Centurion Technologies

Installation Guidelines for Windows OS

Updated 03/26/14

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

Introduction

This document details the best way to install SmartControl and SmartShield on a Windows computer or server. In some instances, special steps may be needed for certain networks or setting up WAN based SmartShield and SmartControl communication, but that is outside the scope of this document. This document will reflect setting up SmartShield and SmartControl in a LAN setting.

Requirements

The requirements for our software are as follows:

- SmartControl OS – Windows XP, Windows 7, Windows 8 for a maximum amount of clients under 500. Windows Server 2003, Windows Server 2008, Windows Server 2012 for any capacity.
- SmartShield OS – Windows XP, Windows 7 or Windows 8.
- .NET Framework 2.0 and 3.5.
- 512MB of dedicated RAM. We recommend at least 2GB of RAM to ensure smooth computer operation.
- 2GHz single core processor. We recommend at least a 2.8 GHz dual core processor.
- At least a 100MB Ethernet card. Wireless is NOT recommended.
- SmartShield and SmartControl cannot be installed on the same computer. You must install one or the other.

If the minimum requirements are met, feel free to go ahead with installation. Either by your salesperson or via e-mail through our evaluation procedure, you should receive a download to both SmartShield and SmartControl. Ensure you have the proper bit-version for your PC and that you install the proper software on the server and client.

Installation Guidelines

If you are using a SmartControl, you will need to install it first. If you are using a stand-alone SmartShield installation, you can skip this step. Please jump to "SmartShield Installation" on page 2.

Be sure the Windows is allowing the SmartShield and SmartControl installers before you start installation. Right click the installer and ensure that it is not being blocked. Under the "General" tab you may see text stating "This file

came from another computer and might be blocked to help protect this computer." along the bottom of the window. If the program is being blocked, unblock it with the button directly to the right and proceed with installation.

SmartControl Installation

We recommend putting the SmartControl on a static IP address, if possible. SmartControl can still work in a DHCP environment; however this can lead to disrupted communication if the networking gear falters in any way.

Installation MUST be completed from an administrator account. Start installation by launching the installer (i.e. CCInstaller2.1.12.1178_x64.exe) for your computer's bit-version. You will be presented with a standard installer and it will ask for your license key. Please fill all fields, as they are mandatory. It is easiest if you leave the default port during installation.

Please write down or save your password, Centurion Technologies cannot recover this in any way. The password files are encrypted and unable to be recovered.

Once you have finished installation, restart your computer. Please log into an administrator account after the reboot to finalize the installation. SmartControl should not be installed and waiting for your clients to connect to it.

SmartShield Installation

SmartShield installation will either begin after you have installed SmartControl or if you are installing a stand-alone copy of SmartShield.

SmartShield installation provides many options for how to set up and run the program. The bulk of customization is done at this level. Since this is a guidelines document, those features will be explained in more detail in a different document.

After the information about our license agreement, you will come to a registration page that asks about how you would like to register your product.

If you are installing this SmartShield product with a SmartControl, select option 1. If the SmartControl is on a static IP, please point the SmartShield client by IP address to the SmartControl. Otherwise, use computer name.

If you are installing this client as a stand-alone, please click option number 2. Only click option 3 if you are behind a proxy or if you have no internet connection. If you are using manual registration, it will be detailed later in this guide.

Please write down or save your password, Centurion Technologies cannot recover this in any way. The password files are encrypted and unable to be recovered. The same is true for keyboard/mouse unlock phrase.

When the installer asks you if you would like to do a default or custom installation, pick default if you are not technical or just want a standard installation. SmartShield will assign 1/3 of the available hard drive space for the temporary storage file in a default installation where a custom install will assign whatever amount you designate.

The stealth mode shortcut can only be customized during installation, so be sure that if you want to use a default button combination you select it now. SmartShield can always be pulled to the front with the shortcut ctrl+alt+` if you forget your custom shortcut so it can be accessed even if stealth mode is enabled.

When to Use Manual Registration for Stand-alone Licensing

Manual registration is an option you can use if you foresee extended disconnection from the internet or the computer will be behind a proxy that blocks access to our licensing server. With internet connection registration your computer must connect to the internet at least once every 30 days or your product will suspend. When your license suspends you will not be able to change protection modes and most commands issued from a SmartControl will automatically fail. Manual registration is recommended in these situations to prevent this kind of behavior from SmartShield.

Setting up Manual Registration for Stand-alone Clients

You can start the manual registration process either by selecting the option during install or going to the "Licensing" area of SmartShield on your client machine. To open the "Licensing" menu, right click the icon in the system tray and go to "About", then press "Licensing". Click the "Manual Registration" tab. Instructions are included on the interface. Please note that once you receive your ctireg.out file from the machine you want to license with manual registration you can upload it to http://registration.centuriontech.com/ from any machine. This is useful if you are stuck behind a proxy on those machines.

SmartControl and SmartShield Over WAN

SmartControl can be configured to connect to SmartShield over the internet by using a public IP address and port forwarding. First, you will need to install your SmartControl and set up port forwarding. The public IP will need to forward ports 25552-25555 to the SmartControl computer. This will allow SmartShield clients to reach the SmartShield for commands and keep alives. To turn on WAN communication on the SmartControl, navigate to "File" > "Preferences" and then click the "Network" tab. Click the checkbox to enable WAN communication. You can then proceed with installation of SmartShield or change the IP address on clients that have already been installed.

During installation of the SmartShield clients you will be asked for the IP address of the SmartControl client. Input the public IP address, not the local address, of the SmartControl here. If port forwarding is set up properly, SmartControl should respond and allow for WAN communication.

SmartShield in a Novell Environment

SmartShield can work in conjunction with a Novell environment. To enable Novell, perform a custom installation. Be sure to click the "Allow Novell" button on the "Persistent Storage, Firewire and Novell" section. This will allow the registry to write properly and SmartShield should function appropriately.

Tips For Security

SmartShield is a driver-based kernel-level protection that loads into Windows OS on boot. This means that users with malicious intent can load outside of the Windows environment if they are able to access your BIOS or Advanced Startup option. Centurion Technologies advises you to lock your BIOS by password. In most BIOs releases, this can be found under your "Security" section. The "Supervisor" password will require a password before the BIOs can be accessed, a "user" password will require a password before the unit can proceed past BIOs at all. In the case described here, the "Supervisor" password will suffice.