Continuous Security
Intelligence™

SecureVue®
STIG Profiler Usage Guide

Copyright, Restricted Rights and Trademark Notices

This notice does not imply unrestricted or public access to these materials which are a trade secret of EiQ Networks, Inc. ("EiQ") and which may not be reproduced, used, sold or transferred to any third party without the prior written consent of EiQ. EiQ's software uses certain third-party libraries/software. The conditions and restrictions required of software users by the owners of such Third Party Software are referenced in *THIRDPARTYLICENSEREADME.txt* under the application install path.

EiQ Networks, EiQ, the EiQ logo, SecureVue, ThreatVue, SOCVue, ComplianceVue, ForensicVue, and Unified Situational Awareness are trademarks or registered trademarks of EiQ Networks, Inc. in the US and/or other countries. All other product names and/or slogans mentioned herein may be trademarks or registered trademarks of their respective companies. All information presented here is subject to change and intended for general information.

U.S. Government Agencies Only

The software described in this Documentation, and this Documentation itself, were developed at private expense and the software is 'commercial computer software' provided with RESTRICTED RIGHTS. Use, duplication and disclosure by civilian agencies shall be in accordance with FAR 52-227-19(c) or other agency data rights provisions, as may be applicable. Use, duplication and disclosure by DOD agencies are subject solely to the terms of a Contractor/Licensor System Sale, Evaluation and License Agreement as stated in DFARS 227-7202. Unpublished - All rights reserved under the Copyright Laws of the United States. Contractor/Licensor: EiQ Networks, Inc., 31 Nagog Park, Acton, MA 01720-3424.

Document Date: March 10, 2015

Contents

STIG Profiler

Introduction to STIG Profiler

During an Audit, it is extremely time consuming for an admin/auditor to identify what STIG policies are applicable to nodes in the network. Organizations would benefit immensely if a tool or utility could suggest STIG policies that are applicable for the Nodes within their network.

To address this need, EiQ Networks has developed STIG Profiler tool. This tool is a free tool which can be used to scan a local network and provide a detailed asset profile report which clearly identifies what all STIG policies are to be evaluated for performing a STIG audit for each node.

STIG Profiler has the capability to Detect the following nodes in the network:

- Windows/Linux/Unix Host
- Firewalls
- Routers/Switches
- WLAN Controllers

STIG Profiler has the capability to perform advanced scanning on the below node types:

- Windows desktop
- Windows server
- RHEL
- Solaris
- SUSE
- HPUX

Pre-requisites for using STIG Profiler

1. Machine on which STIG Profiler tool is deployed should have the following minimum system requirements:
   - **CPU**: Dual Core Processor [Quad Core Recommended]
   - **OS Architecture**: 32/64 bit
   - **RAM**: 2 GB
   - **OS**: Windows Server 2003, Windows 7
   - **JRE**: 1.8 is required for generating PDF reports
   - **PDF Reader**: Adobe Reader 10.x
2. Remote Registry service is running on the machines which are scanned by the STIG Profiler. Refer *Permissions for RSOP WMI Method Provider* (page 13) and *Permissions for Registry* (page 14) for more details.
3. Network Group Policy should allow remote registry access on all the nodes which are scanned by STIG Profiler tool. To ensure remote registry access is allowed:

    a. Go to **Run** > **gpedit.msc** > **User Configuration** > **Administrative Templates** > **System** > **Prevent access to registry editing tools**.
    b. Disable the setting or choose "**Not Configured**".

4. User access control should be turned off for administrator to recommend the STIG policies correctly.
5. WinPcap 3.0 or above and Microsoft Visual C++ 2010 redistributable packages are required in order to run NMAP scan.

How to Use STIG Profiler application

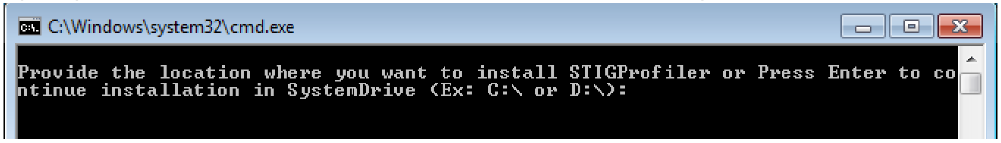
For the Tool to provide a detailed mapping of STIG policies for your network nodes, following activities are to be performed:

1. Identify the IP addresses (nodes) in the Network which needs to be scanned by the tool.
2. Perform a Scan to obtain the Inventory list of organizational assets within the specified IP range. STIG profiler uses Nmap Tool to scan the node inventory details in the specified network IP range.
3. After the Node Inventory list is generated by the scan, users can select nodes of their choice, apply user credentials and generate reports which have STIG Policy recommendation for the respective node.

Installing STIG Profiler

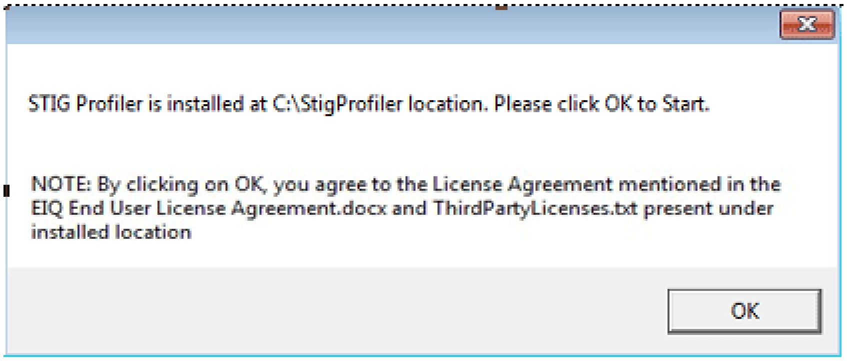
Perform the following steps to install the STIG Profiler:

1. Run the STIGProfilerBuild.exe file.
2. Specify the location where STIG Profiler is to be installed on your machine.



```
Provide the location where you want to install STIGProfiler or Press Enter to co
ntinue installation in SystemDrive (Ex: C:\ or D:\):
```

3. Click Enter to install the STIG Profiler build in the default path i.e., %system drive%\StigProfiler folder.

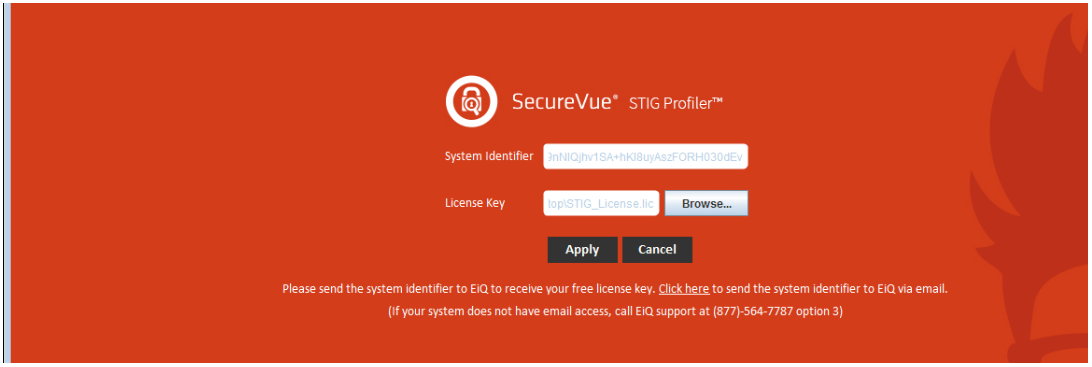


STIG Profiler is installed at C:\StigProfiler location. Please click OK to Start.

NOTE: By clicking on OK, you agree to the License Agreement mentioned in the EIQ End User License Agreement.docx and ThirdPartyLicenses.txt present under installed location

4. Click **OK**. The STIG Profiler window is launched as below. You can also use the STIG Profiler icon on the desktop to open the STIG Profiler application.

5. During first login, you will be prompted to enter a valid license to use the STIG Profiler application.



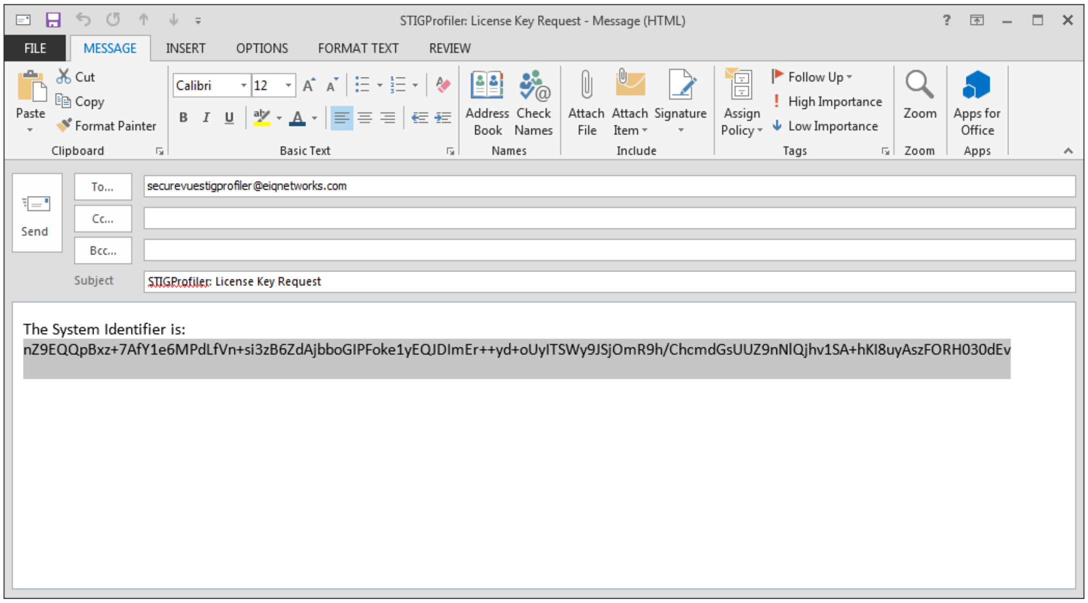
System Identifier nNIQjhv1SA+hKI8uyAszFORH030dEv

License Key top\STIG_License.lic

Please send the system identifier to EiQ to receive your free license key. Click here to send the system identifier to EiQ via email.

(If your system does not have email access, call EiQ support at (877)-564-7787 option 3)

6. For obtaining the license, use click here option and launch the e-mail client to send the systemidentifier details to securevuestigprofiler@eiqnetworks.com.

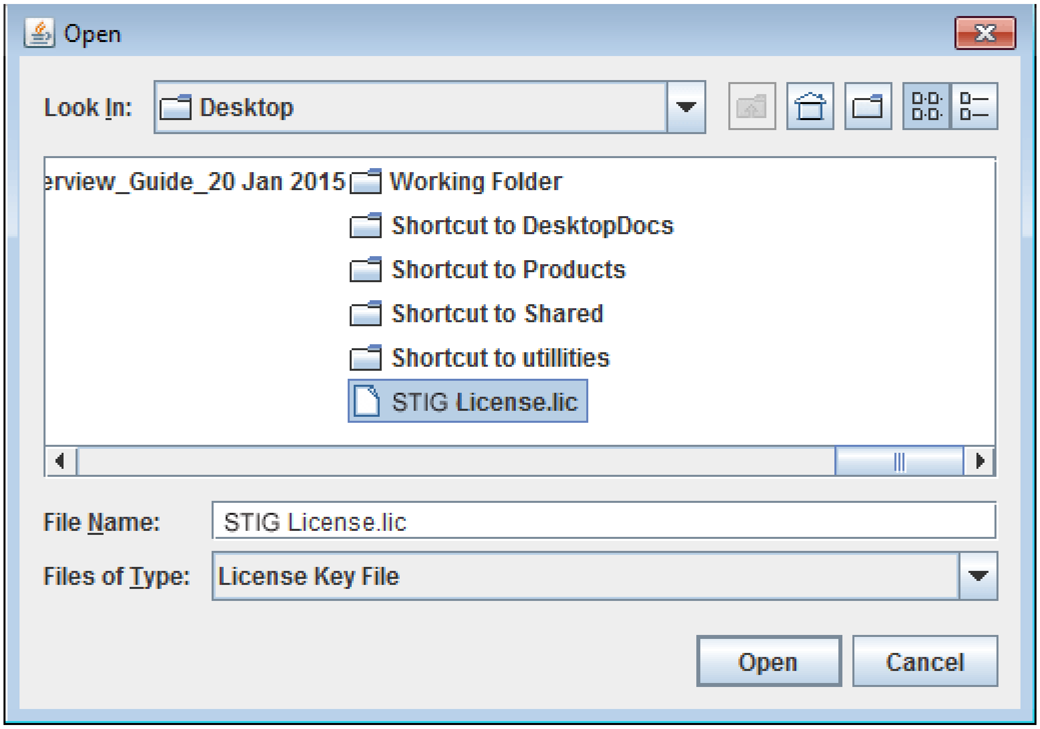


To... securevuestigprofiler@eiqnetworks.com

Subject STIGProfiler: License Key Request

The System Identifier is:
nZ9EQQpBxz+7AfY1e6MPdLfVn+si3zB6ZdAjbboGIPFoke1yEQJDImEr++yd+oUyITSWy9JSjOmR9h/ChcmdGsUUZ9nNlQjhv1SA+hKI8uyAszFORH030dEv

7. EiQ Networks STIG Profiler team generates a valid license for you and is sent to you through e-mail. Save the license onto your local machine and use the **Browse** button to add the License file as shown below.

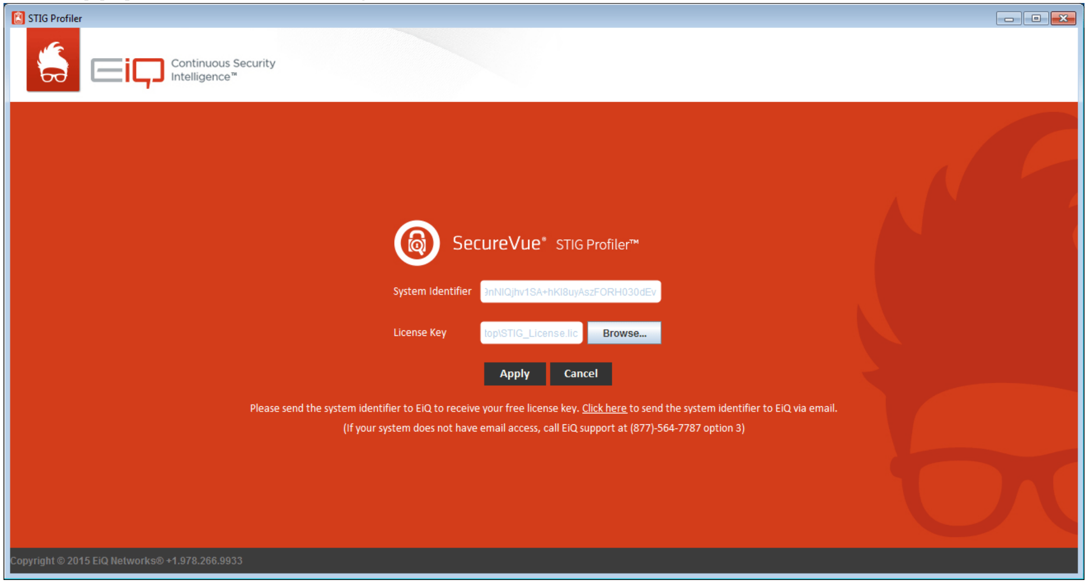


Look In: Desktop

File Name: STIG License.lic

Files of Type: License Key File

8. Click **Apply** button after loading the license file.



System Identifier:)nNIQjhv1SA+hKI8uyAszFORH030dEv

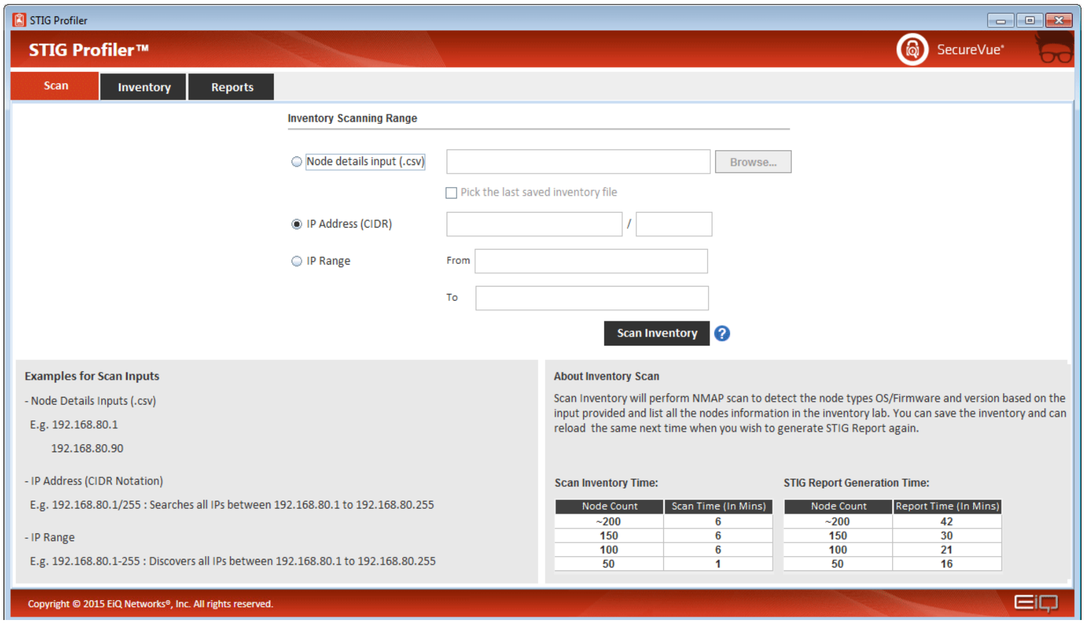
License Key: top\STIG_License.lic

Please send the system identifier to EiQ to receive your free license key. Click here to send the system identifier to EiQ via email.

(If your system does not have email access, call EiQ support at (877)-564-7787 option 3)

Copyright © 2015 EiQ Networks® +1.978.266.9933

9. The license is validated and the STIG Profiler application is launched as shown below graphic.



Inventory Scanning Range

○ Node details input (.csv)

☐ Pick the last saved inventory file

● IP Address (CIDR) /

○ IP Range From

To

Examples for Scan Inputs

- Node Details Inputs (.csv)

E.g. 192.168.80.1

192.168.80.90

- IP Address (CIDR Notation)

E.g. 192.168.80.1/255 : Searches all IPs between 192.168.80.1 to 192.168.80.255

- IP Range

E.g. 192.168.80.1-255 : Discovers all IPs between 192.168.80.1 to 192.168.80.255

About Inventory Scan

Scan Inventory will perform NMAP scan to detect the node types OS/Firmware and version based on the input provided and list all the nodes information in the inventory lab. You can save the inventory and can reload the same next time when you wish to generate STIG Report again.

Scan Inventory Time:

Node Count	Scan Time (In Mins)
~200	6
150	6
100	6
50	1

STIG Report Generation Time:

Node Count	Report Time (In Mins)
~200	42
150	30
100	21
50	16

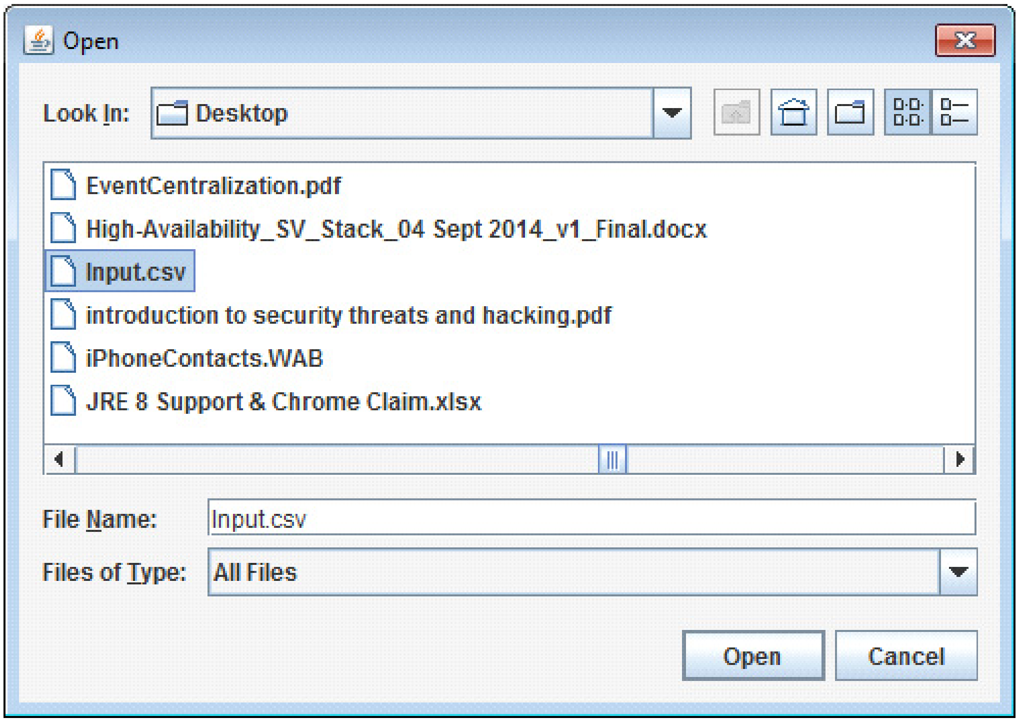
Initiating a Scan

Perform the following steps to initiate a scan:

1. Open the STIG Profiler application.
2. Select **Scan** tab.

   This tab presents 3 options for the user to perform a scan in the network.

a. Scan by using Node details (.csv) file as input.


Open
Look In: Desktop
EventCentralization.pdf
High-Availability_SV_Stack_04 Sept 2014_v1_Final.docx
Input.csv
introduction to security threats and hacking.pdf
iPhoneContacts.WAB
JRE 8 Support & Chrome Claim.xlsx
Open
Cancel

File Name: Input.csv

Files of Type: All Files

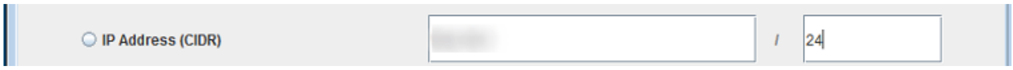
Each row in the CSV file can be defined as following and can contain IP address of the node as shown below.

NodeIp1

NodeIp2

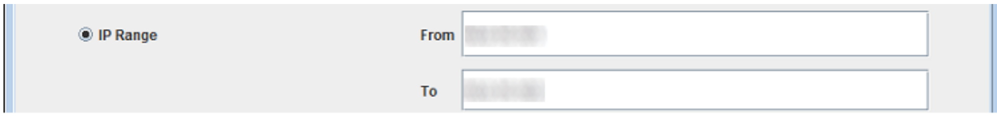
NodeIp3

b. Scan through an **IP Address (CIDR)** format as shown below:



○ IP Address (CIDR) [redacted] / 24

c. Specify IP Range to scan as shown below:



● IP Range

From [redacted]

To [redacted]

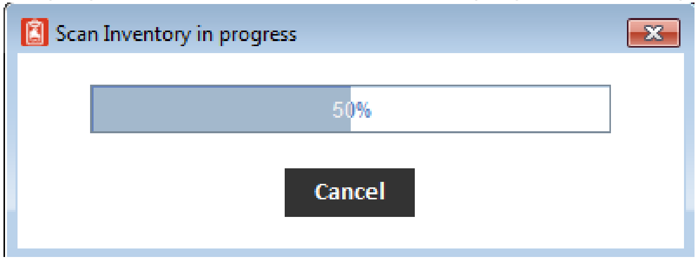
3. Click **Scan Inventory** button to launch the scan.

   Connection time-out option for the scan is user configurable. Users can change the time-out parameter "host-timeout" value from *%system drive%\ StigProfiler\config\ConfigOptions.ext* file.

Note:
Changing the time-out value is mainly needed if the scan is performed on VPN or non-local networks.

---

4. The progress bar notifies the user on the progress and completion of scan.

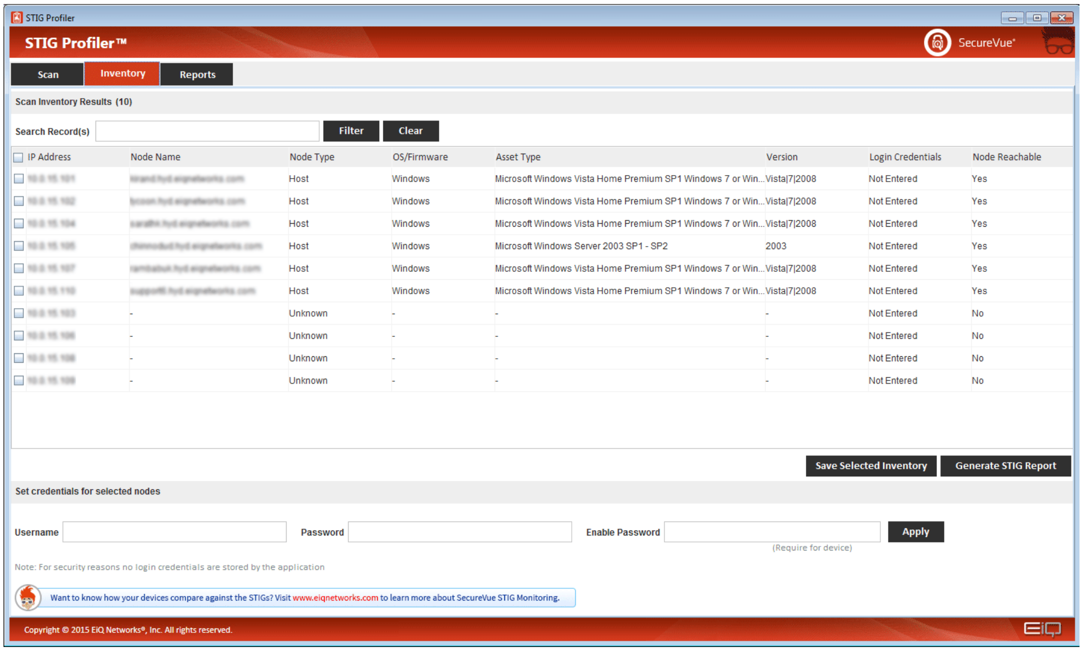


Based on your scan options, nodes in the network are scanned and scan results are populated in the Inventory tab in the form of a list.

Saving Inventory List

After the completion of Scan, scan results are populated in the Inventory tab. To save the scanned inventory list, do the following:

1. Select the IP records you want to save as a Inventory list file.



Scan Inventory Results (10)

Search Record(s)

☐	IP Address	Node Name	Node Type	OS/Firmware	Asset Type	Version	Login Credentials	Node Reachable
☐	[redacted]	[redacted]	Host	Windows	Microsoft Windows Vista Home Premium SP1 Windows 7 or Win...	Vista|7|2008	Not Entered	Yes
☐	[redacted]	[redacted]	Host	Windows	Microsoft Windows Vista Home Premium SP1 Windows 7 or Win...	Vista|7|2008	Not Entered	Yes
☐	[redacted]	[redacted]	Host	Windows	Microsoft Windows Vista Home Premium SP1 Windows 7 or Win...	Vista|7|2008	Not Entered	Yes
☐	[redacted]	[redacted]	Host	Windows	Microsoft Windows Server 2003 SP1 - SP2	2003	Not Entered	Yes
☐	[redacted]	[redacted]	Host	Windows	Microsoft Windows Vista Home Premium SP1 Windows 7 or Win...	Vista|7|2008	Not Entered	Yes
☐	[redacted]	[redacted]	Host	Windows	Microsoft Windows Vista Home Premium SP1 Windows 7 or Win...	Vista|7|2008	Not Entered	Yes
☐	[redacted]	-	Unknown	-	-	-	Not Entered	No
☐	[redacted]	-	Unknown	-	-	-	Not Entered	No
☐	[redacted]	-	Unknown	-	-	-	Not Entered	No
☐	[redacted]	-	Unknown	-	-	-	Not Entered	No

Set credentials for selected nodes

Username

Password

Enable Password
(Require for device)

Note: For security reasons no login credentials are stored by the application

Want to know how your devices compare against the STIGs? Visit www.eiqnetworks.com to learn more about SecureVue STIG Monitoring.

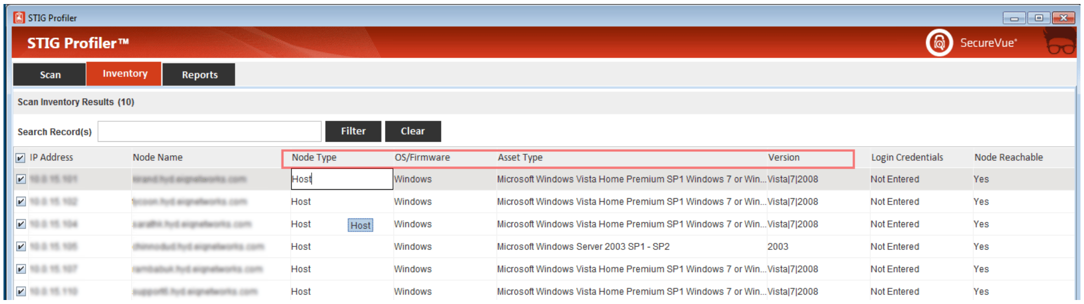
Copyright © 2015 EiQ Networks®, Inc. All rights reserved.

2. You can edit the inventory details collected by the NMAP scan if they are not accurate.

3. STIG Profiler allows the user to edit the following fields

- Node Type (Device/Host/Application)
- OS/Firmware
- Asset Type
- Version

4. To edit the values in any of these fields, select a row from the inventory list and double-click the field. The field is now editable. Change the details (Node Type, OS/Firmware, Asset Type and Version) and click on the same row outside the editable text box to effect your changes.



Scan Inventory Results (10)

Search Record(s)

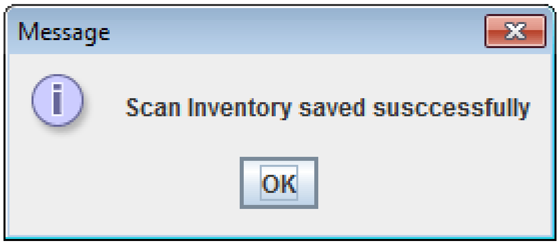
☑ IP Address	Node Name	Node Type	OS/Firmware	Asset Type	Version	Login Credentials	Node Reachable
☑ [redacted]	[redacted]	Host	Windows	Microsoft Windows Vista Home Premium SP1 Windows 7 or Win...	Vista|7|2008	Not Entered	Yes
☑ [redacted]	[redacted]	Host	Windows	Microsoft Windows Vista Home Premium SP1 Windows 7 or Win...	Vista|7|2008	Not Entered	Yes
☑ [redacted]	[redacted]	Host	Windows	Microsoft Windows Vista Home Premium SP1 Windows 7 or Win...	Vista|7|2008	Not Entered	Yes
☑ [redacted]	[redacted]	Host	Windows	Microsoft Windows Server 2003 SP1 - SP2	2003	Not Entered	Yes
☑ [redacted]	[redacted]	Host	Windows	Microsoft Windows Vista Home Premium SP1 Windows 7 or Win...	Vista|7|2008	Not Entered	Yes
☑ [redacted]	[redacted]	Host	Windows	Microsoft Windows Vista Home Premium SP1 Windows 7 or Win...	Vista|7|2008	Not Entered	Yes

5. Use the **Filter** (free text search) option to search for any specific records. Use **Clear** option to clear the filters.

6. Click **Save Selected Inventory** button.

Note

Inventory details of only the latest scan is saved at < STIG Profiler Installation Path>\StigProfiler\savedInventory.csv file. Users can re-use this last saved inventory details for generating a report without performing a new scan.



Scan Inventory saved susccessfully

Generating STIG Report

After the completion of Scan, Scan Inventory results are populated in the Inventory tab. you can select the records of your choice and generate the STIG Profiler reports.

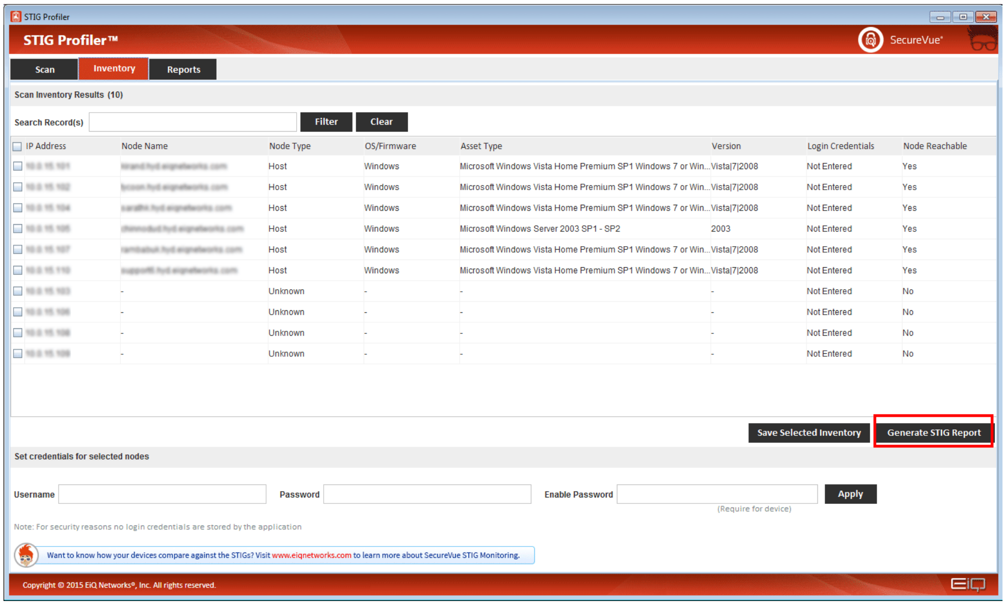
1. Launch the **STIG Profiler** tool.

2. Select the nodes of your choice from the scanned inventory list populated in the **Inventory** tab.

3. Specify the **User Name** and **Password** credentials. **Enable Password** details are required if the selected Node Type is a Device.

4. Click **Apply** button. After the credentials are applied, the Login Credentials column for the selected nodes indicate the value as Entered.

5. Click **Generate STIG Report** button.



Scan Inventory Results (10)

Search Record(s)

☐ IP Address	Node Name	Node Type	OS/Firmware	Asset Type	Version	Login Credentials	Node Reachable
☐ [redacted]	[redacted]	Host	Windows	Microsoft Windows Vista Home Premium SP1 Windows 7 or Win...	Vista|7|2008	Not Entered	Yes
☐ [redacted]	[redacted]	Host	Windows	Microsoft Windows Vista Home Premium SP1 Windows 7 or Win...	Vista|7|2008	Not Entered	Yes
☐ [redacted]	[redacted]	Host	Windows	Microsoft Windows Vista Home Premium SP1 Windows 7 or Win...	Vista|7|2008	Not Entered	Yes
☐ [redacted]	[redacted]	Host	Windows	Microsoft Windows Server 2003 SP1 - SP2	2003	Not Entered	Yes
☐ [redacted]	[redacted]	Host	Windows	Microsoft Windows Vista Home Premium SP1 Windows 7 or Win...	Vista|7|2008	Not Entered	Yes
☐ [redacted]	[redacted]	Host	Windows	Microsoft Windows Vista Home Premium SP1 Windows 7 or Win...	Vista|7|2008	Not Entered	Yes
☐ [redacted]	-	Unknown	-	-	-	Not Entered	No
☐ [redacted]	-	Unknown	-	-	-	Not Entered	No
☐ [redacted]	-	Unknown	-	-	-	Not Entered	No
☐ [redacted]	-	Unknown	-	-	-	Not Entered	No

Set credentials for selected nodes

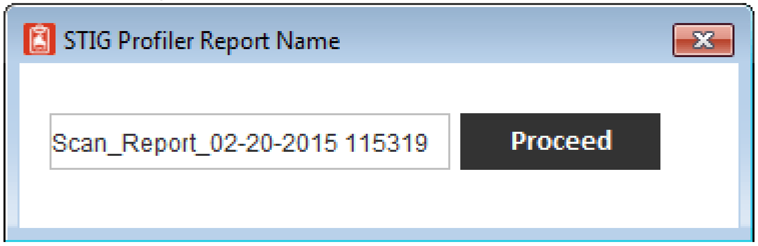
Username Password Enable Password

(Require for device)

Note: For security reasons no login credentials are stored by the application

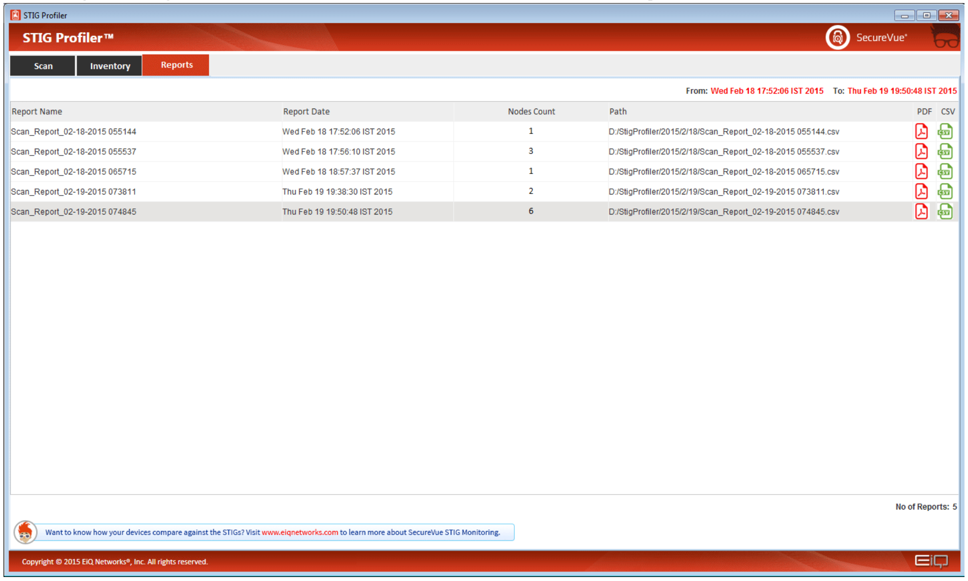
Want to know how your devices compare against the STIGs? Visit www.eiqnetworks.com to learn more about SecureVue STIG Monitoring.

6. You are prompted to provide a name for the report. If no name is provided, STIG Profiler uses the default report nomenclature. Click **Proceed**.



Scan_Report_02-20-2015 115319

7. The report is generated and is made available in the **Reports** tab in **PDF** and **CSV** formats.



From: Wed Feb 18 17:52:06 IST 2015 To: Thu Feb 19 19:50:48 IST 2015

Report Name	Report Date	Nodes Count	Path	PDF	CSV
Scan_Report_02-18-2015 055144	Wed Feb 18 17:52:06 IST 2015	1	D:/StigProfiler/2015/2/18/Scan_Report_02-18-2015 055144.csv		
Scan_Report_02-18-2015 055537	Wed Feb 18 17:56:10 IST 2015	3	D:/StigProfiler/2015/2/18/Scan_Report_02-18-2015 055537.csv		
Scan_Report_02-18-2015 065715	Wed Feb 18 18:57:37 IST 2015	1	D:/StigProfiler/2015/2/18/Scan_Report_02-18-2015 065715.csv		
Scan_Report_02-19-2015 073811	Thu Feb 19 19:38:30 IST 2015	2	D:/StigProfiler/2015/2/19/Scan_Report_02-19-2015 073811.csv		
Scan_Report_02-19-2015 074845	Thu Feb 19 19:50:48 IST 2015	6	D:/StigProfiler/2015/2/19/Scan_Report_02-19-2015 074845.csv		

No of Reports: 5

Want to know how your devices compare against the STIGs? Visit www.eiqnetworks.com to learn more about SecureVue STIG Monitoring.

8. Click the **PDF** or **CSV** icons to launch the report.

Note
By default all the reports generated by STIG Profiler are retained for a period of 1 Year. User can alter the retention period by editing the *retentionPeriod* parameter from StigProfiler\config\ConfigOptions.ext file. Retention period should be provided in Seconds only.

Directions for Updating the DISA STIG Reference list

This section provides directions on how end users of STIG Profiler can update the DISA STIG reference list for new benchmarks published for STIG Policies.

When a STIG Policy benchmark is updated, user can update the same in the mapping file by following the steps below:

1. Open the <%System Drive%>\StigProfiler\config\mapping.txt file, search for the STIG policy that is being updated.
2. Change the benchmark values to reflect the latest version. For example if there is a updated version for "Windows 2003 DC STIG - Version 6, Release 1.35", user need to search and replace the policy entry in the mapping.txt file with the latest revision.
3. Save the file.

When STIG report is generated next time, STIG Profiler would recommend the latest STIG Policy version for the Windows 2003 Hosts.

Failure Cases

This section provides details on the common errors encountered by users while working with STIG Profiler

Failure Cases:
When the target node is not reachable, user need to check whether the target node is up and running in the network.
Connection to the target node may time out if connection is not established in the specified time.
Target nodes are not accessible when the provided credentials are wrong.
Cannot recommend STIG Policies if remote registry, RSOP and WMI services on the target windows node is not running or not accessible.

Permissions for RSOP WMI Method Provider

RSOP (Resultant Set of Policy) is a report of all Group Policy settings within Active Directory that shows how those settings can affect a network, or how existing Group Policy Objects (GPOs) affect various combinations of users and computers when the local security policy is applied.

To set WMI permissions exclusively for certain namespaces, refer to

http://technet.microsoft.com/en-us/library/cc771551.aspx

http://msdn.microsoft.com/en-us/library/aa393613%28v=vs.85%29.aspx

The following link provides the useful information on RSOP and WMI classes:

http://msdn.microsoft.com/en-us/library/aa375082(v=vs.85).aspx

Permissions for Registry

For "Registry” collection, user is required to have read access to all registry locations.

Registry method is used to collect the data from the windows registry. The registry method seeks key and value (if any) as collection parameter from the defined rule.

For details about security permissions for Registry, refer to http://technet.microsoft.com/en-us/library/cc728310(v=ws.10).aspx