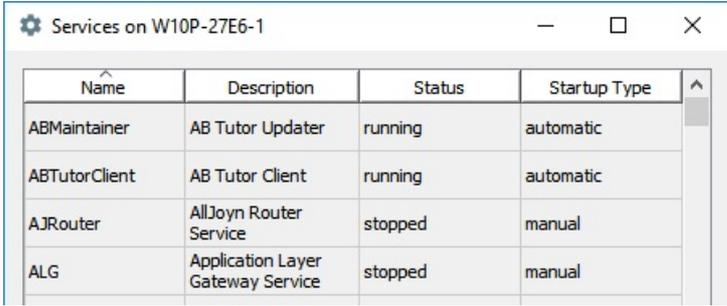
If required, the inventory information can be exported as an html file, allowing it to be viewed in external software.

If multiple computers have been selected, you can select **Compare Inventories** in the context bar. The inventories will be displayed simultaneously in multiple columns allowing direct comparisons to be made. Historical inventories can be viewed in exactly the same way, via the [Log file viewer](#).

Services

This tool will show all the services running on a Client - it can only be used on one Client at a time. If you have multiple Clients selected in the Main window, then the **Services** option will be disabled. When selected, a popup window will open, showing a list of current services and their statuses.

You can use this tool to start, stop and re-start remote services. Right-click on any service to show a menu with the commands you are able to issue.



The screenshot shows a window titled "Services on W10P-27E6-1" with a table of services. The table has four columns: Name, Description, Status, and Startup Type. The services listed are ABMaintainer, ABTutorClient, AJRouter, and ALG.

Name	Description	Status	Startup Type
ABMaintainer	AB Tutor Updater	running	automatic
ABTutorClient	AB Tutor Client	running	automatic
AJRouter	AllJoyn Router Service	stopped	manual
ALG	Application Layer Gateway Service	stopped	manual

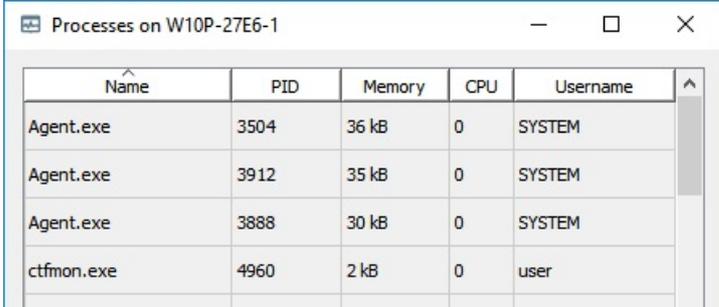
Click on the column headings to sort the list alphanumerically by that column.

Processes

This tool allows you to view all processes running on a Client and can only be used on one Client at a time. If you have multiple Clients selected in the Main window, then the **Processes** tool will be disabled. As with services, when selected, a popup window will show open, showing a list of running processes and the associated details.

If you want to forcibly end a remote process, right-click on the process to end and select **Terminate this process**.

 If you are killing a remote application then it will terminate it immediately and not prompt the user to save any work.

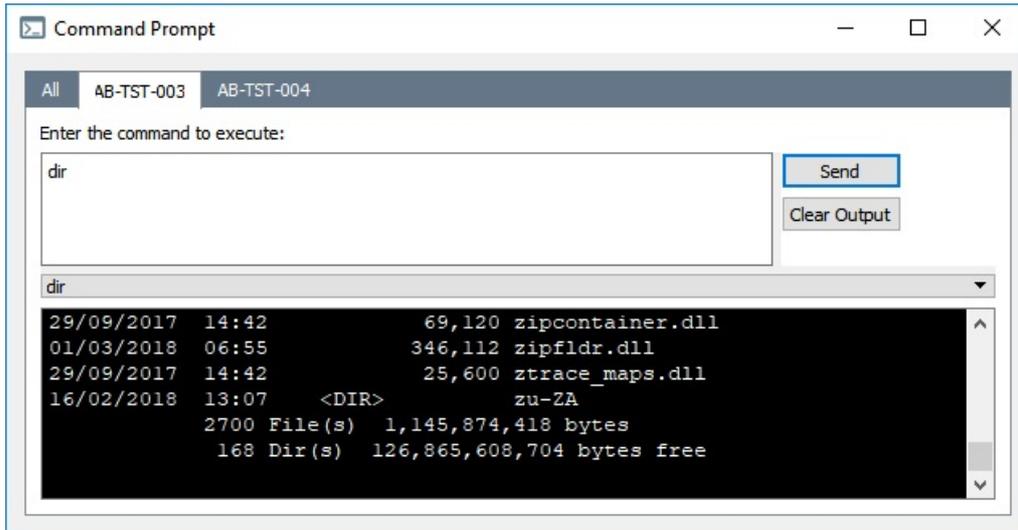


Name	PID	Memory	CPU	Username
Agent.exe	3504	36 kB	0	SYSTEM
Agent.exe	3912	35 kB	0	SYSTEM
Agent.exe	3888	30 kB	0	SYSTEM
ctfmon.exe	4960	2 kB	0	user

Click on the column headings to sort the list alphanumerically by that column.

Command prompt

This option allows command line instructions to be sent to the client machine. For Windows, this command allows you to send DOS based commands to one or more selected remote machines, and Bash commands for Mac clients.



To send a command, select one or more computers on the Main window and select the **Command Prompt** command. A popup window will open, showing a tab for each computer, and an **All** tab. Commands entered in the **All** tab will be sent to all the clients, however no output will be shown. The output can be viewed, and commands sent to individual computers, by going to the relevant tab. Multiple commands can be entered by pressing return to get to the next line - commands will be executed in sequence top to bottom and one per line when the **Send** button is pressed.

A history of previously sent commands is stored and can be retrieved from the drop-down list. Entries can be removed from the list by selecting them, then right clicking and selecting **Remove**.

Windows Event Log

This command will open the Windows Event Log Viewer on the Tutor machine and display the logs from the selected Client. Please note that the Windows Event Log Viewer can take a while to open - if you click the button again, it will open multiple copies. Note that for this to work, you need to be sharing a domain with that computer and have access to open its logs.

Using AB Tutor

Policies

Policies are generally restrictions or logging options which can be applied to a remote client. They allow a Policy User to apply ongoing commands to the clients, as opposed to manual commands that run once and then end. They can be always active, set to trigger on a schedule or based on network connections and to automatically remove themselves after a set time period.

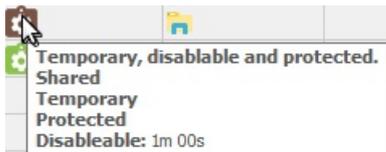
Policies can be applied to various different targets:

-  **Sessions:** This is the simplest application of a policy. The policy will take effect on the session and disappear when the user logs off.
-  **Device:** If a policy is applied to a device, it will affect any user that logs in on it. It will stay on that device until it expires or is removed.
-  **User:** If a policy is applied to a user, it will affect that user on any computer they log in on. It will stay applied to that user until it expires or is removed. When the user logs off a device, the policy will stop affecting that device.
-  **Group:** If a policy is applied to a group, it will affect all devices/users which are members of that group. If a device joins the group (eg because it gets added by an admin or because it's a group of users and one of the relevant users logs in on it) the policy will immediately take effect.
-  **Default Device:** If a policy is set as a default device policy, it will be automatically applied to all Clients registered with the Central Server. This will always be applied.
-  **Default Session:** If a policy is set as a default session policy, it will automatically apply when any user logs in to any Client. It will be automatically removed when the user logs off.

The overlaid icon in the bottom right of the policy icon shows why that policy is applied to the Client (eg, whether it's come from a group, is a default policy etc). If no overlay is shown, it was applied in the current view (ie Device, Session, User).

If you hover the mouse over an applied policy icon, a popup 'tool-tip' will be displayed showing:

- The policy's name
- Why the policy is applied (eg, from a group, the user etc)
- Who owns the policy, or **Shared** if it's a public one
- The time remaining on the policy if it's temporary
- If the policy is protected
- If the policy is disableable, and if so how long for
- If the policy is disabled, and if so how long remains



The policy icons will be displayed in several places. On the **List View** the Policies column shows all policies applied to that Client. In **Thumbnail View**, you can get the Client information popup by hovering the mouse over a client, clicking to select it or by clicking the **Expanded View** button at the bottom of the main panel. Finally, when one or more Clients are selected, all policies applied to those Clients will be shown under the thumbnail at the top of the Context Panel.

The List view has a **Policies** column which will display the icons of any policies applied to the relevant machine. In the Thumbnail view, these icons are shown on the pop up information box when the thumbnail is selected or the hovered over with the mouse. They are also shown under the thumbnail at the top of the Context Panel when a Client is selected.

To apply a policy to a Device, User or Session, simply drag the policy from the **Policies** panel onto the Client in question. If multiple Clients are selected and a policy is dragged onto one of those Clients, the policy will be applied to all selected Clients. To apply a policy to a group, a Console Admin can open the group properties menu, select Default Policies and add from there. To add as a **Device Default** or **Session Default** policy, a Console Admin can right click on **All Items** and select which type of default policy they wish to apply.

 Any Console User with the **Policy User** role can apply and remove policies, unless they are protected in which case they need the **Console Administrator** role.

If a policy was set as **Disableable** during creation, when a user right clicks on it they will have the option to disable it. This deactivates it temporarily, but it will reactivate automatically after the set time. This allows

teachers to remove a policy during a lesson but they don't need to worry about reapplying them afterwards.

If a policy has been set as **Protected** during creation, Console Users won't be able to remove it. It can only be applied or removed by Console Admins.

To remove a policy from a client, right click on its icon (in any location) and select **Remove Policy**. If multiple Clients are selected, and **Remove Policy** is selected from the Context Panel, the policy will be removed from all selected clients.

 Note that policies that are applied via a group or as default policies can't be removed like this - they must be removed through the group properties menu.

 The **Policy User** role is also required to remove policies. The **Console Administrator** role is required to remove protected policies.

Creating policies

Private Policies can be created by any user with the **Policy Creator** role. These policies are only available to the user who created them, but when applied can be removed by other users. **Shared Policies** can only be created by **Console Admins**, however once created (if not protected) they can be applied and removed by any **Policy User**. This allows an admin to create policies in advance for other users to use.

Conditions and Effects tab

To create a policy, right click on the folder you wish to add it to (Private or Shared). This will open the following window:

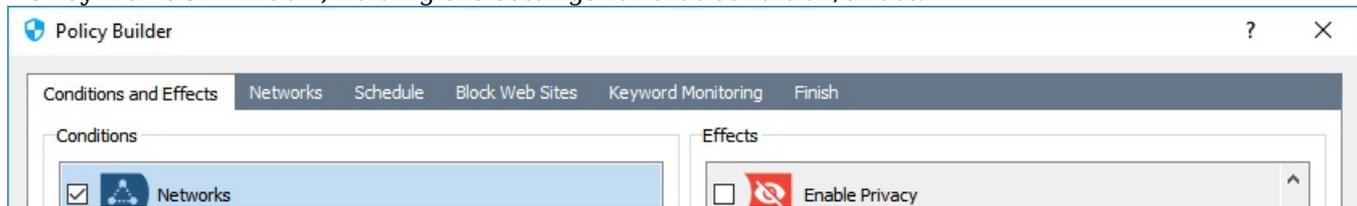


From here, three types of setting are available:

- **Conditions** affect when the policy is active or inactive. This could be based on a schedule or what network the Client is on.
- **Effects** are the rules that are applied to the Client, or commands which will be triggered.
- **Device Only Effects** are rules which can only apply to devices, not to sessions or users (for example, a session or user can't be shut down, but the device they are on can be). If you try to apply one of these to a session or user it will be applied as normal, but be aware that it will affect any other users on that device as well.

Multiple conditions and effects can be applied in a single policy. If multiple conditions are applied, they must all be

"true" in order for the policy to be active. Most conditions and effects will add additional tabs at the top of the **Policy Builder** window, holding the settings for that condition/effect.



Clicking the **Next** button at the bottom of the window will progress through the tabs in order.

For more information on any of the conditions or effects, please see the appropriate page.

Finish tab

The final tab allows the basic settings of the policy to be configured:

- **Policy Name** allows you to give the policy an identifying name. The name is entirely cosmetic, so it doesn't affect the workings of the policy, but it allows it to be identified in the list, or when applied to a Client.
- **Icon** options allow the displayed icon for the policy to be altered. A colour can be chosen from the dropdown and an icon from the list. The **Preview** will show what the policy icon will look like.
- **How long...** allows you to choose whether the policy is applied permanently, or whether it will be automatically removed after the set amount of time. This is separate from the schedule **condition**, so a policy could be set to activate between 8 and 3 in the schedule, but be removed after 10 days in the specified time.
- **Share this policy...** is an admin only option which sets whether the policy can be seen and used by other users. With the option here, you can move a policy from the private list to the shared list or vice versa without having to recreate it.
- **Can be disabled** sets the policy to be disableable, meaning a Console User can temporarily deactivate it. The policy can be set to **automatically re-enable** after a set amount of time, or **when user logs off**, so if one a policy is disabled for one user, it will put the policies back to normal when they're done.
- **Protected Policy** is an admin only option which prevents non-admins from applying or removing the policy. If it's shared, it will also be hidden from non-admins.

Exporting and importing policies

Users can export any policy they can see as a json file. These files can then be imported as a private policy by any

user with the **Policy Creator** role, or as a shared policy by a **Console Admin**. To export a policy, right click on it in the policies panel and select **Export**, to import a policy, right click on **Private Policies** or **Shared Policies** in the policies panel and select **Import**. This will open the policy creation wizard, with the imported policy settings shown, allowing any required changes to be made before the policy is created.

Using AB Tutor

Policy Conditions

Network restrictions

If you chose to have a **Networks** condition, you will get the following tab:



Specify applicable networks for this policy.

Active when any of the following conditions are met
 Inactive when any of the following conditions are met

Connected subnet:

192.168.1.0/24	Add
	Remove

Or network disconnected

This allows you to choose which subnets the policy will be active on. The client will use its current IP address to decide whether the policy should be active, so you could make a policy that's only active when the computer is on the school network, or only active when the computer is **not** on a specific network.

To set a network restriction, first choose whether you are entering the address ranges where the policy is to be active, or where it is to be inactive. Then click **Add** and enter the IP address range you wish to monitor for. As shown in the explanation text, you can define a range using wildcards, such as 198.51.100.* or using /n subnet notation, eg 192.0.2.0/24.

Finally, you can also add the case where the adapter is disconnected to the list by ticking the box at the bottom. This allows you to set a client machine to automatically lock when the network cable is unplugged, for example.

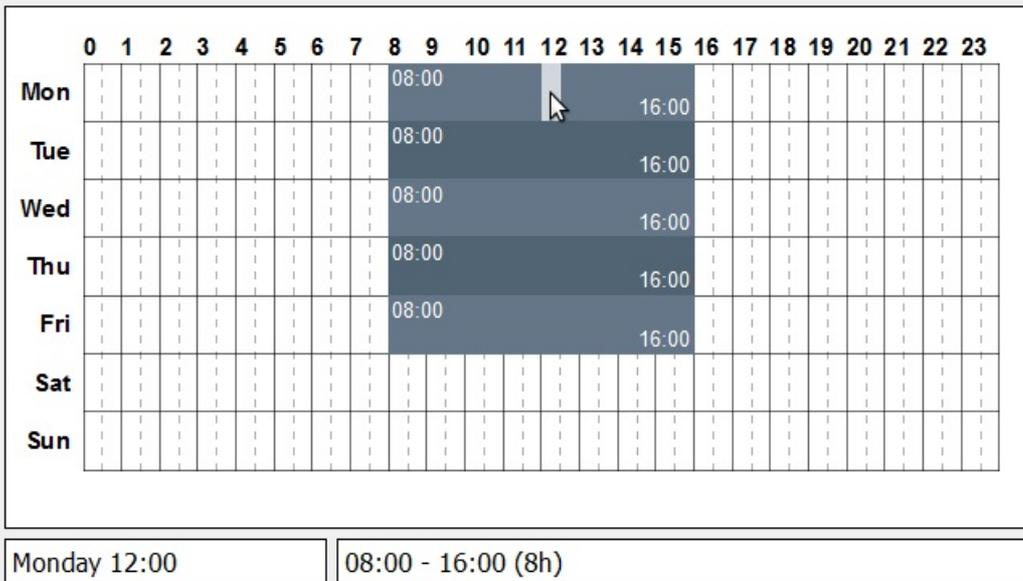
Schedule

If you choose the Schedule condition, you will be given a tab with the schedule editor:



Schedule

When do you want this policy active?



Click and drag to set the policy to be active/inactive in half hour chunks. If you want to set the time slots more accurately, you can drag the ends of the time blocks or right click on a block and select **edit** to enter the times manually. The dark areas are when the policy will be active - in the example above, the policy is active between 8 and 4 on weekdays.

 The time under the cursor will be displayed in the bottom left and if the cursor is over a block, the start time, end time and duration of the current block will be displayed bottom right.

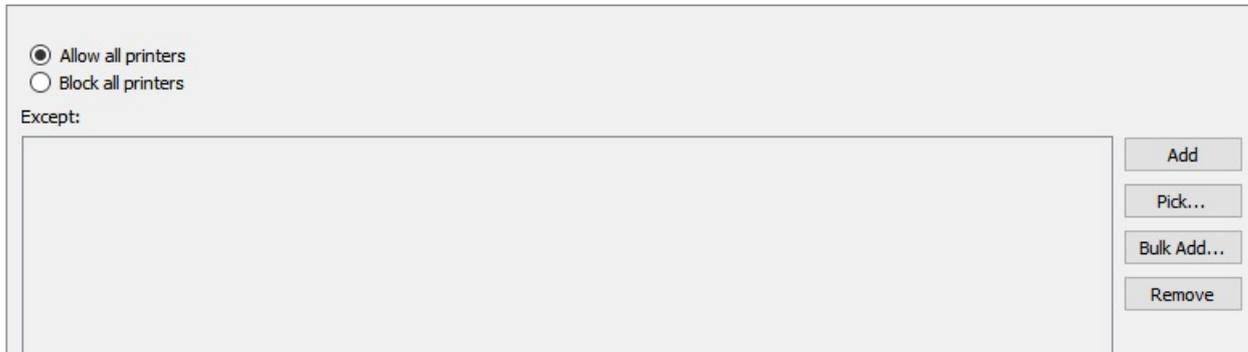
SSID restriction

The SSID restriction is very similar to the Network Restriction, however it acts on the name of the wireless network the Client is connected to, allowing you to configure different policies to be active on different wireless networks. Like networks, you can choose whether the policy is active just on that network, or whenever it's **not** on that network.

Using AB Tutor

Policies - Effects

Block Access to Printers

A screenshot of a policy configuration window. At the top left, there are two radio buttons: "Allow all printers" (selected) and "Block all printers". Below this is a label "Except:" followed by a large empty text area. To the right of the text area are four buttons: "Add", "Pick...", "Bulk Add...", and "Remove".

This policy allows you to control printing from remote machines. You have the option to **Allow all printers**, except ones you specify, or to **Block all printers** except those that you list.

Printers can be added manually by clicking **Add** and typing the name in, with support for wildcards (eg "*Dell*") or by clicking **Pick** and choosing from a list of printers registered on that computer. **Bulk Add** allows a list to be pasted in easily, with one printer name on each line. Again, wildcards are fully supported. Finally, the **Remove** button can be used to delete entries from the list.

Using AB Tutor

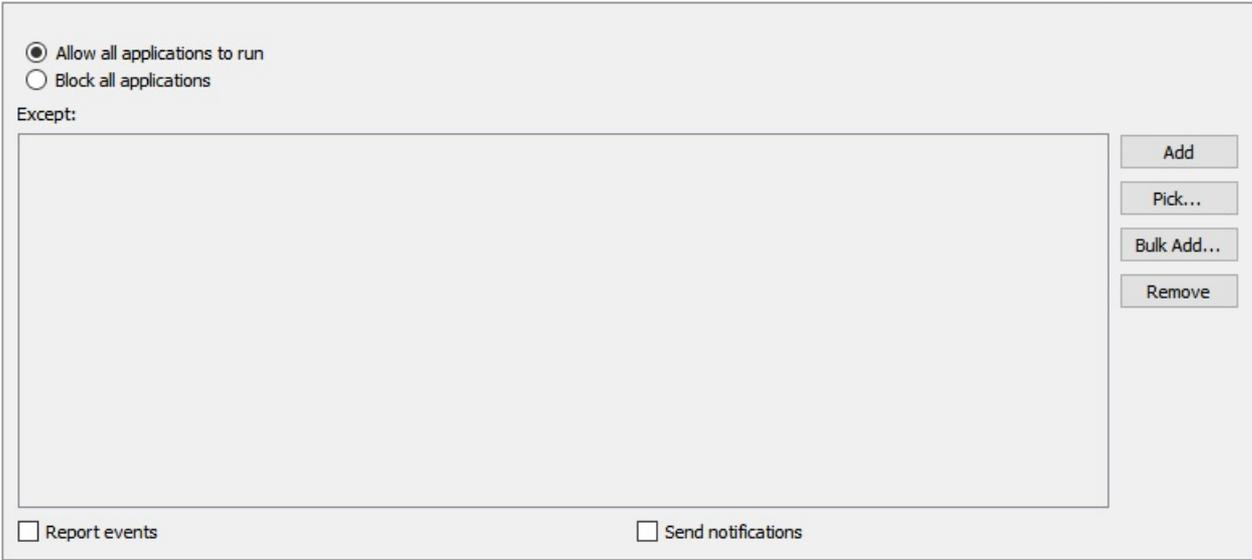
Policies

Block Applications

This allows you to restrict access to one or more applications on the student's machine. You can block/allow an application by giving its full file name or by specifying its window title and/or folder.

 If you apply an application blocking policy to a remote machine and the application you wish to block is already running, then the application will be closed **without** saving any changes.

Block Applications



Allow all applications to run
 Block all applications

Except:

Report events Send notifications

- Start by setting whether you want to **Allow All applications to run** or **Block All applications** apart from your exceptions
- To block by full filename:
 - Press the **Pick** button
 - Browse to and select the program you would like to block
 -  If the program to be blocked does not exist on your machine but does on the student's machine, then simply type the application's file name in the File name box and press Open or add the full path using **Add**.
 - The application's name is added to the list of **Exceptions**
 - Repeat the Add process if you wish to block/allow multiple applications
- To add an exception by matching against the filename or titlebar text using wildcards:
 - Press **Add** to create a new list entry.
 - Enter the text you want to check for. Use wildcards to search for parts of the title or folder. The text is case insensitive so both `*solitaire*` and `*Solitaire*` will work.
 - `*Microsoft Word*` Filters for Microsoft Word
 - `*Solitaire*` Filters for the Solitaire application
 - `F:*` Filters for any application run from the F Drive
 - `*\Microsoft Office*` Filters for all applications located in any `\Microsoft Office\...` folders
 - Multiple Title/Path blocks can be added at once using the **Bulk Add** option, allowing an external list to be pasted in. These are parsed in the same way as individually added ones.
-  Application blocking also includes support for Regular Expressions (regex). This is an extremely powerful tool for creating rules. Any line item which is enclosed in forward slashes (`/`) will be treated as a regex.

Some example rules (this is not by any means an exhaustive list):

- `.` matches any single character.
- `*` matches zero or more of the previous character, eg `.*` matches anything. This is useful for padding the ends of a term, like `*` in standard rules. `ab*` would match "ab", "abb", etc and also "a".
- `+` matches one or more instance of the previous character, eg `ab+` would match with "ab", "abb", "abbb", etc but not "a".

- **[abcd]** will match any single a, b, c or d character. eg **a[bc]d** would match "abd" and "acd"
- **[0-9]** will match any single numerical character.
- **[^a]** specifies any character other than **a**

For example, **/.*setup7[12][29]a+ /** would match foosetup712a, setup719aa, barsetup722aaaaa, but not setup722.

Regex support is not provided by ABT technical support, however there are guides available on the internet.

 Take great care when blocking applications (especially if you are using wildcards) as you may inadvertently block an essential application.

e.g. if you specify ***word*** then applications like **wordart.exe** or any application with **word** in its path name (c:\program files**swordfish**\main.exe) will be blocked.

If **Report Events** is ticked, any applications closed under this policy will be shown in the **Events log**. If **Send Notifications** is ticked as well, those events will be shown in the **Events Panel** at the bottom of the main window on any Console which can see that Client.

Using AB Tutor

Policies

Block Web Sites

This policy allows you to restrict access to one or more web sites. You can block or allow in general and then create a list of exceptions:

A screenshot of the "Block Web Sites" configuration window. At the top, there are two radio buttons: "Allow access to All sites" (selected) and "Block access to All sites". Below this is a large text area labeled "Except:" for listing exceptions. To the right of this area are four buttons: "Add", "Bulk Add...", "Remove", and "Import...". At the bottom of the window, there are three checkboxes: "Report events", "Email on violation", and "Send notification".

- Choose whether to **Allow access to all sites** or **Block access to all sites** apart from your exceptions
- To create the exceptions press the **Add...** button.
- Enter the web address of the site to be an exception (ie, blocked if all are allowed or allowed if all are blocked).
- Press **OK** to confirm.
- Repeat to add multiple web addresses.

 Wildcards can be used to pick up web addresses that contain certain words (e.g. *sex* will block web addresses that contain the word 'sex', including ones like 'Sussex').

We recommend using wildcards when blocking web sites to catch all possible urls that could point to the site. (e.g. *.youtube.* will block www.youtube.com **and** uk.youtube.com **and** www.youtube.co.uk etc.). You can also block file downloads by specifying the file extensions to block. (e.g. *.exe or *.zip will stop the user from downloading these file types.)

Bulk Add allows a list to be pasted in, with one entry per line.

Alternatively, instead of manually adding the addresses, press the **Import...** button and select a csv file located on your hard drive that contains a list of web sites to add.

 If the web site is secure (e.g. **https://www.xyz.com**) you can only block the domain as a whole, and can't block individual pages since the url itself gets encrypted before it leaves the web browser.

Please be aware that there are websites on the internet that allow users to bypass any web address filtering. This is called 'Proxy Tunneling'. Students can use these sites to enter banned web addresses and then browse them freely. This can be defeated by adding the proxy sites to the blocklist or through whitelisting.

 Web site blocking also includes support for Regular Expressions (regex). This is an extremely powerful tool for creating rules. Any line item which is enclosed in forward slashes (/) will be treated as a regex.

Some example rules (this is not by any means an exhaustive list):

- . matches any single character.
- * matches zero or more of the previous character, eg .* matches anything. This is useful for padding the ends of a term, like * in standard rules.
- + matches one or more of the previous character.
- [abcd] will match any single a, b, c or d character.
- [0-9] will match any single numerical character.

- **[^a]** specifies any character other than **a**

For example, `/.*setup7[12][29]a+/` would match `foosetup712a`, `setup719aa`, `barsetup722aaaaa`, but not `setup722`.

Regex support is not provided by ABT technical support, however there are guides available on the internet.

If **Report Events** is ticked, any applications closed under this policy will be shown in the **Events log**. If **Send Notifications** is ticked as well, those events will be shown in the **Events Panel** at the bottom of the main window on any Console which can see that Client.

If **Email on violation** is ticked, the email address configured on the Central Server will be emailed whenever a Client tries to access a blocked site. If used with a whitelist, this can lead to an enormous number of hits, due to Windows frequently contacting Microsoft's servers, however with a relatively small blacklist it can be useful. Note that multiple policies can be applied, one with a short list and email turned on, another with a more complete list and email turned off.

Using AB Tutor

Policies

Enable Logging

This policy allows you to enable logging of specific activities.

Enable Logging

- Log Applications used
- Log Web sites visited
- Log Printer activity
- Log Keyboard activity
- Only log visible characters (Ignores keys like F1, Delete, Return etc.)

- **Log Applications used** - This will log all applications run on the remote machines. It logs the date, time, filename and the application's title.
- **Log Web sites visited** - This logs each unique URL visited using any web browser or other application, including Windows contacting Microsoft.
- **Log Printer Activity** - This logs any files printed, their file names and the computers from which the printing was sent.
- **Log Keyboard Activity** - This logs all keystrokes typed on a remote machine.

Select **Only log visible characters** if you do not want to log non-visible keys pressed by the user (e.g. <BACKSPACE><F1><DELETE><UP><RIGHT> etc)

(See [Viewing Log Files](#))

Using AB Tutor

Policies

Enable Privacy

This policy allows you to indicate to the remote user that the AB Client program is running and that a Console User is watching. If this policy is set on the remote machine, then a small icon is displayed in the user's System Tray (Windows bottom right or macOS top right).



Require User's permission to Watch their session

Privacy policies can also be created such that the Client User has to give permission for a Console User to Watch them. This is done by right clicking on the AB Tutor icon in the Tray and unselecting **Enable Privacy**. Once this is unselected, Console Users will be able to watch and take control as normal. This allows AB Tutor to be used as a support tool, but still reassure Client Users that they aren't being watched without their knowledge. If this option is set, the policy will default to block Watching. The privacy policy will also block thumbnails, snapshots and captures.

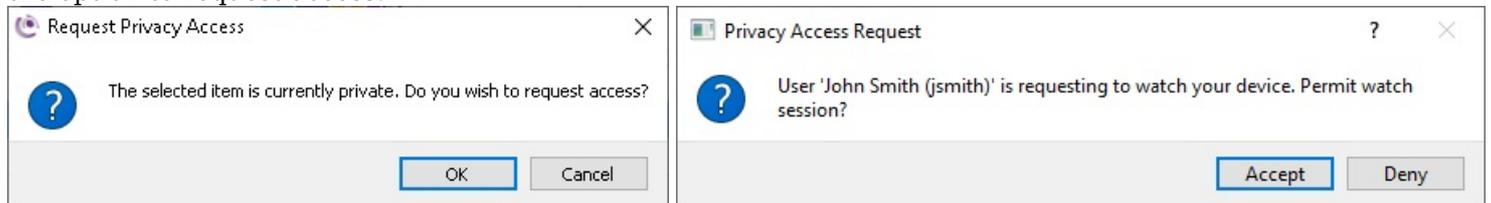
There are 3 states the Tray icon can take:

 A privacy policy is applied, but this Client can be Watched. This is either because the User has allowed Watching or because they only get notifications and can't block.

 This Client is currently being watched.

 This Client cannot be watched.

If a Console user tries to watch a client with an active privacy policy which requires permission, they will be given the option to request access:



If the Client user accepts the request, the Console user will be able to view them as normal.

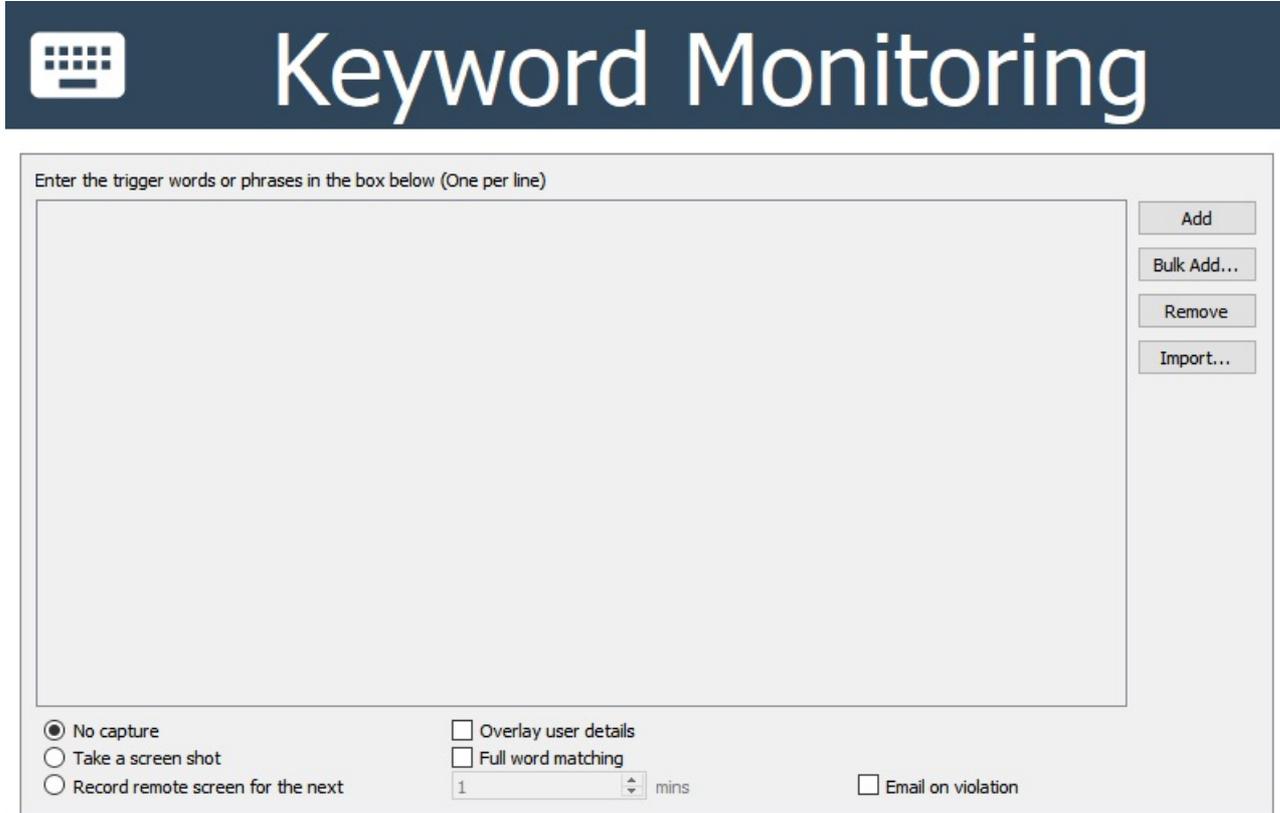
 Clients with an active privacy policy will never display their thumbnail in grid view, even if they have allowed access

Using AB Tutor

Policies

Keyword Monitoring

With keyword monitoring, you can specify a set of words which will trigger a tutor notification and optionally either take a screen shot or record a video when the keyword gets typed.



Enter the trigger words or phrases in the box below (One per line)

Add
Bulk Add...
Remove
Import...

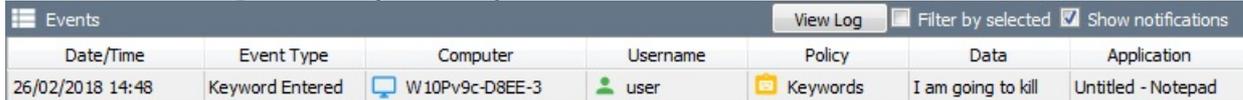
No capture
 Take a screen shot
 Record remote screen for the next

Overlay user details
 Full word matching

1 mins

Email on violation

To configure a keyword monitoring policy effect, enter the trigger words in the main list, one word/phrase per line, using add/bulk add as usual. **Import** allows a csv of words to be added as well. You can also choose what media is collected - **No Capture** will just notify connected Consoles with the basic information about the event:



Date/Time	Event Type	Computer	Username	Policy	Data	Application
26/02/2018 14:48	Keyword Entered	W 10Pv9c-D8EE-3	user	Keywords	I am going to kill	Untitled - Notepad

Screenshot will take a single still image when the keyword is detected and **Capture** will record video for the set time, after the keyword is typed. **Overlay user details** will stamp the top corner of the screenshot/video with the username and computername. **Full word matching** will only trigger on full words - for example if a monitoring policy is set for the word "kill", normally the policy would trigger if the user typed "skill", however with **Full word matching** turned on, this would be ignored. You can also use wild cards, eg "kill*" would trigger on "kill", "killer", "killing" and "killed", but not "skill" or "skillful". Finally, the **Email on violation** option tells the system to send an email with the details of the violation to the address configured in the [Central Server config](#).

If a keyword is entered, the Client will not do anything visible to the user, as there are many cases where a user might be typing in a word on the list (for example, they might type "kill" while writing an essay on war, or because they are threatening a classmate) - it is up to the Console user to decide if any action needs to be taken.

Using AB Tutor

Policies

Launch action

This policy allows you to launch programs on the client machine, running in the currently logged on user's session, and as the current user. It works in the same way as the Launch Action in the right panel, however as a policy it can be triggered on a schedule or other conditions, rather than just manually.

Launch Action

Launch Options	
Repeat every (minutes):	<input type="text" value="30"/>
Enter the application (including path) to launch on the remote client(s):	<input type="text" value="cmd.exe"/>
Program parameters:	<input type="text"/>

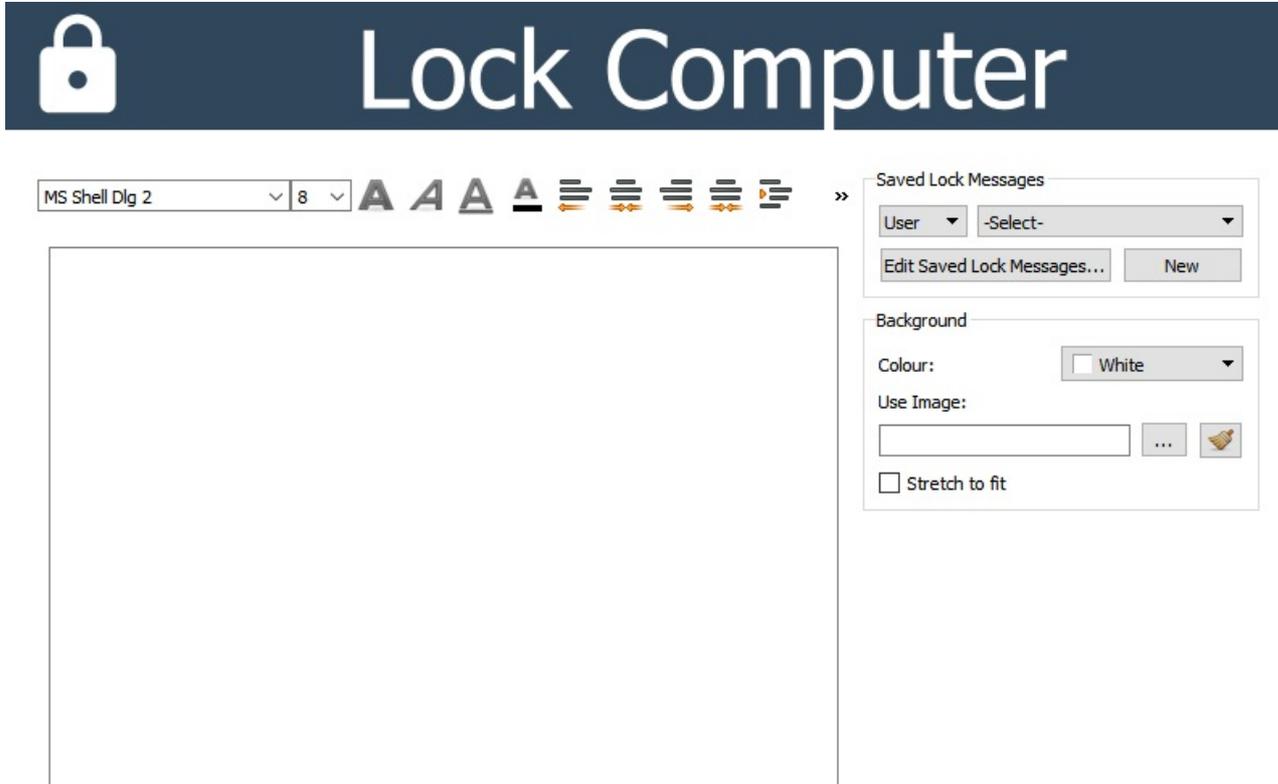
If you only wish the launch to be triggered once, ensure the time in **Repeat every...** is longer than the duration the policy is set to be applied for.

Using AB Tutor

Policies

Lock Computer Policy

This policy locks the Client session, preventing mouse/keyboard input and displaying a message, with optional picture. Applying a lock policy is equivalent to clicking the lock button on the Toolbar, however having them as a policy allows them to be applied based on a schedule, or on network events, such as when the network cable is unplugged.



You can choose a pre-existing lock screen message from the dropdown, or customise the message using the controls. This uses the same interface as the **Lock Messages** option in the **Lock** button dropdown.

The left hand pane allows for the text of the lock message to be edited, including text size, colour and alignment. On the right, you can select the background colour or image and save it to the list. The list is shared between the **Lock** dropdown and the lock policy. A Console Admin can save to the shared **Global** list or their private **User** list - a normal user can only save to their private list. Note that if a lock message is edited after a policy has been created, the message in that policy will NOT be updated.

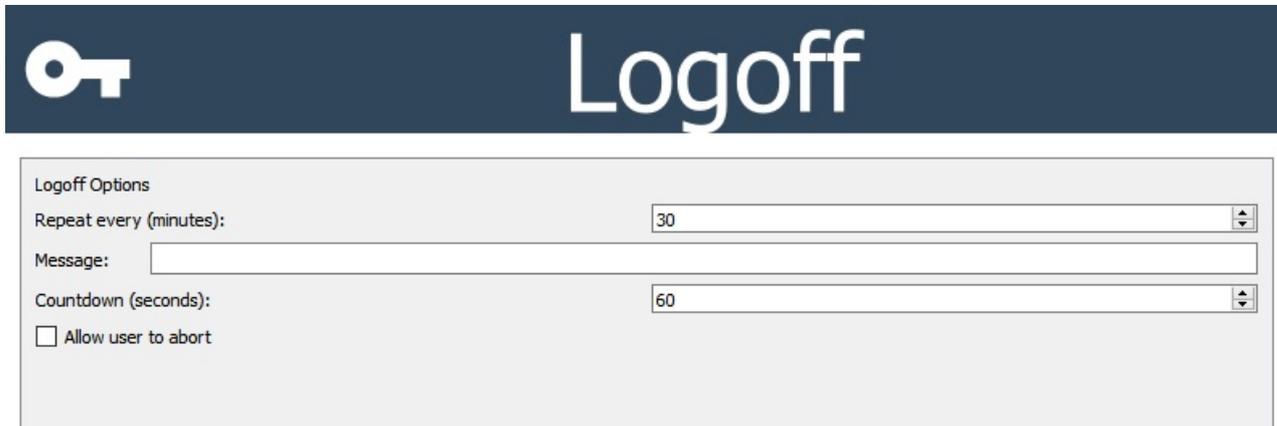
If the student forces the machine to reboot by pulling the power cable, then when the system starts up again this policy will activate and lock the screen, keyboard and mouse again.

Using AB Tutor

Policies

Logoff Policy

This policy logs off the Client session in the same way as if the logoff button on the Actions panel was clicked, however applying it as a policy allows it to be triggered based on a schedule, or on network events, allowing sessions to be automatically logged off at the end of the day.



The image shows a configuration window titled "Logoff" with a key icon. The window contains the following fields:

- Logoff Options**
- Repeat every (minutes):** A dropdown menu with the value "30" selected.
- Message:** An empty text input field.
- Countdown (seconds):** A dropdown menu with the value "60" selected.
- Allow user to abort**

Using the **Repeat every** option, you can allow a user to continue using a computer whilst they're at it, but have it log off automatically after they leave it. This option will try to logoff every n minutes as set, until the logoff happens.

If a **Message** and **Countdown** are set, the user will see a warning message when the logoff triggers, giving them time to save their work or abort the logoff. **Allow user to abort** gives a cancel button which will stop the logoff from happening, but it will trigger again after the **Repeat every** time. If you wish it to only try once, either apply it as a temporary policy with a time set to less than the **Repeat every** time, or set a **Schedule**, with the activation time shorter than the **Repeat every** time.

Using AB Tutor

Policies

Registry Control Policy

The Registry Policy allows certain tweaks to be pushed out from AB. This policy is intended to allow some of the control given through Active Directory Group Policy to smaller sites which don't have full domain setups. This policy is intended for more advanced users as it is quite easy to cause unexpected effects.

 Not all tweaks will work on all Windows versions. We recommend that you test them before deployment.



Microsoft Windows Registry Control (Advanced)

Set/clear the required restrictions from the list below.

- >  Active Desktop
- >  Control Panel
- >  Desktop
- >  Start menu and Taskbar
- >  Login and Authentication
- >  Network
- >  Privacy
- >  File System
- >  General Security
- >  Internet Explorer

Using AB Tutor

Policies

Mute Sound

This policy allows you to mute the sound on Clients. There are no additional options in the policy creation page for this policy - the Clients will either be muted or not. Since there are no additional options, no options page is shown for this effect.

Using AB Tutor

Policies

Request user's name

The request name policy allows AB Tutor to be set to always request a name from a Client User as soon as they log in. This is equivalent to using the **Request Name** button on the Context Panel. There are no additional options for this effect, so no extra page will be shown.

Using AB Tutor

Policies

Screen Capture

By setting a screen capture policy on a remote machine, you can record the on screen activity of that computer.



Capture Options

Rate:

Split video every (mins):

Add user and time details to video

Rate: Select the rate of video capture - you can set this to run from one frame per second to as rarely as one frame a minute. The option you choose will depend on what you wish to use the video for. If you wish to just monitor remote usage, then you can set the rate to, say, 1 frame every 30 seconds. This will be enough to get an overview of what that user has been doing throughout the lesson and will keep the capture file size relatively small.

Split video every: If the policy is set (by the policy duration) to run for a long time, it can be convenient to split the recorded video up into chunks. This option allows for the length of each chunk to be set. For example, if a policy is applied for 1 hour with **Split video** set to 10 minutes, 6 videos will be produced, each 10 minutes long.

You also have the option to add the user details, date and time to the video. This will be printed in the top right-hand corner of the video.

 We recommend against recording large quantities of video as it will quickly fill up the central server, due to the size of the video files. This policy is intended for use in short bursts! Captured videos can be exported from the log file viewer, as webm files.

Using AB Tutor

Policies

Traffic Light Policy

The Traffic Light policy displays a traffic light icon in the system tray on the client computer. When the user right clicks on it, a menu will be displayed, giving a choice of red, yellow, green or clear. When a colour is selected, a traffic light icon will be shown in the appropriate colour in the Notifications area on the Console. If the student left clicks on the traffic light, it will cycle through the colours without showing the menu.



This policy allows students to give instant, simple feedback to their teacher and gives the teacher a feel for how the lesson is going. A typical use for this would be for students to set their light to red if they don't understand, to yellow if they're struggling and to green if they're fine, however a teacher can of course define the colours however they wish.

There are no policy specific options for the Traffic Lights, so no additional tab will be shown in the policy creation dialogue.

Once a student has picked a colour, the Console User can reset it (back to grey/no colour) by right clicking on the traffic light icon and selecting **Reset Traffic Light**.

Using AB Tutor

Policies

Block Access to USB, CD, DVD Drives

This policy allows you to completely disable access to USB and/or CD/DVD drives. Simply tick the types of drive you wish to block. Note that this is a Device Effect and so will affect all users on that computer.

Block Access to USB,CD,DVD Drives

- Disable ALL USB Drives
- Disable ALL CD/DVD Drives

Using AB Tutor

Policies

Block internet access by port number

This policy allows you to block internet access by port, rather than by domain. This allows specific protocols to be blocked, whilst allowing others through. Note that this is a Device Effect and so will affect all users on that computer.



Block Internet Access

Block Access to the Internet by all Web Browsers (Port 80,443)

Block Access to the Internet by all Web Browsers (Port 25,110,465)

Block Access to the Internet by all Web Browsers (Port 21)

Block the following ports:

Using AB Tutor

Policies

Command icon

This policy allows commands to be launched in the background as the system user. This is intended for maintenance tasks which need full access to the computer, as opposed to actions performed by a teacher during a lesson. It will not create any windows in the GUI and so should be entirely self contained command line entries. It works in the same way as the [Command Prompt](#), however as it is a policy it can be triggered on a schedule or other conditions.

If you want a command to run for the current user, in their GUI session, use the [Launch action](#).



Launch Options	
Repeat every (minutes):	<input type="text" value="30"/>
Enter the application (including path) to launch on the remote client(s):	<input type="text" value="cmd.exe"/>
Program parameters:	<input type="text"/>

Using AB Tutor

Policies

Enable Logging

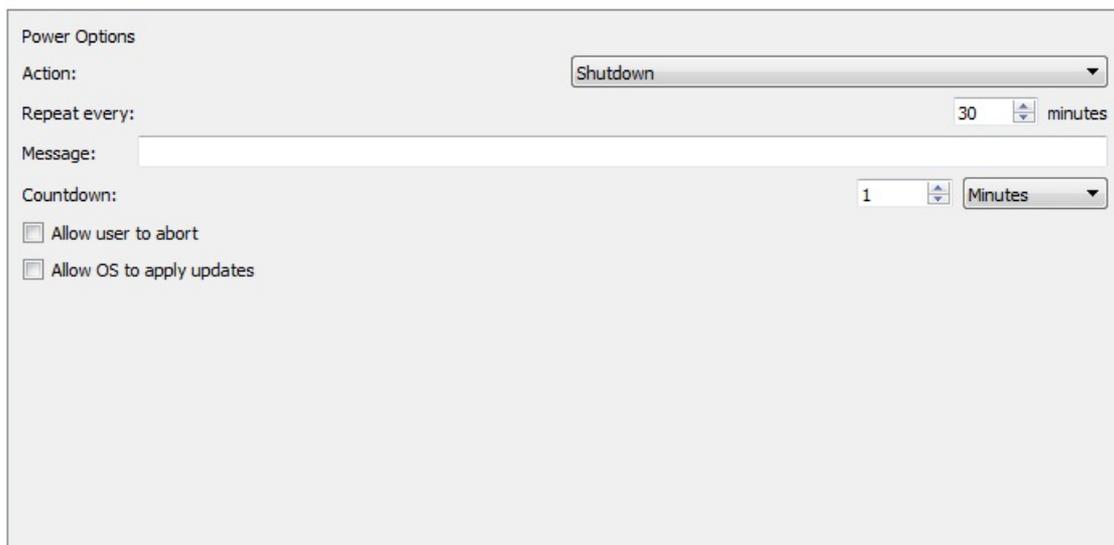
This Effect allows you to log which users have been using a Client machine. This is a Device Only Effect, meaning it can't be applied to Users or Sessions. If applied, a note will be made in the logs on the Central Server whenever a user logs on or off this computer. There are no additional options available for this Effect.

Using AB Tutor

Policies

Power Action

The Power Action Effects allow computers to be shut down or rebooted according to the rules of the policy - for example, turning all the computers on the site off at 5PM. This is equivalent to using the controls in the action panel, however the policy allows them to be automatically applied on certain criteria, such as a schedule.

A screenshot of a "Power Options" configuration window. It features a title bar "Power Options" and a dropdown menu for "Action" set to "Shutdown". Below this is a "Repeat every:" field with a spinner set to "30" and the unit "minutes". A "Message:" field is empty. The "Countdown:" field has a spinner set to "1" and a dropdown menu set to "Minutes". At the bottom, there are two checkboxes: "Allow user to abort" and "Allow OS to apply updates", both of which are currently unchecked.

Using the **Repeat every** option, you can allow a user to continue using a computer whilst they're at it, but have it shutdown/reboot automatically after they leave it. This option will try to shutdown/reboot and if it's cancelled, it will try again after the specified time. This will repeat until the action succeeds or the policy is deactivated/removed.

If a **Message** and **Countdown** are set, the user will see a warning message when the action triggers, giving them time to save their work or abort the shutdown. **Allow user to abort** gives a cancel button which will stop the shutdown from happening, but it will trigger again after the **Repeat every** time. If you wish it to only try once, either apply it as a temporary policy with a time set to less than the **Repeat every** time, or set a **Schedule**, with the activation time shorter than the **Repeat every** time.

If **Allow OS to apply updates** is ticked, the shutdown will tell the OS to update as part of the shutdown, if applicable. Note that sometimes Windows will install updates even if told not to, so it's not possible to definitely prevent updates.

Using AB Tutor

Policies

Block Hotkey

The Block Hotkey effect allows Windows hotkeys (eg ctrl+C for copy, Ctrl+Win+Left to change desktop) to be blocked.



To add a hotkey to block, click the **Add** button and enter the keys, with a plus sign between them, as shown above. Special keys include **Ctrl, Alt, Shift, Win, Left, Right, Up, Down**. To remove an entry, select it and click **Remove**.

Block Virtual Desktops

A specific use of this policy is in combination with a registry policy to block virtual desktops. To do this, create a policy with a **Registry Control** effect and a **Block Hotkey** effect. The Block Hotkey effect should be set to block:

- Win+Tab
- Ctrl+Win+D
- Ctrl+Win+Left
- Ctrl+Win+Right

as shown above and the Registry Control should be set to block

- Start Menu and Taskbar\Hide the Task View button

to prevent access to the button on the taskbar. This policy will prevent creating and switching between virtual desktops, however if it's applied after a user has started using them, it can prevent them getting to open programs if they are on a different desktop. Because of this, we recommend applying this policy before the users log in to prevent data loss.

Using AB Tutor

Policies

Sleep Action

This policy effect puts the Client computer to sleep, giving a choice between **suspend** (low power state, RAM still powered) and **hibernate** (save RAM to hard disk and power off fully). As this is part of a policy, it can be triggered based on a schedule, or on network events, allowing computers to be automatically put to sleep off at the end of the day.



Sleep Options	
Action:	Suspend
Repeat every (minutes):	30
Message:	
Countdown (seconds):	60
<input type="checkbox"/> Allow user to abort	
<input type="checkbox"/> Also log user off	

Using the **Repeat every** option, you can allow a user to continue using a computer whilst they're at it, but have it log off automatically after they leave it. This option will try to logoff every n minutes as set, until the logoff happens.

If a **Message** and **Countdown** are set, the user will see a warning message when the logoff triggers, giving them time to save their work or abort the logoff. **Allow user to abort** gives a cancel button which will stop the logoff from happening, but it will trigger again after the **Repeat every** time. If you wish it to only try once, either apply it as a temporary policy with a time set to less than the **Repeat every** time, or set a **Schedule**, with the activation time shorter than the **Repeat every** time. As this effect only puts the computer to sleep, by default when it is turned back on, the same user will be logged in. **Also log user off** will force a logoff before the sleep.

Using AB Tutor

Assessment

AB Tutor includes a number of ways to assess your students' understanding of the material, of varying levels of depth and complexity.

-  **Easy Polling** allows you to verbally ask the students a question and have them reply from their computers, using simple "yes/no", "true/false" or multiple choice answer options.
-  **Poll** allows you to send written multiple choice questions out to students' computers, and then save the results. You can also create questions ahead of time and save them for future use.
-  **Traffic Lights** allow students to give feedback whenever they want, rather than waiting for a test to start. The simple colour scheme makes it easy to tell which students need more help.
-  **Self-Paced Questions** allows a much larger test, consisting of multiple questions to be sent to students' computers for them to work through at their own pace. This function can also prevent the students doing anything else on the computers during the test to prevent cheating. Again, the results of the test can be exported to a table for future use.

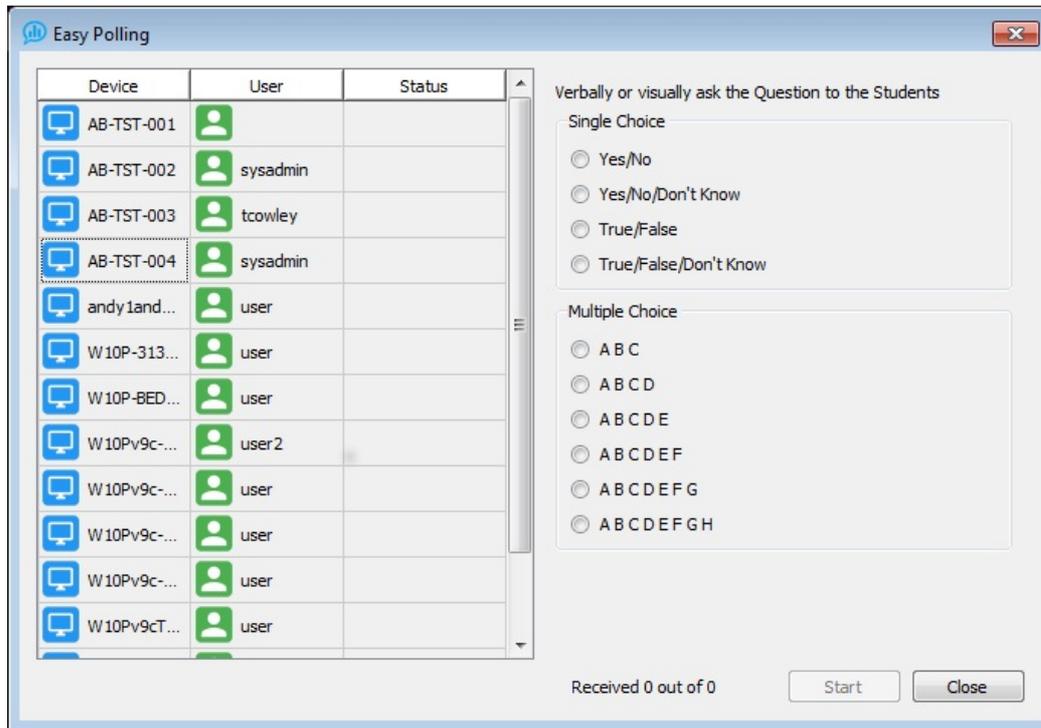
Using AB Tutor

Assessment

Easy Polling

The Easy Polling system is designed to be used during a lesson to allow a teacher to quickly check their students' understanding. Instead of asking an individual student, the entire class can answer independently from their computers. The questions can have yes/no, true/false or multiple choice answers. When the students answer, the teacher will see a summary of the answers given, and can see a detailed breakdown of the answers on the list view.

To send an Easy Poll form, select the relevant computers in AB Tutor, then select the **Assessment** menu and **Easy Polling**. A window will open with the available answer sets:



Select the answer set you want to send, and click OK. The options will appear on the student computers allowing them to answer your question. As they do, feedback will appear on the teacher console. If you want more detailed feedback, each individual student's response will be displayed by their name on the list view.

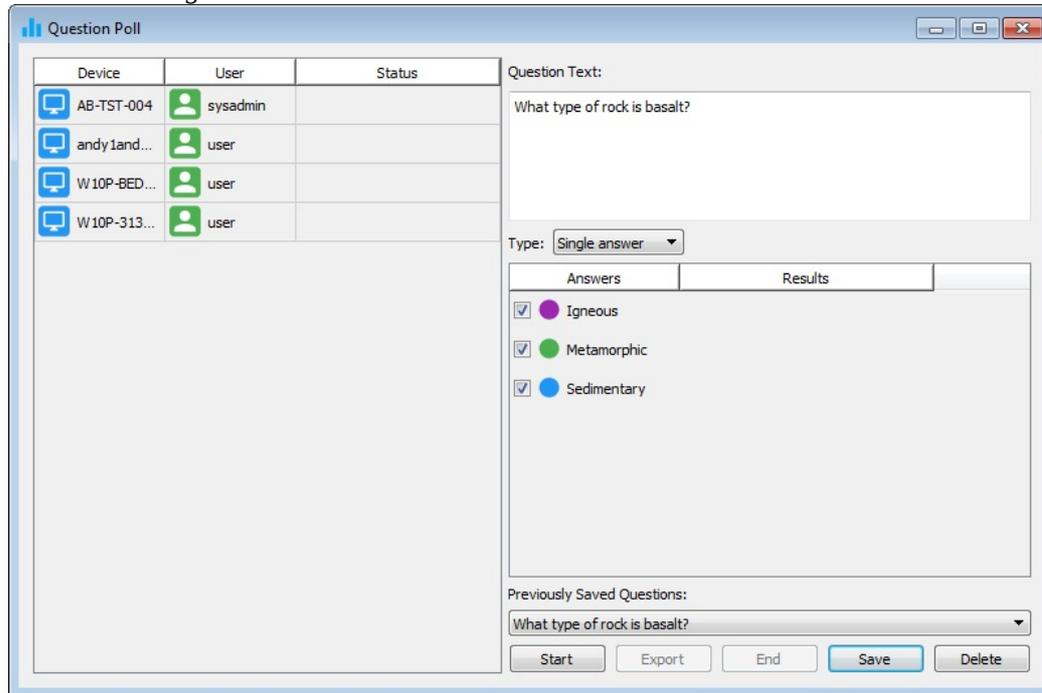


Using AB Tutor

Assessment

Poll

The Poll option is intended for slightly more detailed questions, and will send the question out to the student machine along with the answer form.



To create a question:

- Enter your question text
- Select from the drop down list the type of question. You can send either a **Single Answer** or **Multiple Answer** question.
- Add one or more answers by double-clicking on the **<New>** entry. When you press enter to save the answer, a new blank answer will be added automatically.
- Existing answers can be edited by double-clicking on the answer (alternatively, right-click on the answer and select **Edit**)
- Only answers that have a Tick in the box will be sent to the remote machine.
- To delete an answer, select it (hold down the Ctrl key to select multiple answers) then either press the Delete key or right-click and select **Delete**
- When you are ready to send the question, press the **Send** button.

If you want to save this question and its answers for future use, press the **Save** button bottom right. To restore saved questions, select the required question from the drop-down list of previously saved questions.

If you want to delete a previously saved question, select the question from the drop down list and press the **Delete** button. (If this button is disabled, then it means you have not selected a question yet)

If you want to completely reset the question text and answers, then right-click the mouse in the answers window and select '**Clear All**'

Analysing the Results

As students submit their answers, the results are displayed in the Results columns and in the Status column of the main window list view. By scanning over the Status column, you can easily see who has not yet answered and also actual answers from those who have. Note that if you've allowed multiple answers, the total percentages may add up to more than 100%.

Question Poll

Device	User	Status
AB-TST-004	sysadmin	Igneous
andy1and...	user	Igneous
W10P-BED...	user	Metamorphic
W10P-313...	user	Igneous

Question Text:
What type of rock is basalt?

Type: Single answer Received 4 out of 4

Answers	Results
<input checked="" type="checkbox"/> Igneous	75%
<input checked="" type="checkbox"/> Metamorphic	25%
<input checked="" type="checkbox"/> Sedimentary	0%

Previously Saved Questions:
What type of rock is basalt?

Start Export End Save Delete

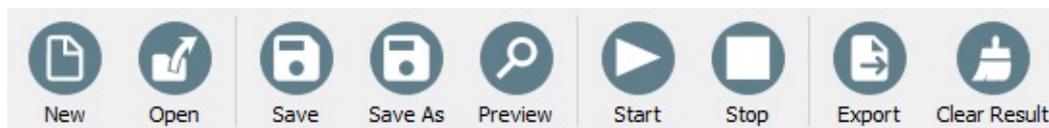
To save the results, press the **Export** button. You will be prompted to specify a folder and filename for the results file. The results are stored in HTML format and can be later opened using any web browser or imported into a spreadsheet package for further analysis.

Using AB Tutor

Assessment

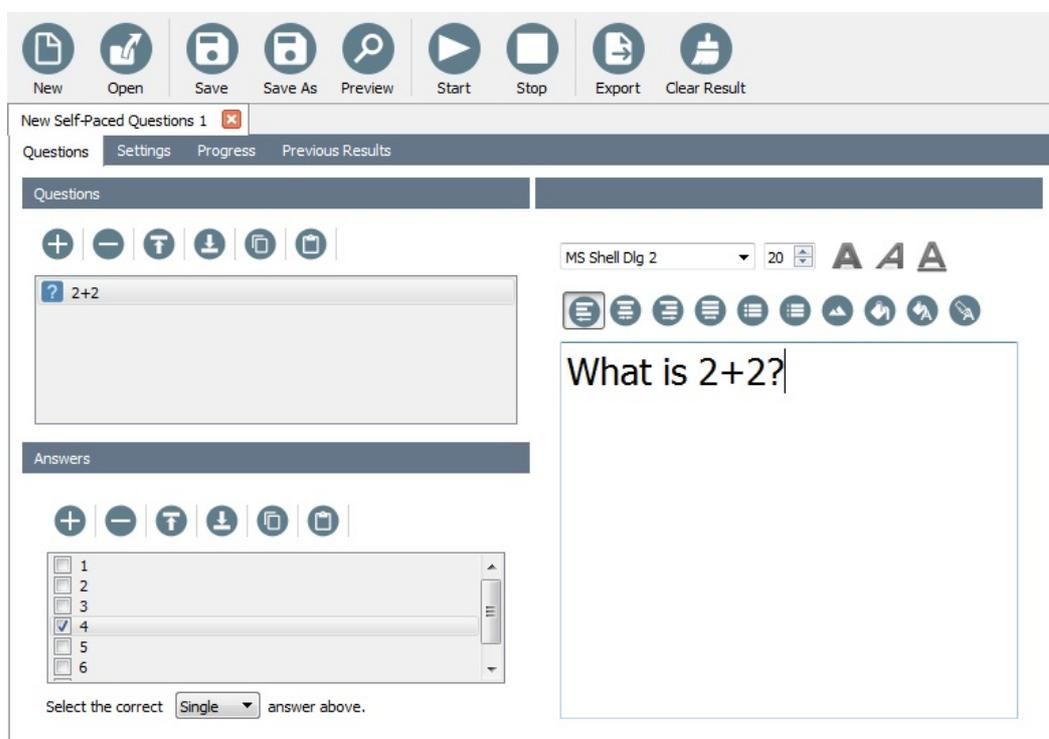
Self-paced Questions

The Self-Paced Questions system allows longer and more in depth testing of students than the single question polls, but is designed along a similar system.



The top row of buttons are for options which affect the entire test, saving and loading allow completed tests to be copied between computers, preview will show you the test as the pupils will see it and allow you to do a dry run through it. Save result and export are for dealing with the results after the test has been taken, and start, stop and clear deal with running the test once it has been created.

Questions



On this tab, the questions for the exam can be entered. The buttons across the top of the first panel allow adding, removing, rearranging and copy/pasting questions, the area on the right allows for the details of the question to be entered.

To create a question:

1. Click the green + button to create a new question.
2. Ensure the new question is selected in the question list.
3. Type the question into the right hand text box. The font and style options can be used if required, and images can be embedded or used as a background.
4. Press the add choice button and edit the text for the first possible answer. Repeat for all possible answers. If you press enter twice after typing in an answer, the next answer will be automatically created.
5. Select "single" or "multiple" from the dropdown box. Single choice means that there is one answer for the question, multiple choice allows the student to select multiple options from the list.
6. Select the "correct answer" tab and tick the correct answer(s). This will allow AB Tutor to automatically mark the exam.

Repeat this process for all the questions in the exam. Once the exam is finished, click save. The preview option will allow you to see the exam as the students will.

Settings

New Self-Paced Questions 1

Questions Settings Progress Previous Results

Title: New Self-Paced Questions 1

Description:

This Self-Paced Question session is timed. Enter the maximum duration: 1 minutes

Randomise question order

Randomise answers on choice type questions

Students are allowed to pause the Self-Paced questions

Allow students to review answers before submitting

Show students the correct answer summary after submitting

Allow students to see their results after submitting

Allow students to switch to and run other applications during the Self-Paced question session

This tab configures the basic settings for the test. It can be given a title and description, and allows the teacher to choose what rules apply. The title will be used as the filename when an test is saved.

- **Exam is timed:** Allows a time limit to be placed on the exam, from 1 minute to 10,000 minutes.
- **Randomise questions:** This option gives the questions in a random order, making copying between students harder.
- **Randomise answers:** This option shuffles the order the possible answers to each question are displayed.
- **Students are allowed to pause:** Allows the timer to be stopped, but prevents input during this time. Note that the current question is still visible at this point.
- **Allow students to review answers before submitting:** Allows the student to view all their answers on one page for easy checking before submitting.
- **Allow students to verify with tutor after submitting:** Shows a summary of correct answers against the ones submitted by the student.
- **Allow students to see their results after sumitting:** After the student submits the exam, they will see a summary of their results, telling them how many questions they answered and right/wrong totals.
- **Allow students to switch to and run other applications:** If this is unticked, the exam will run full screen and prevent access to anything else on the computer.

Progress

A testexam 

Questions Settings Progress Previous Results

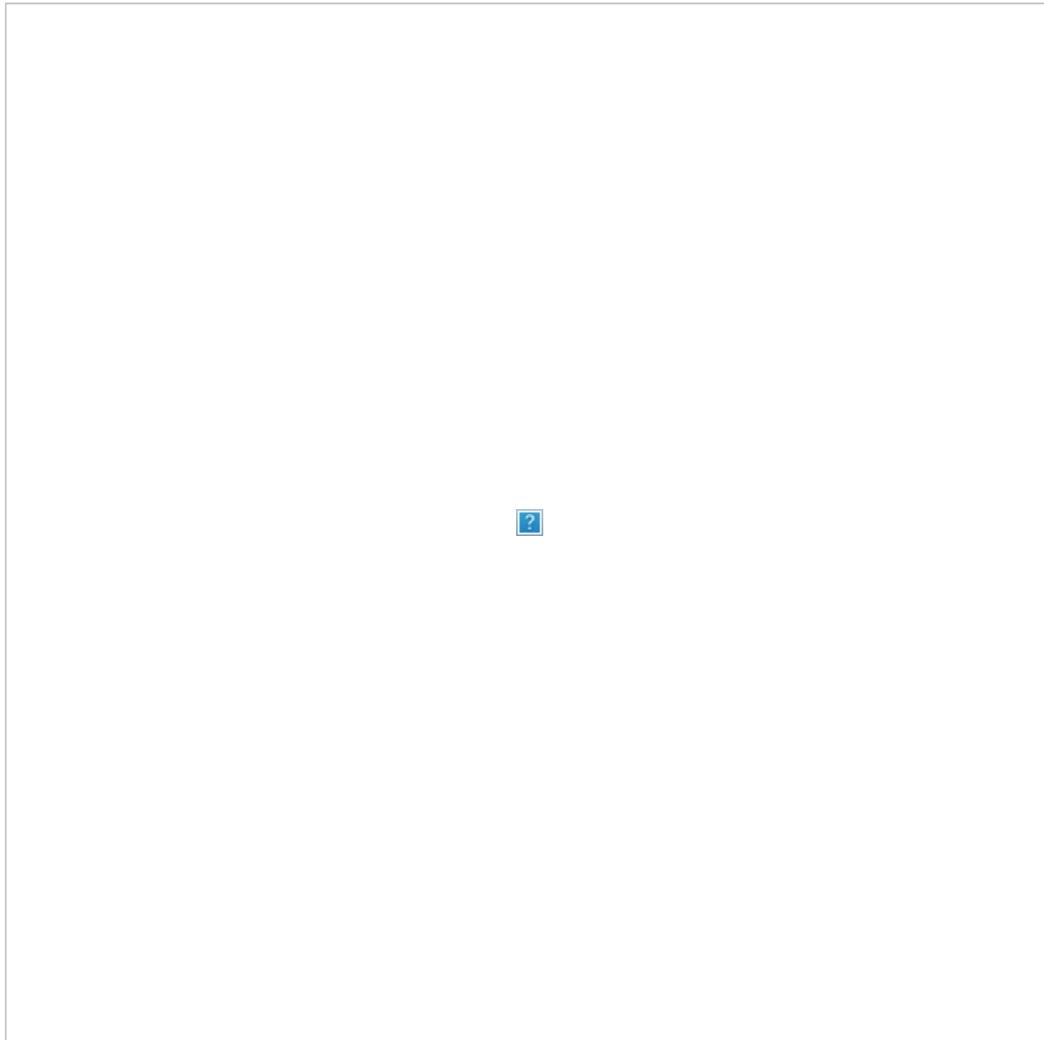
Self-Paced Questions ID: 13297  - Wrong Answers  - Right Answers  - Not Answered  - Not Viewed

Start Date: 21-Jun-2018 02:53:20 PM Total Students: 17

Questions	Progress State	Time Taken(seconds)
Q1 2+2	 3  1  13	21
Q2 3+3	 1  1  1 14	7
Q3 4+4	 3  14	28
Q4 5+5	 2  15	4

When an exam is running, this tab will show you how the exam is going; which questions have been looked at and which have been answered, plus how long each question is taking the students. This allows the teacher to easily tell which questions are proving difficult and how far through the exam the students have got.

Previous Results



This tab gives access to the results from previously taken exams. Results can be shown by student, giving a summary and details (showing which questions they got right, wrong, and whether they looked at unanswered ones) and also by question, giving a summary of which answers were given for each question.

The results can be exported as an html table by selecting the **Export** button from the toolbar.

Using AB Tutor

Logging

When events are triggered by policies or actions, information about the event will be saved in the logs on the Central Server. If the event counts as a **Violation** it will also be reported in the **Events** panel at the bottom of the Console and the user will be notified by a popup in the corner of the screen. For historical events, the Log Viewer allows you to view entries saved on the Central Server, using the search tools to cut down the amount of data displayed.

Events Panel

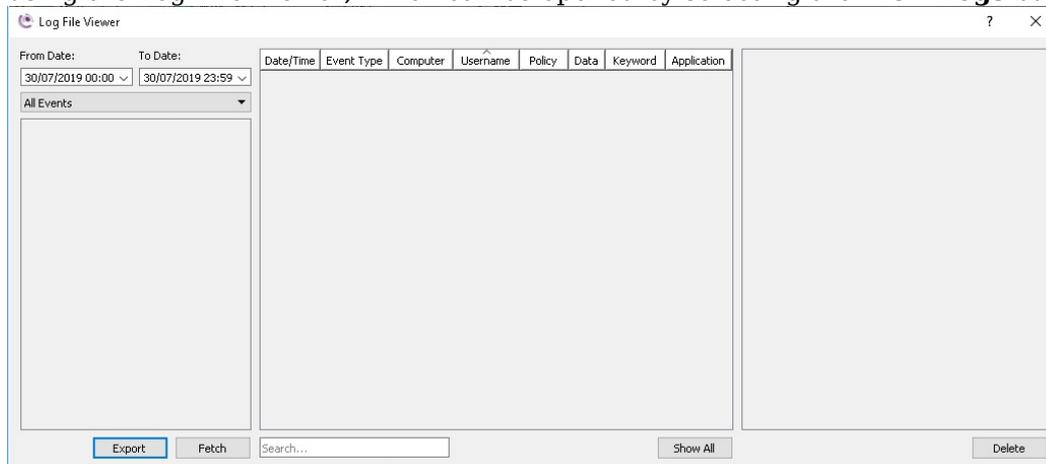
The Events Panel shows events as they come in, displaying the appropriate information in the columns. All column headers can be clicked to sort the events by that column.

- **Date/Time** shows when the event happened.
- **Event Type** shows what caused the event - this could be a snapshot, a keyword event etc.
- **Computer** shows the hostname of the computer where the event was triggered.
- **Username** shows the user who was logged on when the event was triggered.
- **Policy** shows the name of the policy which triggered the event, if applicable. Manually triggered events (eg snapshots) will have a blank entry here.
- **Data** shows any available additional information about the event. What appears here depends on the event type - it may show the keyword that was entered, for example.
- **Application** shows the focussed application at the time of the event. In the case of a website policy, the request may have been made by a background application.

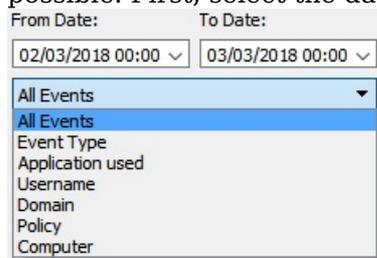
If an event is selected, the information about it will be displayed in the context panel, along with a thumbnail of any screenshot or video associated with it. If the screenshot is clicked on, it will be opened in a larger window. They can be saved out by clicking on the **Save** or **Export** buttons.

Log File Viewer

All events triggered on your site are stored on your Central Server in its logs. These can be viewed from the Tutor using the Log File Viewer, which can be opened by selecting the **View Logs** button at the top of the Events panel.



The Log File Viewer allows you to filter the events shown to help find the ones you're interested in as quickly as possible. First, select the date range using **From** and **To** boxes at the top. Next, select the type of filter to apply:



- **All Events** will show all events from the selected date range.
- **Event Type** allows you to select from types such as **Keyword**, **Application block**, **Website block** and so on.
- **Application used** allows filtering by the application that triggered the event. This works on the application title.
- **Username** will filter according to who was logged in on that session at the time of the event.
- **Domain** filters according to what domain the user was logged on to at the time of the event.
- **Policy** filters by the name of the policy that caused the event.
- **Computer** filters by the hostname of the computer on which the event was triggered.

When the item to filter by is selected, click the **Fetch** button to display the log events matching your filters. The first 250 will be displayed - you can fetch more by clicking **Show All**, however the maximum number of events which can be displayed at once is 15,000 - if your search produces more than that, please filter more strictly to reduce the number, probably by decreasing the time/date range.

Displayed events can be filtered further by typing into the search box at the bottom of the window. This will filter against any column. Events can be deleted from the logs by selecting them and pressing the **Delete** button.

The events will be shown in the main table, using the same columns as the Events Panel above. Additional information on an event or events can be displayed in the right panel by selecting them. Screenshots/captures can be expanded by clicking on them to open them in a new, larger window.

Archiving logs

Old events can be set to be archived automatically after a certain amount of time and optionally deleted some time after the archive is closed. This can be configured through the Central Server. If a closed archive is mounted on the Central Server, it can be viewed in the Console by an admin, by going to **Archive Log Files** in the **Tools** menu. This log viewer functions in exactly the same way as the normal log viewer, except that events can't be deleted.