

General

As PC security concerns increase, Windows® and third-party anti-virus programs restrict software programs such as SK-NET™ from sending or accepting data through various software “ports” used for accessing the internet using HTTP, HTTPS and TCP protocols. Even if SK-NET™ is not using a LAN or WAN connection to communicate with its system control panels, these security restrictions will keep SK-NET™ from running, and a “**Not Responding**” message will appear at the top of the screen. This bulletin explains how to allow SK-NET™ to access the software ports that are required for the software to operate correctly, when used with Windows® 7, Vista, or XP.

If you follow these procedures, including reconfiguring your anti-virus software, and the problem continues, you should have your computer checked by a qualified technician.

For All Operating Systems (Windows® 7, Vista, or XP)

If SK-NET™ is not responding when using Windows 7, Windows® Vista, or Windows XP, you must first edit the ADS.INI file. In Windows Explorer under C:/Secura Key/SK-NET 4.00:

1. Double click on the **ADS.INI** file (this will open the ADS.INI file in Notepad).
2. Insert a line, if necessary, and type **USE_TCP_IP=1** just below [SETTINGS]. (See example below.) Then close and save the changes.



```
ADS.INI - Notepad
File Edit Format View Help
[SETTINGS]
ADS_SERVER_TYPE=2
USE_TCP_IP=1
[Databases]
SKNetServerDB=C:\Secura Key\SK-NET 4.00\Database\SKNetData.add;D
```

For Windows® 7 Users

You must configure Windows® Firewall to allow SK-NET to access ports 8200, 443 and 80, even if the firewall is turned OFF, using the following procedure:

1. First, close SK-NET™, allowing 10-20 seconds for the program to close completely before proceeding.
2. Open the Windows Firewall by clicking the **Start** button, clicking **Control Panel**, and then clicking **Windows Firewall**.
3. Click **Advanced Settings**, and if you are prompted to allow changes, click on **Yes**, then click on **Inbound Rules**. In the right-hand column, click on **New Rules**. Click the **Port** radio button, and then click **Next**.
4. Click radio buttons for **TCP** and **Specific Local Ports**, then in the field next to Specific Local Ports, type: **8200, 80, 443** and click **Next**.
5. Click the radio button labeled **Allow the Connection** and click **Next**.
6. On the following screen do not change the default settings and click **Next**. In the **Name** field, type **SKNet** then click **Finish**.
7. Click **Outbound Rules**, and then in the right-hand column click on **New Rules**. Click the **Port** radio button, and then click **Next**.
8. Click radio buttons for **TCP** and **Specific Local Ports**, then in the field next to Specific Local Ports, type **8200, 80, 443** and click **Next**.
9. Click the radio button labeled **Allow the Connection** and click **Next**.
10. On the following screen, do not change the default settings and click **Next**. In the **Name** field, type **SKNet**, then click **Finish**.

Note: If the above procedure did not solve the problem, you may have to reconfigure your antivirus software to allow SK NET™ to operate by creating an exception for SKNet.exe and the Database folder at C:\Secura Key\SK NET 4.00\SKNet.exe and C:\Secura Key\SK-NET4.00\Database. If your antivirus has a firewall then you need to add these Ports: 8200, 443, 80.

Continued

For Windows® Vista Users

You must configure Windows® Firewall to allow SK-NET™ to access ports 8200, 443 and 80, even if the firewall is turned OFF, using the following procedure:

1. First, close SK-NET™, allowing 10-20 seconds for the program to close completely before proceeding.
2. Open the Windows® Firewall by clicking the **Start** button, clicking **Control Panel**, clicking **Security**, and then clicking **Windows® Firewall**.
3. Click the radio button **Allow a program through Windows® Firewall**. (If you are prompted for an administrator password or permission to continue, type the password or provide permission to continue.)
4. Click the **Add port...** button.
5. In the **Name** field, type **SKNet**
6. In the **Port number** field, type **8200**
7. For Protocol, click the **TCP** radio button, then click **OK**.
8. Repeat steps 3 - 7 to add ports: 443 and 80,
9. Click **OK** and exit the Control Panel.

Note: If the above procedure did not solve the problem, you may have to reconfigure your antivirus software to allow SK NET™ to operate by creating an exception for SKNet.exe and the Database folder at C:\Secura Key\SK NET 4.00\SKNet.exe and C:\Secura Key\SK-NET4.00\Database. If your antivirus has a firewall then you need to add these Ports: 8200, 443, 80.

For Windows® XP Users

You must configure Windows® Firewall to allow SK-NET™ to access ports 8200, 443 and 80, even if the firewall is turned OFF, using the following procedure:

1. First, close SK-NET™, allowing 10-20 seconds for the program to close completely before proceeding.
2. Open the Windows® Firewall by clicking the **Start** button, clicking **Control Panel**, clicking **Security Center**, and then clicking **Windows® Firewall**.
3. Click on the **Exceptions** tab.
4. Click **Add port**.
5. In the **Name** field, type **SKNet**
6. In the **Port number** field, type **8200**
7. Click the **TCP** radio button, then click **OK**.
8. Repeat steps 3 - 7 to add ports 443 and 80
9. Click OK and exit the Control Panel.

Note: If the above procedure did not solve the problem, you may have to reconfigure your antivirus software to allow SK NET™ to operate by creating an exception for SKNet.exe and the Database folder at C:\Secura Key\SK NET 4.00\SKNet.exe and C:\Secura Key\SK-NET4.00\Database. If your antivirus has a firewall then you need to add these Ports: 8200, 443, 80.

SECURA KEY

20301 Nordhoff St. • Chatsworth, CA 91311
phone 818-882-0020 • fax 818-882-7052
Toll Free - 800-891-0020

DATE: 7/15/10
REV.:
AF#: 7450

PAGE 2 OF 2