IRRICAD™
IRRIGATION DESIGN SOFTWARE

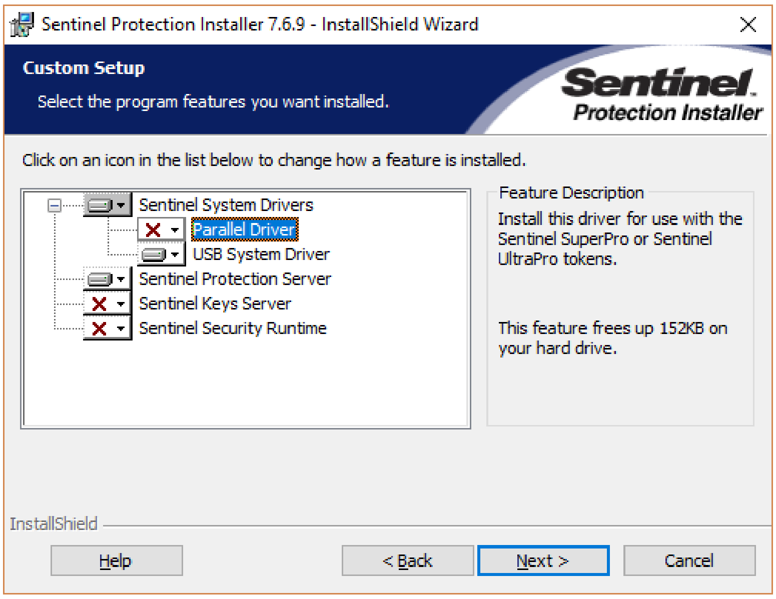
Installation procedure for multi-user network operation IRRICAD Version 17

Requirements

- Windows Network of computers connected either to a server or a presentation computer.
- USB network version of the IRRICAD dongle.
- Access to www.IRRICAD.com to download the installation and patches.
- An internet connection for the duration of the installation process.

Install the dongle driver on the server or presentation computer

- Connect the USB IRRICAD dongle to the server or presentation computer.
- Download the dongle driver (SentinelProtection Installer) from http://www.irricad.com/irricad/download/Drivers/Rainbow/SentinelProtectionInstaller7.6.9.exe and save to the hard-drive.
- Locate where the driver was saved and double-click on it to run the Sentinel Protection Installer. Select the option for Custom Install and ensure the "USB System Driver" and the "Sentinel Protection Server" are selected. If the driver has already been installed select the "Modify" option and enable the "Sentinel Protection Server" option.



Sentinel Protection Installer 7.6.9 - InstallShield Wizard

Custom Setup

Select the program features you want installed.

Click on an icon in the list below to change how a feature is installed.

- Sentinel System Drivers
  - ☒ Parallel Driver
  - USB System Driver
- Sentinel Protection Server
- ☒ Sentinel Keys Server
- ☒ Sentinel Security Runtime

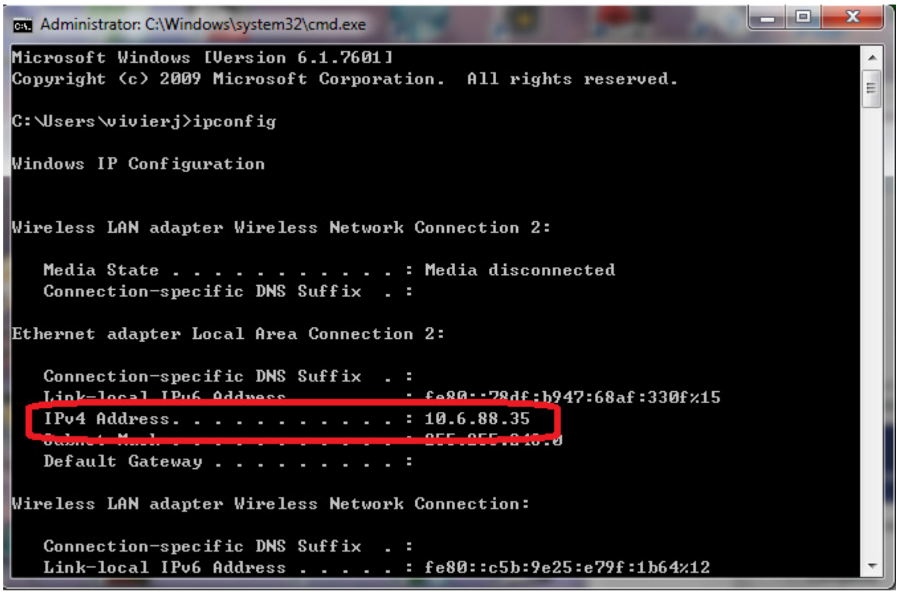
Feature Description

Install this driver for use with the Sentinel SuperPro or Sentinel UltraPro tokens.

This feature frees up 152KB on your hard drive.

Click [No] on the important note about Windows Firewalls on the next screen when it asks if you want to modify these setting now. Click Yes on any security messages during this installation.

- When the installation is complete, go to the command prompt by typing **cmd** in to the *search programs and folders* field and press the Enter key on the keyboard. Type **ipconfig** and press Enter to get the IP address of the server / presenter's computer. The IP address may be presented as "IPv4 Address". Write this down, it will be needed to set up the client computers.



Administrator: C:\Windows\system32\cmd.exe

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\vivierj>ipconfig

Windows IP Configuration


Wireless LAN adapter Wireless Network Connection 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter Local Area Connection 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::78df:b947:68af:330f%15
   IPv4 Address. . . . . . . . . . . : 10.6.88.35
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Wireless Network Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::c5b:9e25:e79f:1b64%12
```

Create exceptions to the firewall on the server or presentation computer

It is necessary to create exceptions to the Windows Firewall for the Sentinel driver. The firewall exceptions can be accessed via:

Windows 7

- Go to Control Panel | System and Security | Windows Firewall
  Click on "Allow a program through Windows Firewall".

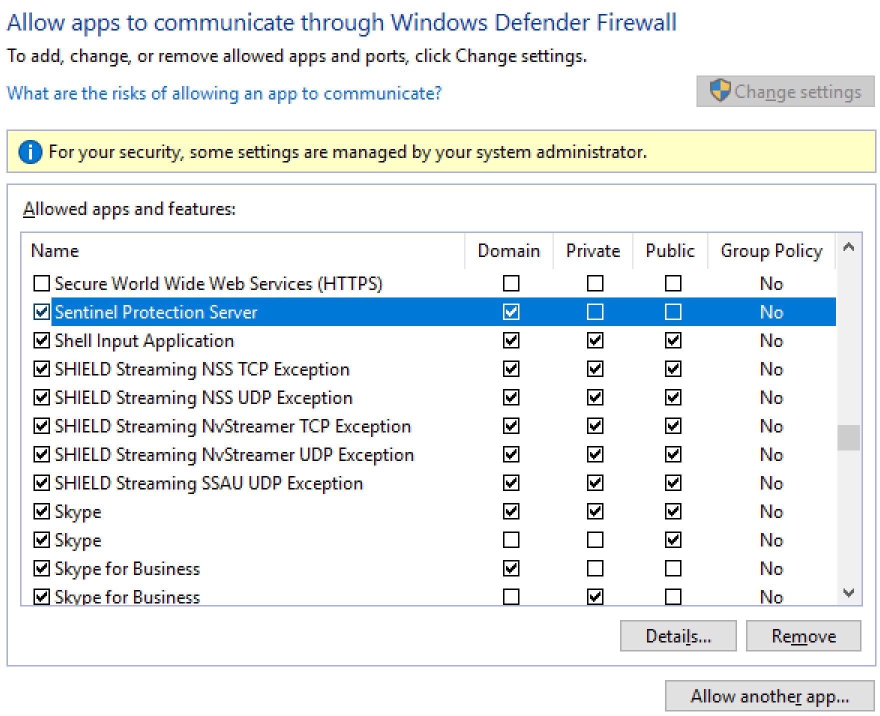
Windows 8

- Swipe and select Settings | Control Panel | System and Security | Windows Firewall
- Click on "Allow an app or feature program through Windows Firewall".

Windows 10

- Go to Control Panel | System and Security | Windows Firewall
  Click on "Allow an app or feature through Windows Defender Firewall program through Windows Firewall".

Enable the Exception as shown in the image below.



Allow apps to communicate through Windows Defender Firewall

To add, change, or remove allowed apps and ports, click Change settings.

What are the risks of allowing an app to communicate?

For your security, some settings are managed by your system administrator.

Allowed apps and features:

Name	Domain	Private	Public	Group Policy
☐ Secure World Wide Web Services (HTTPS)	☐	☐	☐	No
☑ Sentinel Protection Server	☑	☐	☐	No
☑ Shell Input Application	☑	☑	☑	No
☑ SHIELD Streaming NSS TCP Exception	☑	☑	☑	No
☑ SHIELD Streaming NSS UDP Exception	☑	☑	☑	No
☑ SHIELD Streaming NvStreamer TCP Exception	☑	☑	☑	No
☑ SHIELD Streaming NvStreamer UDP Exception	☑	☑	☑	No
☑ SHIELD Streaming SSAU UDP Exception	☑	☑	☑	No
☑ Skype	☑	☑	☑	No
☑ Skype	☐	☐	☑	No
☑ Skype for Business	☑	☐	☐	No
☑ Skype for Business	☐	☑	☐	No

If you cannot see the “Sentinel Protection Server” in the list restart the computer.

Install IRRICAD on the presentation computer

Note this is only required if the computer that has the dongle attached will also be used to run IRRICAD (for example a computer used by a trainer). This is not normally required on a Server.

- Log in as an Administrator and open an internet browser (for example Internet Explorer or FireFox) and browse to an **external** website. **This step is required for successful registration of the CAD Engine.**

- Download the required files and save to the hard-drive or USB flash drive - http://www.irricad.com/download/v17-standalone-installation/?wpdmdl=2290&masterkey=5b3b3d37ec4fe .

- Locate the downloaded files and double-click on IrricadProV17.exe to install Version 17.

Install IRRICAD on the client computers.

- Log in as Administrator and open an internet browser (for example Internet Explorer, or FireFox) and browse to an **external** website. **This step is required for successful registration of the CAD Engine.**

- Download the required files and save to the hard-drive or USB flash drive - http://www.irricad.com/download/v17-standalone-installation/?wpdmdl=2290&masterkey=5b3b3d37ec4fe .

- Locate the downloaded files and double-click on IrricadProV17.exe to install Version 17.

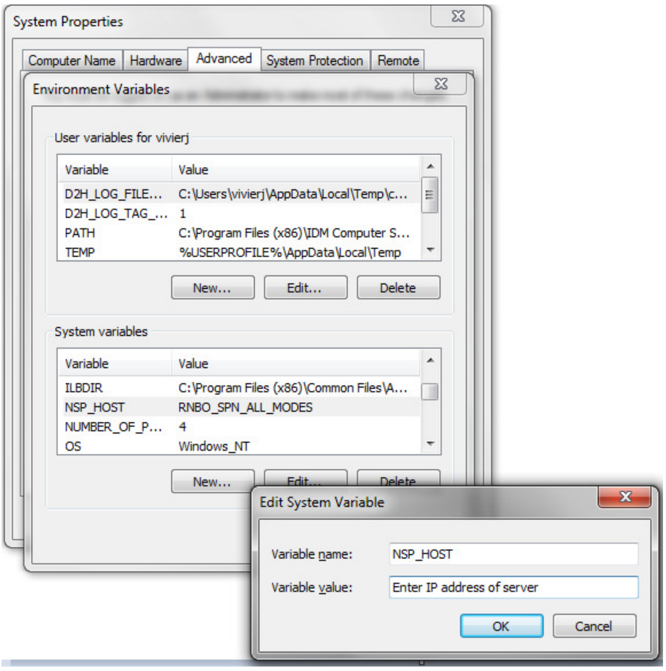
Create exceptions to the firewall on each of the client computers

This process is the same as for the server. Make sure exceptions are checked for IRRICAD and the IRRICAD Database Editor.

Direct the client computers to look at the server for the dongle.

Windows 7

- Click on Start then right click on Computer and select Properties.
- Click on Advanced system settings, the Advanced tab, then Environment variables.
- Locate the variable NSP_HOST.
- Edit the variable so the value is the IP address of the server or presenter's computer.



User variables for vivierj

Variable	Value
D2H_LOG_FILE...	C:\Users\vivierj\AppData\Local\Temp\c...
D2H_LOG_TAG_...	1
PATH	C:\Program Files (x86)\IDM Computer S...
TEMP	%USERPROFILE%\AppData\Local\Temp

System variables

Variable	Value
ILBDIR	C:\Program Files (x86)\Common Files\A...
NSP_HOST	RNBO_SPN_ALL_MODES
NUMBER_OF_P...	4
OS	Windows_NT

Variable name: NSP_HOST

Variable value: Enter IP address of server

Windows 8

- Swipe to select Settings | PC Info.
- Click on Advanced system settings, the Advanced tab, then Environment Variables.
- Locate the variable NSP_HOST.
- Edit the variable so the value is the IP address of the server presenter's computer.

Windows 10

- Right-click on the windows icon (bottom left of screen) and select 'System'.
- Click on Advanced system settings, the Advanced tab, then Environment Variables.
- Locate the variable NSP_HOST.
- Edit the variable so the value is the IP address of the server/presenter's computer.

Run IRRICAD on a client computer

Test the installation by opening IRRICAD on several client computers. Note that each IRRICAD network dongle has a user limit coded into the dongle.

Notes

The standard installation sets the NSP_HOST as “RNBO_SPN_ALL_MODES”. If the client computer is connected to the same network (subnet), and the firewall allows the traffic, then the client computer will find the dongle on the network. However, this is slower than setting the NSP_HOST to the IP address of the ‘server’. If the client computer is connecting via the internet then the ‘server’ must have a publically accessible IP address unless a VPN is used. Latency is more important than the internet speed.

Activating or Upgrading the Dongle from the Server

Although IRRICAD is not required on the server the dongle can be read but not written to from a client computer. Therefore, for upgrading purposes it is helpful to have the “Upgrade Dongle” utility files present on the server. These can be downloaded from http://www.irricad.com/irricad/download/Drivers/FieldExUtil.zip - extract the contents. Run the FieldExUtil.exe to get locking codes or update dongles.