Centurion Technologies

SmartControl Features

Updated 01/21/14

Technical Support Available
Monday to Friday hours: 8:30AM until 5:30PM CST/CDT
1-844-265-6055 support@centuriontech.com

Introduction

This guide will touch on all of the features available in SmartControl. It serves as a consolidated guide to using SmartControl with less pointed advice, as opposed to the other specialized articles. Any of the less complex features such as File Transfer, Log Viewer and User Lockdowns will be explained in this article.

Preferences Section

To access your SmartControl preferences go to “File” > “Preferences”. Most of these preferences have their own descriptors for what they do, but most of your quality of life enhancements can be found here. These options simply make SmartControl easier to use or more customizable to you.

Grouping Clients

SmartShield clients can be put into clusters to make it easier to keep track of individual computers. You can either do this by doing static groups (known as groups) or dynamic groups (known as filter groups). To create a group go to “File” > “New” and select either “Group” or “Filter Group”.

A group will contain any computers you put into that group. Simply drag and drop them from “All Machines” to move them there. You can then organize your machines by lab, building, room or whatever you choose.

A filter group will populate itself, depending on what criteria you specify. If you select “Filter Group”, an option box will pop up that will present you with a list of options you can use to qualify clients. You have options such as name, version, operating system and more. Filter groups support regular expressions for improved sorting and selection.

If you ever want to remove a group, simply right click it and go to “Delete”.

Import/Export Data

This option will allow you to save parts of your SmartControl, which is useful if you ever need to take a backup of your settings, groups or schedules or reinstall your SmartControl. Simply check the options you would like to save then press “Export”. Save the file and you now have a copy of those settings.

If you want to import settings instead, go to "Import" and navigate to a .cenx file you had created previously. Open it and your computer will import those settings and restart.

Log Viewer

There are two Log Viewers for SmartControl. To access the primary Log Viewer in SmartControl go to "View" > "Log Viewer". This Log Viewer displays the success or failure of schedules and commands as well as property changes. If information is given from an error, it will display under the "Result" or "Additional Information" columns.

There is a second Log Viewer, which views the log files of an individual machine. It works in exactly the same way, just highlight a single client and go to "Client Control" > "View Client Log".

Block Keyboard and Mouse

This option is found under "Client Control" > "Protection Mode". SmartControl sends a command to the selected client machines to block the keyboard and mouse inputs. This will block both USB and PS2 keyboard and mouse inputs. It can be unblocked in the same menu.

Stealth Mode

Stealth mode will hide the SmartShield icon on the client PC. It will also cause the SmartShield interface to automatically close if it was opened locally and it detects no activity after a few moments. SmartShield can be opened locally by the key configuration you are asked for during installation. If you navigate to "Client Control" > "Misc. Configuration" you can enable or disable this on any clients you have selected.

Start Client Application

This feature will open the program you specify on the target machines. You will need to know the full path of the application as it exists on the client PC to use this feature. If the argument you supply accepts parameters, you can enter those in the fashion described on the pop up window. To use this feature, find it under "Client Control" > "Misc. Configuration".

File Transfer

The File Transfer option allows you to move files or directories from the SmartControl machine onto the select client machines. You may specify where these files will be placed on the client machine such as their desktop or a custom path (i.e. C:\Documents\Transfers). Highlight the machines you would like to send a file to and go to "Client Control" > "File Transfer" to use this feature.

Client Daily Reboot

This feature will cause the client to reboot every day at the specified time. This is useful because SmartShield will wipe any temporary changes that were made since the last reboot. If you want to enable this feature, navigate to "Client Control" > "Misc. Configuration" > "Client Daily Reboot" and tick the "Enable" box. Edit the time and press "Submit".

One Time Password Entry

Enabling this feature means that you cannot enter SmartShield locally without first entering the SmartShield password. By default, this feature is disabled. To enable it highlight the clients you want to change the setting for then go to "Client Control" > "Misc. Configuration" > "One Time Password Entry". One Time Password Entry in conjunction with Stealth Mode is the safest way to have SmartShield on your client machines in secret.

Print Blocking

Print blocking will disable printing from within Windows. SmartShield will monitor the requisite services and files, being sure to keep them disabled. You can change this setting by going to "Client Configuration" > "Misc. Configuration" and selecting either the "Enable" or "Disable" option.

User Lockdown

The User Lockdown option has several security settings that you can enforce through SmartShield. These options include the following:

- Block Command
- Block Control

- Block Registry
- Block Start
- Block Task Manager
- Block .msi

You can also block specific applications through this command. SmartShield will monitor the active processes on the machine and automatically close any instances that open. To add additional programs, please add them to a new line.

You can access the User Lockdown option by highlighting the machines to be effected and going to “Client Control” > “Misc. Configuration” > “User Lockdown”

Network Test

Doing a Network Test on a SmartShield client will allow you to send a request on port 25553 to see if there is a machine listening at that IP address. It can return a positive, a negative or it will tell you that the request was forcibly denied. Network Tests are great for determining whether a SmartShield client is working properly. For instance, if your request was forcibly denied, the machine may have its firewall enabled and is rejecting incoming SmartControl traffic.