SAINT®

SAINT 8 Security Suite

Ubuntu Operating System

Installation Guide

Table of Contents

Introduction

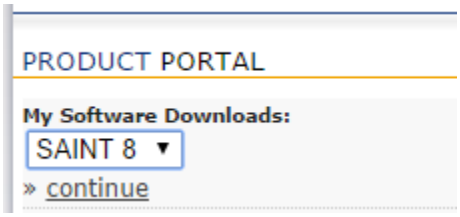
By now, you have received a notification from SAINT Corporation that you have access to SAINT 8. The information contained in the email message will get you started with locating the download site. It also included instructions for installing or setting up SAINT 8 from the bundled virtual machine. The following information is provided to help you –

- Set up SAINT 8 from the installer
- Accept the license agreement
- Configure your key
- Set up the SAINTexpress® update process
- Run your first scan

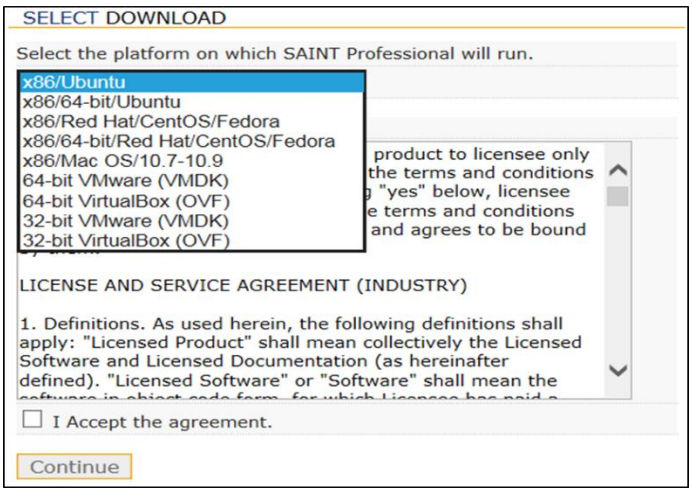
We are always working on new SAINT 8 help content via the Support Portal's knowledge-base and our subscriber-based YouTube content:
http://www.youtube.com/user/saintexploit?feature=watch
Check those sites frequently for more information.

Accepting License and Download SAINT

SAINT software is made available to you via the *mySAINT* customer portal, which can be accessed by logging in at http://www.saintcorporation.com, using your SAINT customer account credentials. Once you've logged into the *mySAINT* portal, you will see the SAINT software listed in the PRODUCT PORTAL download section that you are licensed for, as shown below.

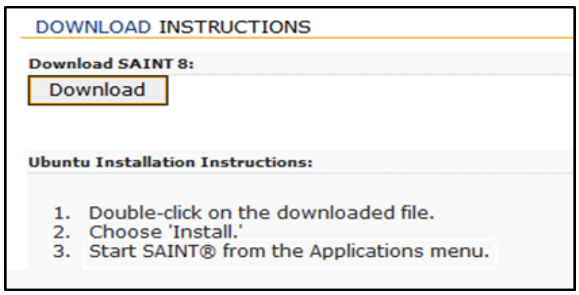


1. Click *continue* once the applicable software product is selected or is already visible.
2. Select the deployment option of the product to be downloaded. In this example, we will download the 32-bit version for the Ubuntu platform. The package downloaded must be compatible with the OS you will be using.

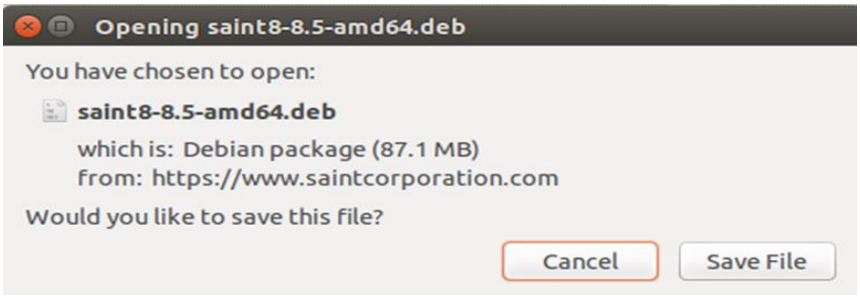


1. Read the Customer License Agreement and click the *I Accept the agreement* checkbox.
2. Click the *Continue* button to access the *downloads* page.

The DOWNLOAD INSTRUCTIONS page will provide a *Download* button for launching the process and downloading the software to a specified destination. This page also provides additional help instructions, applicable to the deployment option and product being downloaded.



Click the *Download* button to start the download process. You will be prompted to Save the File, as show in the Firefox example below:



Save the file in a location that can be located from your target SAINT host.

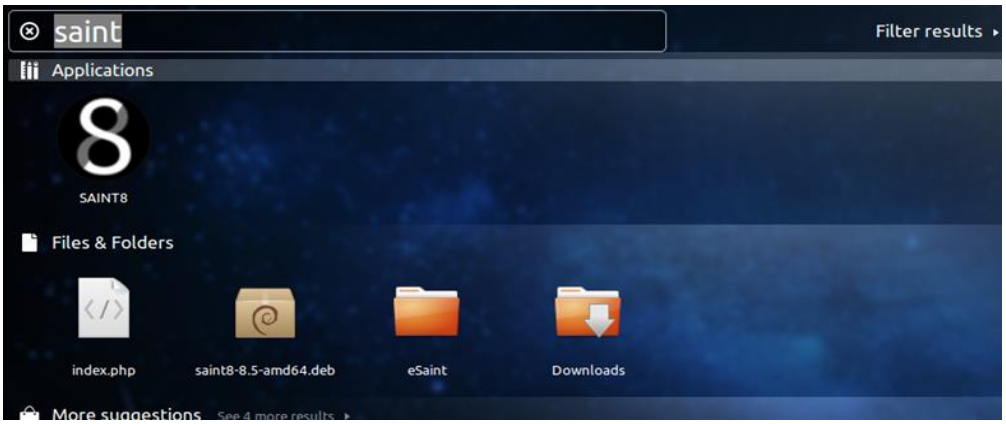
Installation

If this is a fresh Ubuntu installation or one that has not been updated recently, it is recommended that you verify your target host is up-to-date with the latest patches. This can include running the `sudo apt-get update && apt-get upgrade` command in a terminal window, to update any packages/dependencies on the host prior to installing the SAINT 8 Security Suite.

The following describes how to install SAINT from either a graphic user interface or from the command line.

Graphic User Interface (GUI) Install

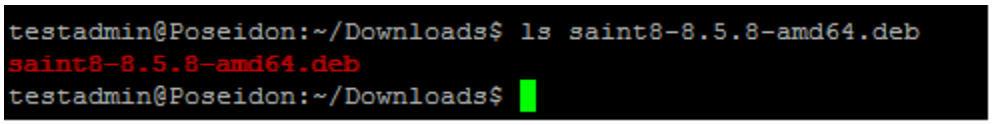
1. Double-click on the file SAINT 8-8.x.x-i386.deb (32-bit) or SAINT 8-x-x-amd64.deb (64-bit), where x.x is the version you downloaded.
2. Choose *Install*.
3. At the Authenticate prompt, enter the Password for the user with administrative privileges on the machine, then click *OK*. The installer will continue applying/installing the software and dependent packages. This process will take several minutes.
4. Next, launch the SAINT Security Suite from the icon in the Applications menu to continue the setup. This process will include setting up and configuring a database, choosing the way the application starts, and logging into the application for the first time. Refer to the Starting SAINT 8 section for help and instructions on the startup process.



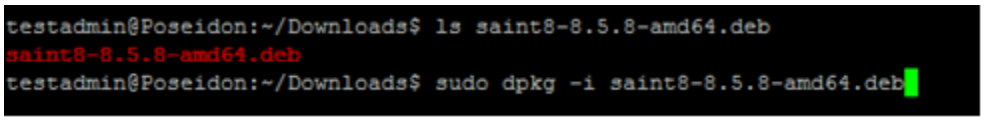
In some instances, such as on the standard installation of Ubuntu 14.04 LTS 64-bit, running the Unity desktop, the SAINT 8 startup icon may not appear in the Applications menu or side bar. If this occurs, you can search for "saint" from the Search icon in the side bar or menu and find the SAINT 8 application, as shown below. You can then add the SAINT 8 startup icon to the Application menu or, in this example, the side bar by dragging the SAINT 8 icon to the side bar. Or, right click on the startup icon and select *Launch* to start.

Command Line Interface (CLI) Install

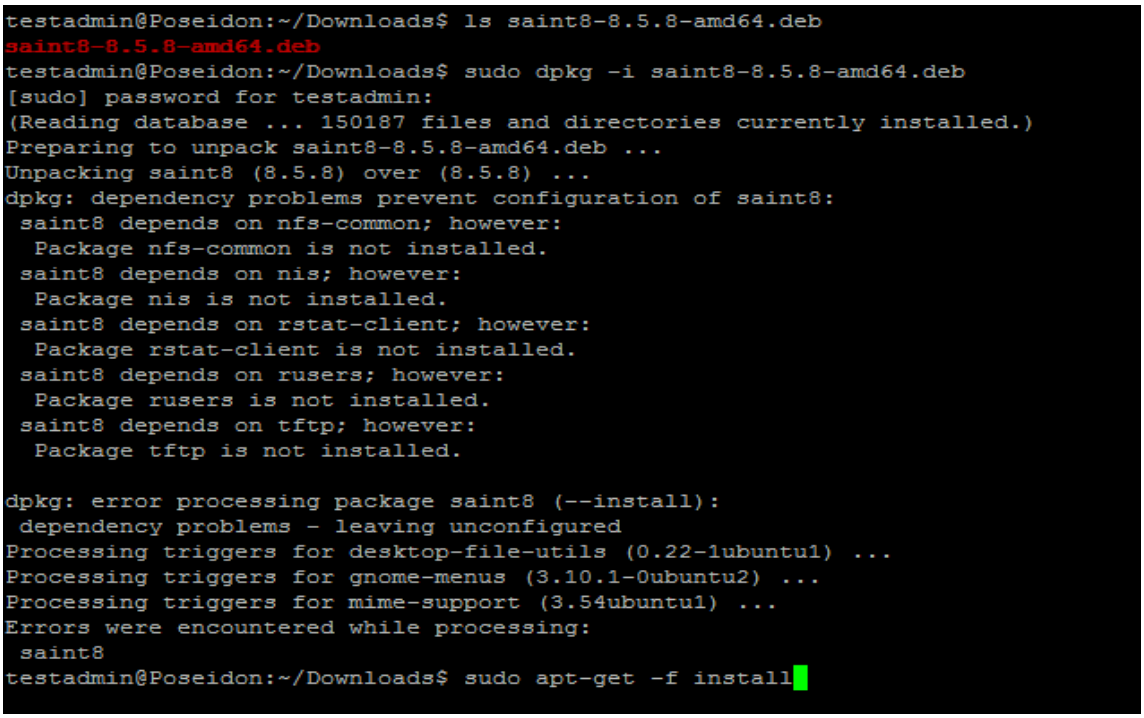
1. Navigate to the Directory where the SAINT 8 package is located. The following example uses the Download Directory.



2. *Enter* the following command to open the debian package.
   `<Download dir> $ sudo dpkg –i SAINT 8.8.x.x.deb`



3. Enter the following command if you encounter package/dependencies error(s):
   `<Download Dir> $ sudo apt-get f install`



4. If no errors are found, continue to the next step by entering *yes* to continue.
5. Select the NIS domain. The default Domain is pre-selected
6. Navigate to the SAINT directory:
   `$ cd /usr/share/saint`
7. Enter the following command from the saint directory:
   `$ sudo ./bin/startmenu8`

```
testadmin@Poseidon:~/Downloads$ cd /usr/share/saint/
testadmin@Poseidon:/usr/share/saint$ sudo ./bin/startmenu8
```

8. The first time you start the application, you will be prompted to install any required packages not found on the host. Enter *y* at the [yes] prompt to continue.
   Note: This list may vary depending on your host machine's current configuration.

```
        php5-cgi
        samba
        libnet-write-perl
        php5-curl
        fastjar
        python-dev

Install the above packages? [yes]
```

9. The installer will gather all of the applicable file information, as well as the amount of disk space required for the required packages**.** Enter *y* at the [y/n] prompt to accept and continue to installation.

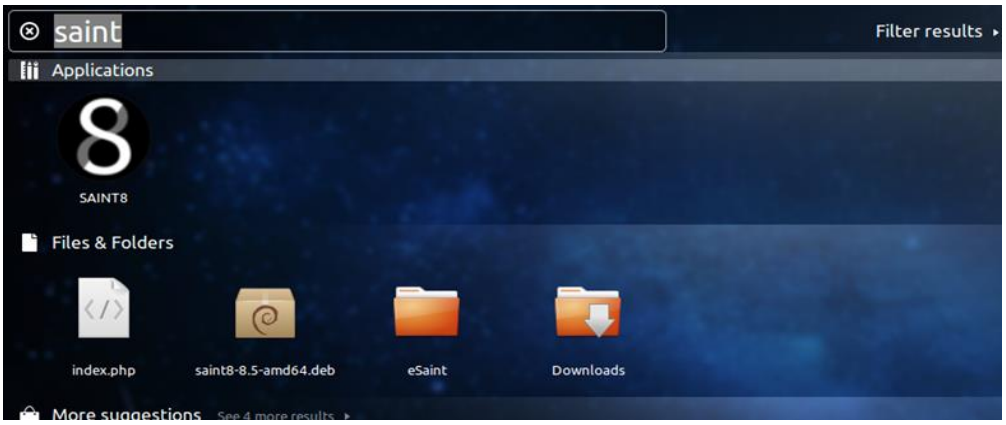
```
The following packages will be upgraded:
  libssl1.0.0
1 upgraded, 47 newly installed, 0 to remove and 175 not upgraded.
Need to get 33.2 MB of archives.
After this operation, 83.8 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

10. There may also be an additional step if the target host does not have the required Python dependencies. Enter *y* at the [yes] prompt if the following messages and prompt are displayed.

```
Creating config file /etc/php5/mods-available/ssh2.ini with new version
Setting up php5-json (1.3.2-2build1) ...
php5_invoke: Enable module json for cgi SAPI
Processing triggers for libc-bin (2.19-0ubuntu6.1) ...
Processing triggers for ufw (0.34~rc-0ubuntu2) ...
Processing triggers for ureadahead (0.100.0-16) ...
Checking PERL dependencies...
All recommended PERL modules are installed.
Checking Python dependencies...
The following pip packages are recommended:
        SQLAlchemy
        sqlsoup
        netaddr
        rpyc
        web.py
        cryptography
        simplejson
        configobj
        dict2xml

Install the above pip packages? [yes]
```

11. Install the required PIP packages by entering *y*, which will then take you to the next stage of the install process.
12. Next, launch the SAINT Security Suite from the icon in the Applications menu to continue the setup. This process will include setting up and configuring a database, choosing the way the application starts, and logging into the application for the first time. Refer to the Starting SAINT 8 section for help and instructions on the startup process.

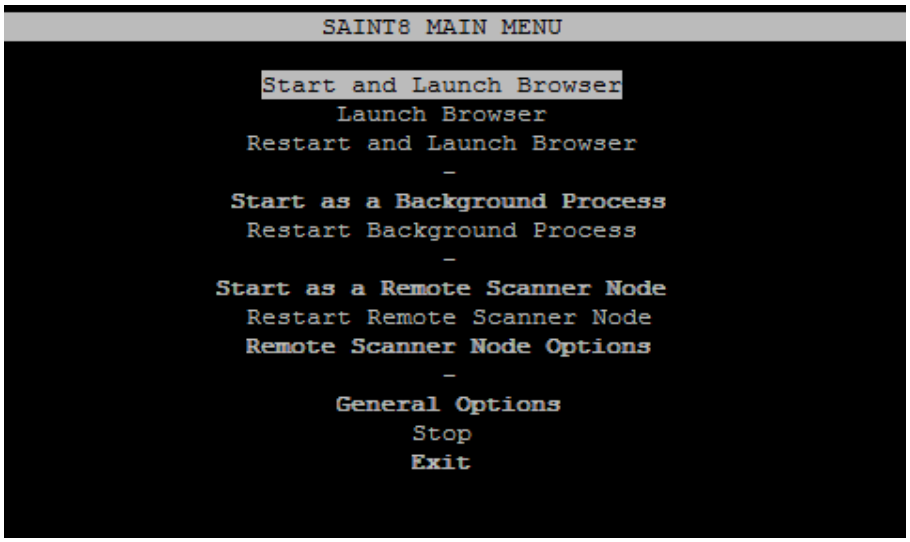


In some instances, such as on the standard installation of Ubuntu 14.04 LTS 64-bit, running the Unity desktop, the SAINT 8 startup icon may not appear in the Applications menu or side bar. If this occurs, you can search for "saint" from the Search icon in the side bar or menu and find the SAINT 8 application. You can then add the SAINT 8 startup icon to the Application menu or the side bar by dragging the SAINT 8 icon to the side bar. Or, right click on the startup icon and select *Launch* to start.

Starting SAINT 8

Starting the SAINT 8 Security Suite software first requires you to login with administrative privileges. This is similar to the way Windows and other modern operating system validate your credentials and permission to install and run applications on the host.

Once your credentials have been validated, the startup process will launch the SAINT8 MAIN MENU that displays the various configuration and startup options for the SAINT software.



An installation can be configured one of three ways:

1. **Standalone Installation** – this installation is typical of most installations, and is typically run with the *Start and Launch Browser* option.
2. **Remote access** – this installation will enable you to run the application on the host without launching the browser, and is initiated by selecting the *Start as a Background Process* option. This is typically selected if you plan to run SAINT on a shared host, and connect to it from another host.
3. **Remote Scanner Node** – this option configures the host installation to act only as a scanning "engine" – requiring a connection back to another SAINT installation acting as a "manager" for user interaction and managing scans against the installed scanner.

You must select the option that describes how you want the software to be started. Your selection here will be stored and used on subsequent startup processes. Each option is defined in more detail in the SAINT 8 Main Menu Options section below.

Initial Start Up

The first time you start SAINT from the menu, the start-up process will evaluate the installation settings and the start option selected, and may require additional configuration settings. For example:

- If the installation is a standalone installation or one that will "manage" other remote installations connected as scanner "nodes," the start-up process will include steps to

select your database preference and account settings. Refer to the Database Setup section for instructions on installing and setting up the database for the host installation.

- If this installation is being started as a Remote Scanner Node, then the setup will require configuration of the IP address and connection port to make a secure connection back to the SAINT installation acting as the "manager." Instructions for that setup can be found in the Start as a Remote Scanner Node section.
- If you are licensed for the SCAP Module, this capability requires the Oracle Java Development Kit (JDK) to be installed on the "manager" host. Refer to the Installing JAVA SDK for SCAP Module section for instructions on how to locate and install the JDK.

Once these processes are complete, the startup process will validate the installation and start the SAINT 8 software for the first time. Refer to the Logging In section for instructions on logging into SAINT for the first time.

SAINT 8 Main Menu Options

Start and Launch Browser

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 8 in a browser window.

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.

Start as a Background Process

SAINT 8 can be started to run as a background process, without launching the browser. This is typical of a shared environment where access will be from various desktop browsers or via command line access from remote hosts.

Start as a Background Process – starts all SAINT 8 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.

Note: In some OS, the port will have to be open for connection to be established. By default, SAINT 8 uses port 1414 for the web browser.

Start as a Remote Scanner Node

The third option is to start SAINT 8 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 8 installation acting as the central "manager."

Start as a Remote Scanner Node – starts all SAINT 8 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 and click the *Enter* key on the *Start as a Remote Scanner Node* option
2. Enter the fixed IP address of the SAINT 8 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
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 in the *Manage* Tab – *Manage* Node page through the "manager" installation.

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 in the *Configuration* tab – *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.

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 8 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* tab, *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* tab, *System Options* submenu in the user interface, by the clicking on the *Nodes* tab, Node Password setting. 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 8 VM deployment option is automatically released with all valid dependencies; and all Installer processes automatically perform these operations during installation. However, this step may need to be run manually if there are any issues or problems with the software or modifications to the host environment affecting the product.
- **Back to Main Menu** – This option closes the options menu and returns to the SAINT 8 MAIN MENU.
- **Exit** – Click this option to close the SAINT 8 MAIN MENU.

General Option

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 in the *Configuration* tab 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 8 web server listens on. This configuration setting is also available in the *Configuration* tab 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 8 VM deployment option is automatically released with all valid dependencies; and all Installer processes automatically perform these operations during installation. However, this step may need to be run manually if there are any issues or problems with the software or modifications to the host environment affecting the product.
- **Back to Main Menu** – This option closes the options menu and returns to the SAINT 8 MAIN MENU.
- **Exit** – Click this option to close the SAINT 8 MAIN MENU.

Stop

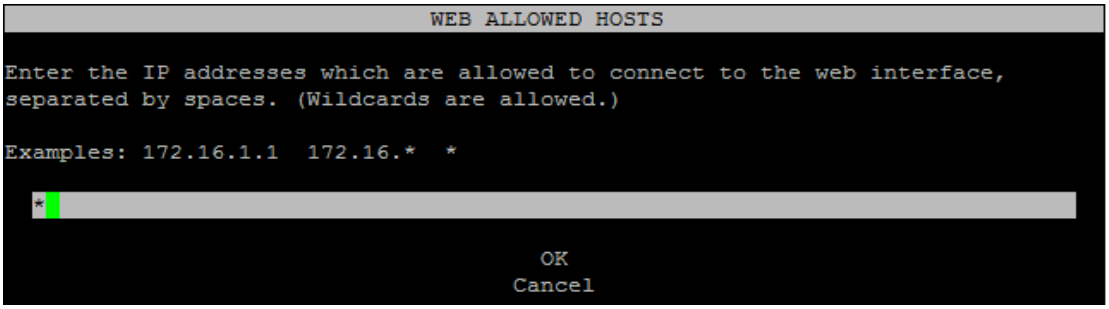
Whether you run SAINT 8 by launching the browser or run strictly in background mode or as a remote mode, the software runs as a background process so scans can continue to be scheduled and executed, even when the browser is closed on the host. This option allows you to manually stop the product, to include any running background processes. This option will be only be available for selection if SAINT 8 is currently running.

Exit

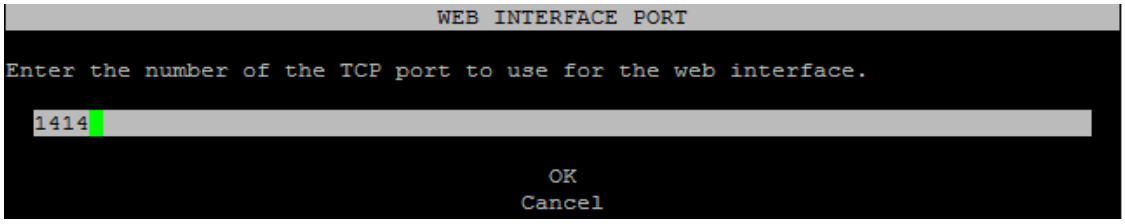
Select this option to quit the startup process and close the startup menu.

What if a service or required configuration setting is not found on startup?

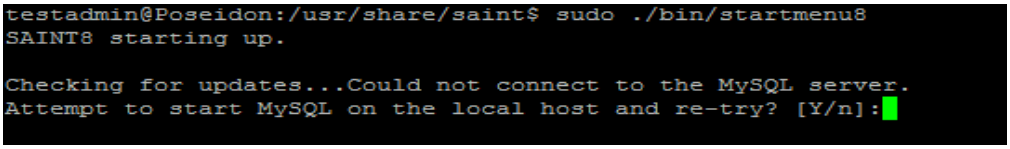
There may be instances during the startup process where a system configuration value or service is not found or should be validated prior to startup. For example, one common configuration setting is related to allowing you control over the hosts that should be allowed to connect to the web-based application. 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.



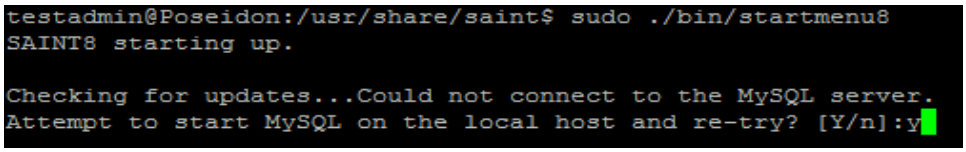
Another possible setting is to define the TCP port to use for allowing the web interface. SAINT uses Port 1414 by default, but this can be changed if local policies dictate. Enter/verify the port number in this field and choose *OK* to continue.



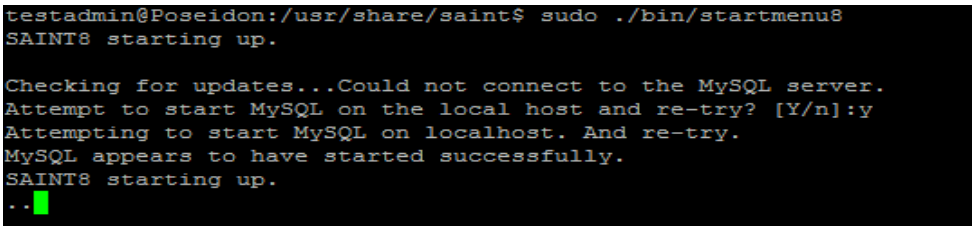
The current installation of SAINT 8 supports either a MySQL or Postgres database backend for application configurations and scan content. In the standard setup, the target database is installed on the same host as the software. In most *nix-based platforms, the database service is started automatically and managed by the SAINT installation and startup processes. However, in some instances (particularly RedHat, CentOS and Fedora) this service may not be started at the same time the OS is launched. SAINT provides a check on startup to verify whether this service is up or not on the local host, and will provide a prompt if the host's database service is not running, as shown in the following example for an Ubuntu operating system running mySQL:



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.



Successful startup of the database service…



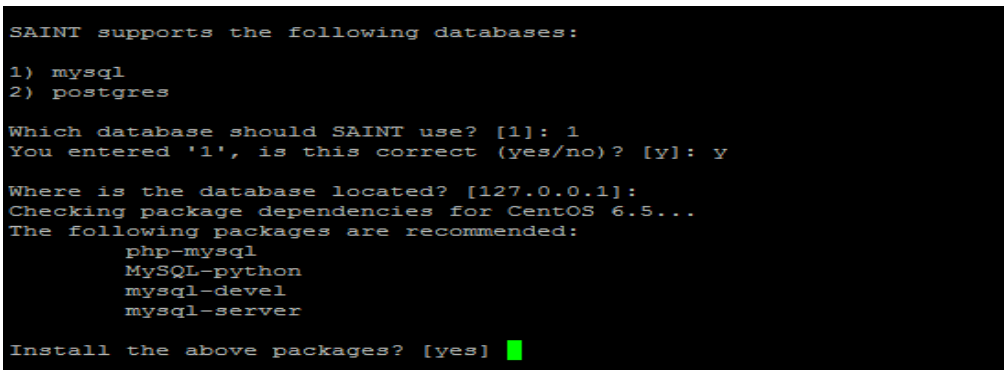
For SAINT installation using an external database
Enter ‘n’ if SAINT 8 is using a database on a separate host. In this configuration, SAINT’s startup process will not perform this check, and responsibility for ensuring the external database is running will be that of a local SAINT administrator.

Database Setup

The SAINT Security Suite architecture requires a database "backend" to support the content, user transactions and scanning processes executed through the browser interface. Follow the instructions provided in this section to select and configure the database platform of choice.

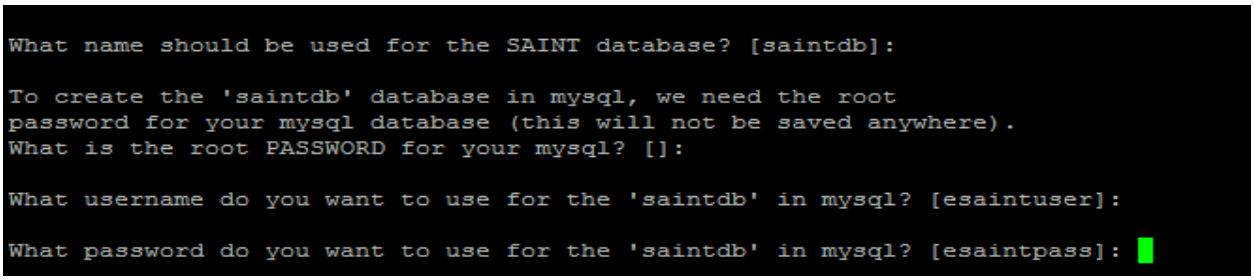
Database Installation and Setup

Once the installation process is complete, the next step is to set up the source database for the SAINT installation. SAINT's Security Suite currently supports either MySQL or PostgreSQL.



1. Select database setup option *1* to use mySQL or *2* for Postgres.
2. Identify the location for the database. The default SAINT configuration is to connect to a local instance of the database, running on the same host as the SAINT installation. However, you may also choose to use a database installed externally to the SAINT 8 host.
    a. **Default Local Database** - If you wish to use the SAINT 8 host, leave the value blank and press the *enter* key to continued.
    b. **Use a Remote Database** - If you wish to use an external database, enter the target host's IP address. Also, refer to the Connect to a Remote Database section for help and an example for connecting a remote database to the SAINT installation.
3. As with the previous package installations, the next prompt validates the packages and the amount of disk space to be used. Enter *y* at the [y/n] prompt to continue with the installation.
4. Give the database a name. The default is **saintdb**. Press the *enter* key to accept this default value.
5. The setup process will prompt you for a password for the database. If you do not have a database installed before installing SAINT 8, press the *enter* key to accept the default password value.
6. Enter the username to be used as the owner of the database. The default value is **esaintuser**. Enter a username or click the *enter* key to accept the default.

    The following example illustrates the setup process, accepting the default values for the database name, root password and user name, as shown in this example for setting up mySQL:



7. Enter the password to be used for the user identified in the previous step. The default value is **esaintpass.** It is recommended that you reset this password to a more secure password and one unique to your environment. In the case of an external database, enter the password for the user for that installation.
8. Click *enter* to continue.

The installation process will perform the applicable connection, creation, setup, content loading and startup for the SAINT 8 database.

Once the database is set up, the launcher will launch SAINT 8 in the local browser on the host. Refer to the steps for Logging In.

Note: On initial login, you will be prompted to change the default password and create a more secure password unique to your installation and accept the End User License Agreement (EULA).

Connect to a Remote Database

Connecting to a Remote MySQL Database

The SAINT Security Suite architecture supports using a remote database rather than a database configured on the same "localhost" as the SAINT software installation. Follow the instructions below to perform the steps required to use a remote mySQL database.

1. The first step is to configure the server that hosts the remote database to allow a remote connection from SAINT. Edit the /etc/my.cnf file and add the following line to the file:

   ```
   bind-address=[DB IP address]
   ```

   The following shows an example for connecting a remote database IP address of 10.0.0.155 from a mySQL database server:

2. Restart the database Server process, as shown in the mySQL example:
   ```
   $ sudo service mysql restart
   ```
   OR
   ```
   $ sudo /etc/init.d/mysqld restart
   ```

3. On the MySQL Shell, grant the necessary privileges to the SAINT DB access. Log in to the MySQL shell with the following command:

   ```
   $ sudo mysql –u root –p (this will prompt you for your
   mysql password).
   ```

4. Enter the following commands to grant access and privileges to the root SAINT machine and SAINT Application database credentials connection:

   ```
   <mysql> GRANT ALL PRIVILEGES ON *.* TO root@'[SAINT Host
   IP]`IDENTIFIED BY '[mysql password]' WITH GRANT OPTION;
   press enter
   <MySQL> GRANT ALL PRIVILEGES ON [saintdb].* TO
   'esaintuser'@[your SAINT host IP]' IDENTIFIED BY
   'esaintpass' WITH GRANT OPTION' press enter
   <mysql> exit
   ```

5. Exit the MySQL shell and restart your MySQL server:

```
$ sudo service mysql restart
     OR
$ sudo /etc/init.d/mysqld restart
```

Note: If you are running IPTABLES, allow the port configured for mySQL. The default mySQL port is 3306.

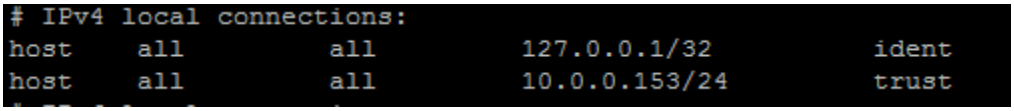
6. Refer to the Database Installation and Setup instructions and follow the steps defined for configuring SAINT to connect and use the external database.

Connecting to a Remote PostgreSQL Database

The SAINT Security Suite architecture supports using a remote database rather than a database configured on the same "localhost" as the SAINT software installation. Following the instructions below to perform the steps required to use a remote PostgreSQL database.

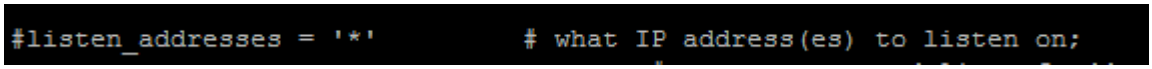
1. On the target PostgreSQL Server, edit the /var/lib/pgsql/data/pg_hba.conf file and add the following line to that file. In this example, the SAINT8 address is 10.0.0.153

```
"host all   all    <SAINT8 host IP Address>/24    trust"
```



2. Next, configure the listen address for the database server. By default, the PostgreSQL listen address is the localhost in the postgresql.conf file. Edit the /var/lib/pgsql/data/postgresql.conf file on the PostgreSQL server, and change the listening address to all, as shown below. **IMPORTANT:** Remember to uncomment the "listen_addresses"

```
listen_addresses = '*'
```



3. Refer to the Database Installation and Setup instructions and follow the steps defined for configuring SAINT to connect and use the external database

Installing JAVA SDK for SCAP Module

The Security Content Automation Protocol (SCAP) is a specification established by the U.S. National Institute of Standards and Technology (NIST) for expressing and manipulating security data in standardized ways. Currently, SCAP can enumerate product names and vulnerabilities (both software flaws and configuration issues); identify the presence of vulnerabilities; and assign severity scores to software flaw vulnerabilities. The SAINT installation, if licensed for the SCAP module, requires the installation of the Java Software Development Kit (SDK) to perform various benchmark assessments defined for that standard. SAINT 8 requires Oracle Java 1.7 JDK or higher to perform these scans. The JDK installer can be downloaded from the Oracle download site: http://www.oracle.com/technetwork/java/javase/downloads/index-jsp-138363.html.

The following instructions describe the JDK installation process to support running SCAP scans in SAINT 8.

Command Line installation

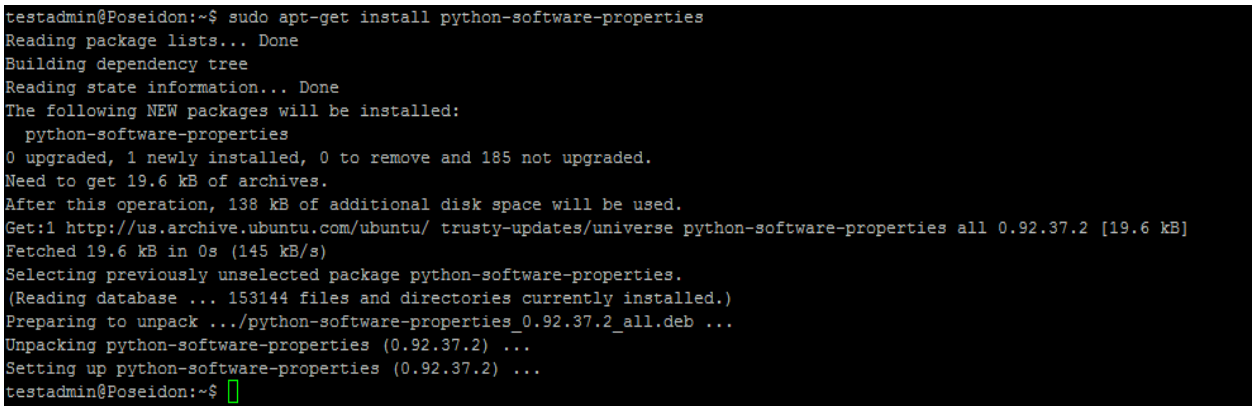
The following describes the Oracle JDK installation process on a 64-bit Ubuntu 14.04 host.

1. Purge any previously installed java JDK and JRE versions installed on the system.

```
$ sudo apt-get purge openjdk-\*
$ sudo apt-get purge openjre-\*
```

2. Install the python-software-properties

```
$ sudo apt-get install python-software-properties
```



3. Install the Java team repository used to install and configure the Oracle JDK.

```
$ sudo add-apt-repository ppa:webupd8team/java
```

4. Press *enter* to continue the process

```
testadmin@Poseidon:~$ cd Downloads/
testadmin@Poseidon:~/Downloads$ sudo add-apt-repository ppa:webupd8team/java
 Oracle Java (JDK) Installer (automatically downloads and installs Oracle JDK6 /

More info:
- for Oracle Java 7: http://www.webupd8.org/2012/01/install-oracle-java-jdk-7-in
- for Oracle Java 8: http://www.webupd8.org/2012/09/install-oracle-java-8-in-ubu

Debian installation instructions: http://www.webupd8.org/2012/06/how-to-install-
 More info: https://launchpad.net/~webupd8team/+archive/ubuntu/java
Press [ENTER] to continue or ctrl-c to cancel adding it
```

5. Run a package/dependencies update

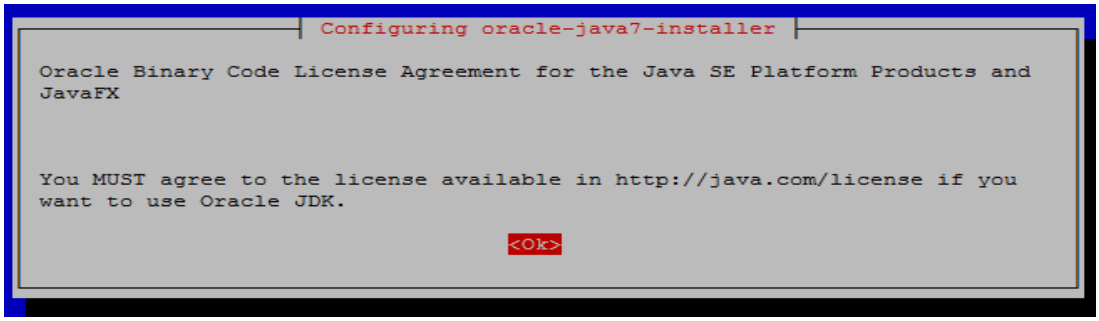
```
$ sudo apt-get update
```

6. Proceed with the Oracle Java JDK installation process

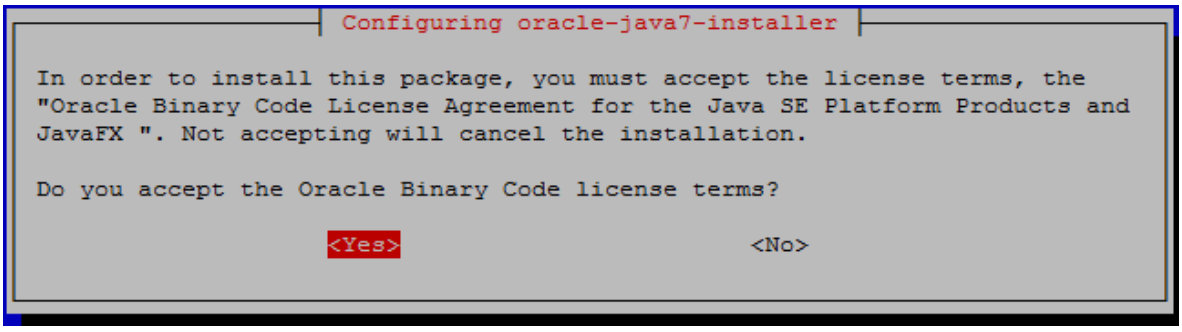
```
$ sudo apt-get install oracle-java7-installer
```

You will be prompted to accept the License Agreement for the JAVA SE Platform and the "Oracle Binary Code License Agreement for the Java SE Platform products and JavaFX"

7. Click <*OK*> to accept the Oracle Java license terms



8. Click <*Yes*> to accept the Oracle Binary Code license terms.



After the install is completed, the output should be as shown below:

```
Oracle JDK 7 installed
update-alternatives: using /usr/lib/jvm/java-7-oracle/jre/lib/amd64/libnpjp2.so to
provide /usr/lib/mozilla/plugins/libjavaplugin.so (mozilla-javaplugin.so) in auto m
ode
Oracle JRE 7 browser plugin installed
```

9. Next, verify the version of the Java installed and running with your system. The displayed version should be the same as the version just installed, as shown in this example.

```
testadmin@Poseidon:~/Downloads$ java -version
java version "1.7.0_72"
Java(TM) SE Runtime Environment (build 1.7.0_72-b14)
Java HotSpot(TM) 64-Bit Server VM (build 24.72-b04, mixed mode)
testadmin@Poseidon:~/Downloads$
```

10. As a best practice, it is recommended that you run the check_deps8 script as a last step, to verify all the packages and dependencies are installed. Run the following command from the following directory:

    /usr/share/saint/ directory

    ```
    $ sudo ./scripts/check_deps8
    ```

The output should be as shown in the following example:

```
testadmin@Poseidon:/usr/share/saint$ sudo ./scripts/check_deps8
[sudo] password for testadmin:
Checking package dependencies for Ubuntu 14.04...
All recommended packages are installed.
Checking PERL dependencies...
All recommended PERL modules are installed.
Checking Python dependencies...
All recommended pip packages are installed.
Reconfiguring...
Checking to make sure all the targets are here...
Trying to find Perl... /usr/bin/perl5.18.2
Changing the source in PERL scripts...
Trying to find Python 2.7 or higher...python
Java Version OK.
Trying to find HTML/WWW browser... /usr/bin/firefox
Looking for UNIX commands...
Can't find xprobe2
Doing substitutions on the shell scripts...
Changing paths in config/paths.pl...
Changing paths in config/paths.sh...
Looking for libssl.../usr/lib64/libssl.so
Looking for libcrypto.../usr/lib64/libcrypto.so
testadmin@Poseidon:/usr/share/saint$
```

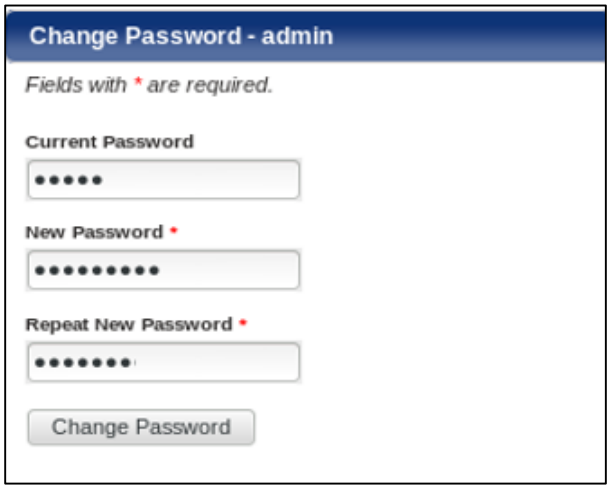
Logging In

Accepting the agreement will load SAINT 8 into the browser window and provide a login dialog (shown below). For those familiar with SAINT Professional, SAINT 8 now includes user access controls formerly only offered in the SAINT Enterprise Edition through the SAINTmanager tool. SAINT 8 now enables all customers to create individual user accounts for all users, and manage role-based security to core functionality and content. Each account owner is provided access to the administrative credentials to support 1st login and perform administrative functions such as creating user accounts and setting up permissions.

The default administrative user account is "admin." The default password for this account is included in the Welcome email that included your customer account information and link to the download site.

1. Enter the default credentials when prompt to login.

2. It will then prompt you to change/create a new unique password for your admin account.



3. Proceed with the acceptance of the License agreement as instructed in the next section.

Accepting the License Agreement

Unlike earlier versions of SAINT, SAINT 8 does launch a Terminal window or require you to read and page through the License Agreement through the terminal. SAINT 8 will launch a browser window and display the License Agreement within the browser.

> *Note: Some versions of Linux may not automatically launch a browser window. If SAINT 8 was installed from a Linux DEB or RPM package and you are launching the system directly from the install host, some installations of Linux may not automatically launch a browser window. If that happens, you can choose SAINT 8 from the Applications menu. (It may appear under a sub-menu such as "Other" in some Linux versions.) Otherwise, if the SAINT 8 installation program created a SAINT 8 icon on your desktop, double-click on the icon. For those using the SAINT 8 VM version, we have also included browser tabs to our public website and technical support portal.*

Please read through the agreement and then accept at the bottom of the page.

Note: The License Agreement will only be displayed and require acceptance during the initial setup and whenever major releases are delivered.

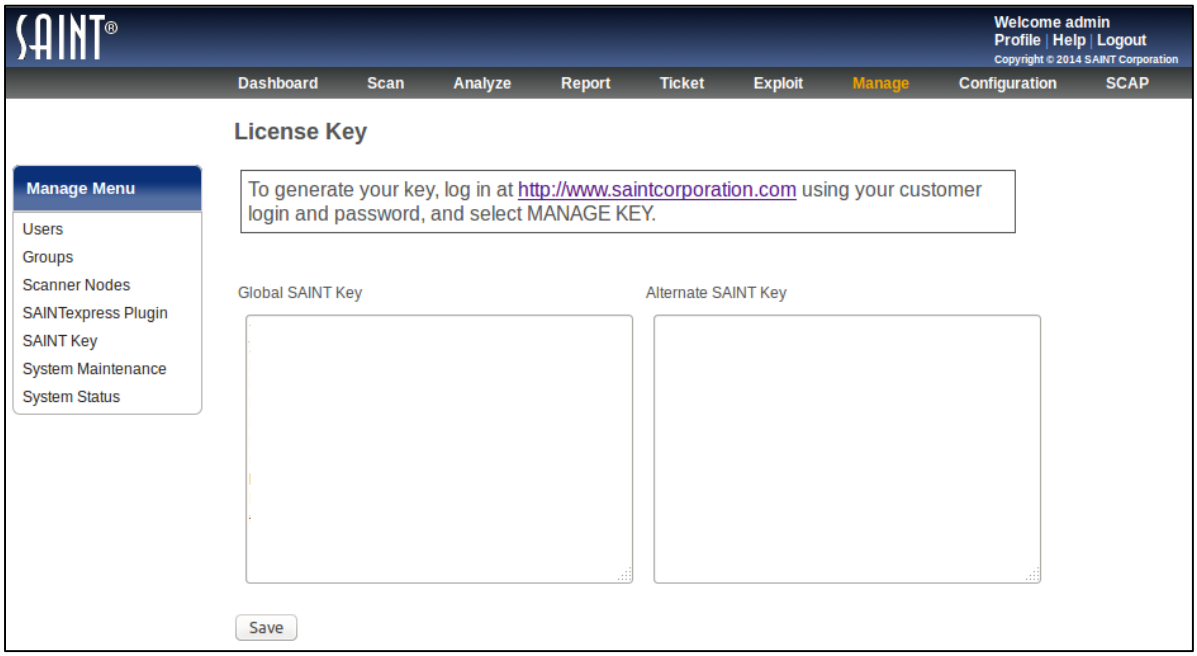
Setup License Key

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 8 verifies your current license key and provides a notification if no key has been configured.

Instructions for setting up your license key are found in the *Administrative Guide* section of the Help documentation (Help hyperlink is in the upper right corner of the *mySAINT* portal), as well as shown below:

Configure SAINT Key

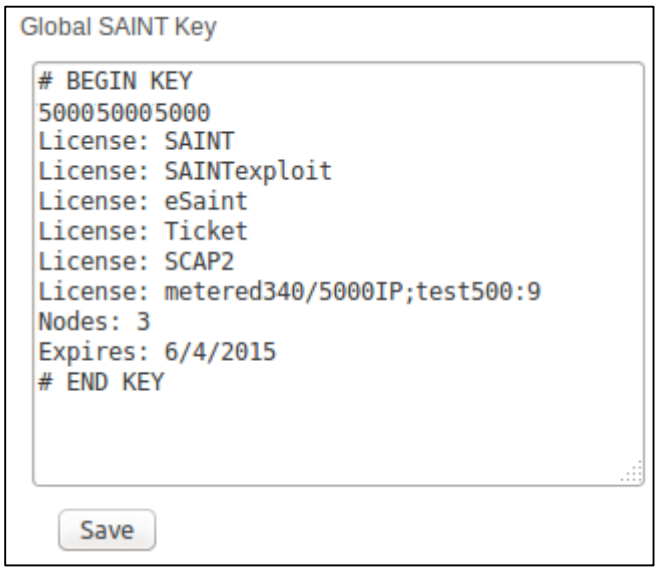
1. The first step is to navigate to the *Manage* tab from the *configure your license key* hyperlink, and then click on the *configure SAINT Key* menu option.



2. Open a second browser tab and login in to the *mySAINT* customer portal (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 the *Forgot your Password?* link on the login page if you don't know your password. This link will auto-generate a new password.

3. You will be prompted to generate a new key.
    a) Click the *View SAINT key* on the left side or click on *Manage Key*.
    b) Generate a Key.
4. Copy/paste the entire SAINT key content (including Transmission Key and Password) from the *mySAINT* portal page into the Configure SAINT Key window in SAINT 8, as shown below:



6. Click *Save*.

Configure SAINTexpress Plug-In

The first time you install a SAINT key (including the user name, transmission password, and transmission key at the bottom) via the *Configure SAINT Key* option, SAINT automatically configures SAINTexpress with the user and transmission information. If you later change your user name (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 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 with SAINTexpress

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

1. Navigate to the *System Status* page, and click the *Restart and Update* button. SAINT 8 will use the SAINTexpress update plug-in to pull the latest updates and publish them to your new installation. The SAINTexpress Status will always be displayed on the *System Status* page, and provides the ability to control whether SAINTexpress obtains product updates, using the *Disable/Enable* button.

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.

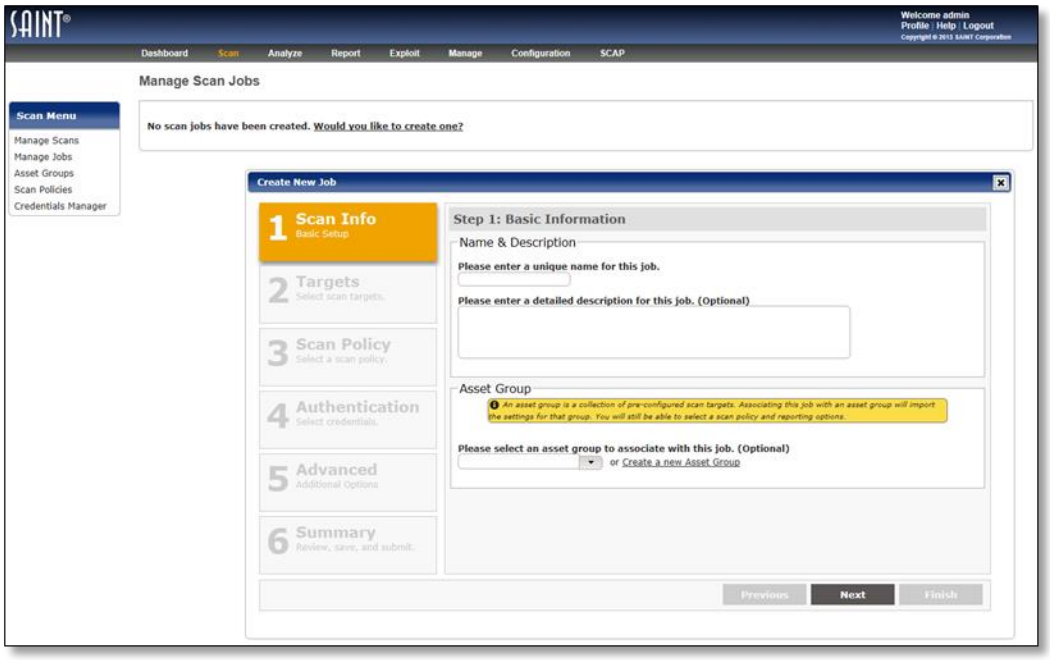
Run your First Scan Job

The following is a quick exercise to get you started with your first scan and to introduce the core features of the new scan wizard:

1. Click on the *Scan* tab.
2. Click on the *Manage Jobs* scan menu option.

   The first time you access the system, SAINT 8 will prompt you that there are no scan jobs in the system: "Would you like to create one?"

3. Click that hyperlink to set up your first job. SAINT will launch the *Scan Job setup Wizard* and 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. 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. Optionally, you can enter a description to assist in identifying the scan Job at a later time. Asset groups are used to create a pre-defined list of common targets (assets). In Job setup, you can choose a pre-defined Asset Group to auto-populate the target list to speed scan setup workflows and make it easier to manage 'like' assets (i.e., by vendor, by function, by subnet, by owner, etc.). We will skip this option for this example.

Step 2: *Targets* – Click *Next* to enter the host targets to be scanned. 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 separated list in the *Enter target(s)* field or you can use the Free Form target entry option.

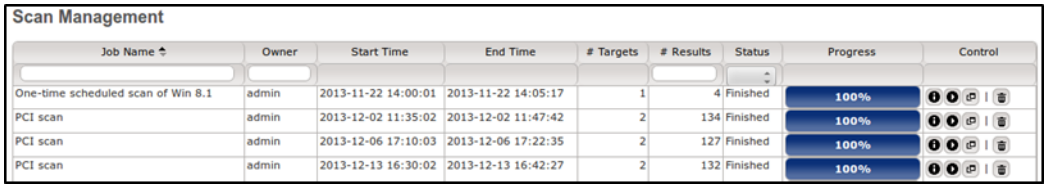
Step 3: *Scan Policy* – Click *Next* to define the type of scan to be executed for the scan Job. SAINT provides many pre-defined scan policies that are based on various types of vulnerability, content, and configuration assessment needs from general vulnerability scanning to specially configured scans tailored for various industry compliance controls. For this scan, select the Vulnerability Policy Category. Next, select a specific policy. For this example, select a Heavy Vulnerability scan. Check the Exhaustive option to configure this policy to enforce more thorough check methods. This type of scan executes all of SAINT's vulnerability checks applicable to the type of target being assessed.

Step 4: *Authentication* – Optional. This step allows you to enter administrative credentials to be used on the target hosts to support deeper scans. This step can be skipped in this example.

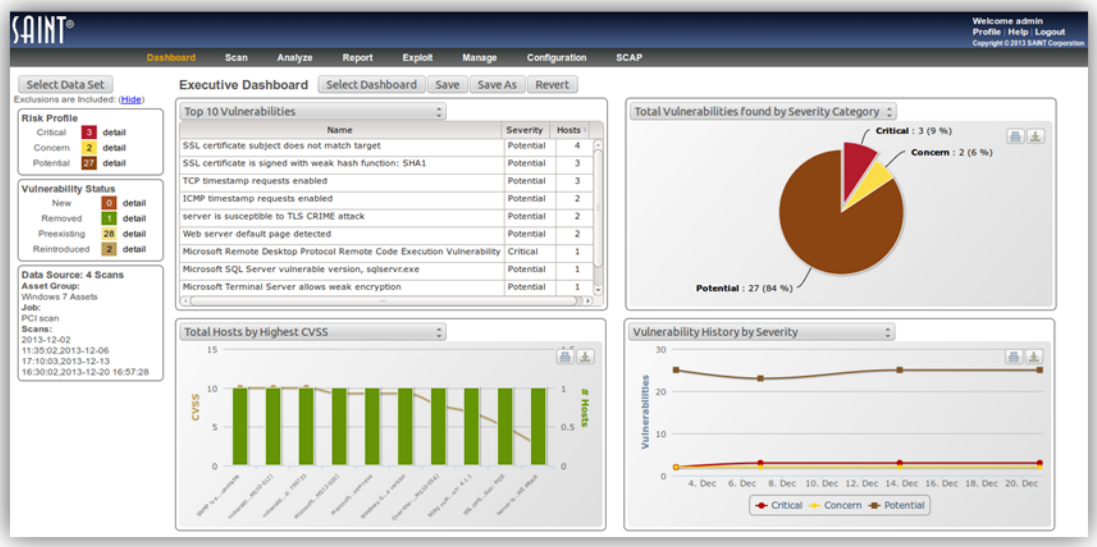
Step 5: *Advanced* – Optional. This step provides access to dozens of advanced configuration options, such as host type fingerprint settings, scan performance, email notifications and report attachments when scans are complete, port settings, anti-virus scan rules, and others. This step can be skipped in this example.

Step 6: *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*.

4. Click on the *Manage Scan* menu option to see your new job running. The Job defines all of the settings required for a scan activity. Scans are individual executions of the Job's instructions. This means that you can create single scans, recurring scans or even "re-scan" the same Job manually whenever you choose, to see results for the defined targets across time, as in the following example of a Job run once and another run three times between Dec. 2 and Dec. 13th.



Once the scan is complete, you can use the various product features to view strategic graphs in the *Dashboard* tab (shown below), perform detailed analysis in the *Analyze* tab, and create reports from pre-defined or customized reports.


SAINT®
Welcome admin
Profile | Help | Logout
Dashboard
Scan
Analyze
Report
Exploit
Manage
Configuration
SCAP
Select Data Set
Exclusions are Included: (Hide)
Risk Profile
Critical 3 detail
Concern 2 detail
Potential 27 detail
Vulnerability Status
New 0 detail
Removed 1 detail
Preexisting 28 detail
Reintroduced 2 detail
Data Source: 4 Scans
Asset Group:
Windows 7 Assets
Job:
PCI scan
Scans:
2013-12-02 11:35:02,2013-12-06 17:10:03,2013-12-13 16:30:02,2013-12-20 16:57:28
Executive Dashboard
Select Dashboard
Save
Save As
Revert
Top 10 Vulnerabilities
Name
Severity
Hosts
SSL certificate subject does not match target
Potential
4
SSL certificate is signed with weak hash function: SHA1
Potential
3
TCP timestamp requests enabled
Potential
3
ICMP timestamp requests enabled
Potential
2
server is susceptible to TLS CRIME attack
Potential
2
Web server default page detected
Potential
2
Microsoft Remote Desktop Protocol Remote Code Execution Vulnerability
Critical
1
Microsoft SQL Server vulnerable version, sqlservr.exe
Potential
1
Microsoft Terminal Server allows weak encryption
Potential
1
Total Vulnerabilities found by Severity Category
Critical : 3 (9 %)
Concern : 2 (6 %)
Potential : 27 (84 %)
Total Hosts by Highest CVSS
CVSS
Hosts
Vulnerability History by Severity
Vulnerabilities
4. Dec
6. Dec
8. Dec
10. Dec
12. Dec
14. Dec
16. Dec
18. Dec
20. Dec
Critical
Concern
Potential