

By: Matteo Scarponi

Date: 01/06/2026

Subject: Sentinel HASP Network license setup

1 SCOPE

This technical note describes how to set up a Sentinel HASP Network dongle for your Wolfson Software on a simple Windows 11 Enterprise (x64) network.

The network dongle used for these tests is a Sentinel HL Net 50 and the networked machines are:

| Device name | Device type | Operating System (OS) | OS Version |
|-------------|-------------|---------------------------|-----------------|
| uos-9tsdb94 | server | Windows 11 Enterprise x64 | 10.0.26200 25H2 |
| uos-3ch6d44 | client | Windows 11 Enterprise x64 | 10.0.26200 25H2 |

NOTE: any **Windows machine can act as a Sentinel license server**, you do not need a dedicated server. If a standard machine is used as a server, ensure its Power Plan is adjusted so the computer never sleeps and licenses can be served 24/7. The power plan can typically be changed at: Control Panel > Hardware and Sound > Power Options.

2 SERVER-SIDE CONFIGURATION

- Download and install the 'Sentinel LDK Windows GUI Runtime Installer 10.31' (file name: **DOW0003347**) from [this link](#) on the Thales Customer Support Portal.
- Open a web browser and type: http://localhost:1947/_int_/devices.html This brings up the Sentinel Admin Control Center (ACC).
- Plug in your Sentinel HASP Network dongle.
- In the ACC select 'Sentinel Keys' on the left hand side menu. Your Sentinel key should be listed in the main page as a 'Sentinel HL Net' Key Type, eg:

Figure 1 Sentinel ACC > Sentinel Keys page

| Location | Vendor | Key ID | Key Type | Configuration | Version | Sessions | Actions |
|----------|---------------|------------|-------------------------|---------------|---------|----------|---|
| Local | 89648 (89648) | 1878642919 | Sentinel HL Net 50 | HASP | 4.27 | | Products Blink on |
| Local | WCKRM (89648) | 800492322 | Sentinel HASP Master | Midi | 3.25 | | Features Sessions Blink on C2V |
| Local | 89648 (89648) | | Reserved for New SL Key | SL | 10.31 | | Fingerprint |

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

Figure 2 Configuration > Basic Settings page

Ensure the Machine Name edit box shows the server’s name. Leave all other settings as per default (click the ‘Set Defaults’ button to restore the default settings if necessary). Click ‘Submit’.

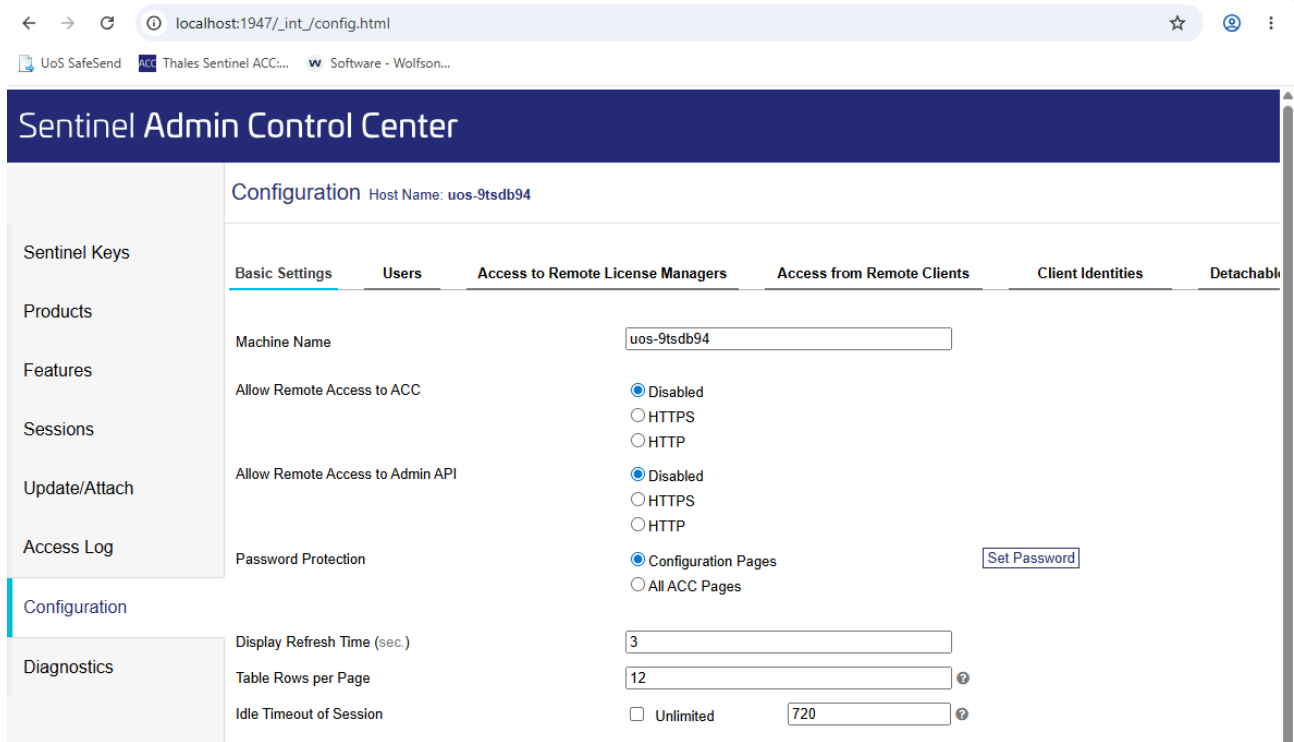


Figure 3 Configuration > Users page

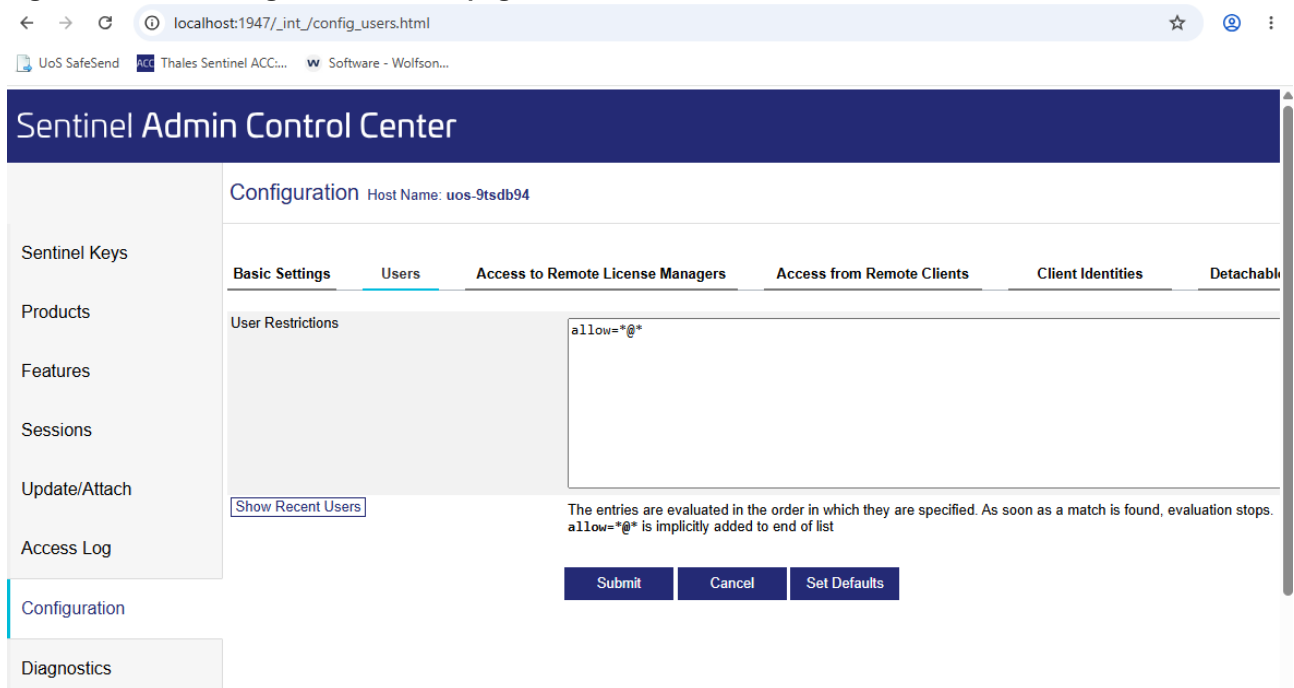
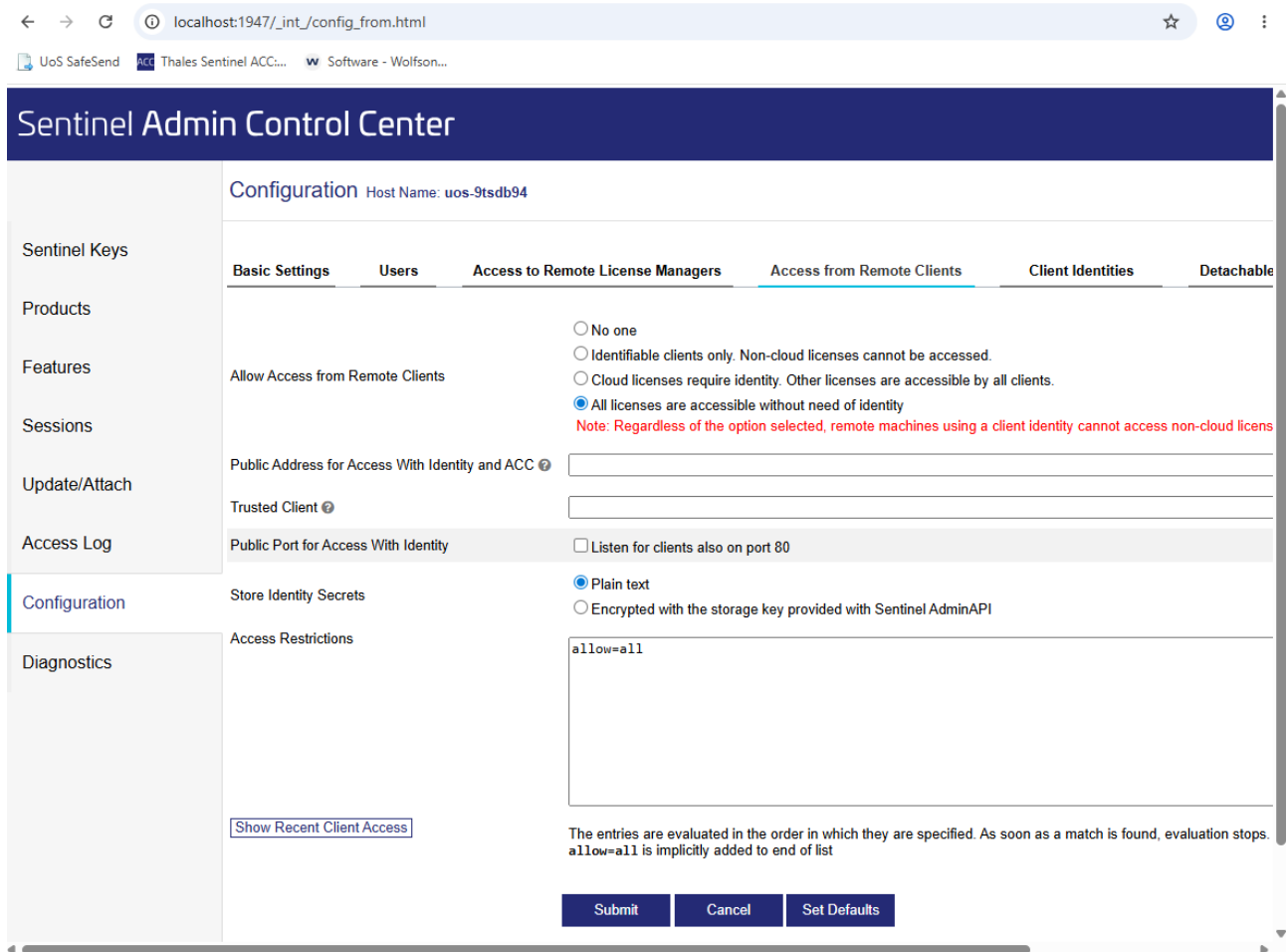


Figure 4 Configuration > Access from Remote Clients page



3 CLIENT-SIDE CONFIGURATION

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

Figure 5 Configuration > Basic Settings page

Again, type the server's name and leave all other settings as per default:

Sentinel Admin Control Center

- Sentinel Keys
- Products
- Features
- Sessions
- Update/Attach
- Access Log
- Configuration
- Diagnostics

Configuration Host Name: uos-3ch6d44

Basic Settings
Users
Access to Remote License Managers
Access from Remote Clients
Client Identities

Machine Name

Allow Remote Access to ACC
 Disabled
 HTTPS
 HTTP

Allow Remote Access to Admin API
 Disabled
 HTTPS
 HTTP

Password Protection
 Configuration Pages
 All ACC Pages

Display Refresh Time (sec.)

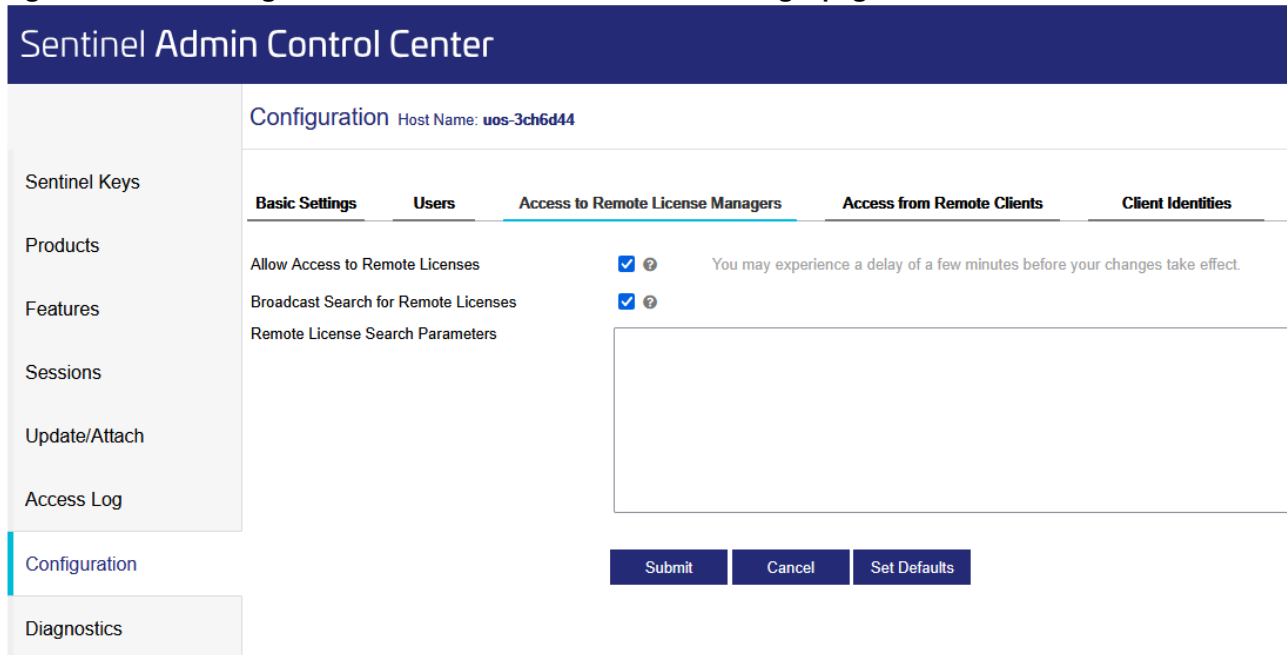
Table Rows per Page ?

Idle Timeout of Session
 Unlimited ?

Write an Access Log File
 Size Limit (KB): ?

Include Local Requests

Figure 6 Configuration > Access to Remote License Manager page



- d. Is the network dongle listed in the Sentinel Keys page?
- e. If not, go to http://localhost:1947/_int_/config_to.html 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.

4 OFF SITE SERVER & VPN CONNECTION AVAILABLE

NOTE: to enable this facility, the customer's Network dongle must have been coded with the 'Network accessibility' option enabled. This additional facility is not available on standard Network dongles. For more information, please contact the Wolfson Unit.

4.1 Server configuration

As per Section 2.

4.2 Client configuration

Connect via VPN with your usual login details, then proceed as per Section 3 but type the **server's IP address** in the Access to Remote License Manager page (Figure 6) > Remote License Search Parameters edit box.

5 NOTES FOR ADVANCED USERS

5.1 What if the client's Admin Control Centre does not show the network dongle?

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

Figure 7 – Example of successful server ping from client

```

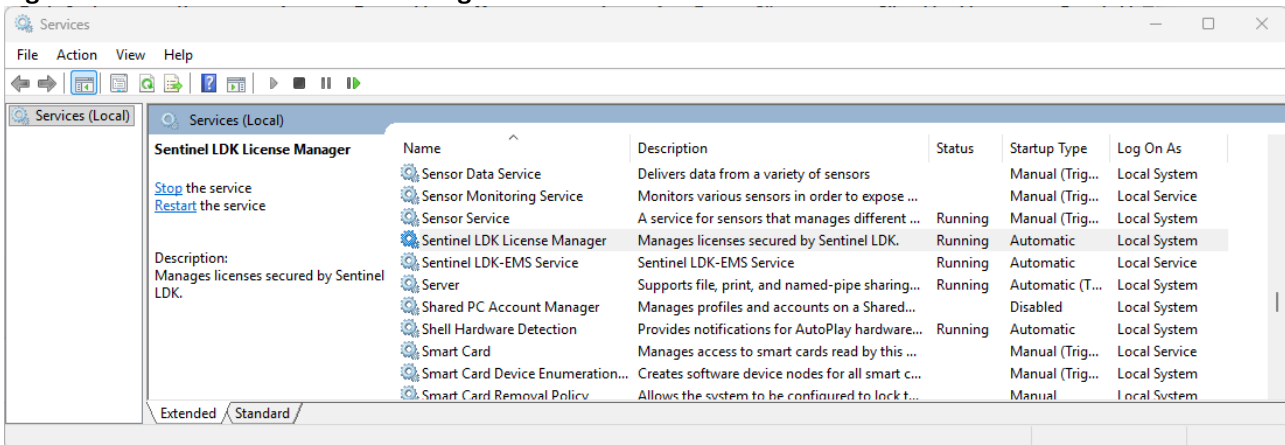
Windows PowerShell
PS C:\> ping uos-9tsdb94

Pinging uos-9tsdb94.clients.soton.ac.uk [10.15.49.170] with 32 bytes of data:
Reply from 10.15.49.170: bytes=32 time=1ms TTL=128
Reply from 10.15.49.170: bytes=32 time=2ms TTL=128
Reply from 10.15.49.170: bytes=32 time=1ms TTL=128
Reply from 10.15.49.170: bytes=32 time=1ms TTL=128

Ping statistics for 10.15.49.170:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
PS C:\>
    
```

- b. Ensure the Client-side License Manager is switched on. Type 'services.msc' in the Windows 11 Search box by the Start button. This brings up the Services window. Right click the 'Sentinel LDK License Manager' and restart this service via the 'Restart' option in the pop-up menu.

Figure 8 – 'Sentinel LDK License Manager' service restart



- c. Is a Firewall or Antivirus blocking port 1947 (ie the Sentinel port)? If so, open that port. On Windows Defender Firewall this means:
- creating a new Inbound Rule on the server, and
 - creating a new Outbound Rule on the client.

Open the Windows Defender Firewall > Advanced Settings then follow the process described in Figure 9 to Figure 15 to create an Inbound Rule on the server. Follow the same procedure for the client.

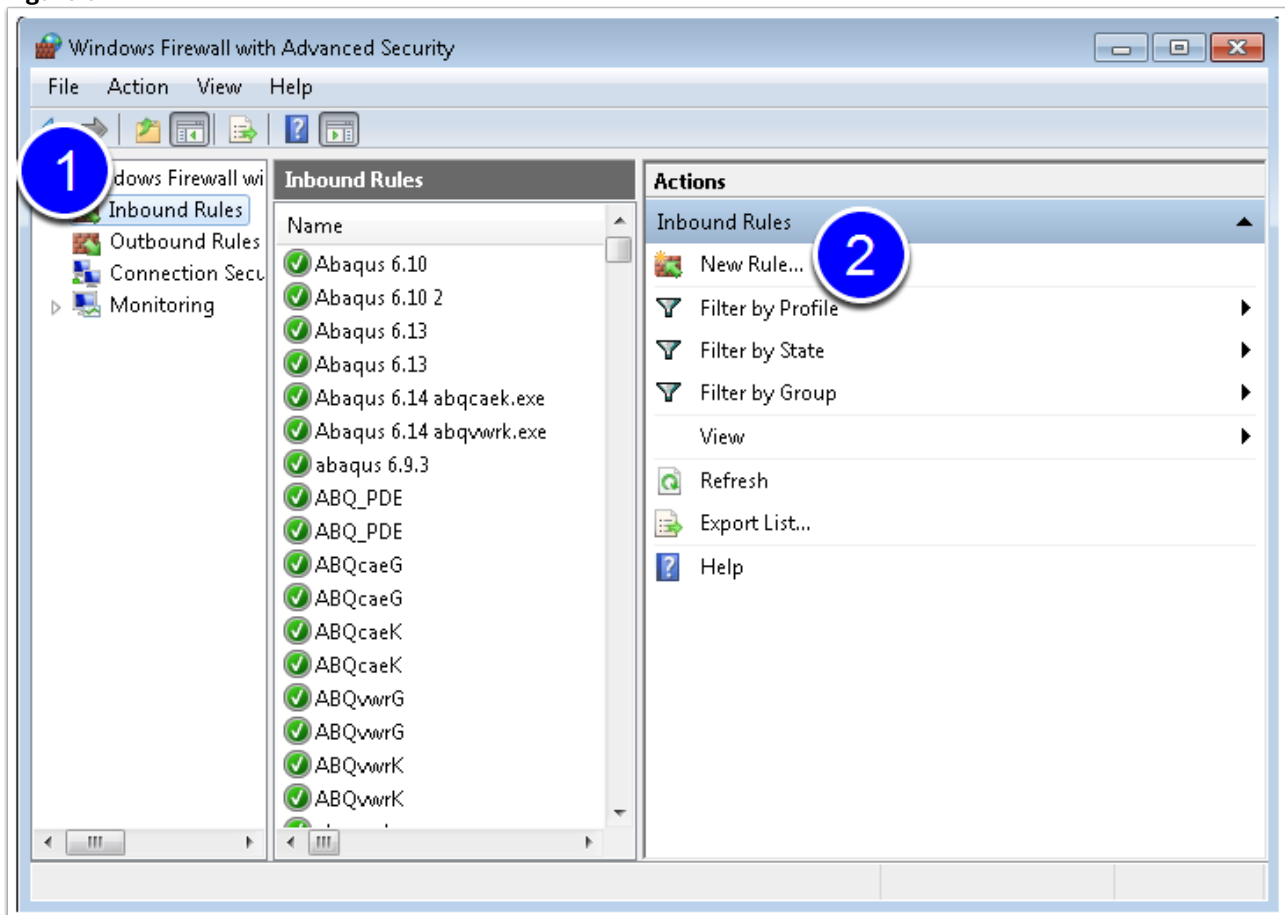
Figure 9

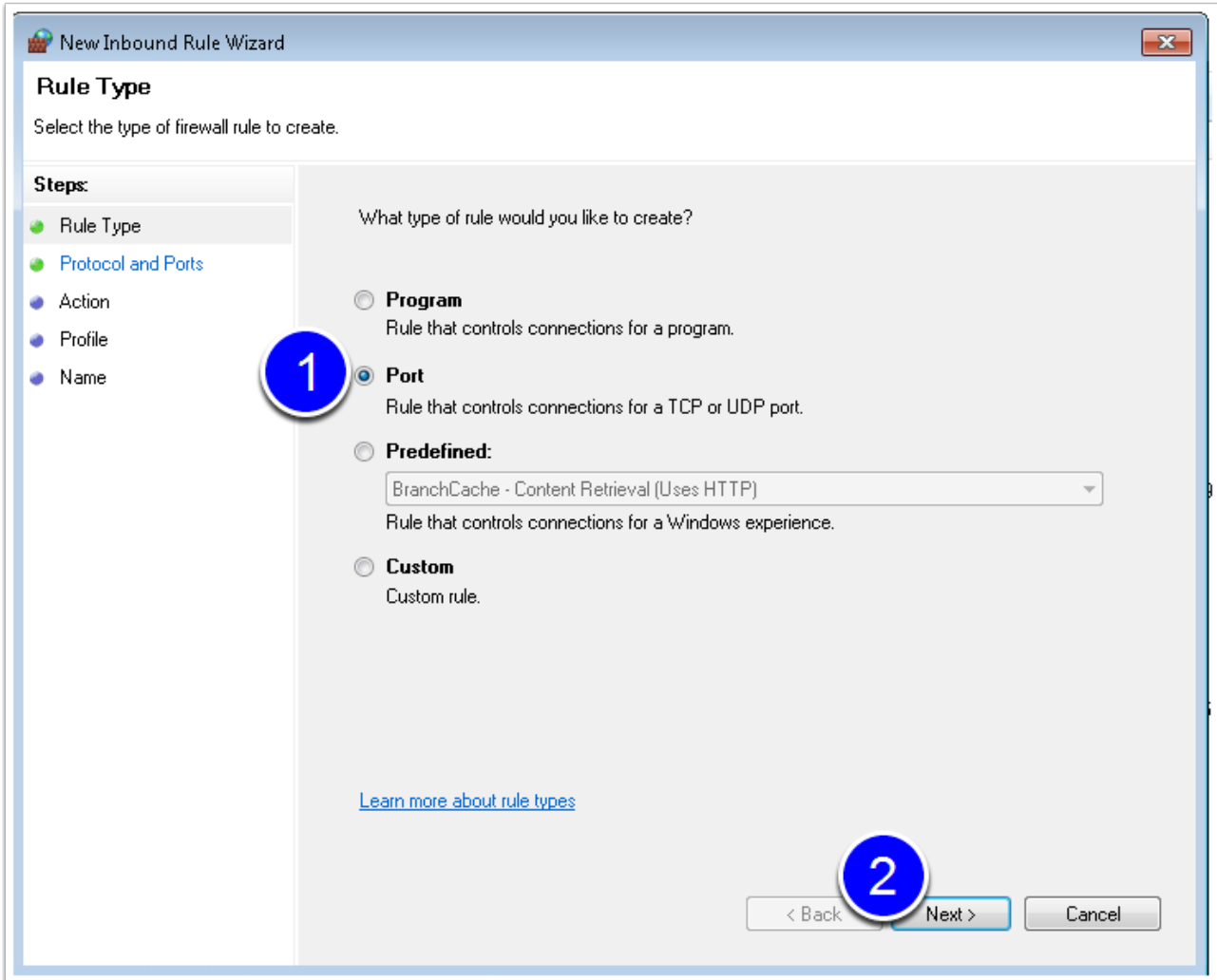
Figure 10

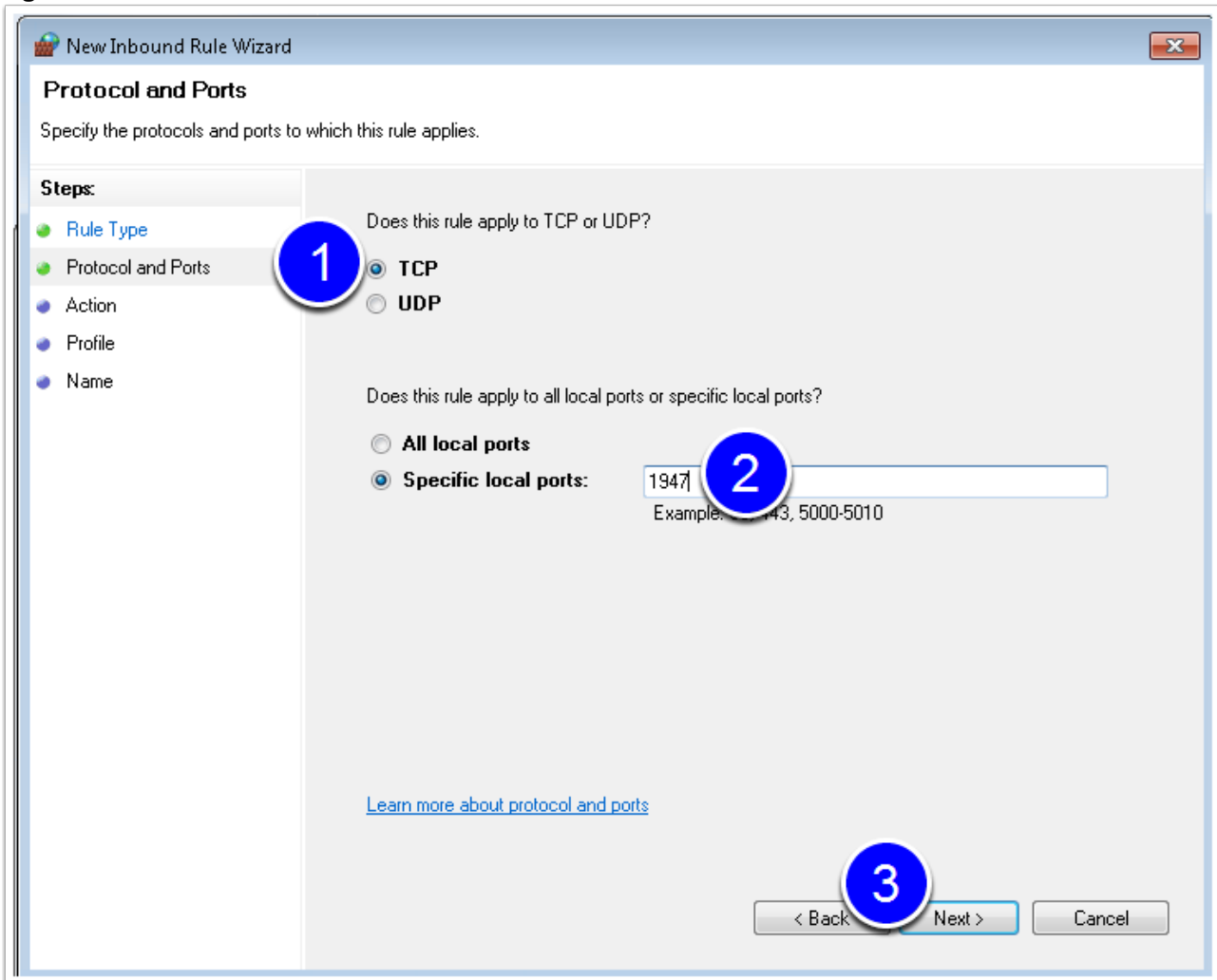
Figure 11

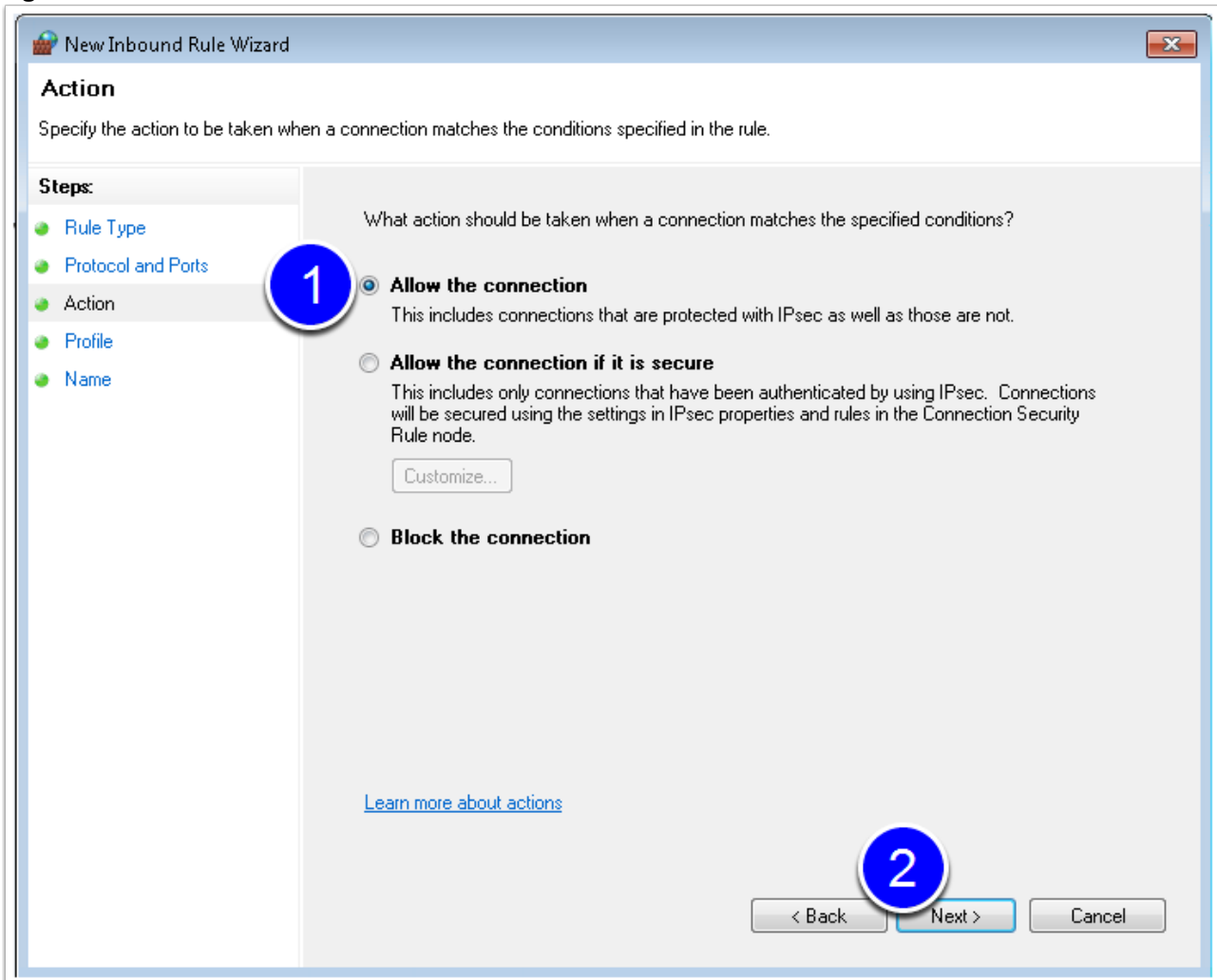
Figure 12

Figure 13

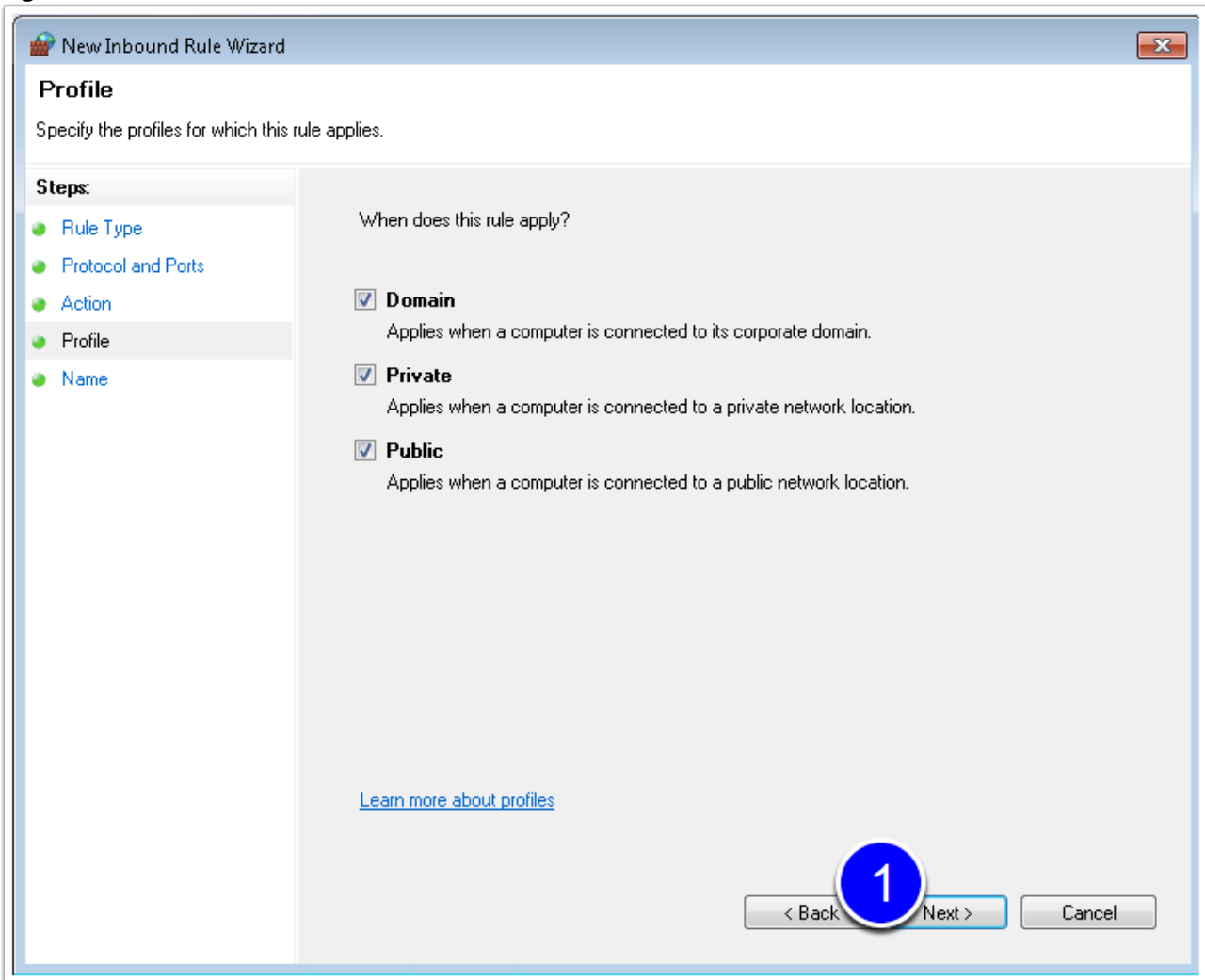


Figure 14

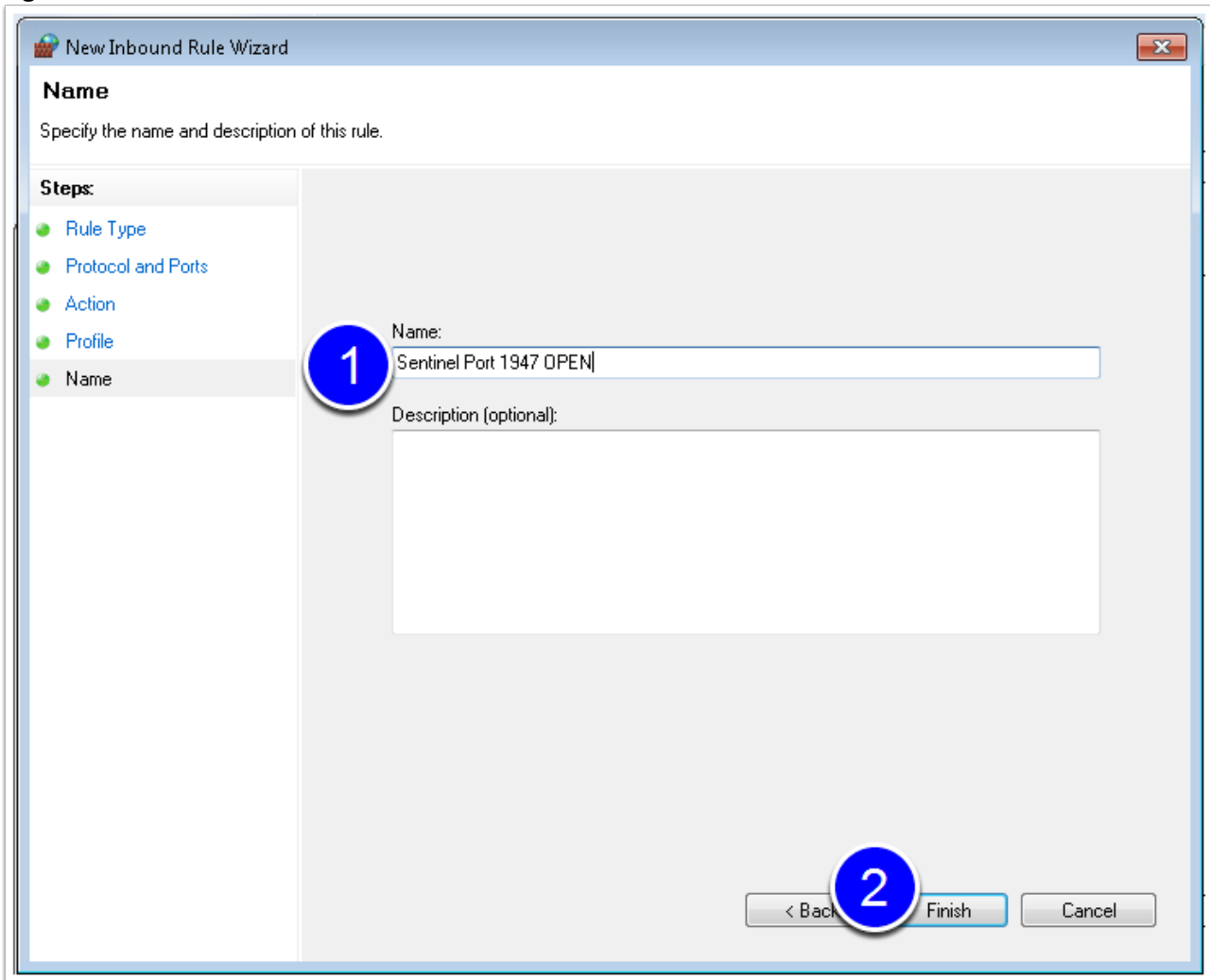
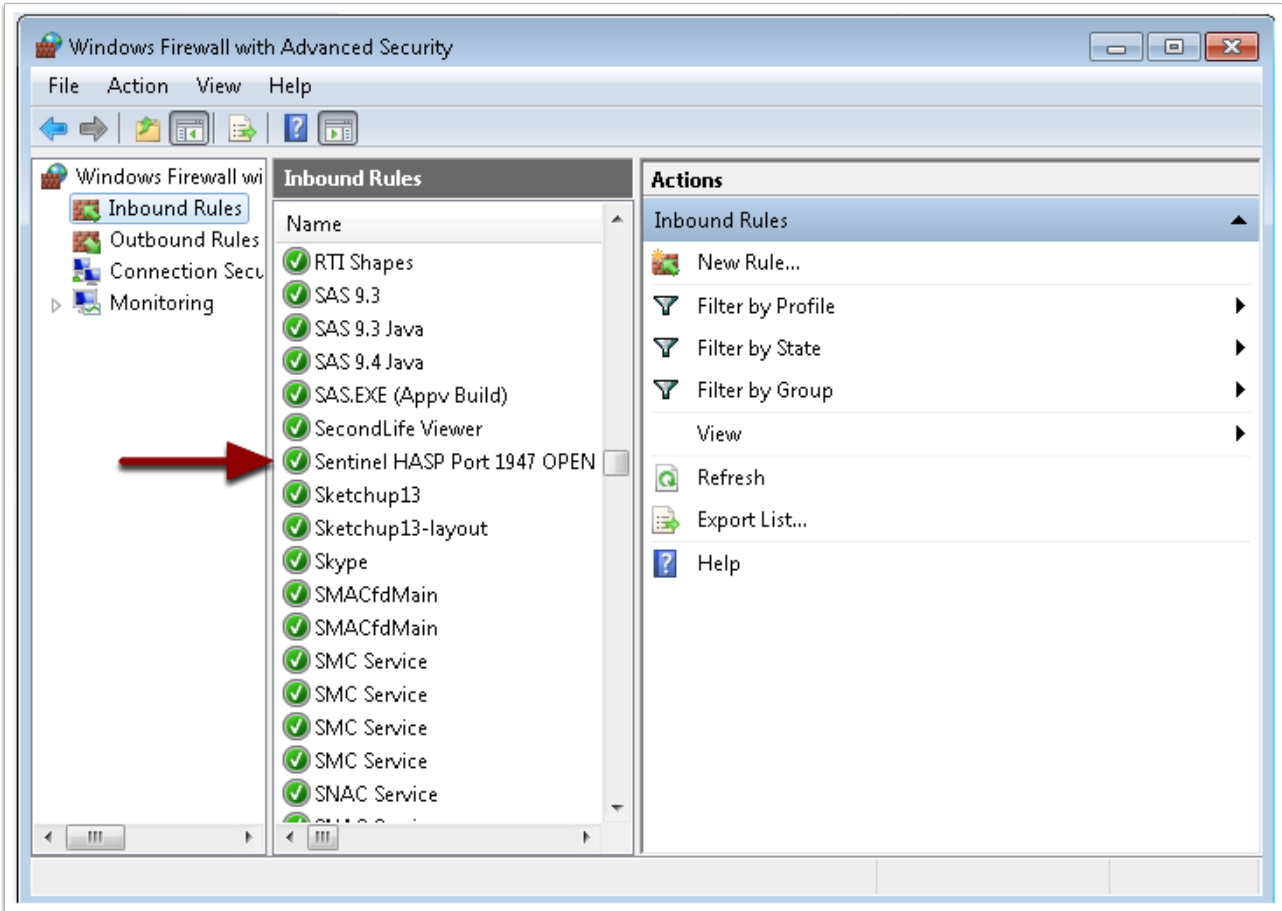


Figure 15



- d. Can you access port 1947 at all? Try checking port access via the Windows PowerShell **Test-NetConnection** command, or 'tnc'. On the server, tnc the client and vice-versa.

If the tnc is successful, Powershell will return a 'TcpTestSucceeded : True' as per the Figure 16 screenshot below:

Figure 16 Outcome of a successful Test-NetConnection on the license server, port 1947

