NetCertScanner User Guide

Contents

Running NetCertScanner GUI Application

Important Tip: For faster scan performance, run NetCertScanner on Windows Server editions (Windows 2008, 2012, 2016 etc) or latest Windows desktop editions (like Windows 10/8/7).

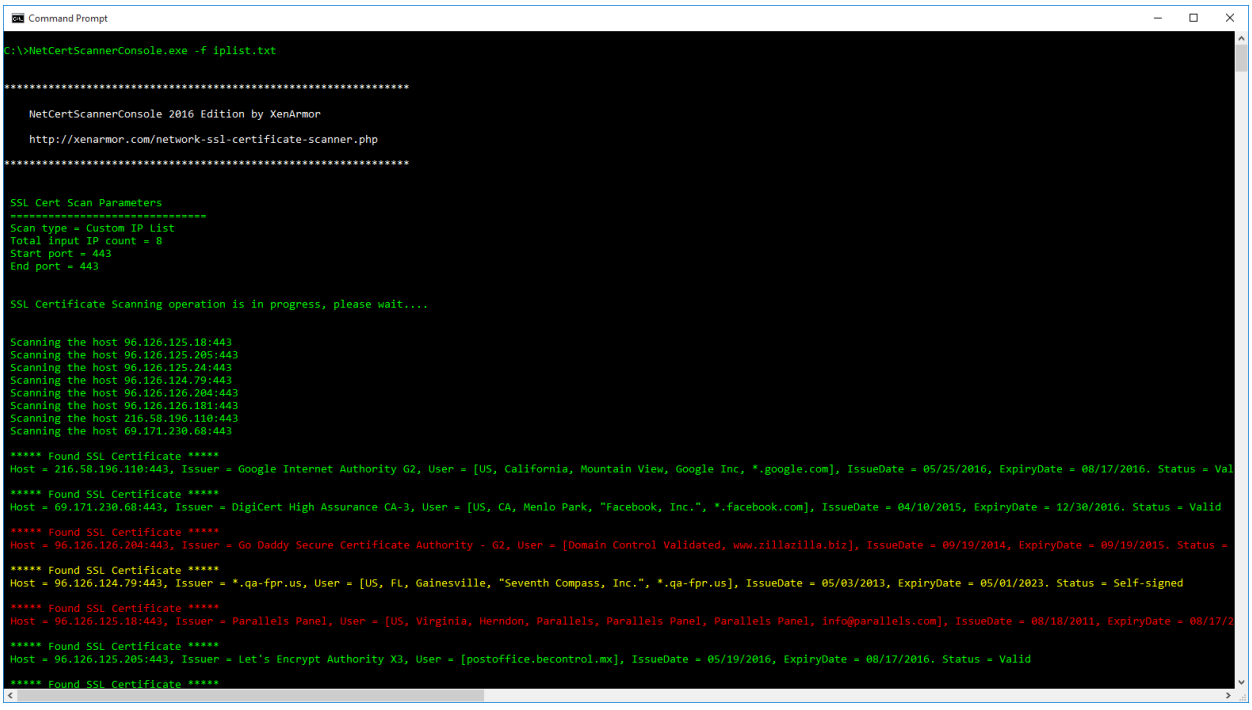
Here are the simple instructions for using NetCertScanner GUI version as shown in the above screenshot. For additional settings refer to section on 'Basic Settings of NetCertScanner'.

- Launch the NetCertScanner as administrator (recommended)
- Select "Single Host" or "Entire Network" to scan either one host or range of hosts.
- Now specify the IP address of the host or network range to be scanned.

- For example, '192.168.1.5' or google.com or ' 192.168.1.1 to 192.168.1.50'
- Next choose the type of SSL service. You can select LDAPS, HTTPS or Custom (range of ports). Look at "Special Instructions" section at the end of this document for list of various popular SSL service ports.
- Now click on 'Start Scan' button to begin the SSL scanning operation. During scanning the detailed report of the progress is displayed. You can stop the scanning operation at any time by pressing "Stop Scan" button.
- Once the certificate scanning is over, you can click on any of the certificate entries in the report to view the certificate if database setup is done. Also you can click on Report button to generate detailed HTML report.

Running NetCertScanner Console Application

NetCertScanner command-line version supports all the main features of the GUI application. In addition to this it also has unique feature to scan list of custom IP addresses from the input file. Console version is mainly designed to facilitate automation of SSL scanning operation to reduce manual work.



Here is the typical usage and examples of command-line version

NetCertScannerConsole [-h host/host-range | -f c:\iplist.txt] -p port/port-range

Examples:

```
// Single host with single port scan
NetCertScannerConsole -h 192.168.5.1 -p 443

// Scanning single port on entire network.
NetCertScannerConsole -h 192.168.5.1-254 -p 443

// Scanning range of ports on single host
NetCertScannerConsole -h 192.168.5.1 -p 1-1024

// Scanning range of ports on entire network.
NetCertScannerConsole -h 192.168.5.1-254 -p 900-1000

// Scanning list of IP addresses from input file (port 443)
NetCertScannerConsole -f c:\iplist.txt

// Scanning list of IP addresses from input file with port range
NetCertScannerConsole -f c:\iplist.txt -p 1-1024
```

Note that Console version automatically uses the settings configured by NetCertScanner GUI version.

For IP list file (iplist.txt above) you can create text file and put IP address of each host on a single line. This is very useful when regularly scanning your own web or directory servers.

Settings of NetCertScanner

Launch the NetCertScanner application and then click on 'Settings' button (at bottom right) to modify various options. Note that for any Database Settings to take effect, you need to restart the application.

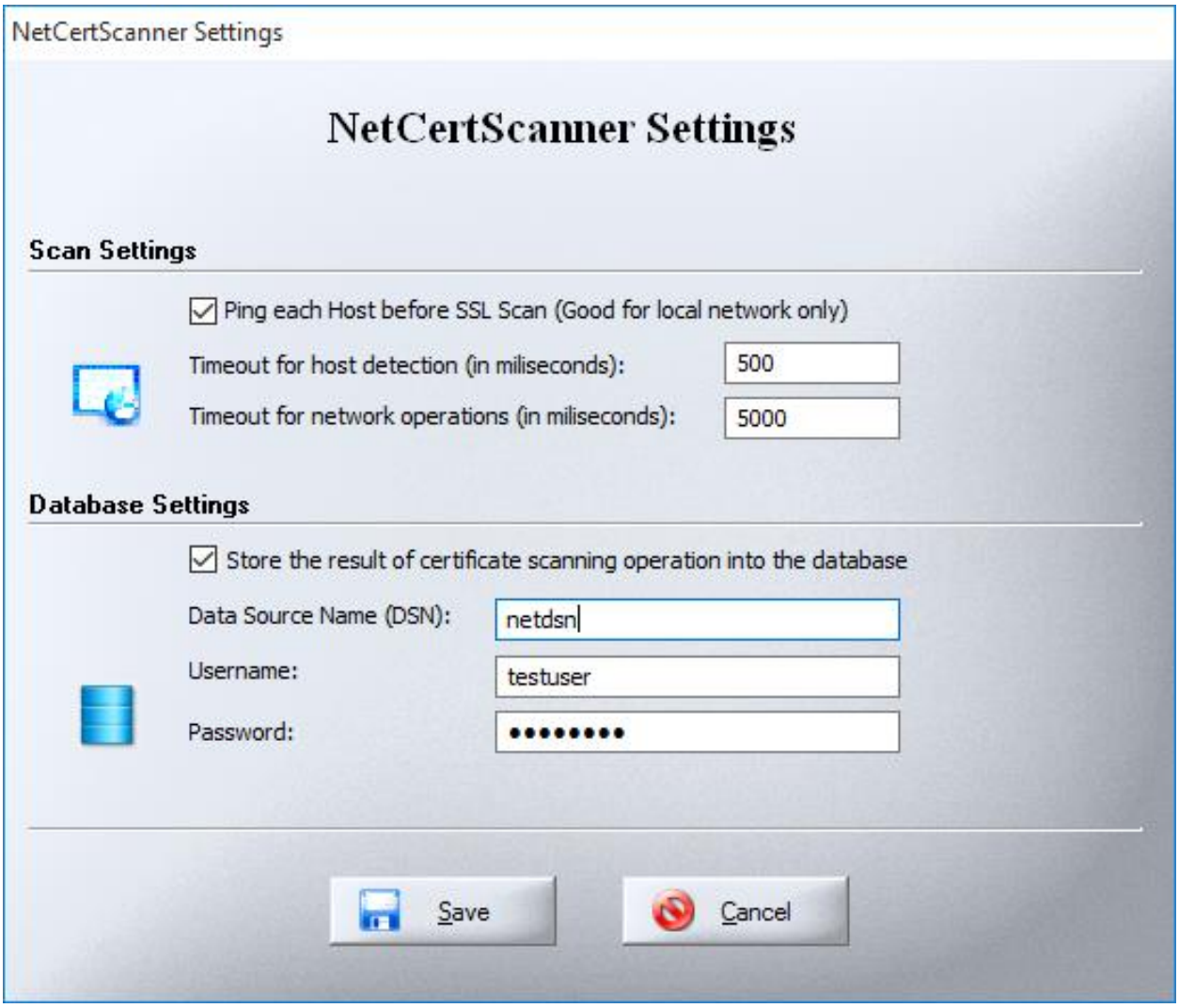


Figure 1: ***NetCertScanner's Settings Wizard to help you in fine tuning the Performance and Database Integration features.***

a) Scan Settings

- **Ping Each Host Before SSL Scan**

  It performs PING test of host to check if the host is alive before beginning the SSL scan operation. It greatly improves the speed especially when large number of port scanning is involved. Generally this is recommended for the hosts only on your local network. For internet oriented hosts it should be unchecked.

- **Timeout for host detection**

  If the above 'Ping Each Host Before SSL Scan' option is selected, then this timeout value specifies the waiting time for receiving the PING reply from the remote host. Typical value ranges between 200 ms to 500 ms based on the speed of your local network.

- **Timeout for network operations**

  This option specifies the timeout used for various network operation such as connecting to port and receiving data from the port. This is very important setting which greatly affect the performance of the scanning operation. For intranet, this can be set to 2000 to 5000 ms and for internet it can be set to 10000 ms or more. By default Windows uses time out of 20 seconds for various network operations.

b) Database Settings

Please refer to separate database setup guide provided with the application for configuring database settings.

Known Limitations on Windows Platform

There are few issues one may encounter while using the NetCertScanner on Windows platform. These problems are due to the limitation of Windows and the way it behaves in various situations. Here are some of these issues,

- Maximum number of outgoing connections is limited to 10 on Windows XP as a security measure. This will cause network timeout leading to non-reliable results while scanning large number of hosts or ports on XP. However this limitation is not present on Windows 2003 server and higher editions of Windows.

  More information on the same can be found at http://www.tech-faq.com/concurrent-connections-limit-in-windows-xp.shtml

  Solution: Use Windows Servers (Windows 2003, 2008, 2012, 2016) or Desktop editions such as Windows 7/8/10 for optimum and faster scan performance.

Advanced Performance Tips for NetCertScanner

Here are some of the advanced instructions which will help in fine tuning the performance of the NetCertScanner application based on the running environment. It will also help greatly during testing phase.

- **Host detection (PING TEST) before scanning operation**

  (Refer to 'Settings Dialog' instructions above) Using this setting on the local network (intranet) will greatly improve the speed of the scanning operation especially when it is combined with large number of ports. While scanning the hosts on the internet, you can either increase the host time out value or simply disable it. For security reasons, most of the hosts do not reply to PING requests from the remote hosts. If you see around 80-90% of "host not reachable" message in the SSL scan report then disable this check box (Ping Each Host Before SSL Scan) and scan again.

  Host detection timeout for intranet = 200 ms
  Host detection timeout for internet > 500 ms

- **Tweaking the network operations timeout**

  It controls time out for various network operations such as connecting to port or receiving data from a port. Setting it to low value will cause the most of these operations to be timed out in a slow network. If you see lot of "Network operations time out" messages in the SSL scan report then its good idea to increase the timeout value.

  Network operations timeout for intranet 2000-5000 ms
  Network operations timeout for internet > 10000 ms

[Continued on Next Page…]

Appendix I: List of Popular SSL Services

Here is the list of popular SSL services with their port numbers.

Port (TCP)	Name of SSL Service
261	IIOP name service over SSL (IIOPS)
443	HTTP over SSL (HTTPS)
465	SMTP over TLS/SSL (SMTPS)
585	IMAP over SSL (IMAPS)
636	LDAP over SSL (LDAPS)
989	FTP (data) over SSL (FTPS)
990	FTP (control) over SSL (FTPS)
992	Telnet protocol over SSL
993	IMAP over SSL (IMAPS)
994	IRC protocol over SSL (IRCS)
995	POP3 protocol over SSL (POPS)
3269	Active Directory: Global catalog LDAPS

For latest information, please visit online product page of NetCertScanner