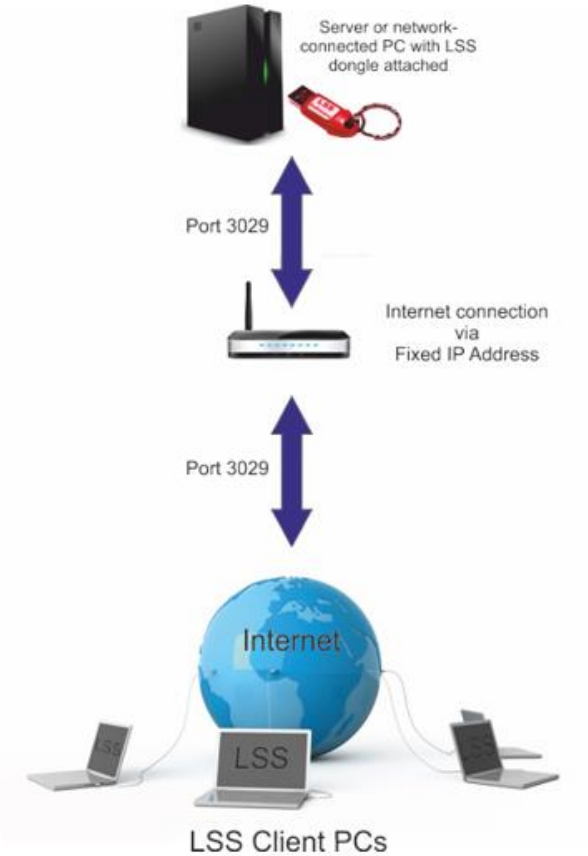
McCarthy Taylor Systems Ltd, Aerial View, Acorn House, Shab Hill, Birdlip, Gloucester, GL4 8JX
www.dtmsoftware.com support@dtmsoftware.com 01452 864244

Sharing the LSS dongle on a Local or Wide Area network



A. Server Side: Configuring an LSS network dongle

Installing an LSS dongle on a Windows server or PC on your network, for access by a remote worker

1) You will need either a fixed IP address, or a Dynamic DNS address for the location at which the dongle is installed. Make a note of the IP address of this PC. Ideally it should be a staic IP address.
2) Download, unzip and install the LSS Server Dongle drivers. https://www.dtmsoftware.com/downloads/deskey/server/DK2_v30_Install.zip Connect the LSS dongle to a USB port on the server and follow the driver install instructions.
3) On the router/modem that connects to the internet you need to create a port forwarding rule for TCP & UDP port 3029 to the IP address from (1).
4) Ensure any hardware/software firewalls in the system allow all traffic on TCP & UDP port 3029. This rule is already added on the machine from (1) after installing the drivers in (2)
5) From the DK2 network server machine visit www.whatosmyip.org and note the IP address.
6) Do not install LSS on the server unless it is to be used as an LSS user PC.

B. Client Side: Configuring LSS to access a network dongle

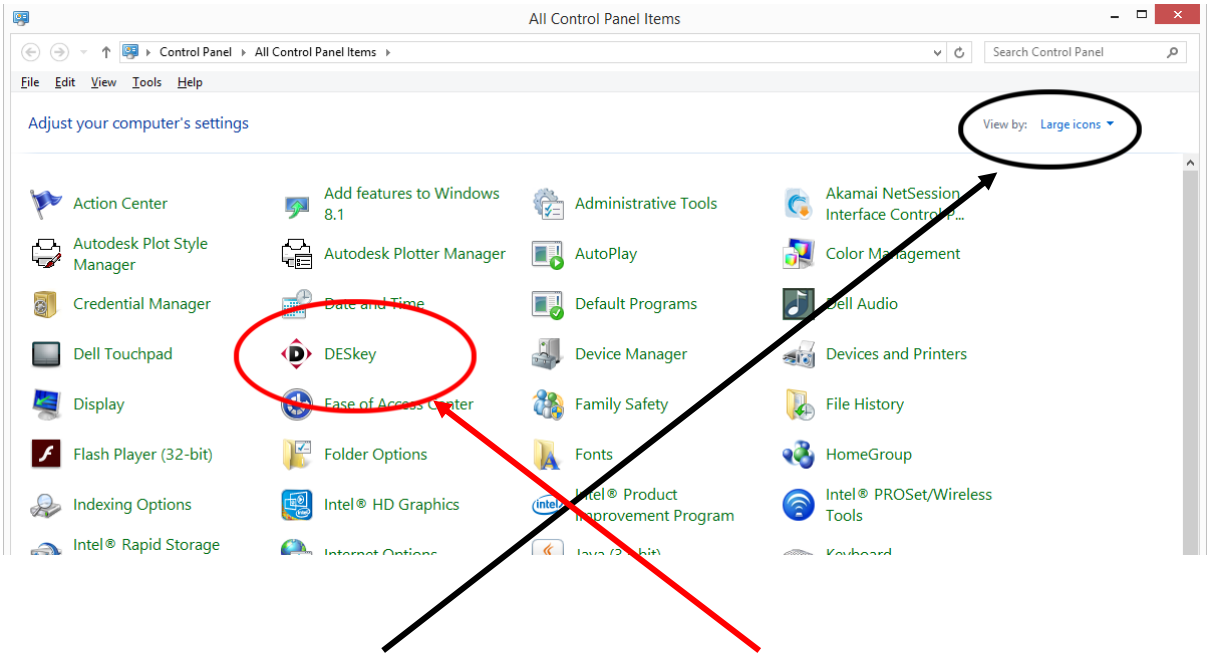
7) Install LSS and the client dongle drivers. During the dongle install you will be prompted for the location of the LSS dongle. Enter the IP address you noted down in (5)

Otherwise, if the drivers are already installed on the client PC, here's how to manually configure LSS to use a remote dongle…

C. Client Side: Manually configuring the client

If LSS has already been working on the client PC with a locally-connected dongle, you may choose to reconfigure it to access the server.

8) Access Control Panel on your computer. Windows 7 and 8 - Right mouse on the Windows (Start) icon in the lower left of your screen and select 'Control Panel'. Windows 10 - Either Right Mouse on the Windows (Start) icon in the lower left of your screen and select 'Run' and type 'Control Panel' or select Cortana and type 'Control Panel'



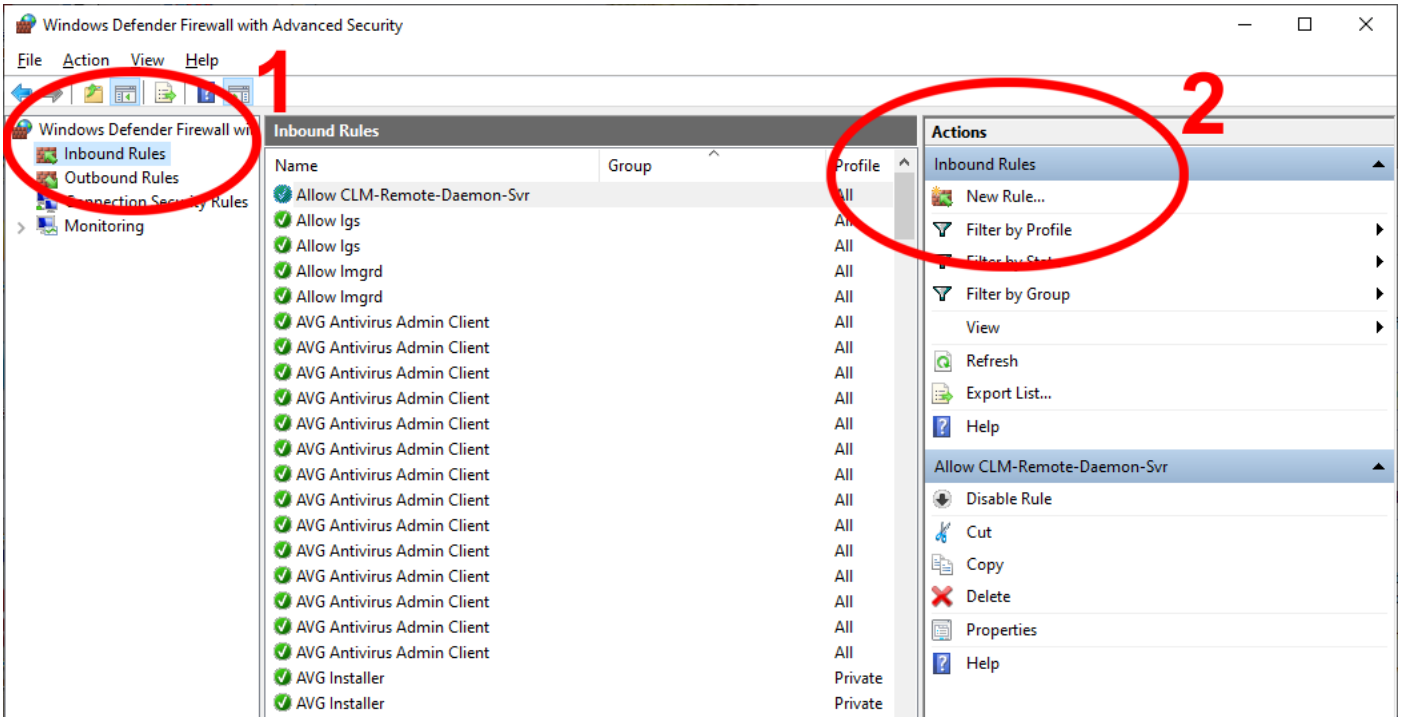
Make sure you select 'View by: large icons' and then select 'Deskey'

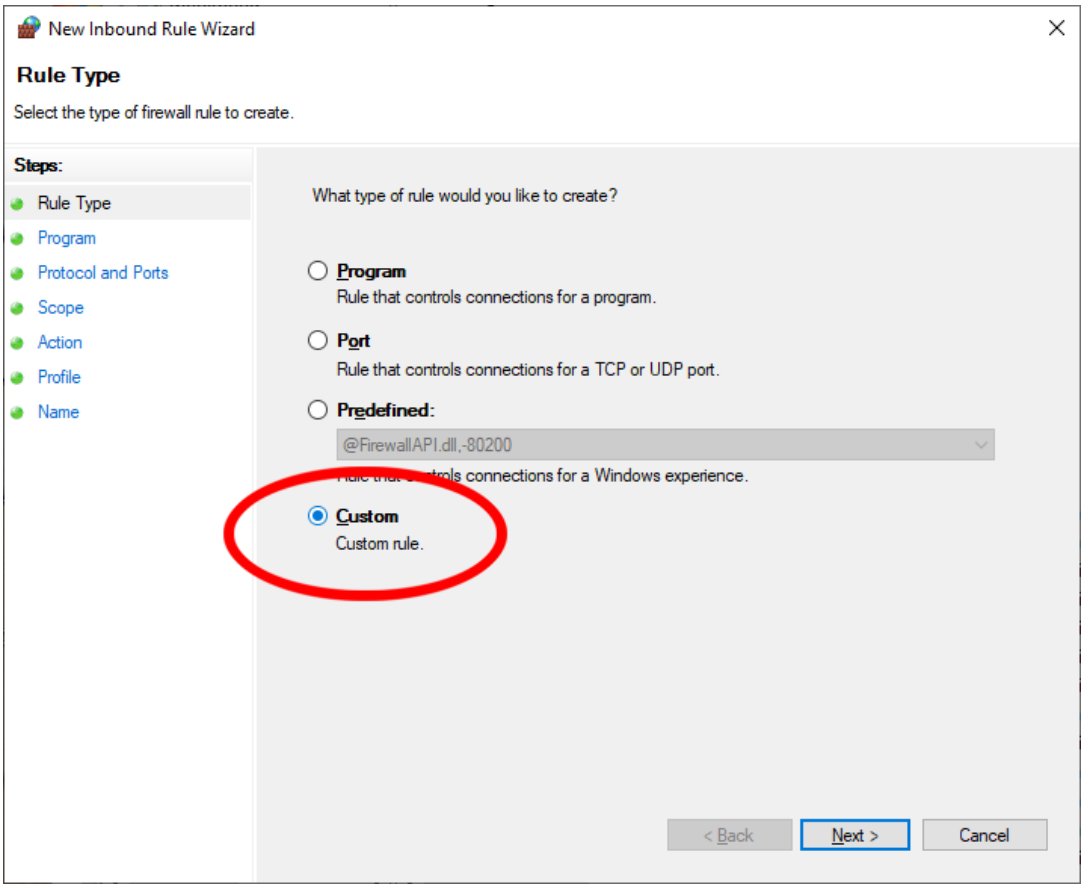
Alternatively, for a quick way in, Type "CTRL+R" and then type "dkcpanel.exe". This will take you straight to the Deskey control panel item.

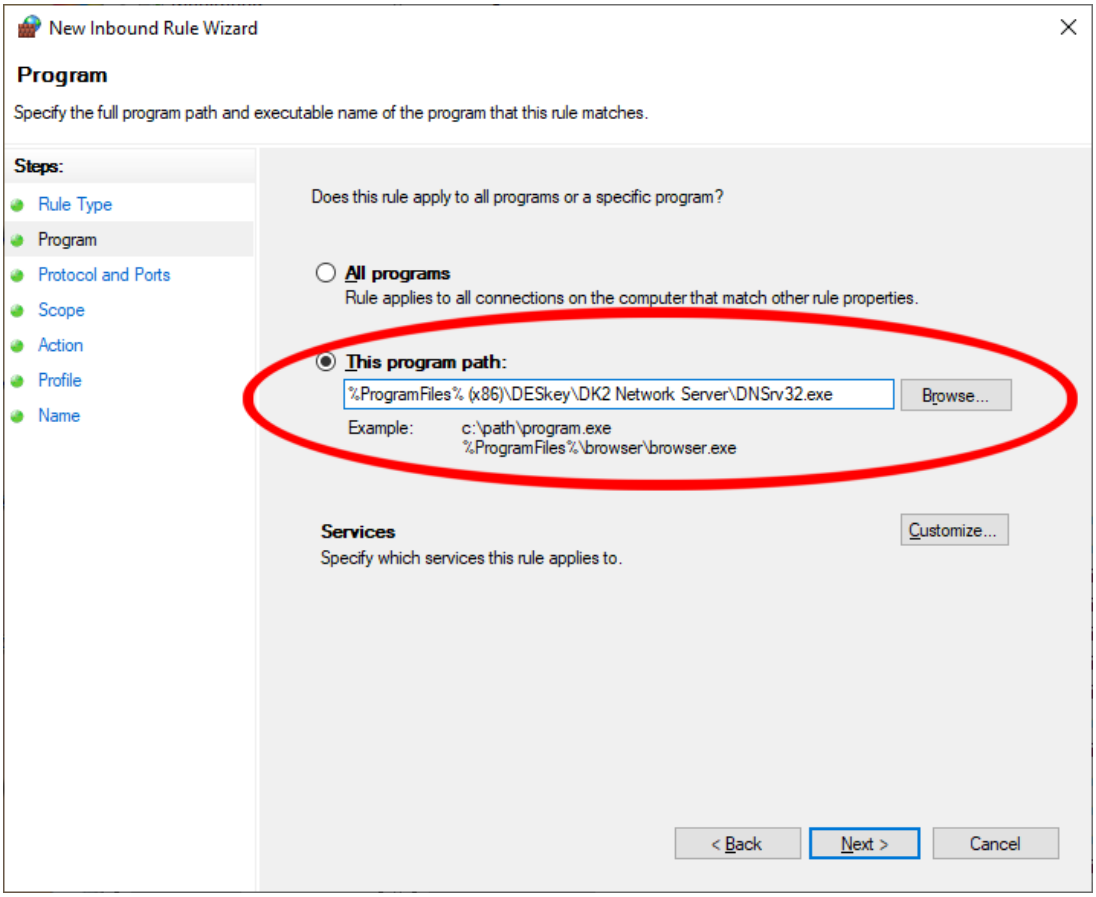
Firewall settings – Windows firewall – for non-IT personnel

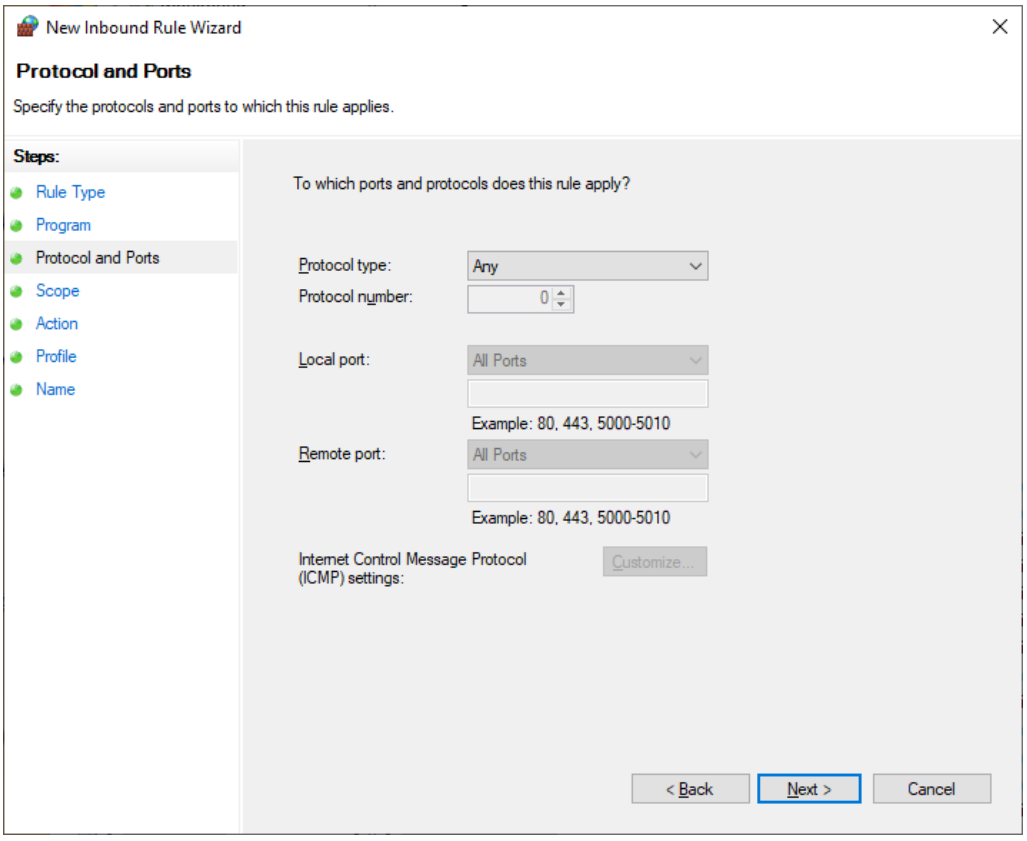
In the Windows search field type “Windows firewall” and select the app.

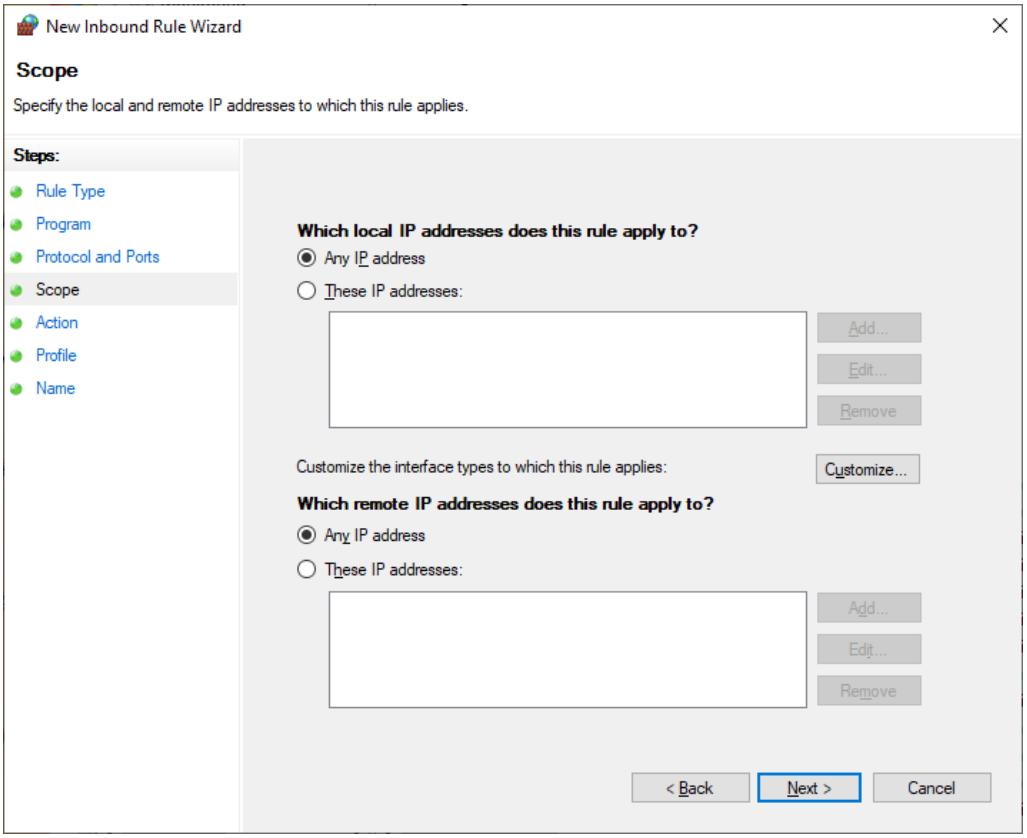
You must create one inbound and one outbound rule to allow the Dongle to communicate within and outside of your organisation

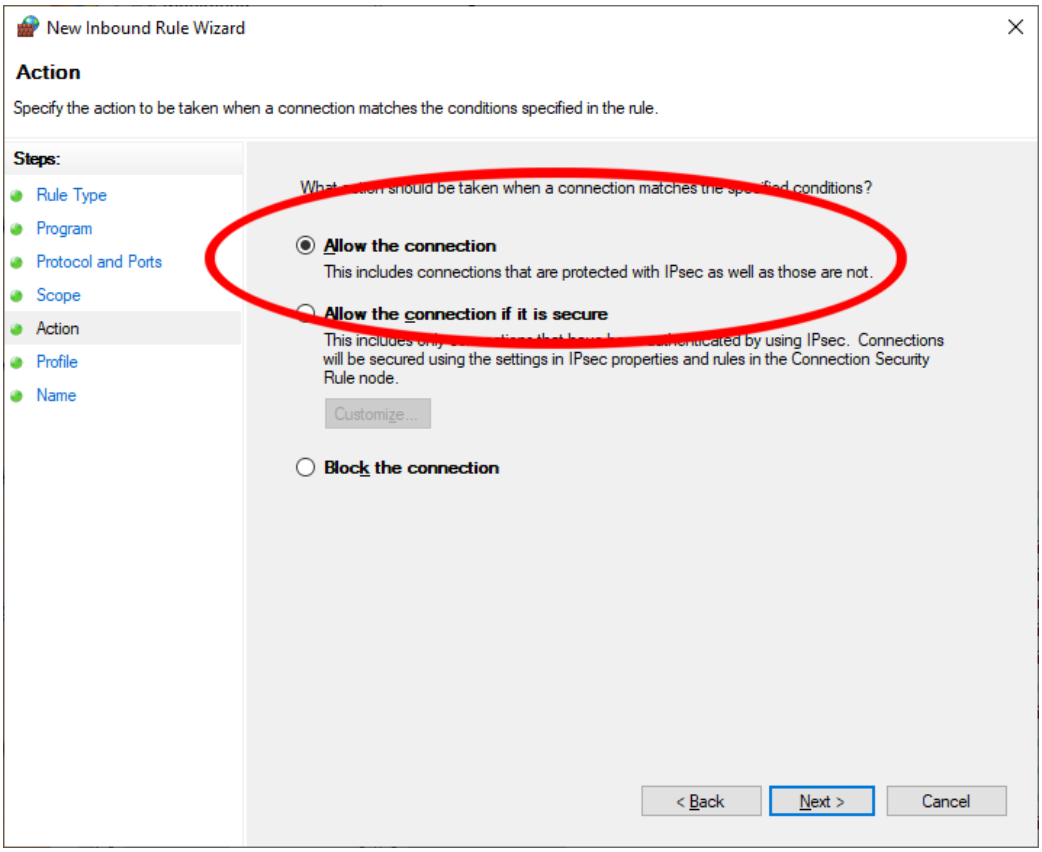

Windows Defender Firewall with Advanced Security
File Action View Help
1
2
Windows Defender Firewall wi
Inbound Rules
Outbound Rules
Monitoring
Inbound Rules
Name
Group
Profile
Allow CLM-Remote-Daemon-Svr
Allow Igs
Allow Igs
Allow Imgrd
Allow Imgrd
AVG Antivirus Admin Client
AVG Installer
Private
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by Group
View
Refresh
Export List...
Help
Allow CLM-Remote-Daemon-Svr
Disable Rule
Cut
Copy
Delete
Properties
Help

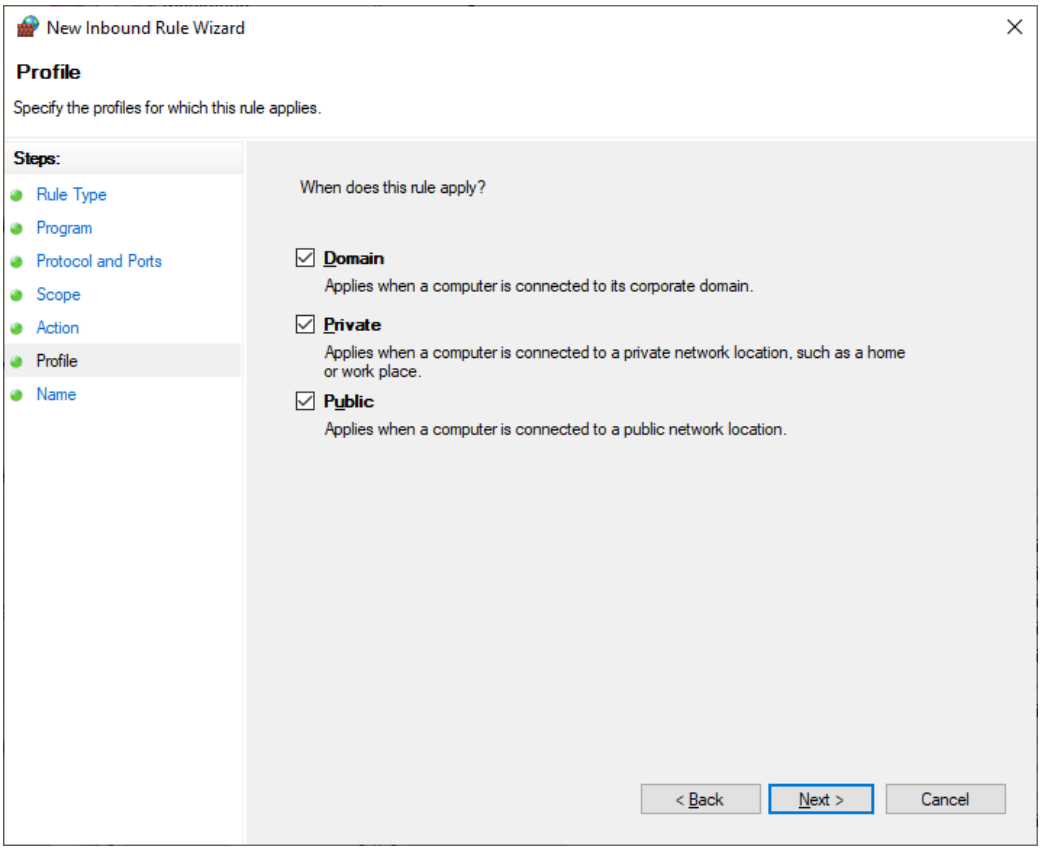

New Inbound Rule Wizard
Rule Type
Select the type of firewall rule to create.
Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
What type of rule would you like to create?
Program
Rule that controls connections for a program.
Port
Rule that controls connections for a TCP or UDP port.
Predefined:
@FirewallAPI.dll,-80200
Custom
Custom rule.
< Back
Next >
Cancel

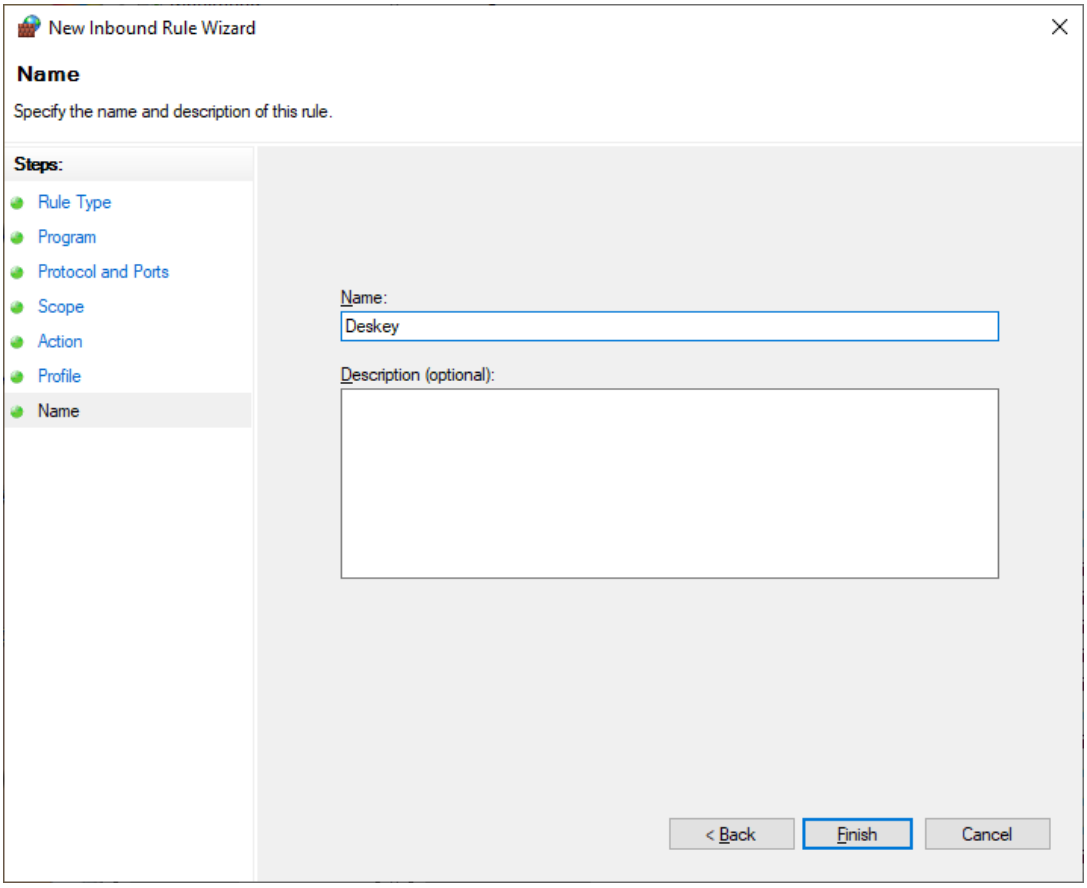

New Inbound Rule Wizard
Program
Specify the full program path and executable name of the program that this rule matches.
Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
Does this rule apply to all programs or a specific program?
All programs
Rule applies to all connections on the computer that match other rule properties.
This program path:
%ProgramFiles% (x86)\DESkey\DK2 Network Server\DNSrv32.exe
Browse...
Example: c:\path\program.exe
%ProgramFiles%\browser\browser.exe
Services
Specify which services this rule applies to.
Customize...
< Back
Next >
Cancel


New Inbound Rule Wizard
Protocol and Ports
Specify the protocols and ports to which this rule applies.
Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
To which ports and protocols does this rule apply?
Protocol type:
Any
Protocol number:
0
Local port:
All Ports
Example: 80, 443, 5000-5010
Remote port:
All Ports
Example: 80, 443, 5000-5010
Internet Control Message Protocol (ICMP) settings:
Customize...
< Back
Next >
Cancel


New Inbound Rule Wizard
Scope
Specify the local and remote IP addresses to which this rule applies.
Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
Which local IP addresses does this rule apply to?
Any IP address
These IP addresses:
Add...
Edit...
Remove
Customize the interface types to which this rule applies:
Customize...
Which remote IP addresses does this rule apply to?
Any IP address
These IP addresses:
Add...
Edit...
Remove
< Back
Next >
Cancel


New Inbound Rule Wizard
Action
Specify the action to be taken when a connection matches the conditions specified in the rule.
Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
Allow the connection
This includes connections that are protected with IPsec as well as those are not.
Allow the connection if it is secure
Customize...
Block the connection
< Back
Next >
Cancel





Repeat the above steps for 'Outbound'.

Firewall settings – Windows firewall – for IT personnel

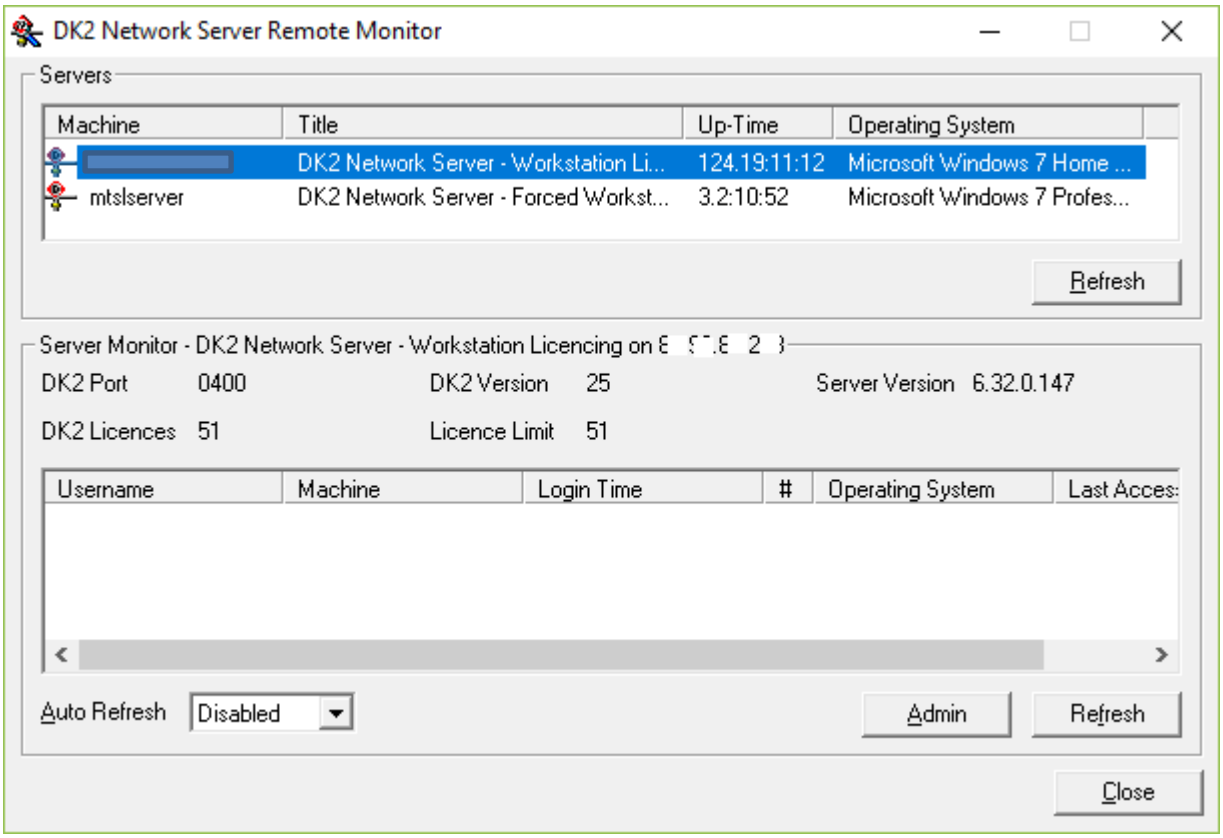
If the DK2 Network Server rules in Windows Defender have already been set then

1. Open Windows Defender Firewall
2. Delete the “DK2 Network Server” rule
3. Open an administrator command line and run : netsh advfirewall firewall add rule name="DK2 Network Server" dir=in action=allow program="C:\Program Files (x86)\DESkey\DK2 Network Server\DNSrv32.exe"

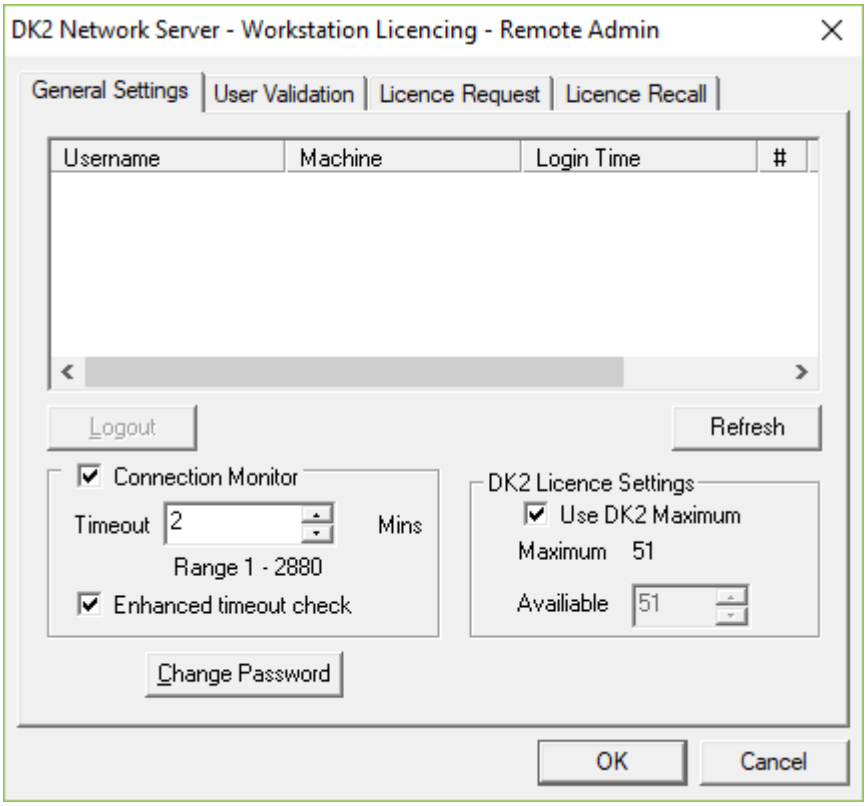
D. Server Side: Password protecting access to LSS

If you want to restrict access to registered users only then you need to set up user accounts inside the Deskey driver as follows.

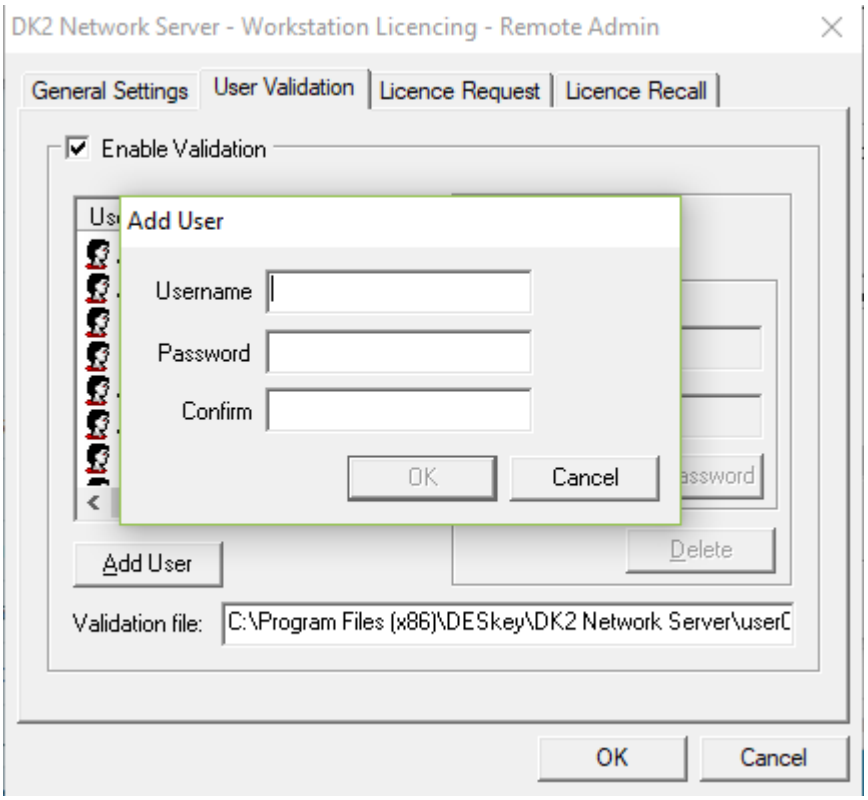
1) Run the DK2 Network Server Monitor on the server



2) Select the server from the list and hit 'Admin'
3) Enter the default password, which is "**deskey**" (please change this once you are in).
4) Make sure that "Connection Monitor" and "Enhanced timeout check" are selected and that the "Timeout" is set to 2 minutes.

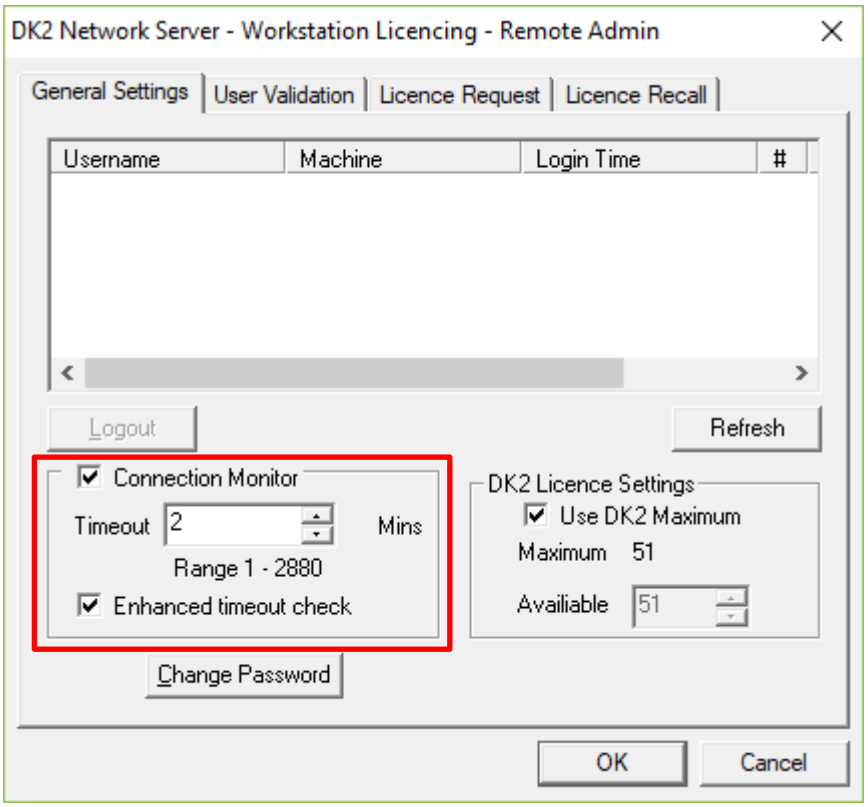


5) Add users via the 'User Validation' tab



E. Server Side: Important setting

If any of those LSS users connected to the server dongle experience a computer crash or quit LSS illegally (shutting down their computer when LSS is still open etc) then their licence won't be released by the server unless two settings are activated.



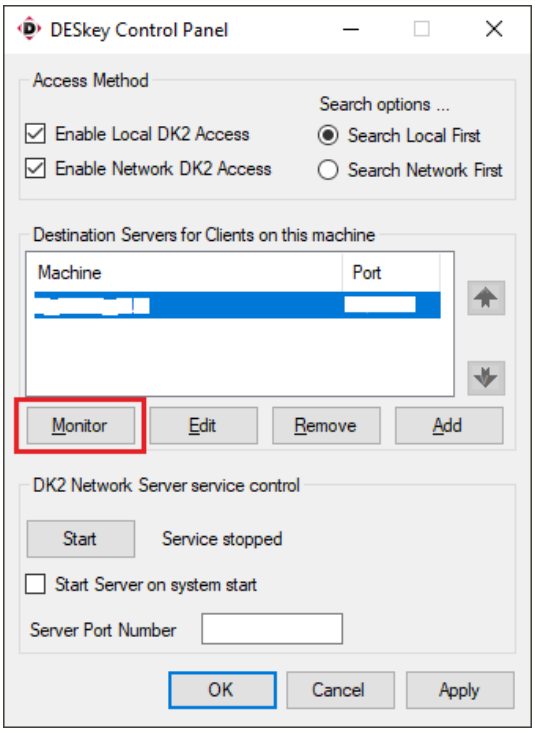
On the remote admin screen, make sure that you turn on 'Connection monitor' with a timeout of 1 or 2 minutes and also select 'Enhanced timeout check'.

The maximum time you will then have to wait after an illegal exit from LSS will be that timeout setting.

F. User controls:

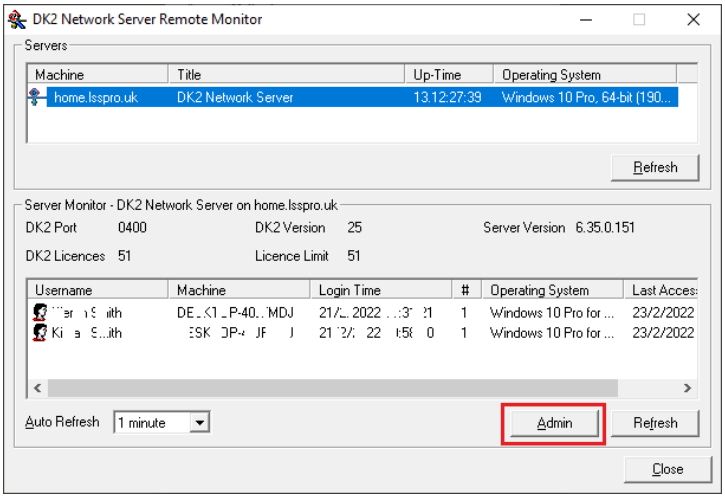
You don't need IT support to fix server problems.

Please also be aware that any LSS user is able to change the above settings (see section D: 3). If the default 'deskey' password has been changed then you will need to enter this new password instead.

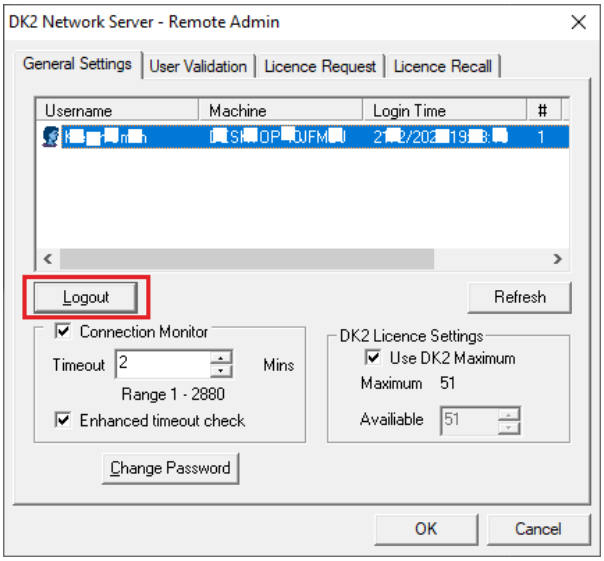


In windows Control Panel, select 'Deskey'

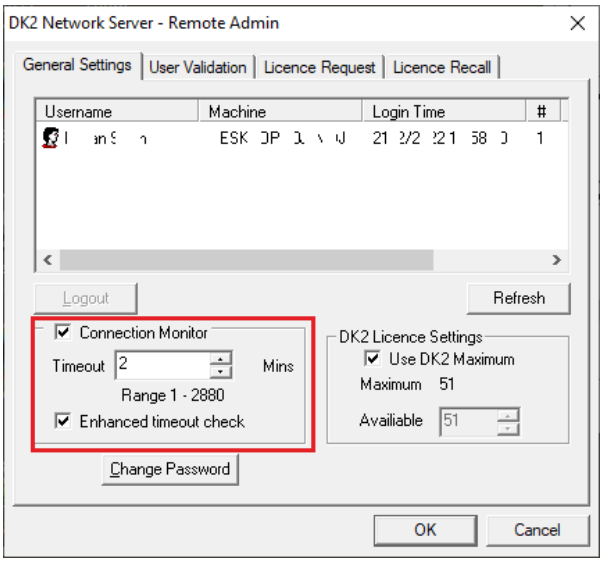
Select the dongle server and hit 'Monitor'



Hit 'Admin', type the dongle server password (**deskey** is the default)



Select the user who is no longer connected to LSS and hit 'Logout'. Their licence will be released.



To prevent this from happening again, set the Connection Monitor and Enhanced timeout check.