CARSON & SAINT

SAINT® Security Suite

Installation Guide

Table of Contents

Welcome to the SAINT Security Suite 4

This guide is designed to walk you through the following: 4

- Downloading and installing the platform on which you want to run SAINT Security Suite (either Linux or Windows) 4
- Downloading and installing SAINT Security Suite 4
- How to run your first scan 4

1. Ensure You Have Your License: Accept License, and Access Licensed Product 4

2. Download SAINT Security Suite, or Access Licensed Product 4

3. Install SAINT Security Suite (and Platform if necessary) 5

3.1 Install in preexisting environment: 5

Install on Ubuntu 5

Install on Red Hat / CentOS / Fedora 5

3.2 Deploy a Pre-Configured Virtual Machine 5

3.3 How to Unzip Your Files 6

VMware Workstation 6

VMware Player 6

VMware Fusion 6

3.4 How to Use the OVA File 7

VMware 7

Oracle Virtualbox 7

3.5 Using the VMware vCenter Converter Standalone Software 7

4. Start SAINT Security Suite 10

4.1 Start the Virtual Machine 10

4.2 Set the VM's System Clock 10

4.3 Launch SAINT Security Suite 10

4.3 Choose your Startup Option 10

4.4 Start and Launch the User Interface Directly on the Installed Host 10

4.5 Start and Run as a Background Process 11

4.6 Start and Run as a Remote Scanner Node 11

4.7 General Options 12

4.8 Stop 12
4.9 Exit 13
5. Log In 14
6. Apply License Key 14
Configure SAINT Key 14
7. Update SAINT Security Suite and Configure System Updates. 15
Get the Latest Updates 15
8. Run Your First Scan. 15
Step 2: Targets 16
Steps 3 & 4. In this quick scan, we will skip optional steps 3 and 4. 16
Step 5: Review, Schedule and Finish 16

Welcome to the SAINT Security Suite.

This guide is designed to walk you through the following:

- Downloading and installing the platform on which you want to run SAINT Security Suite (either Linux or Windows)
- Downloading and installing SAINT Security Suite
- How to run your first scan

There are just a few steps and decisions for you to make, which are detailed in the next section:

1. Ensure you have your license.
2. Download SAINT Security Suite (also requires platform download for Windows users).
3. Install SAINT Security Suite and/or the platform.
4. Start SAINT Security Suite.
5. Log in.
6. Apply license key.
7. Update SAINT Security Suite.
8. Run your first scan.

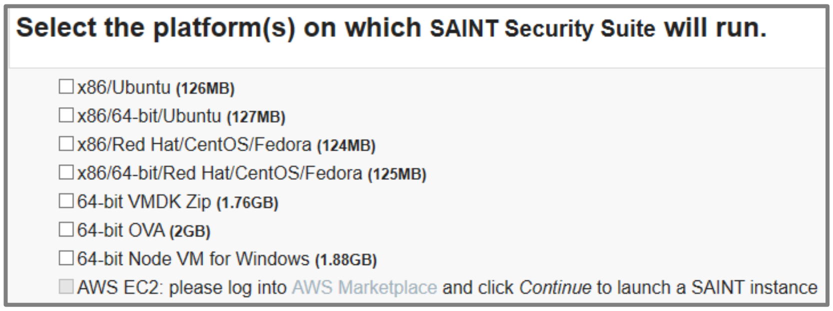
1. Ensure You Have Your License: Accept License, and Access Licensed Product

The SAINT software is made available to you via the mySAINT Customer portal, which can be accessed by logging in at https://my.saintcorporation.com, using the account credentials you were provided in the first email you received from our Support Team. Once you've logged into the portal, click on the **Downloads** menu option, then choose **Licensed Products** to view all deployment options for software you are licensed for.

2. Download SAINT Security Suite, or Access Licensed Product

On the home screen of my.saintcorporation.com you will first be asked to select a platform.

A. Select the target platform you wish to run SAINT Security Suite **within:**



Select the platform(s) on which SAINT Security Suite will run.

□x86/Ubuntu **(126MB)**
□x86/64-bit/Ubuntu **(127MB)**
□x86/Red Hat/CentOS/Fedora **(124MB)**
□x86/64-bit/Red Hat/CentOS/Fedora **(125MB)**
□64-bit VMDK Zip **(1.76GB)**
□64-bit OVA **(2GB)**
□64-bit Node VM for Windows **(1.88GB)**
□AWS EC2: please log into AWS Marketplace and click *Continue* to launch a SAINT instance

- **X86/Ubuntu** – Use this option when you already have a 32-bit Ubuntu installed and want to download and install SAINT Security Suite.
- **X86/64-bit/Ubuntu** – Use this option when you are already running a 64-bit Ubuntu environment.
- **X86/Red Hat/CentOS/Fedora** – Use this .rpm (Red Hat Package Manager) option when you have either of these 32-bit distributions already in production and wish to run SAINT Security Suite within those environments.
- **X86/64-bit/Red Hat/CentOS/Fedora** – Use this .rpm option when you have either of these 64-bit distributions already in a 64-bit production and wish to run SAINT Security Suite within those environments.
- **64-bit VMware (VMDK)** – Use this option to download and install SAINT and Ubuntu to be later imported into VMware Virtual Machine.

- **64-bit VirtualBox (OVA)** – Use this option to download SAINT Security Suite and Ubuntu to be later imported into VirtualBox Virtual Machine.
- **64-bit Node VM for Windows** – Use this option when installing SAINT Security Suite as a Node virtual machine to be controlled by an existing SAINT manager installation.
- **AWS EC2** – Please log into AWS Marketplace and click ***Continue*** to launch a SAINT instance.

B. After you have checked the appropriate box:

- Read the End User License Agreement.
- If you agree, select "accept the license agreement."
- Click ***Continue***.
- When the ***Downloads*** link appears, select ***Save***.

Note to SAINT Amazon Web Services customers:

SAINT Security Suite provides pre-configured Amazon Machine Images (AMIs) for deployment in AWS. To launch an instance of a SAINT AMI, click on the AWS Marketplace hyperlink for the AWS EC2 option, and follow steps described in the SAINT Amazon Machine Image Guide provided under the ***Resources*** menu –> ***Installation Guides*** option to deploy a licensed SAINT AMI.

3. Install SAINT Security Suite (and Platform if necessary)

For all Security Suite installations, ensure all System Requirements and dependencies described under the System Requirements section of the Admin Guide have been met before continuing. *Platform installation is only required for Windows users.*

3.1 Install in preexisting environment:

Install on Ubuntu

1. Double-click on the file **SAINT8.x.x-i386.deb** (where x.x is the version you downloaded).
2. Choose ***Install***.
3. Start SAINT Security Suite from the ***Applications*** menu.

Install on Red Hat / CentOS / Fedora

1. Double-click on the file **SAINT8.x.xx-1.i586.rpm** (where x.x is the version you downloaded).
2. Start SAINT Security Suite from the Applications menu.

3.2 Deploy a Pre-Configured Virtual Machine

SAINT Security Suite pre-configured virtual machines are provided as a fast and easy method of deploying SAINT Security Suite into your environment without the need for purchasing our pre-configured hardware or installing and maintaining a manual software installation on a Linux (*nix) operating system.

- Each virtual machine has been built with SAINT Security Suite software installed on the latest Ubuntu operation system LTS and exported as both an .ova file and .zip file.
- These VMs can be deployed into VMware Player, VMware Workstation, VMware Fusion, ESXi server, or Oracle Virtualbox.

- If none of these deployment options are compatible with your requirements, each can be converted into an existing VMware server environment using the Converter Standalone Client.

Minimum configuration of environment:

- 3GB of RAM
- 40 GB HD when thick provisioned; 5 GB as thin provisioned which will grow over time.
- Network adapter is set for NAT and DHCP.
- Video settings should be set at 128 MB.

Downloads:

- VMware Downloads
  - VMware Player: VMware Player Download
  - VMware ESXi Server: VMware ESXi Server Download
  - WMware Converter Standalone Client (only if no other option available): VMware Converter Standalone Client
- Oracle Virtualbox Download
  Oracle Virtualbox: Oracle Virtualbox Download

3.3 How to Unzip Your Files

VMware Workstation

1. Download and unzip the *SAINT[version]VM64.zip* file on your local host.
2. Double-click on the file *SAINT[version]VM64.vmx*. It will open automatically in the Workstation software.

VMware Player

1. Open VMware Player.
2. Choose Open a Virtual Machine.
3. Browse to the unzipped *SAINT[version]VM64.vmx* file.
4. Open the file. It will then be added to your VMware Player as *SAINT[version]VM*.

VMware Fusion

1. Unzip the downloaded files with your favorite zip utility for unzipping Windows zip files.
   NOTE: The built-in zip utility for Mac OSX has been found to compress contents more, thus is not a supported utility for this operation.
2. Launch Fusion on your MAC OSX.
3. Navigate to ***Home***.
4. Click ***Install Windows or another operating system in a new Virtual Machine***.”
5. Click ***Continue without disk***.
6. On the next page, click ***Use an existing virtual disk***.
7. Navigate to the directory where you unzipped the downloaded file.
8. Choose SAINT[version]VM64.vmdk.
9. Click ***Continue***.

10. On the next page, click ***Customize Settings*** to change the memory to 3 GB as a minimum. 4 GB is the suggested amount of RAM.
11. Click ***Finish***.

3.4 How to Use the OVA File

VMware

From a VMware ESXi or VMware server:

1. Select ***File***.
2. Choose ***Deploy OVF Template***.
3. Follow the wizard while setting the Name, Disk Format store, and Network settings.

Oracle Virtualbox

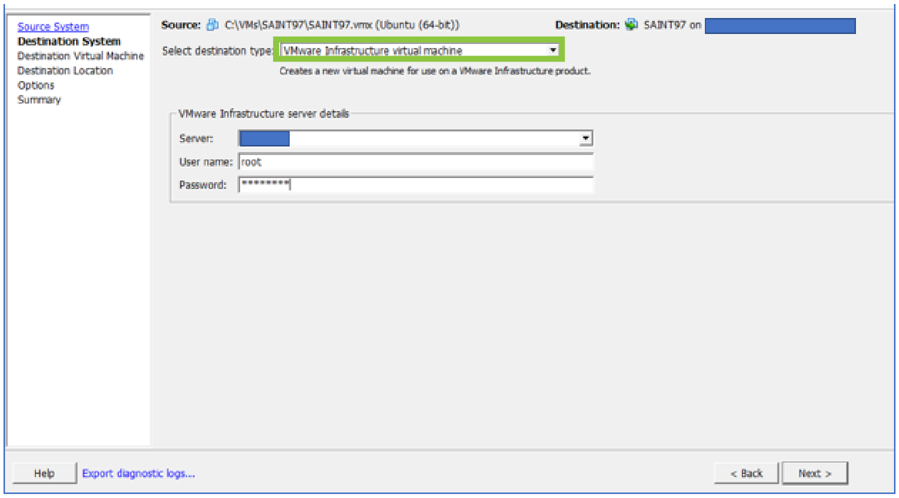
1. Select ***File****.*
2. Choose ***Import Appliance***.
3. Navigate to the downloaded .ova.

3.5 Using the VMware vCenter Converter Standalone Software

If neither virtual machine deployment options are compatible with your requirements, each can be converted into an existing VMware server environment, using the Converter Standalone Client. Use this option only if the previous recommended options are not available.

1. Download and install the VMware converter:
   - WMware Converter Standalone Client (only if no other option available):
     - ○ Download here: [VMware Converter Standalone Client]()
   - Install converter then click ***Convert***.

2. Select a host for the new virtual machine:



Source: C:\VMs\SAINT97\SAINT97.vmx (Ubuntu (64-bit))

Destination: SAINT97 on [redacted]

Select destination type: VMware Infrastructure virtual machine

Creates a new virtual machine for use on a VMware Infrastructure product.

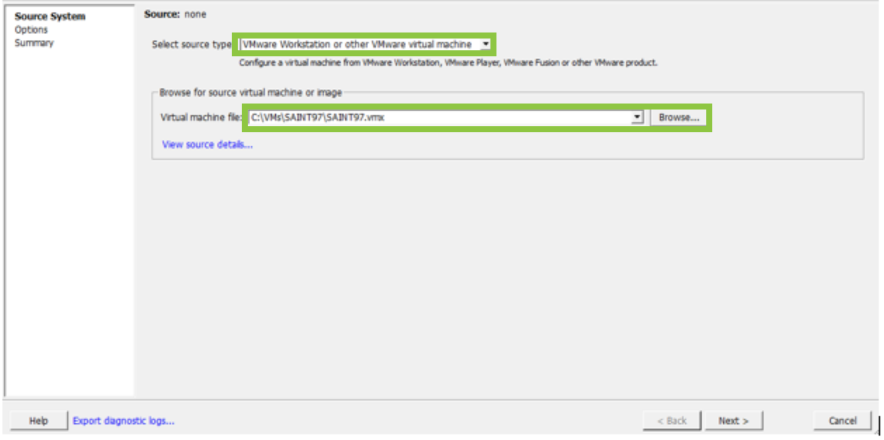
VMware Infrastructure server details

Server: [redacted]

User name: root

Password: ********

3. Select the Virtual Machine type you want to reconfigure.



Source System
Options
Summary

Source: none

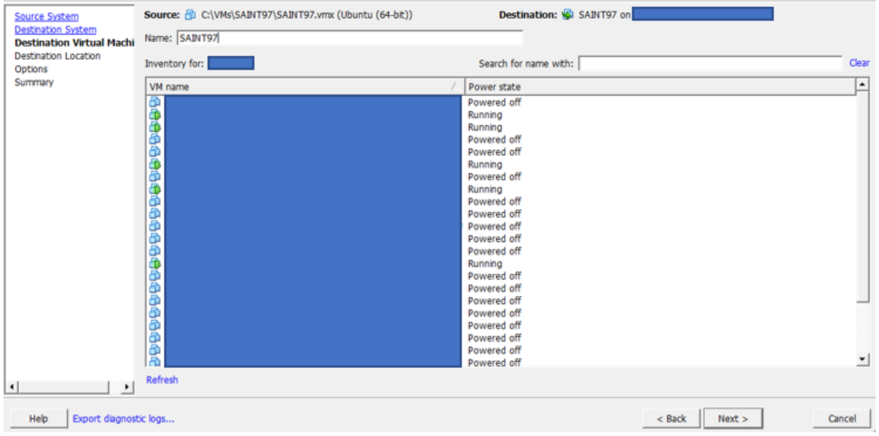
Select source type: VMware Workstation or other VMware virtual machine

Configure a virtual machine from VMware Workstation, VMware Player, VMware Fusion or other VMware product.

Browse for source virtual machine or image

Virtual machine file: C:\VMs\SAINT97\SAINT97.vmx

4. Select the destination VM name and folder.



Source System
Destination System
Destination Virtual Machi
Destination Location
Options
Summary

Source: C:\VMs\SAINT97\SAINT97.vmx (Ubuntu (64-bit))

Destination: SAINT97 on [redacted]

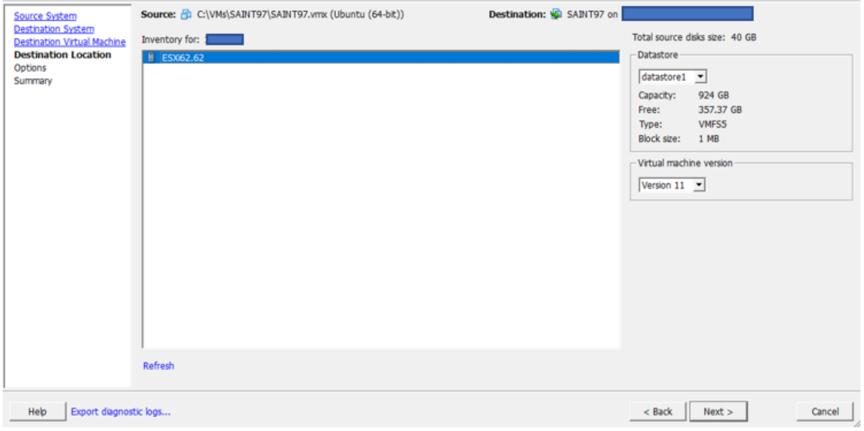
Name: SAINT97

Inventory for: [redacted]

Search for name with:

VM name	Power state
[redacted]	Powered off
[redacted]	Running
[redacted]	Running
[redacted]	Powered off
[redacted]	Powered off
[redacted]	Running
[redacted]	Powered off
[redacted]	Running
[redacted]	Powered off
[redacted]	Powered off
[redacted]	Powered off
[redacted]	Powered off
[redacted]	Powered off
[redacted]	Running
[redacted]	Powered off
[redacted]	Powered off
[redacted]	Powered off
[redacted]	Powered off
[redacted]	Powered off
[redacted]	Powered off
[redacted]	Powered off
[redacted]	Powered off
[redacted]	Powered off

5. Select the location for the new virtual machine.



Source System
Destination System
Destination Virtual Machine
Destination Location
Options
Summary

Source: C:\VMs\SAINT97\SAINT97.vmx (Ubuntu (64-bit))

Destination: SAINT97 on [redacted]

Inventory for: [redacted]

ESXi62.62

Total source disks size: 40 GB

Datastore

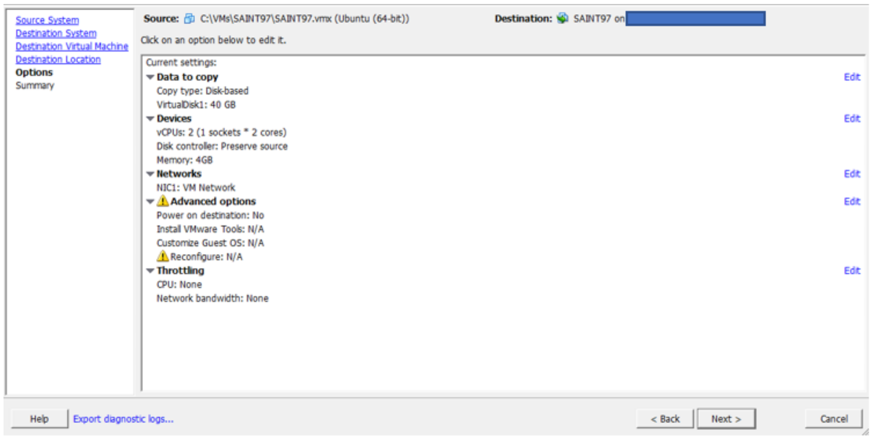
datastore1

Capacity:	924 GB
Free:	357.37 GB
Type:	VMFS5
Block size:	1 MB

Virtual machine version

Version 11

6. Set up the parameters for the conversion task:



Source: C:\VMs\SAINT97\SAINT97.vmx (Ubuntu (64-bit))
Destination: SAINT97 on [redacted]

Click on an option below to edit it.

Current settings:

Data to copy
Copy type: Disk-based
VirtualDisk1: 40 GB

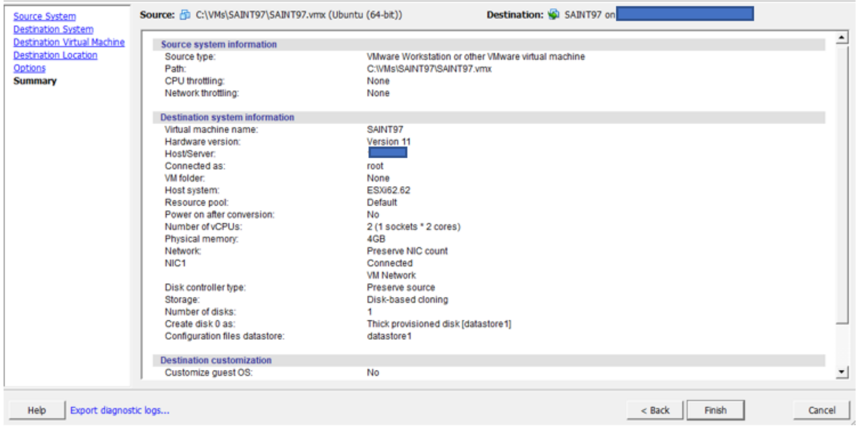
Devices
vCPUs: 2 (1 sockets * 2 cores)
Disk controller: Preserve source
Memory: 4GB

Networks
NIC1: VM Network

⚠ Advanced options
Power on destination: No
Install VMware Tools: N/A
Customize Guest OS: N/A
⚠ Reconfigure: N/A

Throttling
CPU: None
Network bandwidth: None

7. Review the conversion parameters:



Source: C:\VMs\SAINT97\SAINT97.vmx (Ubuntu (64-bit))
Destination: SAINT97 on [redacted]

Source system information

Source type:	VMware Workstation or other VMware virtual machine
Path:	C:\VMs\SAINT97\SAINT97.vmx
CPU throttling:	None
Network throttling:	None

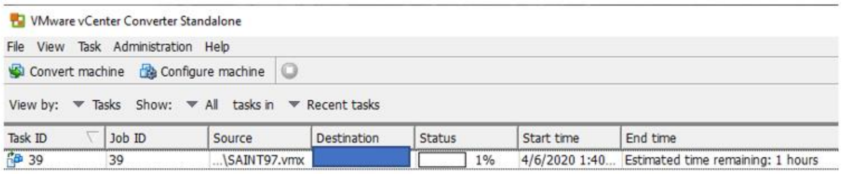
Destination system information

Virtual machine name:	SAINT97
Hardware version:	Version 11
Host/Server:	[redacted]
Connected as:	root
VM folder:	None
Host system:	ESXi62.62
Resource pool:	Default
Power on after conversion:	No
Number of vCPUs:	2 (1 sockets * 2 cores)
Physical memory:	4GB
Network:	Preserve NIC count
NIC1	Connected VM Network
Disk controller type:	Preserve source
Storage:	Disk-based cloning
Number of disks:	1
Create disk 0 as:	Thick provisioned disk [datastore1]
Configuration files datastore:	datastore1

Destination customization

Customize guest OS:	No

8. Monitor conversion status:



VMware vCenter Converter Standalone

Task ID	Job ID	Source	Destination	Status	Start time	End time
39	39	...\SAINT97.vmx	[redacted]	1%	4/6/2020 1:40...	Estimated time remaining: 1 hours

4. Start SAINT Security Suite

4.1 Start the Virtual Machine

If you are running SAINT Security Suite from a pre-configured Virtual Machine (VM), the first step is to start the VM, using the default VM's admin credential. If you are using a native installation, see the next step for launching the product.

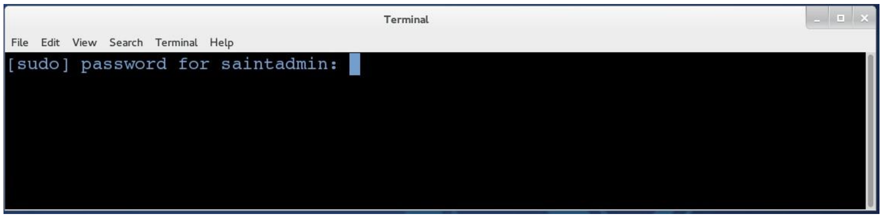
- **UID: saintadmin**
- **Password: SAINT!!!**

4.2 Set the VM's System Clock

On first login of the VM, you must confirm the operating system's system clock is set to the time zone and time applicable to your location. By default, the VM's system clock is set to Eastern Standard Time (EST).

4.3 Launch SAINT Security Suite

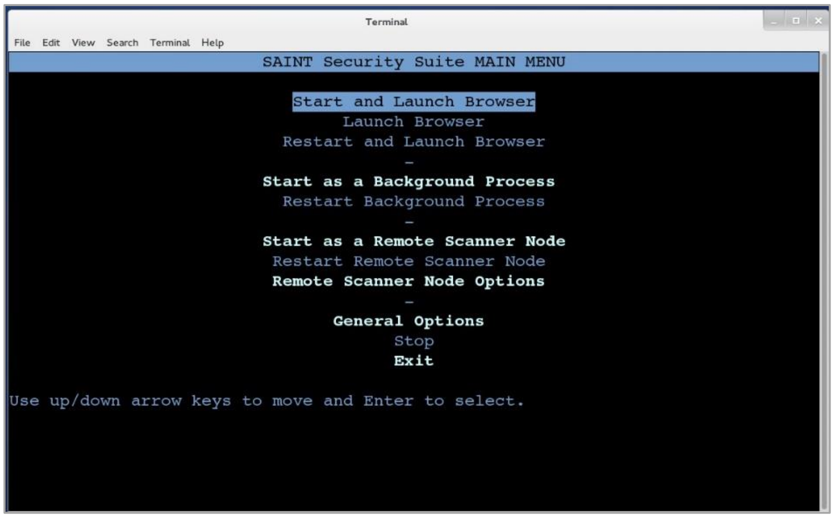
Click on the SAINT Security Suite icon: ʃ or click on the ***SAINT Security Suite*** option from the application menu. SAINT Security Suite must run with administrative permissions on the installed host. Therefore, the startup process begins with a terminal window prompt to enter these credentials – much like newer versions of Windows and MAC OS X do when software requires administrative rights.



```
[sudo] password for saintadmin:
```

4.3 Choose your Startup Option

SAINT Security Suite can be run in a number of ways. On the initial installation and setup, the following startup MAIN MENU will be displayed. You must select the option that describes how you want the software to be started. Making a selection here will be stored and used on subsequent startup processes. The MAIN MENU will be displayed in case you wish to restart, stop, or change how the software is started.



```
                    SAINT Security Suite MAIN MENU

                        Start and Launch Browser
                            Launch Browser
                      Restart and Launch Browser
                                  -
                     Start as a Background Process
                      Restart Background Process
                                  -
                      Start as a Remote Scanner Node
                      Restart Remote Scanner Node
                       Remote Scanner Node Options
                                  -
                            General Options
                                 Stop
                                 Exit

Use up/down arrow keys to move and Enter to select.
```

4.4 Start and Launch the User Interface Directly on the Installed Host

The first option is to start the software and launch a browser to support direct access on the installed host or even from a remote location if the host can access the installed host. This option is most typically used for standalone, desktop installations, or even server installations where access to the user interface will be directly on the installed host.

- **Start and Launch Browser** – Starts SAINT Security Suite in a browser window – as you are used to in previous versions of the SAINT Professional edition – to access the browser interface.
- **Launch Browser** – This option will be available if the software has already been started and is still running in background. Select this option just to open a browser on the installed host.
- **Restart and Launch Browser** – This option will stop and restart the software, check for any product updates, and launch the user interface in a browser window.

4.5 Start and Run as a Background Process

SAINT Security Suite can be started to run as a background process, without launching the browser. This is typical of a shared environment where access will be done from various desktop browsers or via command line access from remote hosts.

- **Start as a Background Process** – Starts all SAINT Security Suite processes, but does not launch the browser-based user interface.
- **Restart Background Process** – This option will stop and restart the software and check for any product updates. This step does NOT launch the user interface in a browser window.

4.6 Start and Run as a Remote Scanner Node

The third option is to start SAINT Security Suite as a remote scanner node to support a distributed, multi-scanner node environment. In this configuration, the initial setup will include steps to connect this installation to a separate SAINT Security Suite installation acting as the central “manager.”

- **Start as a Remote Scanner Node** – Starts all SAINT Security Suite processes, checks for any product updates, and initiates a secure connection to the “manager” installation. This process does NOT launch the browser-based user interface. The following describes the steps required to configure the remote scanner node the first time you start up the installation to “start as a remote scanner node:”
  1. Scroll down, locate the ***Start as a Remote Scanner Node*** option, and click the ***Enter*** key.
  2. Enter the fixed IP address of the SAINT Security Suite installation acting as the “manager.”
  3. Click ***Return*** or the ***down-arrow key***.
  4. Click ***OK*** to save the change and return to the MAIN MENU.

     Note: The Scanner Node Connection Port and Scanner Node Connection Password are already set by default for all installations. However, you can change these default settings under the Configuration menu –> System Options –> Nodes tab in the “manager” installation. If you have changed these settings, navigate to the ***Remote Scanner Node Options*** *menu (described below) and update those settings before returning to the MAIN MENU and starting the scanner node.*
  5. Click on the ***Start as a Remote Scanner Node*** option to start the scanner node and make a secure connection to the “manager.” You should now see the new node listed in the list of connected nodes under the *Manage* menu – Scanner *Nodes* page through the “manager” installation.
- **Restart Remote Scanner Node** – This option will stop and restart the software, check for any product updates, and re-initiate a secure connection to the “manager” installation. This step does NOT launch the user interface in a browser window.
- **Remote Scanner Node Options** – Select this option to configure the installation as a remote scanner “node” and configure a secure connection to a separate installation acting as a central “manager.” The following describes the node options in more detail:
  - **Manager Address** – This configuration setting contains the fixed IP address of the SAINT Security Suite installation acting as the manager that will control communication and scan activity on the scanner node.

- **Scanner Node Connection Port** – This configuration setting contains the TCP port on the manager that the node will use to connect. This configuration setting is defined through the user interface, in the ***Configuration*** menu, ***System Options*** submenu, by clicking on the ***Nodes*** tab.
- **Scanner Node Connection Password** – Each remote node must supply this password to authenticate the connection to the "manager" installation. This is the password configured through the ***Configuration*** menu, ***System Options*** submenu in the user interface, by the clicking on the ***Nodes*** tab – See the *Node Password* setting block. If this option is left blank, then no password is required when connecting a scanner node to the manager.
- **Check Software Dependencies** – This option checks the installation host for third-party software dependencies or other system requirements to ensure the software can be installed and configured properly on the host. Note that the SAINT Security Suite VM deployment option is automatically released with all valid dependencies, and all Installer processes automatically perform these operations during installation. However, you may need to run this step manually if there are any issues or problems with the software or modifications to the host environment that affect the product.
- **Back to Main Menu** – This option closes the options menu and returns to the SAINT Security Suite MAIN MENU.
- **Exit** – Click this option to close the SAINT Security Suite MAIN MENU.

4.7 General Options

These options support modifying configuration settings related to web ports and control over remote host access, as well as manually checking your system to valid third-party dependencies or other system-related settings.

- **Web Allowed Hosts** – This configuration setting stores the hosts that are authorized to connect to the SAINT application. The default is ALL (*). However, you can use this setting to enter comma-delimited IP addresses to limit access to only authorized hosts if needed. This configuration setting is also available on the ***Configuration*** menu in the user interface, through the ***System Options*** submenu, by clicking on the ***Web Server*** tab.
- **Web Port** – This configuration setting stores the TCP/IP port that the SAINT Security Suite web server listens on. This configuration setting is also available on the ***Configuration*** menu in the user interface, through the ***System Options*** submenu, by clicking on the ***Web Server*** tab.
- **Check Software Dependencies** – This option checks the installation host for third-party software dependencies or other system requirements to ensure the software can be installed and configured properly on the host. Note that the SAINT Security Suite VM deployment option is automatically released with all valid dependencies, and all Installer processes automatically perform these operations during installation. However, you may need to run this step manually if there are any issues or problems with the software or modifications to the host environment affect the product.
- **Back to Main Menu** – This option closes the options menu and returns to the SAINT Security Suite MAIN MENU.
- **Exit** – Click this option to close the SAINT Security Suite MAIN MENU.

4.8 Stop

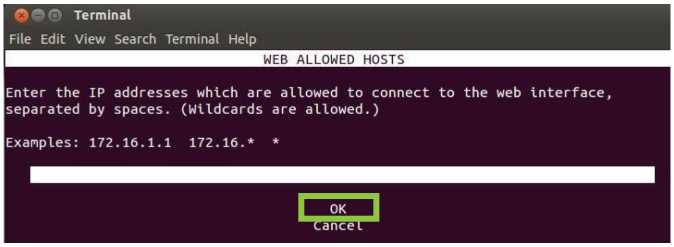
Whether you run SAINT Security Suite by launching the browser, strictly in background mode, or as a remote node, the software runs as a background process so scans can continue to be scheduled and executed, even when the browser is closed on the host. This option allows you to manually stop the product to include any running background processes. This option will only be available for selection if SAINT Security Suite is currently running.

4.9 Exit

Select this option to quit the startup process and close the startup menu.

What if a Service or Required Configuration Setting is not Found on Startup?

There may be instances during the startup process where a system configuration value or service is not found or should be validated prior to startup. For example, one common configuration setting is related to allowing you control over the hosts that should be allowed to connect to the web-based application. If this prompt is displayed, enter/verify the explicit IP addresses of specific hosts (if you wish to restrict access down to that level) or enter/verify * to indicate remote access from any potential host and then select ***OK*** to continue. The latter is the most common use-case.

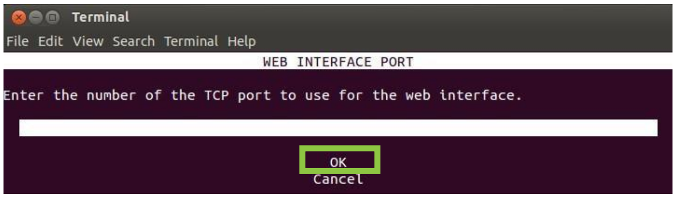


```
WEB ALLOWED HOSTS

Enter the IP addresses which are allowed to connect to the web interface,
separated by spaces. (Wildcards are allowed.)

Examples: 172.16.1.1  172.16.*  *
```

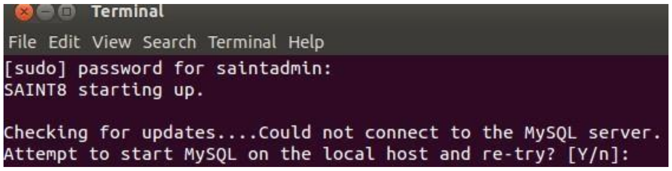
Another possible setting is to define the TCP port to use for allowing the web interface. SAINT uses Port 1414 by default, but this can be changed if local policies dictate. Enter/verify the port number in this field and choose **OK** to continue.



```
WEB INTERFACE PORT

Enter the number of the TCP port to use for the web interface.
```

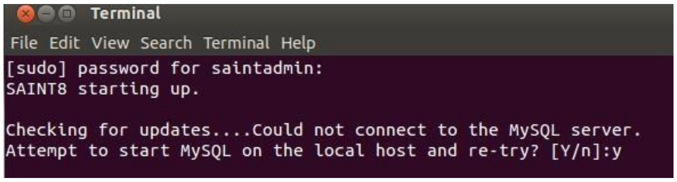
The current installation of SAINT Security Suite uses a MySQL database backend for application configurations and scan content. In the standard setup, the target database is installed on the same host as the software. In most *nix-based platforms, the MySQL service is started automatically and managed by the installation and startup processes. However, in some instances (particularly RedHat, CentOS, and Fedora) this service is not always started at the same time the OS is launched. A check process is run on startup to verify whether this service is up or not on the local host, and will provide a prompt if the host's MySQL service is not running, as shown in the following example for an Ubuntu operating system ➔



```
[sudo] password for saintadmin:
SAINT8 starting up.

Checking for updates....Could not connect to the MySQL server.
Attempt to start MySQL on the local host and re-try? [Y/n]:
```

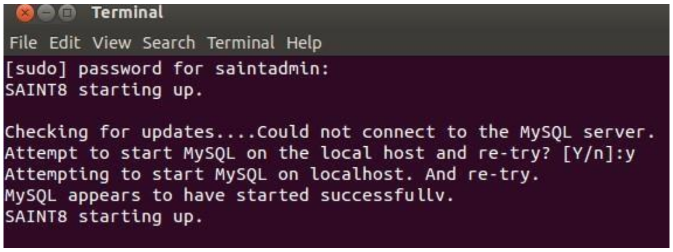
If you are using the standard setup with the database on the same host as the software, you should enter "y" at the prompt to start the service.



```
[sudo] password for saintadmin:
SAINT8 starting up.

Checking for updates....Could not connect to the MySQL server.
Attempt to start MySQL on the local host and re-try? [Y/n]:y
```

Successful startup of the MySQL service ➔



```
[sudo] password for saintadmin:
SAINT8 starting up.

Checking for updates....Could not connect to the MySQL server.
Attempt to start MySQL on the local host and re-try? [Y/n]:y
Attempting to start MySQL on localhost. And re-try.
MySQL appears to have started successfully.
SAINT8 starting up.
```

Enter "n" if SAINT Security Suite is using a database on a separate host. In that case, the startup process will not perform this check, and responsibility for ensuring the external database is running will be that of a local SAINT administrator.

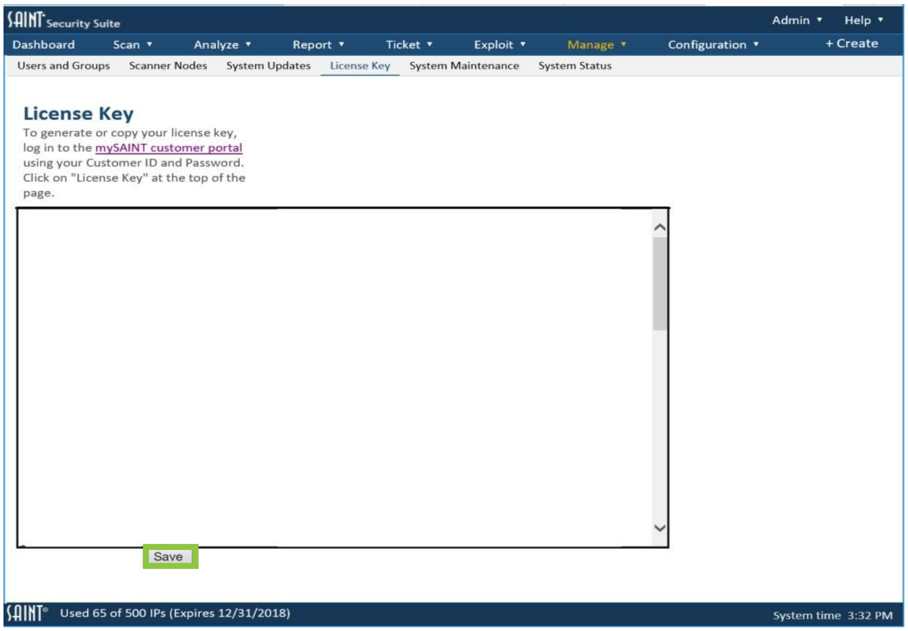
5. Log In

Accepting the EULA will load Security Suite into a browser window and provide a login dialog. Each account owner is provided access to the administrative credentials to support first login and performing administrative functions such as creating user accounts and setting up permissions. Log in with the default administrator account on first login, to set up your product, or use a custom user account provided by your administrator.

Note: *The default administrative user account is "admin." The default password for this account can be found on the downloads page, after you accept the license agreement.*

6. Apply License Key

All SAINT products and deployment options require you to configure your license key, based on the type of license you have purchased. On startup, SAINT Security Suite verifies your current license key and takes you to the License Key page if no key has been configured.



License Key

To generate or copy your license key, log in to the mySAINT customer portal using your Customer ID and Password. Click on "License Key" at the top of the page.

Used 65 of 500 IPs (Expires 12/31/2018)

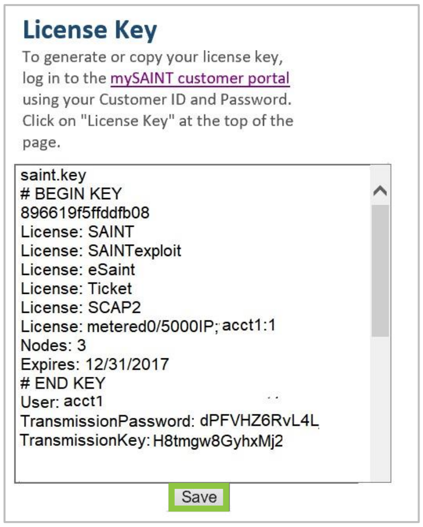
System time 3:32 PM

Configure SAINT Key

1. Click on the link for https://my.saintcorporation.com.

   Open a second browser tab and login in to the *mySAINT* customer portal at https://www.saintcorporation.com/cgi-bin/secure/customer/logon.pl to generate your license key. Use the account name and password you received in the Welcome email that included your license and account information. Note: Click on ***Forgot your Password?*** link on the login page if you don't know your password. This link will auto-generate a new password. You will be prompted to generate a new key.
2. Click the License Key link at the top of the page.
3. Generate a Key.
4. Copy/paste the entire key content (including Transmission Key and Password) from the *mySAINT* portal page into the ***License Key*** window, as shown to the right ➔

   Note: Command line users may also place the content into a file in their saint directory and name it "saint.key."
5. Click ***Save***.



License Key

To generate or copy your license key, log in to the mySAINT customer portal using your Customer ID and Password. Click on "License Key" at the top of the page.

```
saint.key
# BEGIN KEY
896619f5ffddfb08
License: SAINT
License: SAINTexploit
License: eSaint
License: Ticket
License: SCAP2
License: metered0/5000IP; acct1:1
Nodes: 3
Expires: 12/31/2017
# END KEY
User: acct1
TransmissionPassword: dPFVHZ6RvL4L
TransmissionKey: H8tmgw8GyhxMj2
```

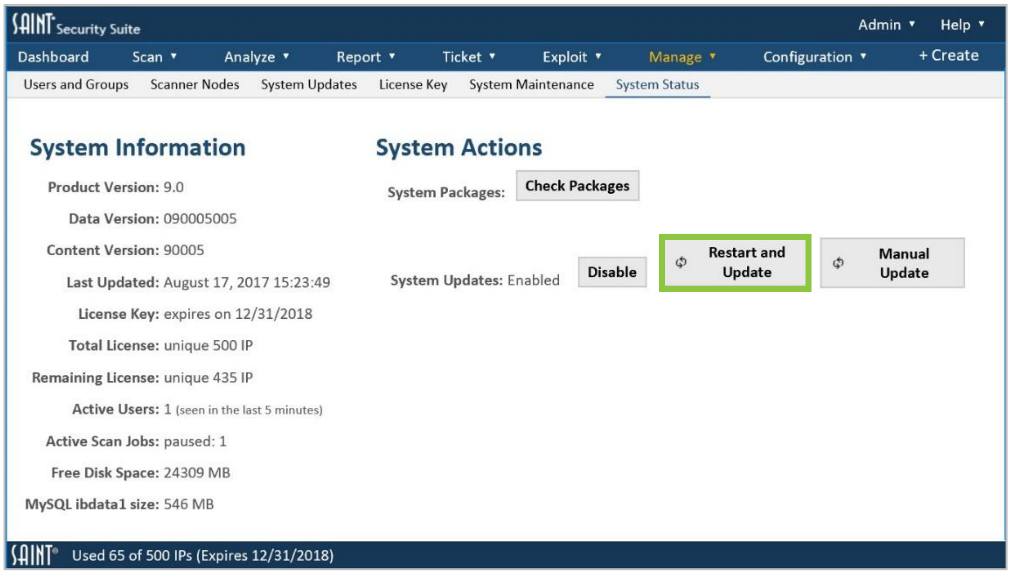
7. Update SAINT Security Suite and Configure System Updates.

The first time you install a key (including the username, transmission password, and transmission key at the bottom) via the *License Key* page, the process automatically configures the update scripts (aka “SAINTexpress”) with the user and transmission information. If you later change your username (e.g., when upgrading from an evaluation license to a purchased license). Or if your network environment includes a proxy, you need to enter that information in this form.

This page also provides a checkbox to temporarily disable the automatic update process (uncheck ***Enable SAINTexpress***) to prevent automatic update of your installation when SAINT restarts. This option may be preferable to comply with local change management policies or if you are in a closed network environment and must manage updates without an Internet connection.

Get the Latest Updates

The last step is to ensure you have all of the latest vulnerability checks, exploits, tutorial content, bug fixes, and feature updates.



System Information

Product Version: 9.0
Data Version: 090005005
Content Version: 90005
Last Updated: August 17, 2017 15:23:49
License Key: expires on 12/31/2018
Total License: unique 500 IP
Remaining License: unique 435 IP
Active Users: 1 (seen in the last 5 minutes)
Active Scan Jobs: paused: 1
Free Disk Space: 24309 MB
MySQL ibdata1 size: 546 MB

System Actions

System Packages:
System Updates: Enabled

SAINT® Used 65 of 500 IPs (Expires 12/31/2018)

1. Navigate to the ***Manage*** menu’s ***System Updates*** page, and click the ***Restart and Update*** button. SAINT Security Suite will connect to SAINT’s update server, pull the latest updates and publish them to your new installation. The System Update status will always be displayed in the ***System Status*** page.
2. The update process will be completed once you see the ***Restart*** dialog and a status of ***Restarted***.
3. Close this window and navigate to the ***Scan*** tab to set up your first scan job.

8. Run Your First Scan.

Whether you are new to SAINT Security Suite or you’re an existing customer who has used other products or editions, we are confident that the many new features and enhancements to previous versions will provide value to your orgzanization. **Note: We offer a free, no obligations, first scan results review with any new install. Call us at 1.301.656.0521 or 1.800.596.2006 or email us at be.secure@carsoninc.com and we will help you explore the power of SAINT.**

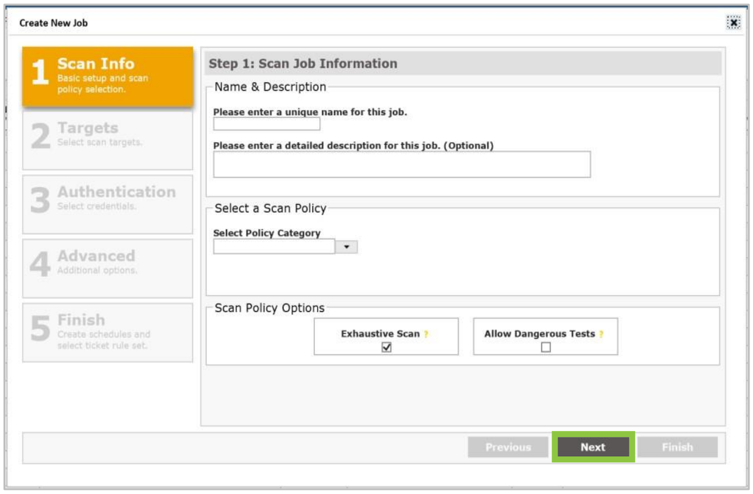
The following is a quick exercise to get you started with your first scan:

1. Click on the ***Scan*** menu.
2. The first time you access the system, SAINT Security Suite will prompt you that there are no scan jobs in the system by displaying ***Would you like to create one?***

3. Click that hyperlink to launch the ***Scan Job set up Wizard***, and it will walk you through the process of setting up your first job. In the following example, we will set up a Job, using only the minimum required steps, and then run your first scan for the new Job. Refer to the Scan section of the User Guide for more information on all of the available options for running various types of scans.

Step 1: Scan Info

- Enter a ***Name*** for your scan Job. Optional: ***Description*** – enter a short description to assist in identifying the scan Job at a later time.
- Scan Policy –SAINT provides many pre-defined scan policies that are based on various types of vulnerability, content, and configuration assessment needs from general vulnerability scanning to specially configured scans tailored for various industry compliance controls. For this scan, select the ***Vulnerability*** Policy Category. Next, select a specific ***Policy***. For this example, select a ***Full Vulnerability*** scan.
- Click the ***Next*** button to move to the next step.


Create New Job

Step 1: Scan Job Information

Name & Description

Please enter a unique name for this job.

Please enter a detailed description for this job. (Optional)

Select a Scan Policy

Select Policy Category

Scan Policy Options

Exhaustive Scan ☑

Allow Dangerous Tests □

Step 2: Targets

- Enter the address(es) of the target(s) to be scanned. This can be individual IP addresses, Subnets, CIDR for IPv4 or IPv6 addresses, or domain names. This can be done through a comma-delimited list in the ***Enter target(s)*** field, or you can use the ***Free Form*** target entry option.

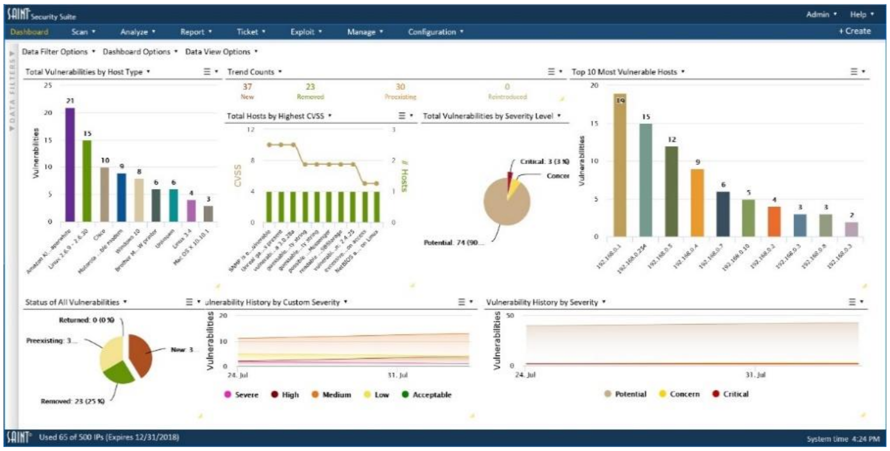
Steps 3 & 4. In this quick scan, we will skip optional steps 3 and 4.

Click the ***Finish*** button. Choose ***Yes*** at the prompt to schedule the job.

Step 5: Review, Schedule and Finish

This step shows you a summary of the Job's setup and provides features to define when to run the job. Jobs can be run at a predetermined date/time or even as a recurring job. In this example, choose to run the job ***Immediately***. Click ***Finish***.

- Click on the ***Scan*** menu to see your new job running in the Scan status grid:
- Once the Scan is complete, you can use the various product features to view strategic graphs in the ***Dashboard*** page (shown to the right), perform detailed analysis on ***Analyze*** pages, and create reports from pre-defined or customized reports.


SAINT Security Suite
Admin
Help
Dashboard
Scan
Analyze
Report
Ticket
Exploit
Manage
Configuration
+ Create
Data Filter Options
Dashboard Options
Data View Options
Total Vulnerabilities by Host Type
Vulnerabilities
21
15
10
9
8
6
6
4
3
Amazon Ki... appwhite
Linux 2.6.9 - 2.6.30
Cisco
Motorola ...ble modem
Windows 10
Brother M...W printer
Unknown
Linux 3.4
Mac OS X 10.10.1
Trend Counts
37 New
23 Removed
30 Preexisting
0 Reintroduced
Total Hosts by Highest CVSS
CVSS
# Hosts
Total Vulnerabilities by Severity Level
Critical: 3 (3 %)
Concer
Potential: 74 (90...
Top 10 Most Vulnerable Hosts
Vulnerabilities
19
15
12
9
6
5
4
3
3
2
192.168.0.1
192.168.0.254
192.168.0.5
192.168.0.4
192.168.0.7
192.168.0.10
192.168.0.2
192.168.0.3
192.168.0.8
192.168.0.3
Status of All Vulnerabilities
Returned: 0 (0 %)
Preexisting: 3...
New: 3...
Removed: 23 (25 %)
...ulnerability History by Custom Severity
Vulnerabilities
24. Jul
31. Jul
Severe
High
Medium
Low
Acceptable
Vulnerability History by Severity
Vulnerabilities
24. Jul
31. Jul
Potential
Concern
Critical
Used 65 of 500 IPs (Expires 12/31/2018)
System time 4:24 PM