WOLFSON UNIT
FOR MARINE TECHNOLOGY &
INDUSTRIAL AERODYNAMICS

Technical Note

By: Matteo Scarponi **Date** 13/01/16

Subject: Sentinel HASP Net Dongle Setup

1 SCOPE

This technical note describes the deployment of Sentinel HASP Net dongles for use with Wolfson Software. These tests were conducted on a Windows 7 Enterprise (x64) office network. Licenses were served by a standard machine acting as a server, not by a dedicated server.

The network dongle used for these tests is a Sentinel HL Net 10 enabled for Wolfson Software.

The machine names used for this exercise are: UOS-207790 (server) and UOS-12356 (client).

2 ON SITE SERVER

2.1 Server configuration

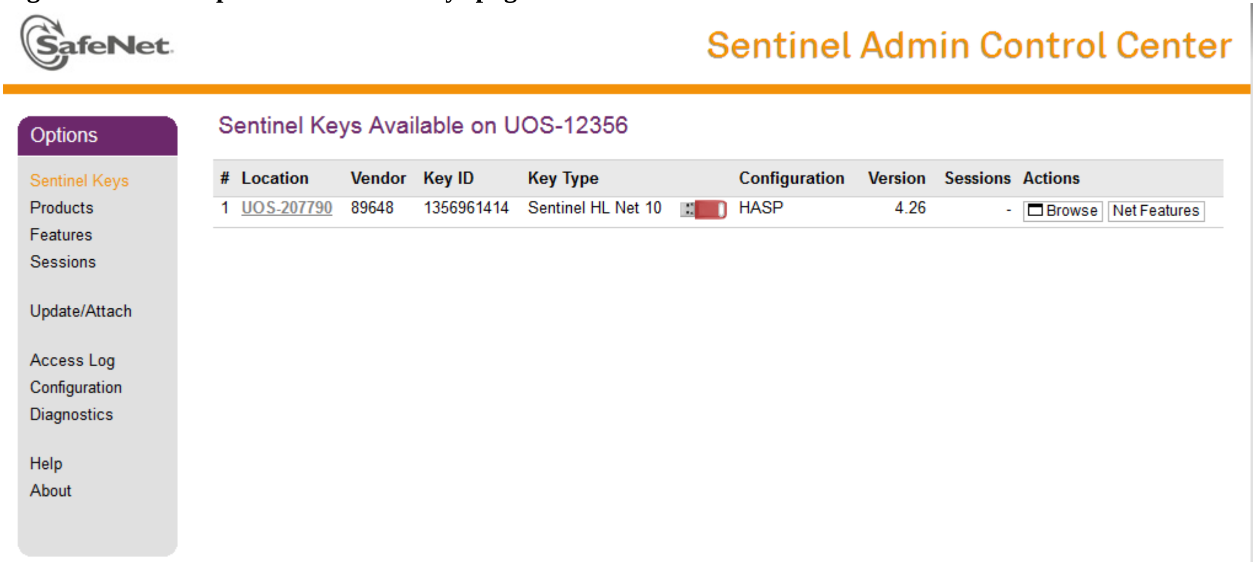
a. Download and install the Sentinel Run Time Environment:
http://sentinelcustomer.safenet-inc.com/DownloadNotice.aspx?dID=8589947119

b. Open a web browser and type: http://localhost:1947/_int_/devices.html
This brings up the Sentinel Admin Control Center.

c. Plug in the Sentinel HASP Network key supplied by the Wolfson Unit.

d. In the Sentinel Admin Control Center select the ‘Sentinel Keys’ link found under Options, LHS of page. Your Sentinel key should be listed in the main page as a Sentinel HL Net <seats> Key Type, eg:

Figure 1 **Options > Sentinel Keys page.**

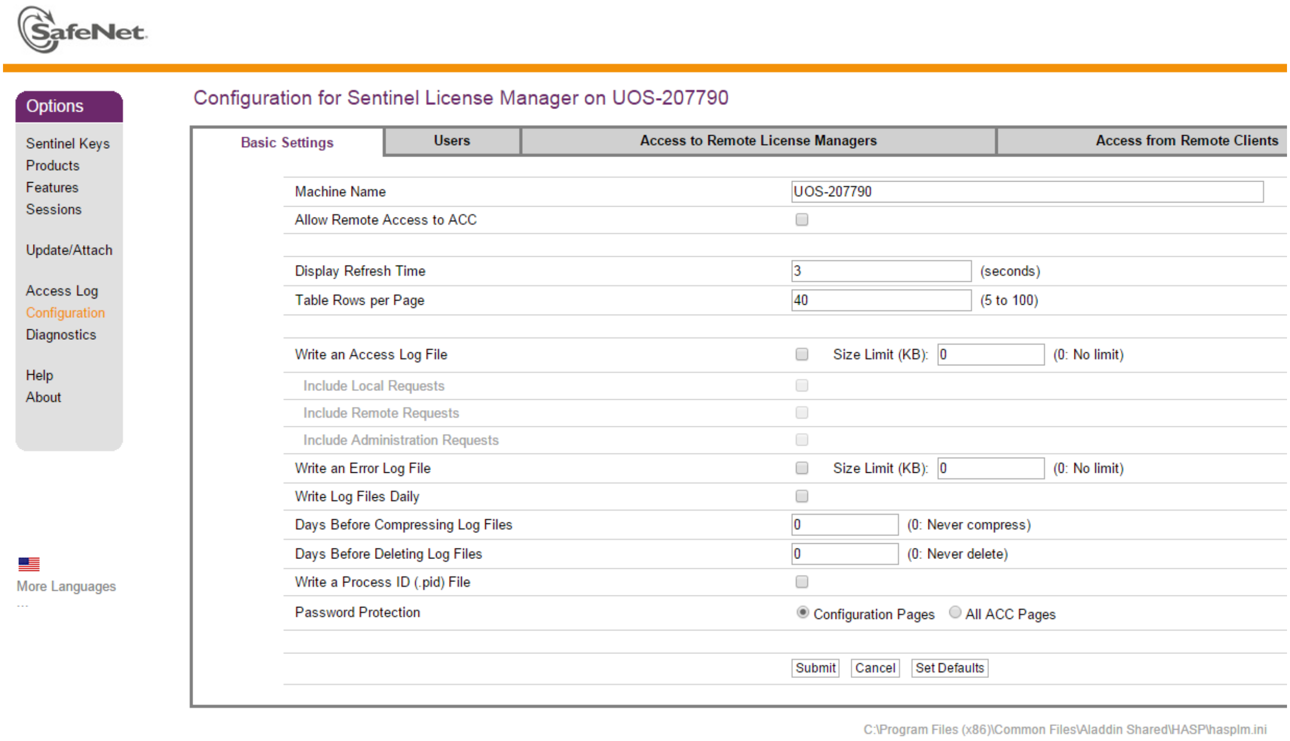


Sentinel Keys Available on UOS-12356

#	Location	Vendor	Key ID	Key Type	Configuration	Version	Sessions	Actions
1	UOS-207790	89648	1356961414	Sentinel HL Net 10	HASP	4.26	-	Browse Net Features

e. Configure the Sentinel License Manager as shown in Figure 2 to Figure 4 below. Click Submit.

Figure 2 Basic Settings Page

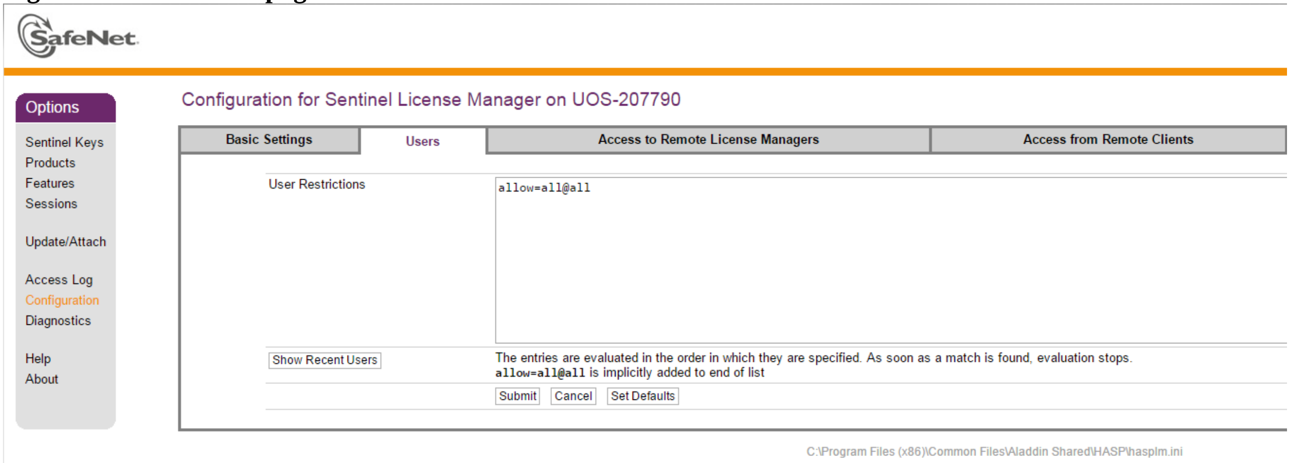


Configuration for Sentinel License Manager on UOS-207790

Machine Name	UOS-207790	
Allow Remote Access to ACC	□	
Display Refresh Time	3	(seconds)
Table Rows per Page	40	(5 to 100)
Write an Access Log File	□ Size Limit (KB): 0	(0: No limit)
Include Local Requests	□	
Include Remote Requests	□	
Include Administration Requests	□	
Write an Error Log File	□ Size Limit (KB): 0	(0: No limit)
Write Log Files Daily	□	
Days Before Compressing Log Files	0	(0: Never compress)
Days Before Deleting Log Files	0	(0: Never delete)
Write a Process ID (.pid) File	□	
Password Protection	● Configuration Pages ○ All ACC Pages	

C:\Program Files (x86)\Common Files\Aladdin Shared\HASP\hasplm.ini

Figure 3 Users page



Configuration for Sentinel License Manager on UOS-207790

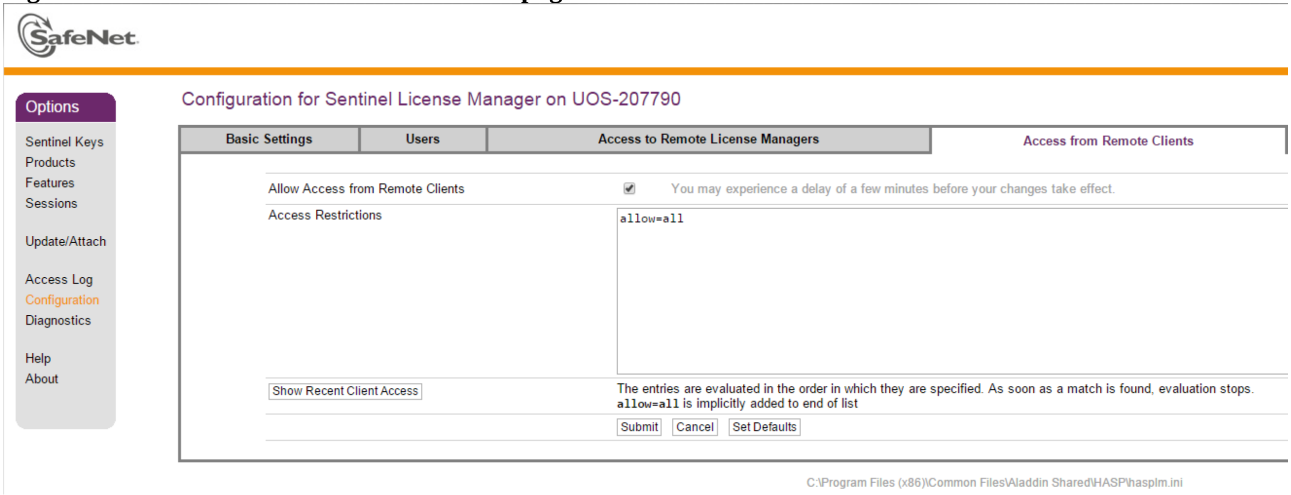
User Restrictions

```
allow=all@all
```

The entries are evaluated in the order in which they are specified. As soon as a match is found, evaluation stops.
`allow=all@all` is implicitly added to end of list

C:\Program Files (x86)\Common Files\Aladdin Shared\HASP\hasplm.ini

Figure 4 Access from Remote Clients page



Configuration for Sentinel License Manager on UOS-207790

Allow Access from Remote Clients ☑ You may experience a delay of a few minutes before your changes take effect.

Access Restrictions

```
allow=all
```

The entries are evaluated in the order in which they are specified. As soon as a match is found, evaluation stops.
`allow=all` is implicitly added to end of list

C:\Program Files (x86)\Common Files\Aladdin Shared\HASP\hasplm.ini

2.2 Client configuration

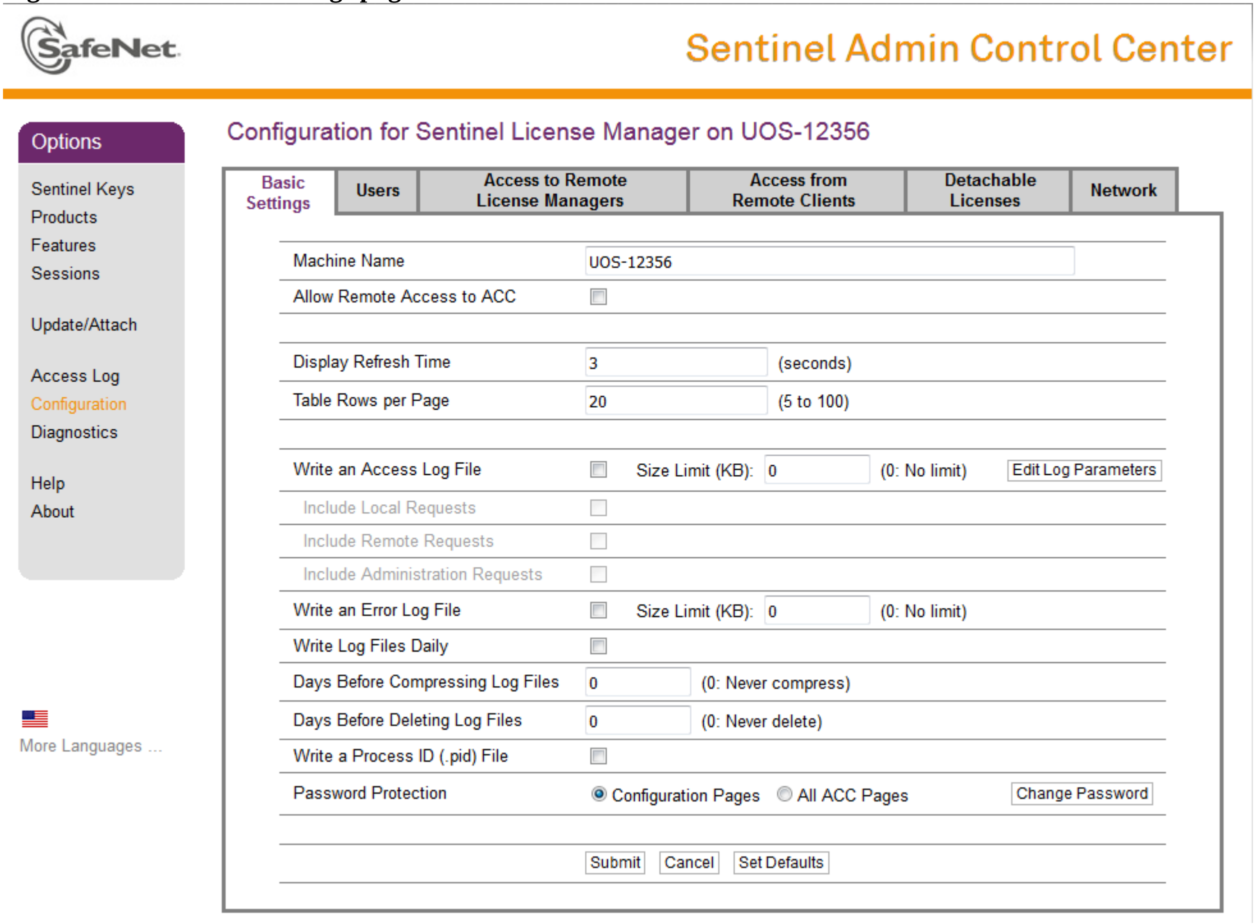
Server Name: UOS-207790
Client Name: UOS-12356

a. Download and install your Wolfson program. The Sentinel Run Time Environment will be installed automatically.

b. Open a web browser and type: http://localhost:1947/_int_/devices.html
This brings up the Sentinel Admin Control Center

c. Configure the Sentinel License Manager as shown in Figure 5 and Figure 6 below. Click Submit to confirm all changes:

Figure 5 **Basic Settings page:**

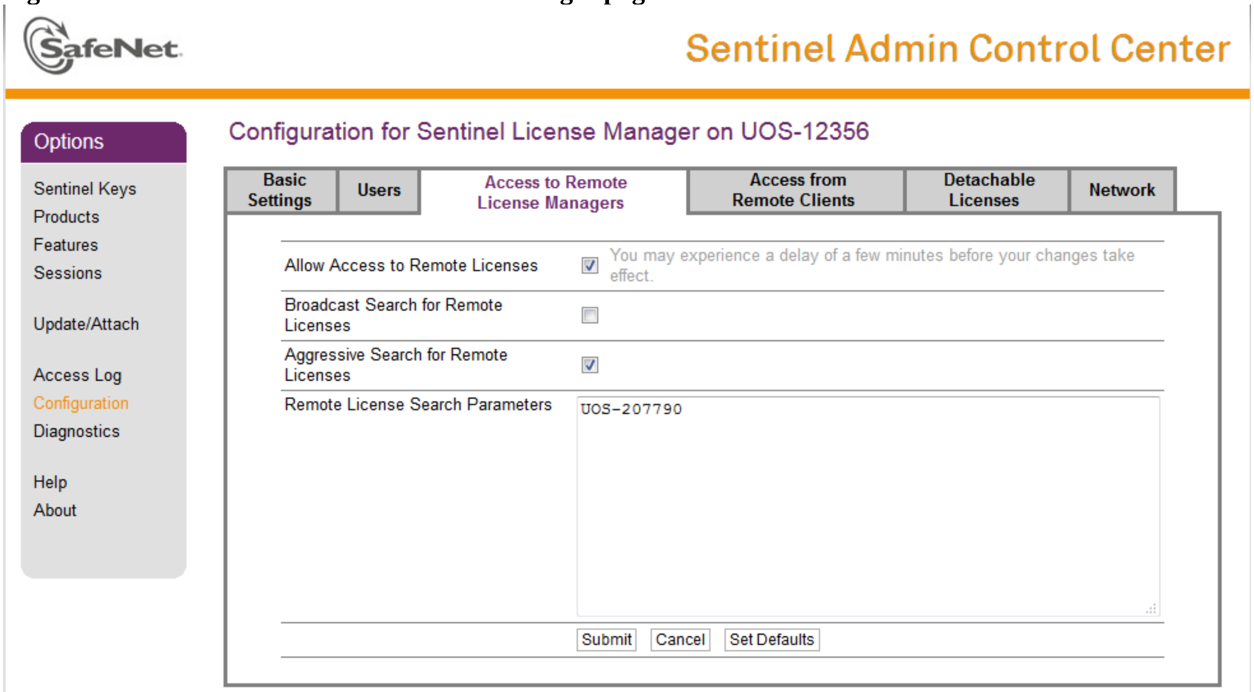


Configuration for Sentinel License Manager on UOS-12356

Machine Name	UOS-12356			
Allow Remote Access to ACC	□			
Display Refresh Time	3	(seconds)		
Table Rows per Page	20	(5 to 100)		
Write an Access Log File	□	Size Limit (KB): 0	(0: No limit)	Edit Log Parameters
Include Local Requests	□			
Include Remote Requests	□			
Include Administration Requests	□			
Write an Error Log File	□	Size Limit (KB): 0	(0: No limit)	
Write Log Files Daily	□			
Days Before Compressing Log Files	0	(0: Never compress)		
Days Before Deleting Log Files	0	(0: Never delete)		
Write a Process ID (.pid) File	□			
Password Protection	● Configuration Pages	○ All ACC Pages		Change Password

Submit | Cancel | Set Defaults

Figure 6 **Access to Remote License Manager page:**



Configuration for Sentinel License Manager on UOS-12356

Allow Access to Remote Licenses ☑ You may experience a delay of a few minutes before your changes take effect.

Broadcast Search for Remote Licenses □

Aggressive Search for Remote Licenses ☑

Remote License Search Parameters UOS-207790

d. Is the network dongle listed in the Options > Sentinel Keys page?

e. If not, go to http://localhost:1947/_int_/config_to.html, ensure the Aggressive Search for Remote Licenses checkbox is checked and ensure the correct server name or IP address is set in the Remote License Search Parameters edit box.

f. Click Submit and wait a few minutes to see if the network dongle is detected by the client.

3 OFF SITE SERVER & VPN CONNECTION AVAILABLE

3.1 Server configuration

As per Section 1.1.

3.2 Client configuration

Connect via VPN with your usual login details, then proceed as per 2.2 but type the server's IP address in the Access to Remote License Manager page (Figure 6) > Remote License Search Parameters edit box.

4 NOTES FOR ADVANCED USERS

4.1 How to gain remote access to the server’s Admin Control Center (not recommended)

a. Ensure the client is connected to the network.

b. On the client, open a web browser and type
http://<server’s machine name or server’s IP address>:1947
eg http://UOS-207790:1947

c. If you get a ‘403 Forbidden’ access denied error message, then the server side Admin Control Centre may not allow remote connections. This option can be enabled as follows:

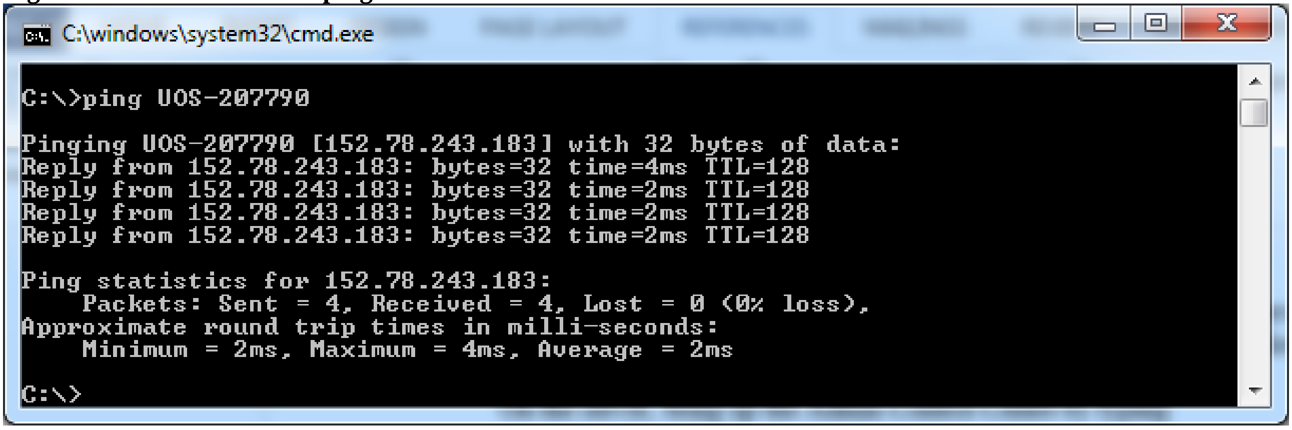
On the server, bring up the Admin Control Centre by typing
http://localhost:1947
in the server’s web browser and ensure the ‘Allow Remote Access to ACC’ option found in Options>Configuration>Basic Settings is checked.

d. Repeat step b. above.

4.2 What if the client’s Admin Control Centre does not show the network dongle?

a. Ensure the client is seeing the server and vice versa? On each machine, ping the other one from the command prompt. If either ping is unsuccessful the remote license cannot be obtained.

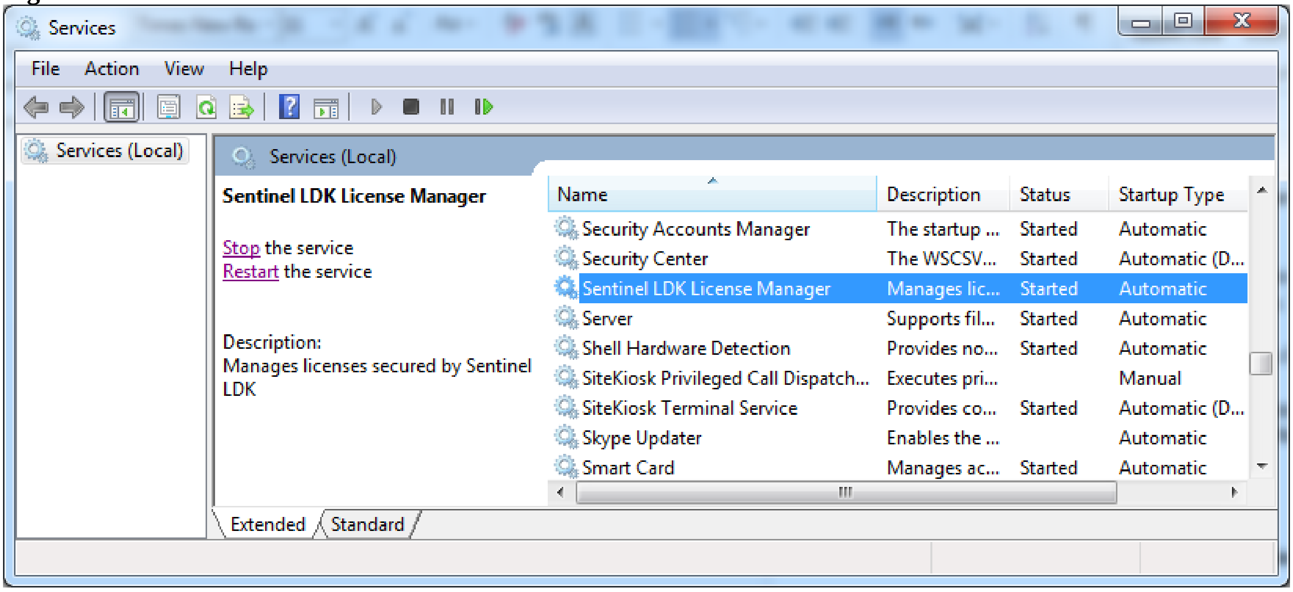
Figure 7 - Successful server ping from client



```
C:\>ping UOS-207790

Pinging UOS-207790 [152.78.243.183] with 32 bytes of data:
Reply from 152.78.243.183: bytes=32 time=4ms TTL=128
Reply from 152.78.243.183: bytes=32 time=2ms TTL=128
Reply from 152.78.243.183: bytes=32 time=2ms TTL=128
Reply from 152.78.243.183: bytes=32 time=2ms TTL=128

Ping statistics for 152.78.243.183:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 4ms, Average = 2ms

C:\>
```

b. Ensure the License Manager is switched on. Type ‘services.msc’ in the W7 start button > search field. This brings up the Services window. Select the ‘Sentinel LDK License Manager’ and restart this service via the ‘Restart’ option.

Figure 8 – Service restart



Sentinel LDK License Manager

Stop the service
Restart the service

Description:
Manages licenses secured by Sentinel LDK

Name	Description	Status	Startup Type
Security Accounts Manager	The startup ...	Started	Automatic
Security Center	The WSCSV...	Started	Automatic (D...
Sentinel LDK License Manager	Manages lic...	Started	Automatic
Server	Supports fil...	Started	Automatic
Shell Hardware Detection	Provides no...	Started	Automatic
SiteKiosk Privileged Call Dispatch...	Executes pri...		Manual
SiteKiosk Terminal Service	Provides co...	Started	Automatic (D...
Skype Updater	Enables the ...		Automatic
Smart Card	Manages ac...	Started	Automatic

c. Is a Firewall or Antivirus blocking port 1947 (Sentinel port)? If so, you should open that port. On Windows Firewall this means creating a new Inbound Rule on the server and (possibly) a new Outbound Rule for the client. Open the Win Firewall by searching for Windows Firewall with Advanced Security in the Start button > Search box. Figure 9 to Figure 15 below show how to create an Inbound Rule on the server:

Figure 9

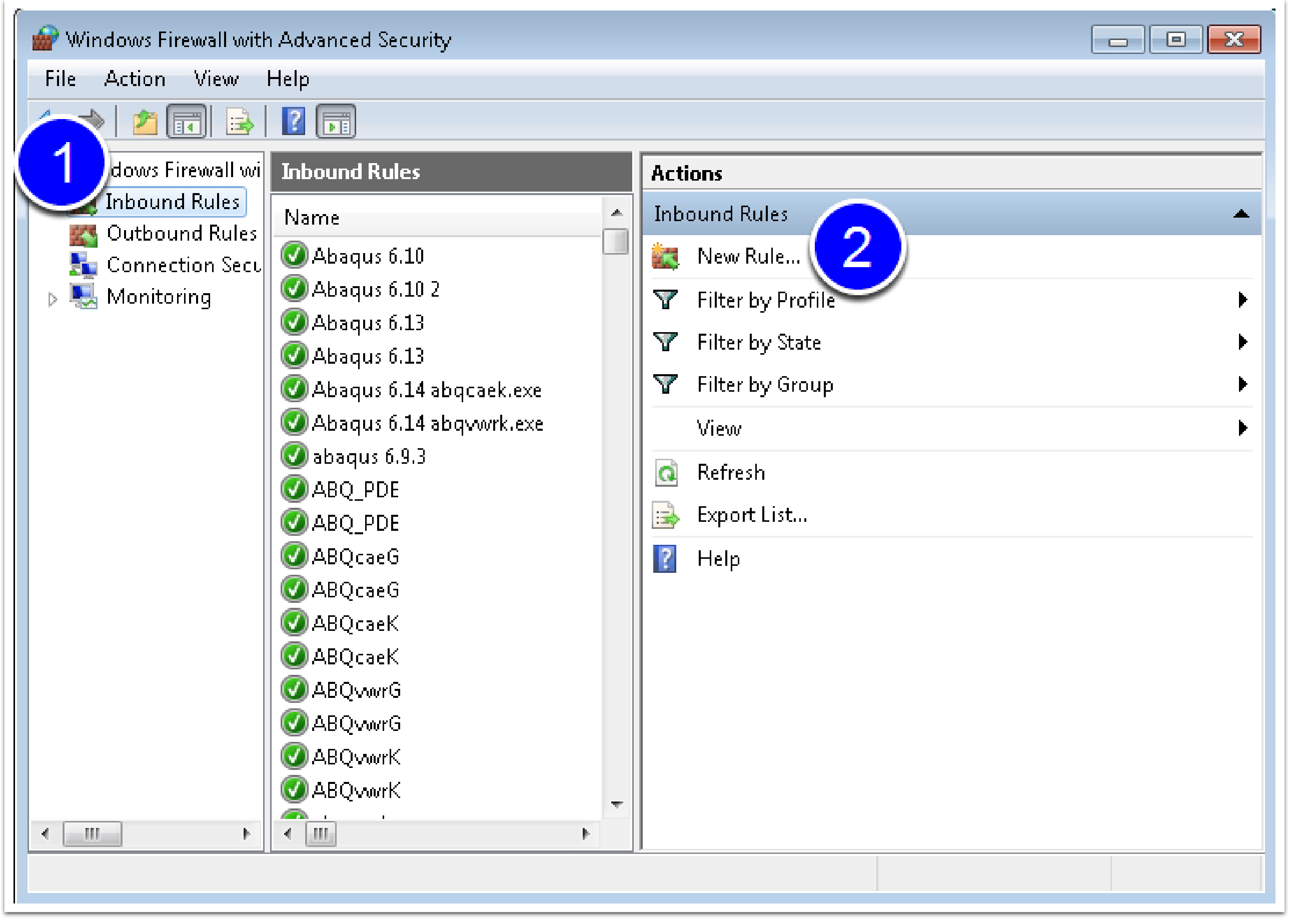
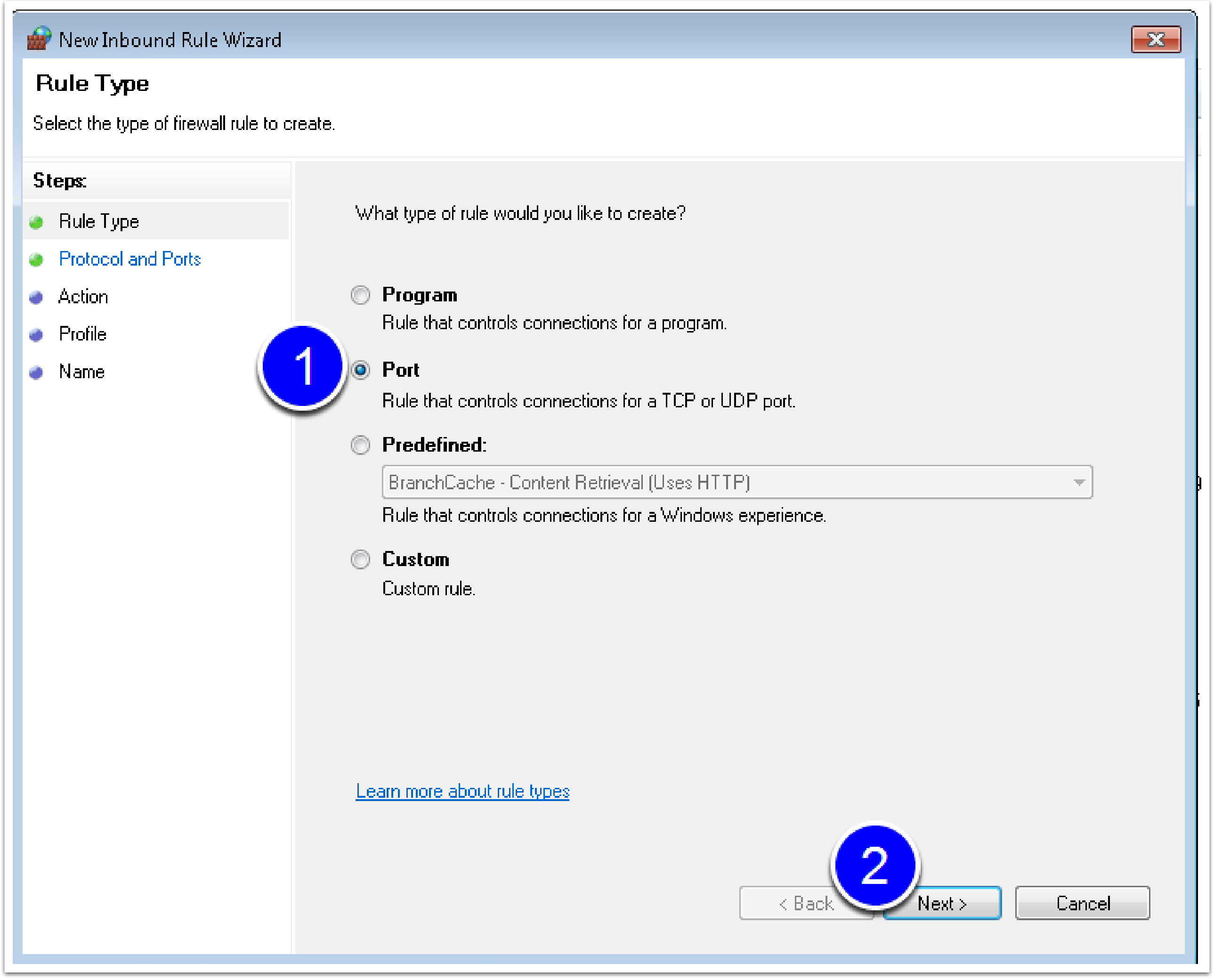


Figure 10



Rule Type

Select the type of firewall rule to create.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

What type of rule would you like to create?

○ **Program**
Rule that controls connections for a program.

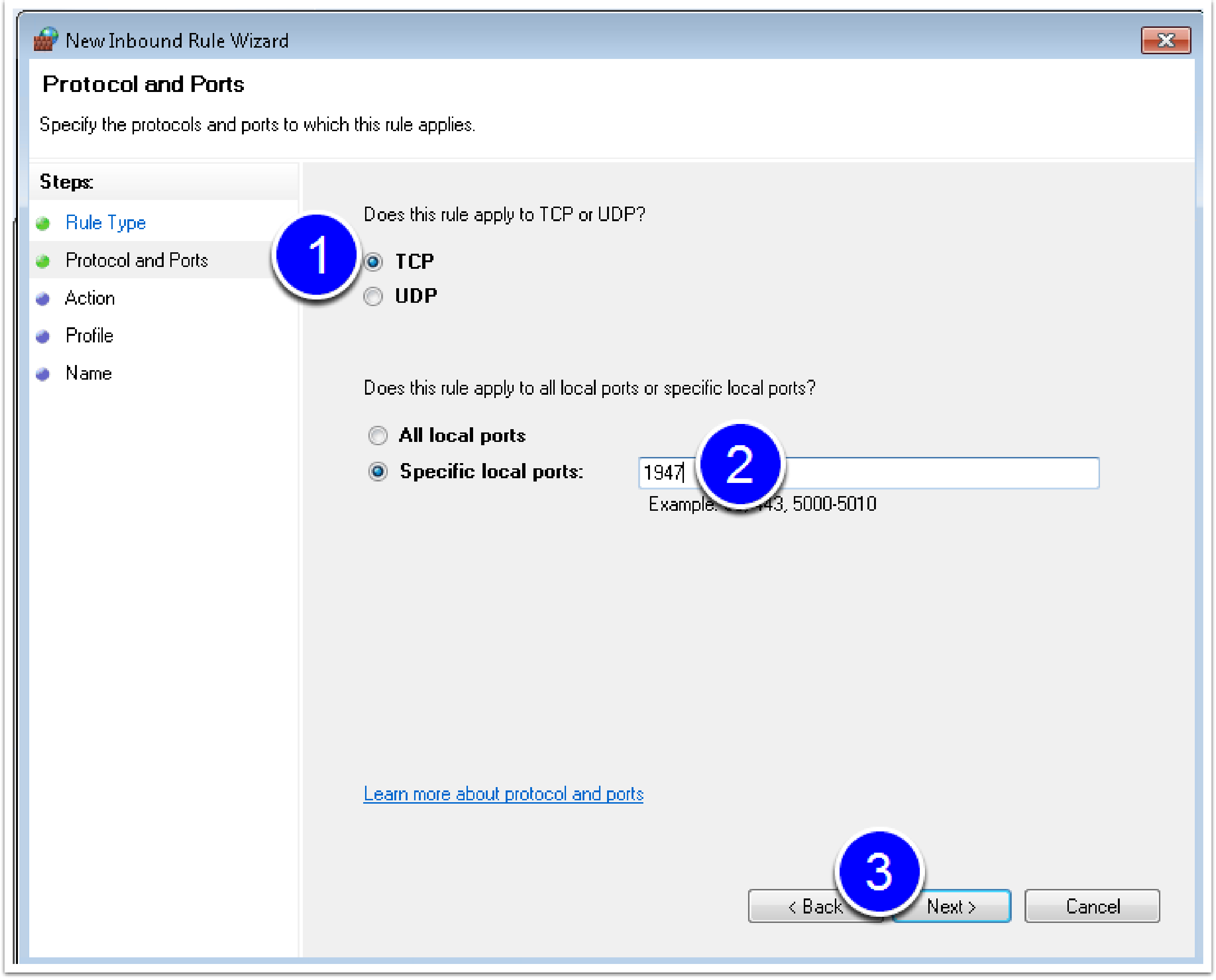
● **Port**
Rule that controls connections for a TCP or UDP port.

○ **Predefined:**
BranchCache - Content Retrieval (Uses HTTP)
Rule that controls connections for a Windows experience.

○ **Custom**
Custom rule.

Learn more about rule types

Figure 11



New Inbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Does this rule apply to TCP or UDP?

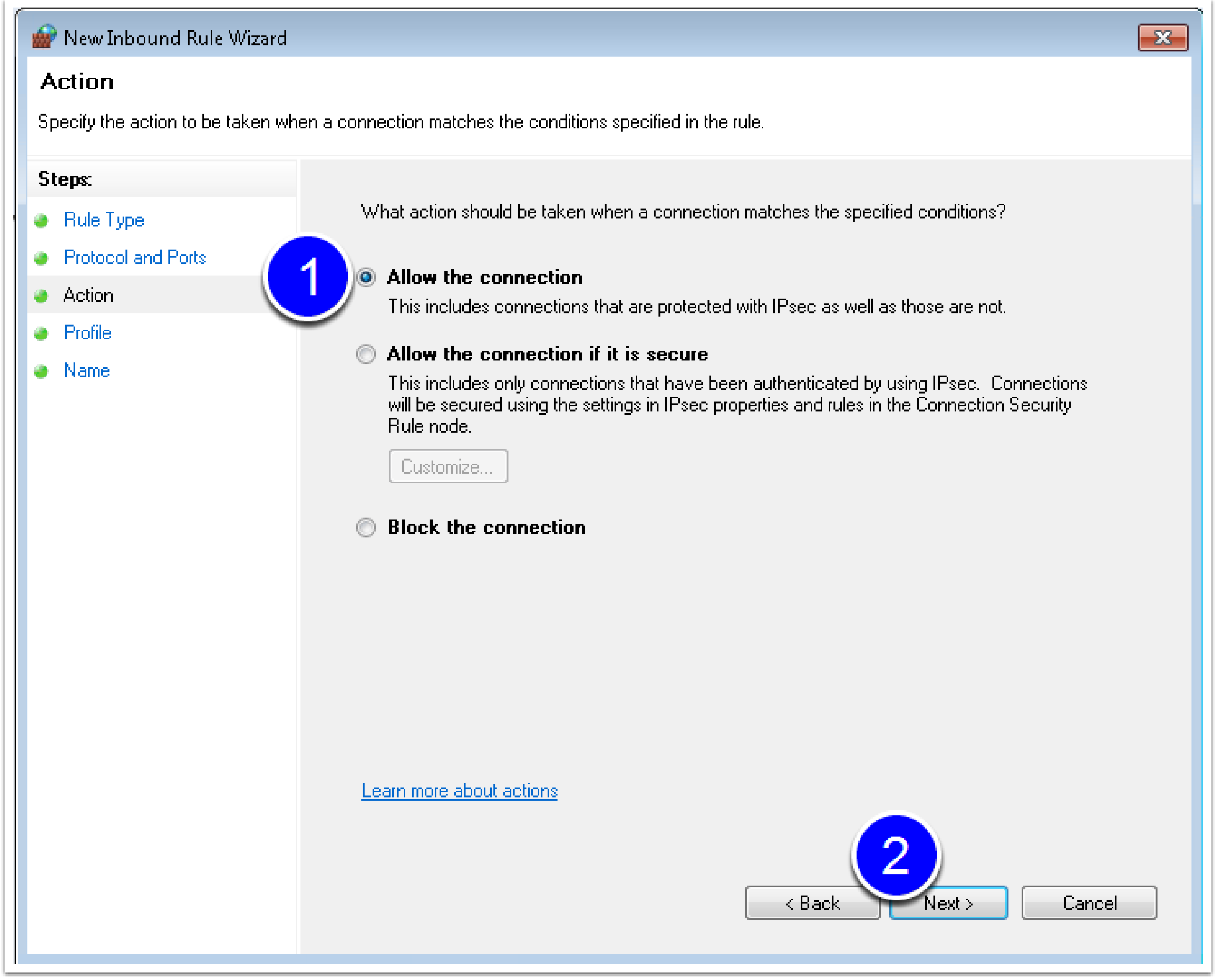
● TCP
○ UDP

Does this rule apply to all local ports or specific local ports?

○ All local ports
● Specific local ports: 1947

Example: 80, 443, 5000-5010

Figure 12



New Inbound Rule Wizard

Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

What action should be taken when a connection matches the specified conditions?

● Allow the connection

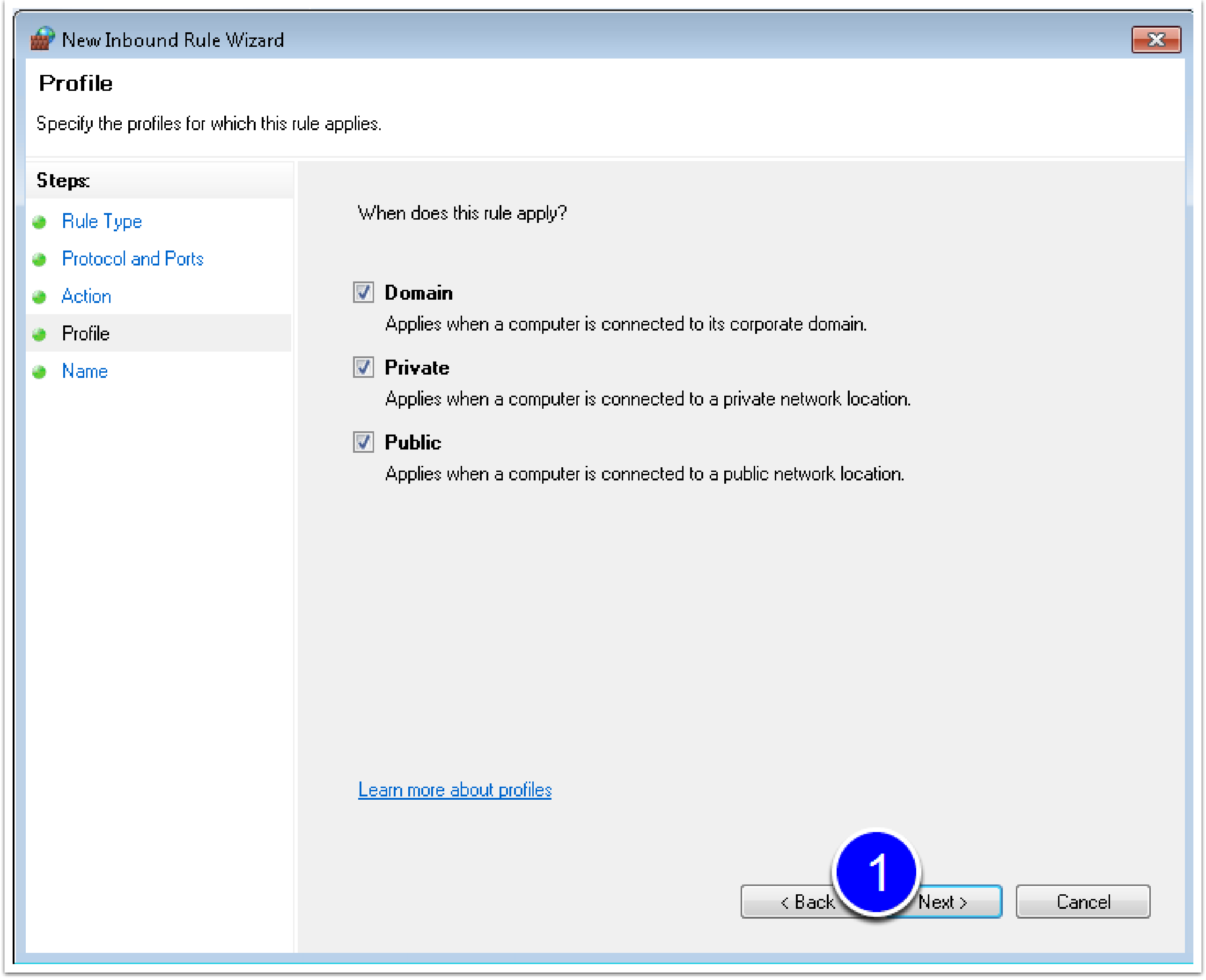
This includes connections that are protected with IPsec as well as those are not.

○ Allow the connection if it is secure

This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

○ Block the connection

Figure 13



New Inbound Rule Wizard

Profile

Specify the profiles for which this rule applies.

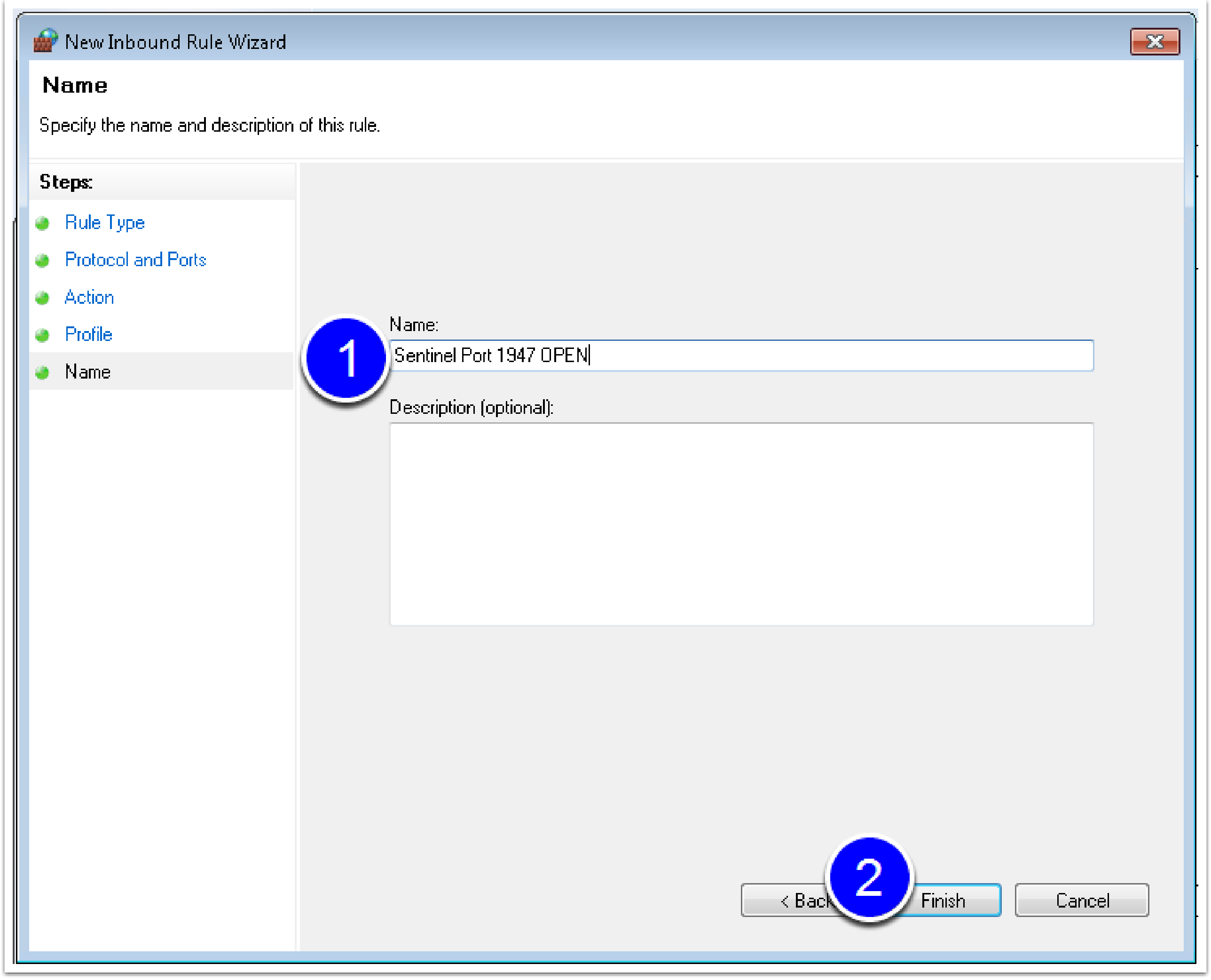
When does this rule apply?

☑ **Domain**
Applies when a computer is connected to its corporate domain.

☑ **Private**
Applies when a computer is connected to a private network location.

☑ **Public**
Applies when a computer is connected to a public network location.

Figure 14



New Inbound Rule Wizard

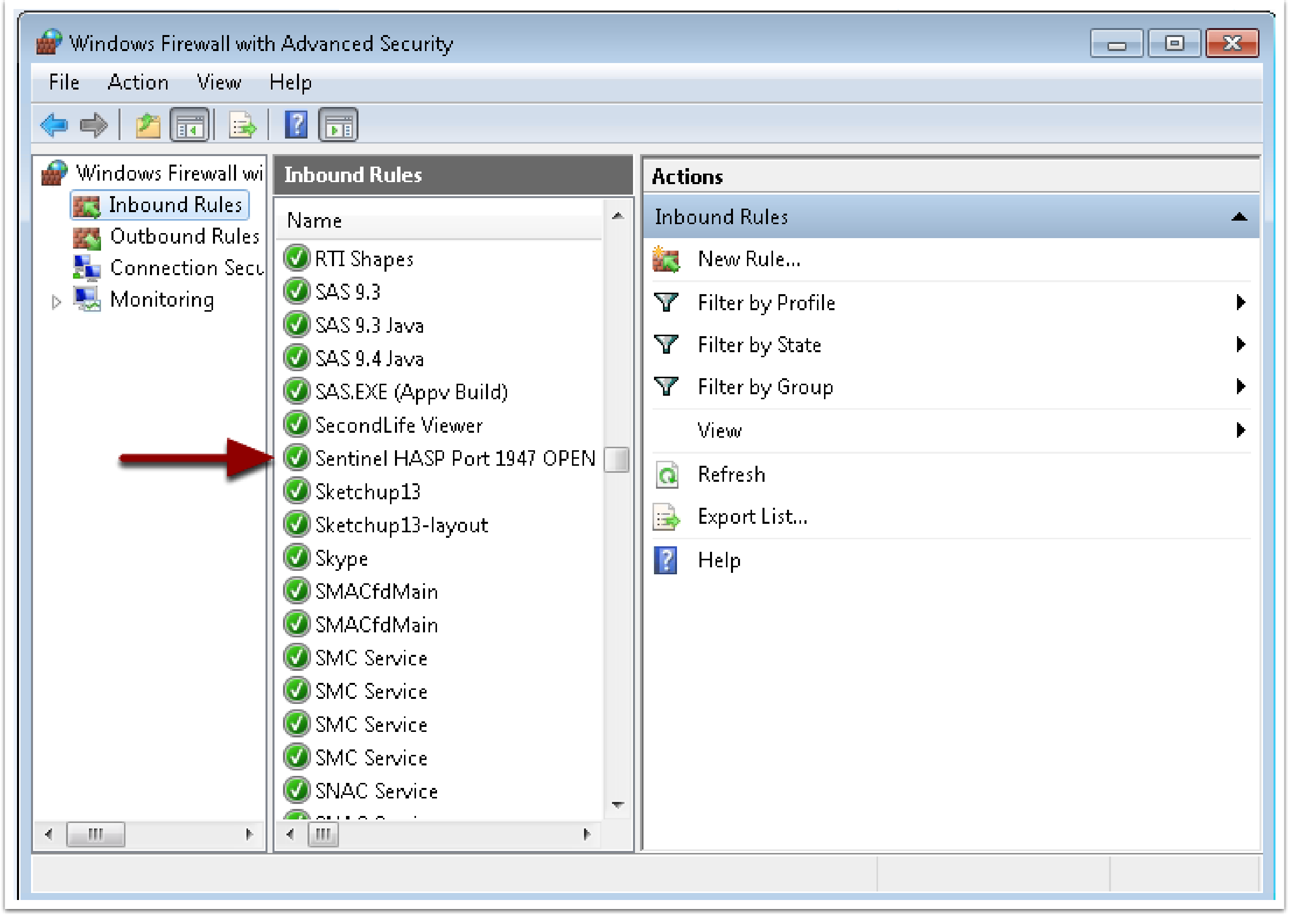
Name

Specify the name and description of this rule.

Name: Sentinel Port 1947 OPEN

Description (optional):

Figure 15



Windows Firewall with Advanced Security

Inbound Rules

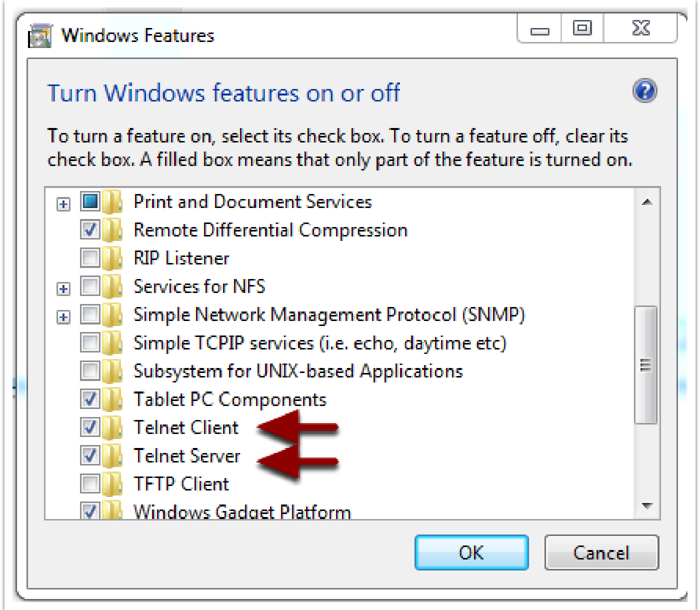
Name

- RTI Shapes
- SAS 9.3
- SAS 9.3 Java
- SAS 9.4 Java
- SAS.EXE (Appv Build)
- SecondLife Viewer
- Sentinel HASP Port 1947 OPEN
- Sketchup13
- Sketchup13-layout
- Skype
- SMACfdMain
- SMACfdMain
- SMC Service
- SMC Service
- SMC Service
- SMC Service
- SNAC Service

d. Can you access port 1947 at all? Try checking port access via the **telnet** command.

First, enable the telnet feature via Control Panel > Programs & Features > Turn Windows features on or off > check Telnet Client and Telnet Server as indicated in Figure 16.

Figure 16



Windows Features

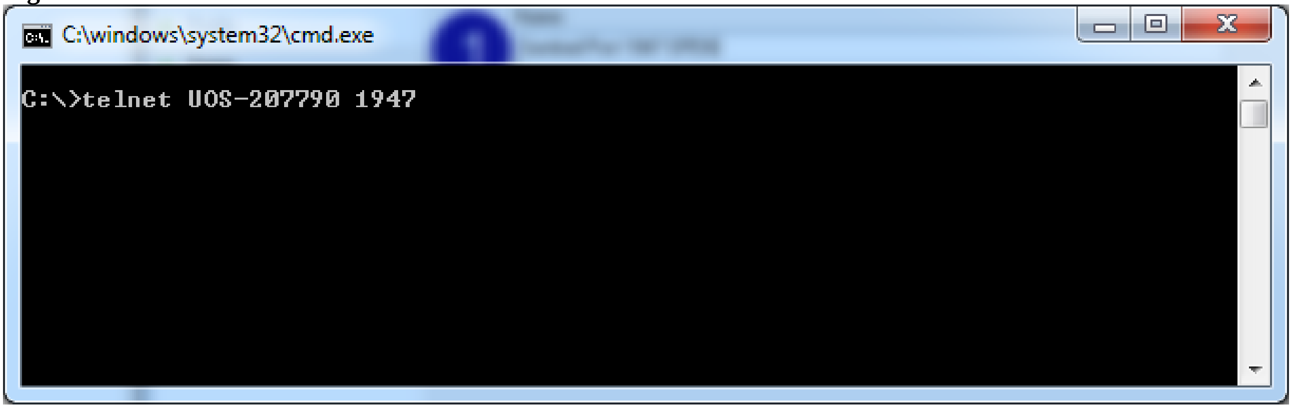
Turn Windows features on or off

To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.

- ■ Print and Document Services
- ☑ Remote Differential Compression
- □ RIP Listener
- □ Services for NFS
- □ Simple Network Management Protocol (SNMP)
- □ Simple TCPIP services (i.e. echo, daytime etc)
- □ Subsystem for UNIX-based Applications
- ☑ Tablet PC Components
- ☑ Telnet Client
- ☑ Telnet Server
- □ TFTP Client
- ☑ Windows Gadget Platform

Then open a command prompt window by clicking on the Windows Start button and typing ‘cmd’ in the ‘Search programs and fields’. Hit enter, then type
telnet <name or IP address of other machine> 1947, syntax as per Figure 17 below.

Figure 17



```
C:\>telnet UOS-207790 1947
```