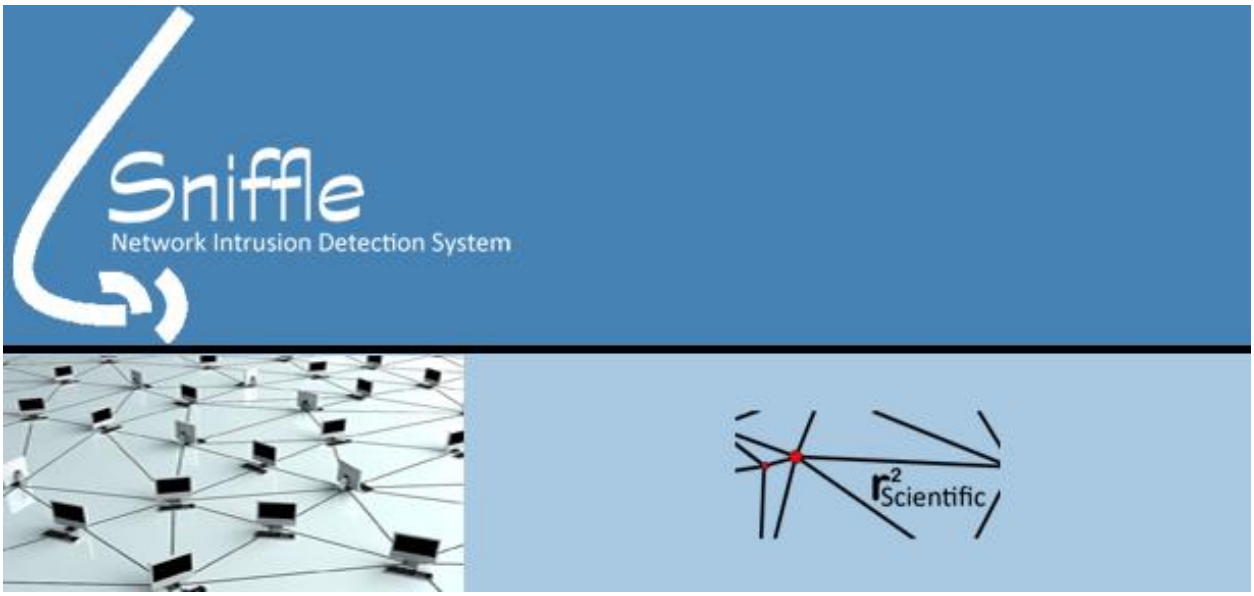


Is all this really necessary?

Sniffle Server Software Setup Guide V1.0.2.0

Answer: Only if you want Sniffle to work. Otherwise, no.

Sniffle Server is a Windows service that runs quietly in the background on a Windows 64-bit computer. Sniffle Server does not require a dedicated computer. It can easily run on a general-purpose network computer.

Getting Started

Your Microsoft and your virus software are not going to be happy about installing Sniffle. Also, your firewall might give you a hard time. You will need to temporarily disable your virus software to install Sniffle. You will also need to open ports 12155, 12156 and 12157 on your firewall.

Additionally, you will need to forward data received from the internet on port 12155 to the Sniffle server machine. (Port forwarding on your internet router)

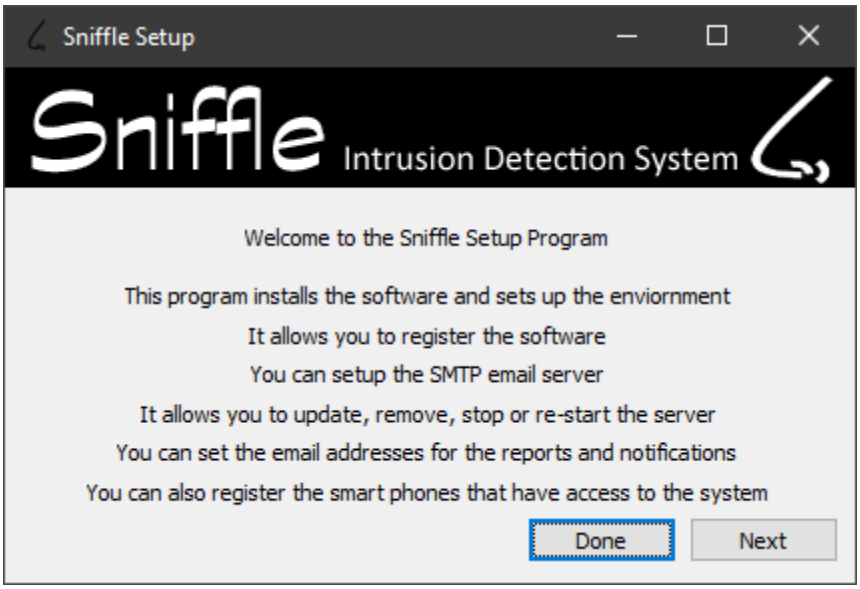
Sniffle installs in the Windows\Sniffle directory. Sniffle Firewall in the Windows\Sniffle Firewall directory. You need to convince your virus software to ignore these directories.

WinPcap or Win10Pcap (for Windows 10) needs to be installed on the machine prior to running the Sniffle setup program or Sniffle server. It is not required if you are just running Sniffle Firewall. It is included in the install zip file.

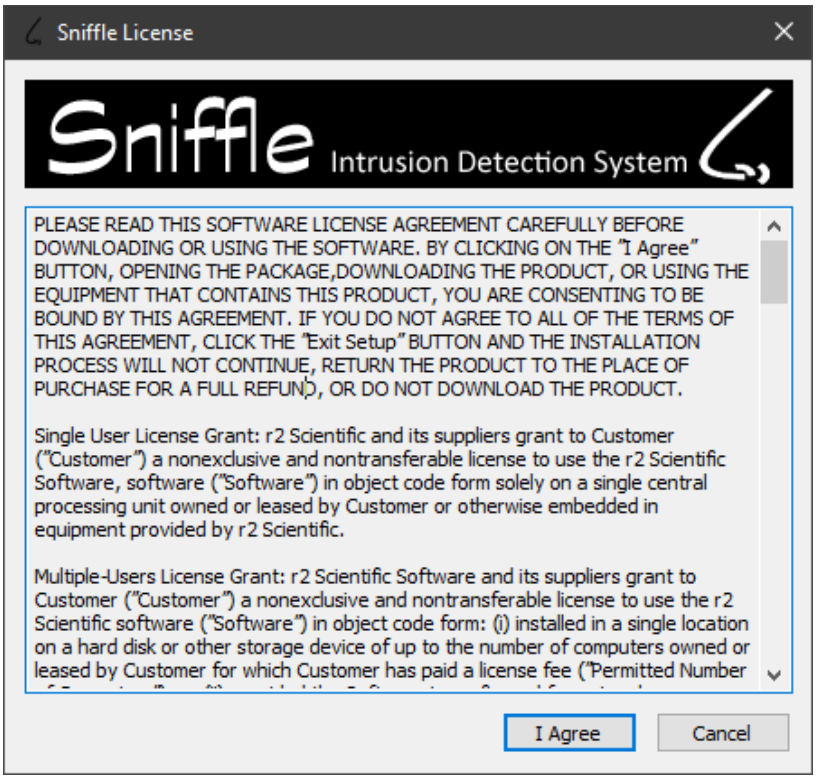
The Sniffle setup program must be run as an administrator.

Before you begin, you will need the following information
#1 Up to 6 email addresses that will receive exploit reports
#2 Setup information for an SMTP server (gmail or yahoo is fine)
#3 Device identifiers for up to 6 Android devices (Setup on the Sniffle app)

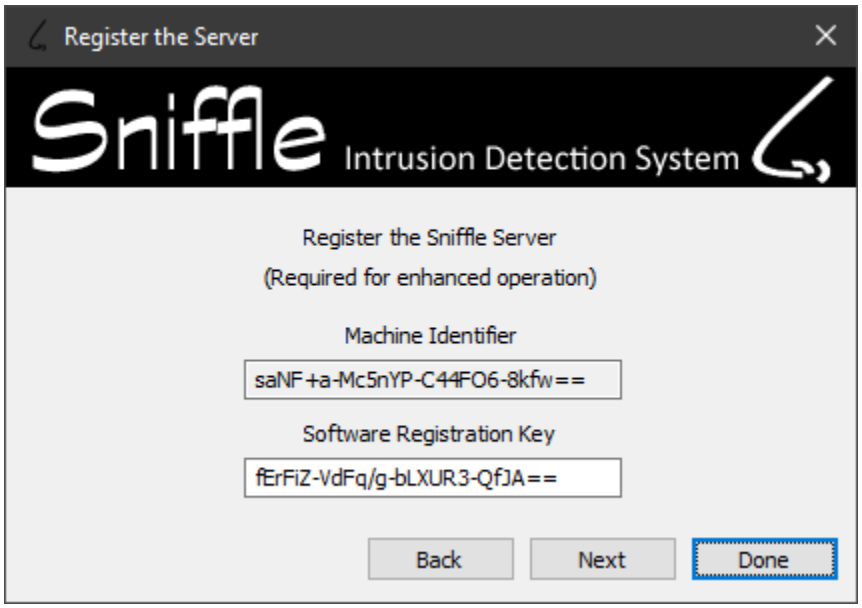
Welcome to Sniffle Setup



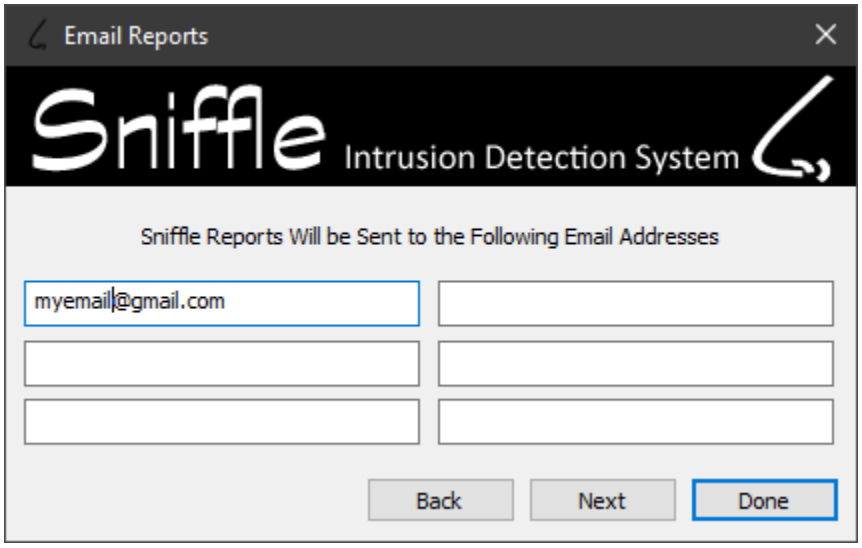
Of course, the license page is the most important part of the setup. It is advisable that you read and understand the complete license. It may also be a good idea to commit the more important passages to memory for later reflection.



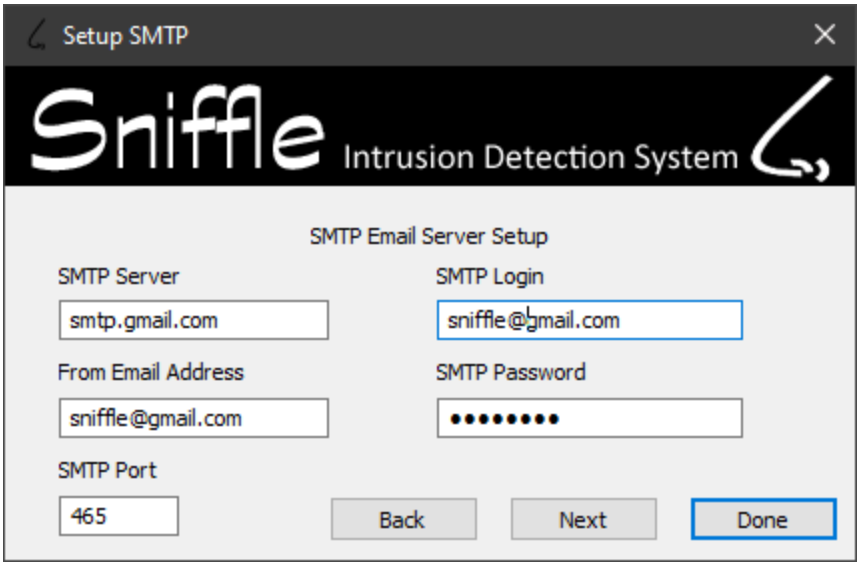
Sniffle self-registers. There is no need to change any information on this page.



Sniffle sends exploit reports to you via email. You enter the recipients email addresses here.

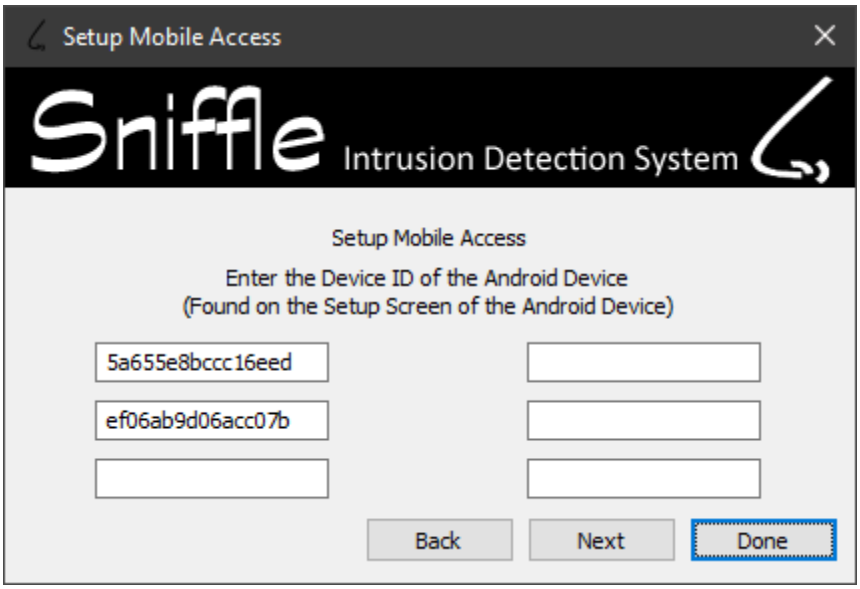


To send email, Sniffle needs access to a SMTP server. If you use gmail as shown below, Google we ask you to allow less secure programs.

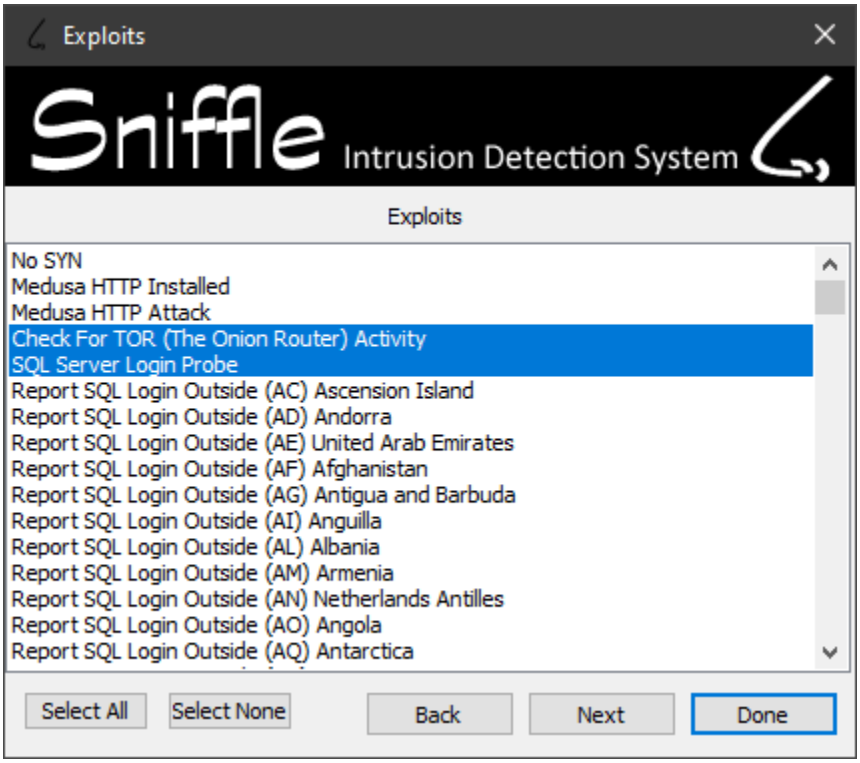


If you use a Yahoo email address, the settings would be:
SMTP Server – smtp.mail.yahoo
SMTP Port – 465

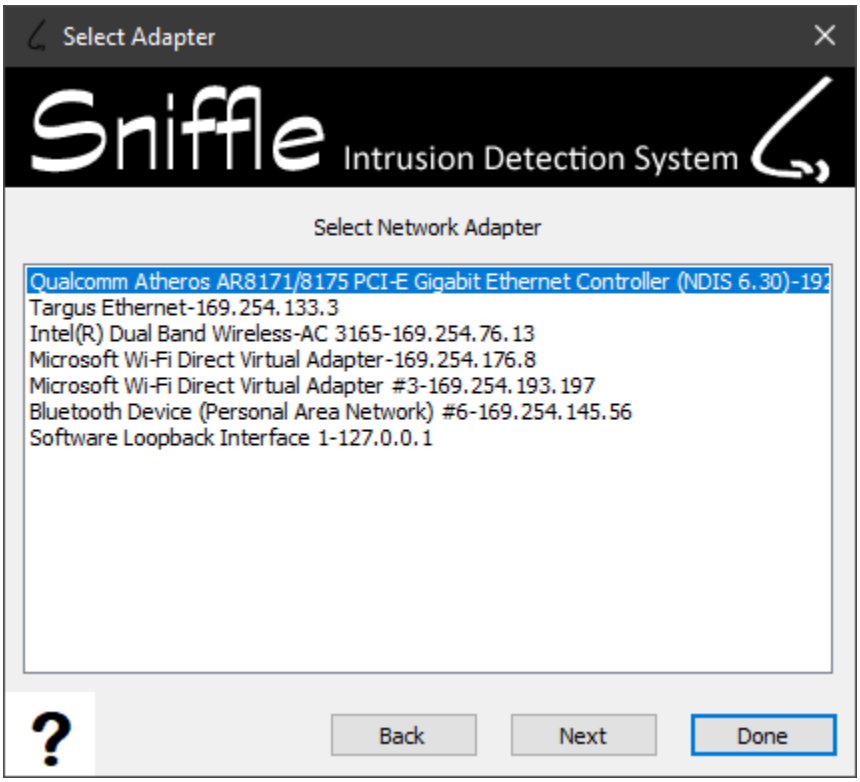
You need to register the Android devices that have access to Sniffle. Hitting the setup button on the sniffle app will show you the identifier for that device. Enter it here.



Pick the exploits you wish to monitor. If you intend to using the Sniffle Firewall option, you must enable “Update Windows Firewall On This Subnet” on this screen and install Sniffle Firewall on each machine you wish to protect.



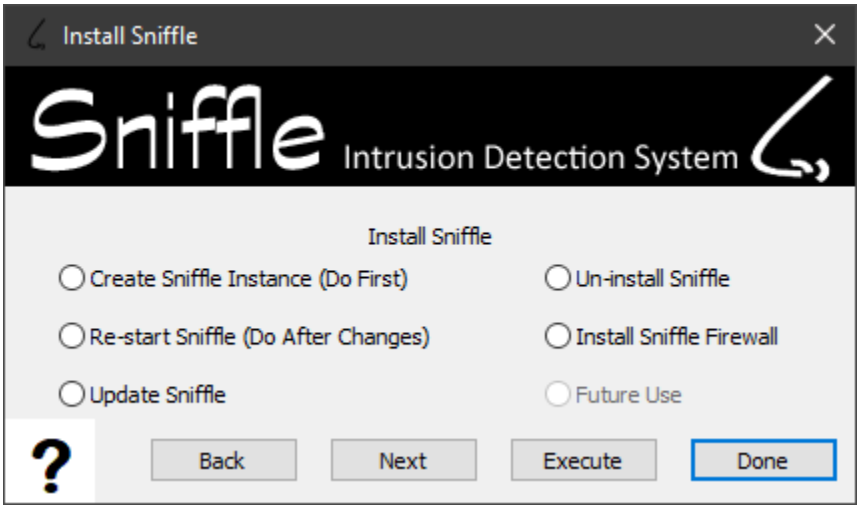
Choose your network adapter.



Here you can install or remove the server software, restart the server if it gets confused (you can also do this from a registered Android device), and update the Sniffle server software.

You can also install Sniffle Firewall which automatically adds a problem IP to Windows Defender Firewall on every computer on your subnet. If you are just installing Sniffle Firewall on a computer, there is no need to enter any of the other setup information. Sniffle Firewall needs to be installed on every machine on your subnet that you wish to protect including the machine running Sniffle. There is no further setup required for Sniffle Firewall.

Select the option you wish to install and click Execute.



Now that wasn't so bad, was it? Sniffle or Sniffle Firewall is now running. Enjoy!