



SAINT[®]



**SAINT v9 Security Suite
User Documentation**

Copyright © 2022 SAINT Corporation. All Rights Reserved

Table of Contents

Welcome to SAINT Help	1
Administrator's Guide	2
System Requirements	2
Getting Started	4
Software Installation	5
Using a SAINT Virtual Machine after Setup.....	5
Starting Security Suite	5
Configure the License Key	13
Configure System Updates	15
System Status.....	16
Running your First Scan.....	17
The SAINT Console	21
View/Delete Scan Status File	21
The Asset Tracker Agent.....	22
User Guide	26
Introduction to SAINT®	26
Start, Login, User Profile	28
Access Controls.....	33
Configuration.....	37
Data Filter Options	115
Grid Actions	125
Using the Results Grids	126
Scan.....	131
Analyze.....	220
Reporting.....	254
Ticket.....	290

Exploit	306
Manage	327
Benchmark Scanning	359
Command-Line Mode	391
Architecture	395
Overview.....	395
Vulnerability Hierarchy.....	398
SAINT Probes	401
Exploit Plugins.....	404
Rule Sets	409
Database Format	419
Database Structure	419
Legacy Database Structure	419
Glossary and Terms.....	427
Asset	427
Asset Tag	427
Asset Identification (AI)	427
Asset Reporting Format (ARF).....	428
CCE™	428
Checks (Vulnerability Check).....	429
Confirmed Vulnerability.....	429
CPE™	429
CVE®	429
CVSS	430
Distributed Node	431
Exploits.....	431
FDCC.....	432
FISMA.....	432

SAINT Security Suite

HIPAA	433
Inferred Vulnerability	433
Job.....	433
Key (SAINT key)	434
Local Node.....	434
mySAINT.....	434
Nodes	434
OVAL®	434
OWASP	435
Pause Window.....	435
PCI.....	435
Policy.....	436
Probes	436
Remote Node	436
SAINT® ASV.....	436
SAINTCloud™	436
SAINTexpress®	437
Scans	437
Scan Window.....	437
Scanner Node	437
SCAP.....	438
STIG.....	439
Target.....	439
Target Group	439
Trust Model for Security Automation Data (TMSAD).....	439
USGCB	440
XCCDF.....	440

Welcome to SAINT Help

SAINT Help includes the following:

- Administrator Guide
- User Guide
- Glossary

For customer technical support, please contact us at <https://support.saintcorporation.com>

For information about your SAINT license and additional details about SAINT content and the latest updates, please log in to your customer portal at <https://my.saintcorporation.com>

We offer free training on SAINT technology and product features. See <https://www.carson-saint.com/about/news/> for more information.

Administrator's Guide

System Requirements

The following describes the major system requirements and key third party software dependencies for setting up a SAINT Security Suite environment.

Note that the setup process will automatically prompt you to resolve any missing prerequisites during the initial setup.

It is also highly recommended that administrators run the *Check Dependencies* option in the Start Menu to verify an environment is configured properly any time there is an issue that hinders the full operation of the product.

Operating Systems

Security Suite can run on most common Linux distributions that meet required dependencies.

The officially supported platforms include:

- Ubuntu 18.04 LTS, 20.04 LTS, or 22.04 LTS
- Amazon Linux 2
- Red Hat 7, 8, or 9
- Debian
- CentOS 7 or 8
- CentOS Stream

RDBMS / SQL Database

The installation process includes the option to select one of the following supported RDBMS platforms.

- MySQL 5.x (or MariaDB*)
- Postgres 9.1 or higher

* MariaDB is a fork of MySQL. If you choose MySQL during setup, SAINT will install and use whichever fork is packaged by the operating system vendor. (Red Hat and CentOS currently package MariaDB instead of MySQL.) It is recommended that you always use the operating system's official packages, to ensure compatibility with Python and PHP modules.

Browsers

- Up-to-date Microsoft Edge
- Mozilla Firefox: v.19.0 or higher
- Up-to-date Google Chrome

Disk Space

1. Security Suite software and system files – 300 MB to download and install
2. Perl and Web browser – approx. 70 MB
3. Database platform
4. Additional storage space required for scan results and reports
5. Optional utilities: See vendor specifications for disk space requirements of individual utilities.

Note: It is not necessary to reinstall any pre-existing utilities installed on the target platform. Both MySQL and OpenSSL are often provided as part of the regular installation package for Linux. The amount of disk space required varies depending on the operating system, the download format, and amount of data being stored in the database.

Memory

Varies depending upon the number of hosts to be scanned, the selected level of multithreading, and other factors. A minimum of 4GB is required—with 8GB RAM recommended for typical installations.. Additional RAM should be considered for optimal performance if there are large-scale scanning requirements.

Oracle Java

Oracle Java 8 is recommended if you are using SAINT for [benchmark scanning](#). On Ubuntu, the *Check Dependencies* option from the start menu will add the Oracle Java Installer PPA from launchpad.net to install and maintain Oracle Java on the system. For other platforms, download and install Oracle Java 8 from www.java.com/download, and ensure that security updates are applied regularly. (*Note:* Although OpenJDK packages may be installed by the *Check Dependencies* option, Oracle Java, not OpenJDK, is recommended for best results from benchmark scans.)

Getting Started

The following describes the routine steps for accessing and downloading licensed software, setting up your license key, and setting up the basic configurations to get started with your first scan.

Accept License and Download Security Suite

There are just a few steps to follow, and then you will be ready to use SAINT capabilities. **To see how easy it is to install the SAINT Security Suite free trial, [watch our installation video](#).**

- 1. Log on at our mySAINT portal at <https://my.saintcorporation.com> with the credentials provided in your welcome e-mail.**

The mySAINT portal is where you:

- maintain your account
- get your license key
- *most importantly*, get instructions and downloads for installing SAINT Security Suite.

- 2. Change your password** (recommended). See the *Change Password link* in the upper-right corner of the portal.

- 3. Optional.** If you are a new user, the mySAINT Assistant automatically opens when you log into the portal. Otherwise, you can open it from the Resources menu. Click on the options in the mySAINT Assistant to be guided to the correct download for your use case. Then follow the installation instructions provided by the Assistant.

If you choose not to use the mySAINT Assistant, continue with the following steps.

- 4. Review the [SAINT Installation Guide](#).**

You can use the link above or navigate to it inside mySAINT: select primary navigation link *Resources*, select *Installation Guides*, and then *SAINT Security Suite Installation Guide*.

- 5. Determine which SAINT Security Suite option you wish to download.** See the Installation Guide, sections 2 and 3. **If you need a virtual machine (VM), install it.** We recommend [VirtualBox](#). See the *Installation Guide, section 3.2*.

- 6. Import the SAINT/Ubuntu open virtual application (OVA) file.** See the *Installation Guide, section 3.4*:

Ubuntu ID: saintadmin

Ubuntu PW: SAINT!!!

7. **Log into SAINT Security Suite** at one of these links:

Username: admin

Password: admin

- <http://127.0.0.1:1414>
- <https://127.0.0.1:1414>

8. **Time to SCAN!**

If you have any problems, call us immediately. We want you to have a great experience!

Software Installation

For all installations, ensure you've validated all requirements specified in the [System Requirements](#) section before continuing. Security Suite can be installed natively on most Linux-based platforms, and as a pre-configured Virtual Machine (VM). Refer to the Installation Quick Start Guide found under Resources – Installation Guides for detailed assistance on supported platforms and installation assistance. Use the SAINT Amazon Machine Image Guide for assistance on setting up a pre-configured AMI on AWS.

Using a SAINT Virtual Machine after Setup

Using a pre-configured Virtual Machine is one of the more common deployments for Security Suite. Once the VM is downloaded to the target location:

1. Run the Virtual Machine from either VMware or Oracle Virtualbox.
2. Log in to the Desktop using the SAINTadmin account and password provided in your Welcome email.

Once you have successfully logged into the VM's desktop, Security Suite can be started and accessed using the same steps as [Starting Security Suite](#) from a native installation.

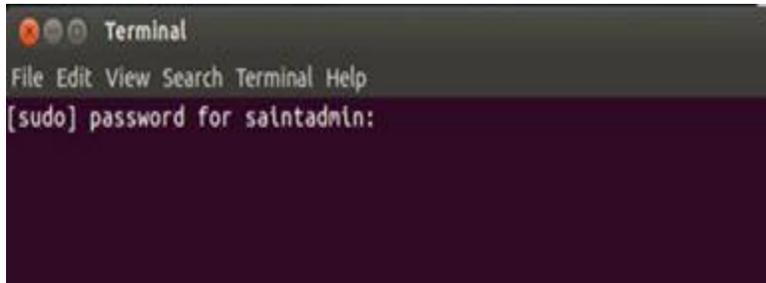
Starting Security Suite

The following describes how to start Security Suite and use the various menu options found during start-up.

Launch Security Suite

The first step is to click on the SAINT icon  or click on SAINT Security Suite from the application menu or desktop hyperlink created during the installation. Starting the Security Suite first requires you to log in with administrative privileges. This is similar to the way Windows and

other modern operating systems validate your credentials and permission to install and run applications on the host. The following example shows logging in from an Ubuntu operating system:



Choose your Start-up Option

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



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, however, in case you wish to restart, stop or change how the software is started.

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 Security Suite in a browser window on the installed host..

Launch Browser – this option will be available if the software has already been started and is still running in the 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 and Run as a Background Process

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 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 operating systems, the port will have to be open for a connection to be established. By default, Security Suite uses port 1414 for the web browser. The default URL for the web interface is: <<https://<address>:1414>>, where <address> is the IP address or registered hostname of the system running the product..

Start and Run as a Remote Scanner Node

The third option is to start 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 installation acting as the central “manager.”

Start as a Remote Scanner Node – starts all 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 and click the *Enter* key on the *Start as a Remote Scanner Node* option
2. Enter the fixed IP address of the 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
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 connected nodes in the *Manage* tab – *Manage Node* page through the “manager” installation.

Note: The Scanner Node Connection Port and Scanner Node Connection String 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 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* tab > *System Options* submenu, by clicking on the *Nodes* tab.
- **Scanner Node Connection String** – The node will send this string to the manager when it connects. This string must match the connection string configured through the *Configuration* > *System Options* > *Nodes* screen in the manager. If this option is left blank in the manager, then no connection string is required.

- **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 Security Suite 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 MAIN MENU.
- **Exit** – Click this option to close the MAIN MENU.

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 for 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 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 > *System Options* submenu, by clicking on the *Web Server* tab.
- **Web Port** – This configuration setting stores the TCP/IP port that the web server listens on. This configuration setting is also available in the *Configuration* tab > *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 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 MAIN MENU.
- **Exit** – Click this option to close the MAIN MENU.

Stop

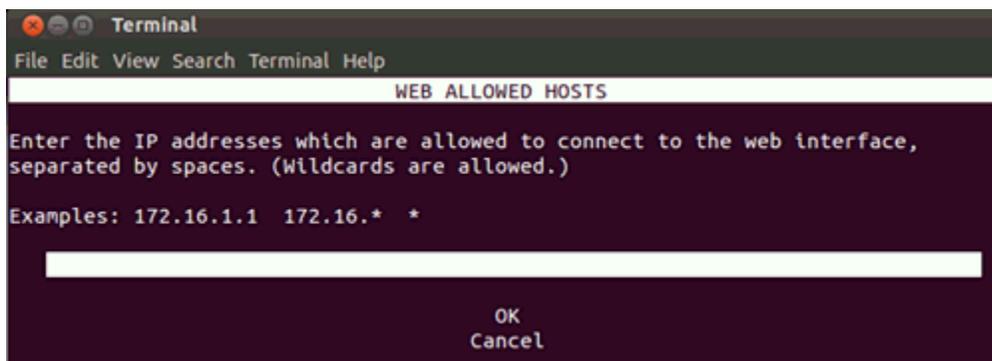
Whether you run Security Suite by launching the browser or run strictly in background mode or as a remote mode, the software runs as a background process so scans can continue to be scheduled and executed, even when the browser is closed on the host. This option allows you to manually stop the product,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

Exit

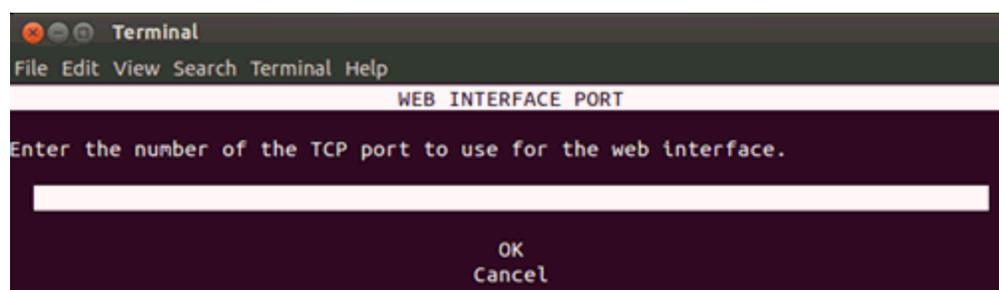
Select this option to quit the startup process and close the startup menu. Use the Up/Down arrow keys to move and Enter key to select.

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.



Database startup for a Security Suite installation using a locally installed database – Security Suite supports either a MySQL or PostgreSQL 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 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. Security Suite 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. If you are using the standard setup, with the database on the same host as the software, you should enter *y* (Yes) at the prompt to start the service.

For an installation using an external database – As described in the installation guide, Security Suite’s architecture also supports the use of a remotely installed database. If this installation connects to a remote database, enter *n* (No) at the database startup message if 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 administrator.

Database credentials -- When the SAINT manager runs for the first time, it creates a database and a database user with the username and password which you provide. In order for the SAINT manager to be able to perform needed functions, it must be able to access the database using these credentials. Therefore, the credentials are stored in the configuration files for both the `saint_manager` daemon (`manager.ini`) and the web application (`main.php`). If you want to encrypt the database password in these files, run the following command on the manager host after the database is initialized: `cd/usr/share/saint; sudo scripts/encrypt_db_pass.py`. This command will encrypt the password in both configuration files using AES-256 encryption. It may result in a slightly slower experience when using the web application.

Accepting the License Agreement

When logging into the product via a browser, Security Suite will launch a browser window and display the End User License Agreement.

The screenshot shows the SAINT Security Suite web interface. The top navigation bar includes 'Dashboard', 'Scan', 'Analyze', 'Report', 'Ticket', 'Exploit', 'Manage', and 'Configuration'. The main content area is titled 'Agreement Required' and contains the following text:

SAINT is willing to license the licensed product to licensee only on the condition that licensee accepts the terms and conditions contained in this agreement. By typing "yes" below, licensee acknowledges that it has read all of the terms and conditions of this agreement, understands them, and agrees to be bound by them.

LICENSE AND SERVICE AGREEMENT (INDUSTRY)

1. Definitions. As used herein, the following definitions shall apply: "Licensed Product" shall mean collectively the Licensed Software and Licensed Documentation (as hereinafter defined). "Licensed Software" or "Software" shall mean the software in object code form, for which Licensee has paid a license fee, all updates and revisions thereto supplied by Licensor during the term hereof, and all permitted copies of the foregoing. "Licensed Documentation" shall mean any documents delivered by Licensor to Licensee that relate to the Licensed Software. "Use" shall mean the reading into and out of memory of the Licensed Software and the execution of such Software.
2. License. Subject to the payment of the license fees and charges to Licensor, Licensor hereby grants to Licensee, and Licensee hereby accepts, a personal, non-exclusive, and non-transferable license (without the rights to sublicense) to use the Licensed Product in accordance with the terms and conditions of this License and Service Agreement. The Licensed Product shall only be used for the number of nodes, networks, or hosts for which Licensee has paid a license fee.
3. License fees and charges, taxes, and payments for services. The license fees and charges for the license herein granted to Licensee shall be the then current license fees and charges of Licensor for the Licensed Product in effect at the time of Licensor's acceptance of this Agreement. Payment for products and services covered in the on-line ordering procedures, are due prior to the release of the Licensed Product or performance of the services. Any license fee, taxes, or other charges for the Licensed Product that is not paid before Licensor provides the Licensed Product shall be paid within thirty days after receipt of such product. Any fee for maintenance and update services, in accordance with Schedule A, that is not paid prior to the beginning of the period of such annual maintenance services shall be paid within thirty days after the beginning of the period of such annual maintenance services. Any additional services that are provided by Licensor to Licensee on a time and materials basis shall be paid within thirty days after receipt of an invoice for such services. If Licensee does not pay all amounts due within the payment periods stated above, Licensor may terminate the Agreement, pursuant to Paragraph 11, and cease performance of any further services.
4. Terms of license agreement and licenses. Unless otherwise terminated or canceled as provided herein, the term hereof and of the licenses granted herein shall commence on the date the Licensee is provided access to the Licensed Software, normally by issuance of a customer ID and password, and shall continue until Licensee discontinues the

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

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

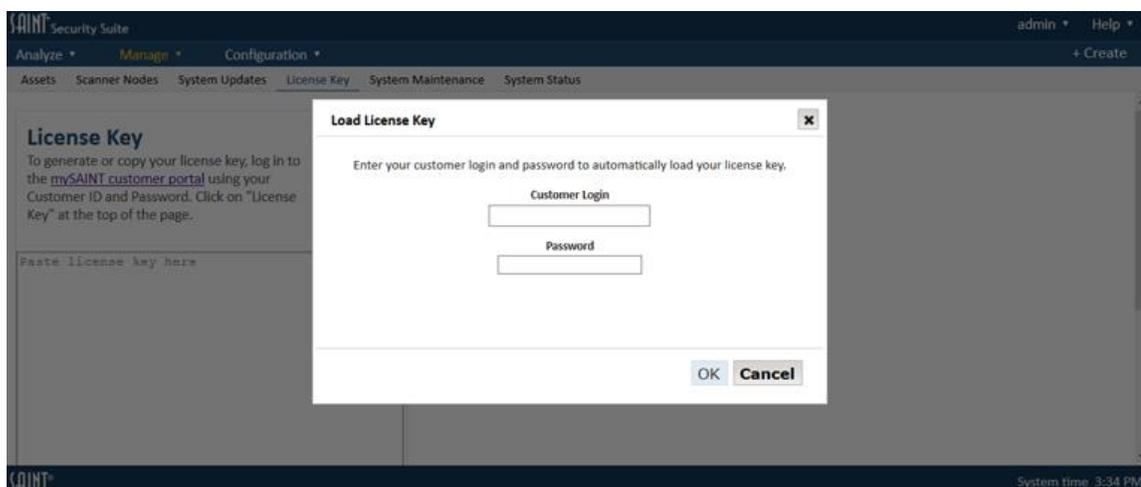
Note: The License Agreement will only be displayed and require acceptance during the initial setup and whenever major releases are delivered.

Logging In

Accepting the agreement will load Security Suite into the browser window and provide a login dialog. Each account owner is provided access to the administrative credentials to support first login and for performing administrative functions such as creating user accounts and setting up permissions. Use this account for your initial login, changing the default administrator password, and establishing your internal user account and access control policies.

Configure the License Key

1. Upon first login, the first step is to configure your license key. If no license key is present, the application will direct you to the License Key page and open a login prompt. Enter your customer login and password to automatically load your license key from the mySAINT server.



Manual License Key Configuration

If you prefer to paste your license key into the application manually, click the *Cancel* button at the login prompt and proceed as follows:

1. To download your key, open a second tab in the browser and return to the *mySAINT* customer portal (<https://my.saintcorporation.com>). Login to the portal with the account name and password you received in your Welcome email message. Note: Click on "Forgot your Password?" link on the login page if you do not know your password. This link will auto-generate a new password.
2. Navigate to the *License Keys* page in the *mySAINT* customer portal.

3. Click on the clipboard icon beside the desired license.
4. Paste the entire SAINT key content (including the SAINTexpress transmission information at the bottom) from the *mySAINT* portal page into text area of the License Key page in the application.

Global 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;User1000:12
Nodes: 3
Expires: 12/31/2017
# END KEY
User: User1000
TransmissionPassword:
dPFVHZ6RvL4Ljeep
TransmissionKey: H8tmgw8GyhxMj2vw
```

Save

Note: For command line users, alternatively, you can also place the content into a file in your saint directory and name it `saint.key`.

5. Click *Save*.

Understanding the Key

There are two types of licenses. The key structure must be consistent with the license type and total usage volume purchased under the current subscription:

- **Unique Target License:** This key is based on a fixed number of static IP-based target addresses. For example, purchase a key that allows you to scan up to 100 unique targets, and scan that number of targets, as many times as you wish over the course of the license period. Target IPs are not added to this count (metered usage) until a target

is discovered live and assessed via a scan policy. Note that once an IP has been counted, it cannot be removed and replaced with another IP. However, you can increase the license size during your license period as demand increases, by contacting your account representative.

- **Metered Scan License:** This key is based on counting the total number of host targets scanned over a license period. For example, scanning 10 hosts weekly over 52 weeks equates to 520 total scans. In this key structure, specific IP addresses, size of the network or dynamic addresses are of no concern because every target assessed in every Job's scan is counted.

Configure System Updates

The first time you install a License key (including the user name, transmission password, and transmission key at the bottom) via the [Configure the License Key](#) option, this process automatically configures the system update process (a.k.a. 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 into this form.

System Updates Configuration

To determine your Transmission Key and Password, log in to the [mySAINT customer portal](#) using your Customer ID and Password. Click on "License Key" at the top of the page, the Transmission Key and Password are located at the bottom of the key. The "User Name" field is the same as your Customer ID.

User Name:

Transmission Password:

Transmission Key:

Proxy variables (leave blank if you don't have a proxy)

Proxy Host Name:

Proxy Port:

Proxy Login:

Proxy Password (leave blank if not required):

Enable SAINTexpress:

Restart and Update

After saving your System Updates Configuration, click the below button to perform a system update.

Manual Update

A manual update file can be obtained from your mySAINT portal under DOWNLOADS - MANUAL UPDATES.

Before proceeding with a manual update, ensure you have configured your Update User Name, Transmission Key and Password, and checked "Enable SAINTexpress."

Note: This feature currently only supports updating the management console and the local scanner node.

Update file:

SAINT Security Suite | Admin | Help | System time 10:42 AM

Dashboard | Scan | Analyze | Report | Ticket | Exploit | Manage | Configuration | System time 10:42 AM

Users and Groups | Scanner Nodes | System Updates | License Key | System Maintenance | System Status |

Used 0 of 5000 IPs (Expires 12/31/2017)

This page also provides a checkbox to enable (by default) or temporarily disable the update process (Uncheck the "Enable SAINTexpress" checkbox) to prevent automatic updates of your installation on 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.

The System Updates page also provides options to perform a manual check for updates via the "Restart and Update" option, as well as perform a "Manual Update" for instances, such as a closed network that cannot conduct automated update processes.

Get the Latest Updates

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

From the System Updates page, click the *Restart and Update* button. Security Suite will use the SAINTexpress update process to pull the latest updates and publish them to your new installation. The System Update Status will always be displayed on this page. This updates the manager and the local node. If your installation includes remote/distributed nodes, restart those nodes from the *Manage Scanner Nodes* page.

Note: Security Suite updates can also be controlled via the Command Line Interface (CLI). You can start Security Suite from the command line with the `-Q` argument. This will start Security Suite and NOT check for updates. This process will only be valid for this run-time instance. It does not control the stored configuration/status of the SAINTexpress System Update plugin.

System Status

The System Status page provides a summary of details for your Security Suite installation. Information, such as product version, date of the last update, license key status, as well as information about current active usage.

Note that the product version information is defined by three (3) values. SAINT's product version is defined as follows:

- **Product Version:** [Major Product Number] [Current Software Update Release Number]. This number is associated with the software updates that package code and scripts related to software features, product functionality, bug fixes and database changes.

Major product versions have historically been introduced every 5-6 years. Software updates to these major releases are typically in quarterly update cycles.

- **Date Version:** This version number is associated with the version of the database, as it relates to the product version. This value assists engineers in researching possible issues whenever there is a problem with your installation.
- **Content Version:** This number sequence corresponds to the current number of content updates for the version of the software. Content updates are typically associated with vulnerability checks, exploit code and remediation Tutorials. Content updates are routinely released twice weekly.

The screenshot displays the SAINT Security Suite interface. At the top, there is a navigation bar with the following menu items: Scan, Analyze, Report, Ticket, Exploit, Manage, Configuration, and + Create. Below this is a secondary navigation bar with links for Users and Groups, Assets, Scanner Nodes, System Updates, License Key, System Maintenance, and System Status. The main content area is split into two columns. The left column, titled 'System Information', lists various system details: Product Version: 9.0, Data Version: 090030005, Content Version: 90030, Last Updated: November 07, 2017 20:15:28, License Key: expires on 9/23/2018, Total License: Static License, Active Users: 2 (seen in the last 5 minutes), Active Scan Jobs: n/a, Free Disk Space: 2907 MB, and Database: MySQL 5.5.34-0ubuntu0.12.04.1-log. At the bottom of this section, it shows 'MySQL ibdata1 size: 13982 MB' with a 'Cleanup' button. The right column, titled 'System Actions', shows 'System Packages: Check Packages', 'System Updates: Enabled', and buttons for 'Disable', 'Restart and Update', and 'Manual Update'. At the bottom of the page, a status bar indicates 'SAINT (Expires 9/23/2018)' and 'System time 10:57 AM'.

Running your First Scan

1. Click on the *Scan Jobs* option under the Scan menu.
2. The first time you access the system, you will be prompted 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

The Scan Job Wizard will be displayed to walk you through the process of setting up your first job. In the following example, we will set up a quick scan, using only the minimum required

steps to 1: give the job a Name, and select the Scan Policy to be used, and 2: enter the host Targets to be scanned; and 3: decide when to schedule your first job. Refer to the [Scan](#) section of the user guide for more details on all of the available options and advanced configurations for running various types of scans.

1. Scan Info.:
 - First, enter a Name for your scan Job.

Optionally, you can enter a description to assist in identifying the scan Job at a later time.

Scan Policy – Select 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, and select a *Full Vulnerability* scan. Leave the *Exhaustive* option checked (shown below) 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.

Create New Job

Step 1: Scan Job Information

1 Scan Info
Basic setup and scan policy selection.

2 Targets
Select scan targets.

3 Authentication
Select credentials.

4 Advanced
Additional options.

5 Finish
Create schedules and select ticket rule set.

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:

Select Policy:

The Heavy/Vulnerability Scan runs all available vulnerability checks against the selected targets.

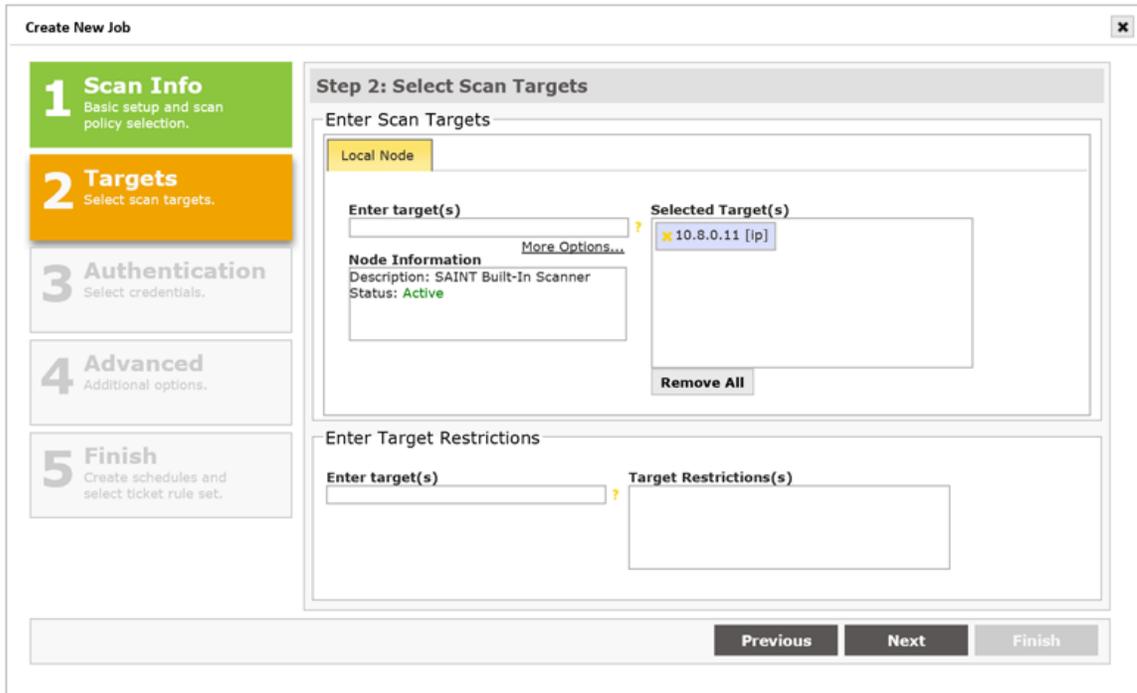
Scan Policy Options

Exhaustive Scan ?

Allow Dangerous Tests ?

Previous Next Finish

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, Subnet, CIDR for IPv4 or IPv6 addresses, or domain names. This can be done through a number of options, to include manual entry, importing target lists, creating and using Target and Asset Groups; as well as connecting to external sources such as Active Directory, Microsoft Azure, and Amazon Web Service (AWS) accounts.



3. Review, Schedule and Finish – There are many other configuration options available for granular control of your scan workflows. These steps are optional and not described in this quick scan example. Click the Finish button to review the Summary information and choose to run the scan “Immediately”.

The screenshot shows a web-based wizard titled "Create New Job" with a close button in the top right corner. On the left side, there is a vertical navigation pane with five steps:

- 1 Scan Info**: Basic setup and scan policy selection.
- 2 Targets**: Select scan targets.
- 3 Authentication**: Select credentials.
- 4 Advanced**: Additional options.
- 5 Finish**: Create schedules and select ticket rule set.

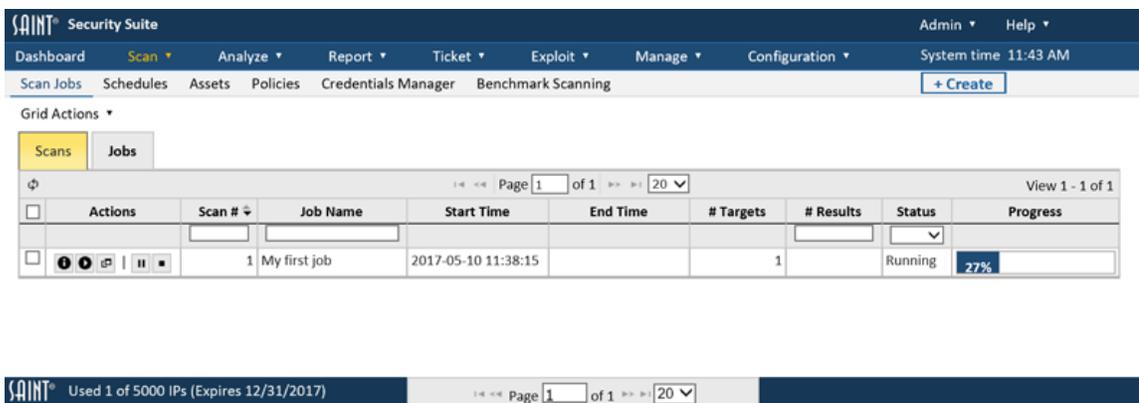
The main content area is titled "Step 5: Schedules and Ticket Rule Set" and is divided into two sections:

- Job Schedule**: Contains a yellow warning bar with the text "You may opt not to create a schedule for this job at this time." Below this, there are two columns. The left column, "Create a new Schedule", has three buttons: "Schedule Immediately" (which is highlighted), "Schedule Once", and "Schedule Recurring". The right column, "Schedule(s)", has a list box containing "Immediate" with a selected state.
- Ticket Rule Set**: Contains a yellow warning bar with the text "You may choose a ticket rule set to apply when this job runs." Below this is a "Select Ticket Rule Set" dropdown menu.

At the bottom of the wizard, there are three buttons: "Previous", "Next", and "Finish".

Click *Finish* in the Summary button once you've chosen when to run the scan. Your scan will now be initiated.

You will now see your new job's scan queued and ready on the *Scan Jobs* page.



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

The SAINT Console

The SAINT console is where SAINT writes its standard output (stdout) and error messages (stderr). By default, the console is the terminal display from which Security Suite was started at the command line. Security Suite can also be run with stdout and stderr redirect to a file on startup (e.g., `./saint... >myoutput 2>&1` sends both stdout and stderr to the file myoutput). Note that SAINTbox appliances also use this technique to write stdout/stderr to a file named saintbox.out.

View/Delete Scan Status File

The scan status file contains time stamped information about scans that have been run, including the session name, the time the scan was started and completed, and the probes which were run. This information can be extremely valuable in reviewing the current progress of a running scan, as well as identifying possible causes of issues identified at the conclusion of a scan.

The Status File scan can be viewed from Security Suite using the following steps:

1. Navigate to the *Scan* grid on the *Scan Jobs* page.
2. Click on the *Details* action button for a scan to be reviewed.
3. Click on the *Execute History* bar to view the scan history and details for each scan.

- Click *View Status File* to display the raw status file content.

The image shows two overlapping windows from a security tool. The top window, titled "Scan Details", displays information for a job named "My first job (SCANID 1)". It includes fields for Job Name, Scan ID, Scan Policy, Start Time, and End Time. Below this is an "Execution History" table with columns for Agent/Node, Start Time, End Time, Status, Status File, Verbose Output, and Results data. The bottom window, titled "Status file", shows a log of scan activities with timestamps and command-line parameters.

Scan Details

My first job (SCANID 1)

Scan Details

Job Name	My first job
Scan ID	1
Scan Policy	Heavy/Vulnerability Scan
Start Time	2017-05-10 11:38:15
End Time	2017-05-10 11:45:34

Execution History

Agent/Node	Start Time	End Time	Status	Status File	Verbose Output	Results data
Local Node	2017-05-10 11:38:15	2017-05-10 11:45:30	finished	View Status File	View Verbose Output	View Results

Status file

```
05/10/17-11:38:27 Maximum concurrent probes = 20 (e22b6a6de3bb485280f7524d1d81e45b)
05/10/17-11:38:29 bin/nmap -sT -n -Pn -O --min_hostgroup 100 --min_parallelism 100 --max_scan_delay 10ms
05/10/17-11:38:31 bin/ncat -sT -n -Pn -O --min_hostgroup 100 --min_parallelism 100 --max_scan_delay 10ms
05/10/17-11:38:33 Heap 90% complete (e22b6a6de3bb485280f7524d1d81e45b)
05/10/17-11:38:35 bin/timeout 120 bin/wdpscan.saint 7,19,21,42,53,67,69,88,111,123,137-138,161-162,177,5
05/10/17-11:38:35 bin/timeout 113 bin/tcpscan.saint 25,80,110,135,139,143,445,587 10.8.0.11
05/10/17-11:38:35 bin/timeout 75 bin/rpc.saint 10.8.0.11
05/10/17-11:38:35 bin/timeout 75 bin/dns.saint 10.8.0.11
05/10/17-11:38:35 bin/timeout 75 bin/adore.saint 10.8.0.11
05/10/17-11:38:36 Finished adore.saint 10.8.0.11
05/10/17-11:38:36 Finished 1/5 in phase 1 (e22b6a6de3bb485280f7524d1d81e45b)
05/10/17-11:38:36 Finished dns.saint 10.8.0.11
05/10/17-11:38:36 Finished 2/5 in phase 1 (e22b6a6de3bb485280f7524d1d81e45b)
05/10/17-11:38:46 Finished wdpscan.saint 7,19,21,42,53,67,69,88,111,123,137-138,161-162,177,389,500,513-
05/10/17-11:38:46 Finished 3/5 in phase 1 (e22b6a6de3bb485280f7524d1d81e45b)
05/10/17-11:38:55 Finished rpc.saint 10.8.0.11
05/10/17-11:38:55 Finished 4/5 in phase 1 (e22b6a6de3bb485280f7524d1d81e45b)
05/10/17-11:39:05 Finished tcpscan.saint 25,80,110,135,139,143,445,587 10.8.0.11
05/10/17-11:39:05 Finished 5/5 in phase 1 (e22b6a6de3bb485280f7524d1d81e45b)
05/10/17-11:39:05 Processing data: 14 records
05/10/17-11:39:05 Generating new records
05/10/17-11:39:05 Done generating new records
05/10/17-11:39:05 Processing data: 9 records
```

The Asset Tracker Agent

The asset tracker agent allows Security Suite to run recurring scans against targets with dynamic IP addresses, without requiring the user to continually change the targets' IP addresses in the job or target group. The agent is a lightweight program on the target which generates a unique asset ID and periodically sends that ID to SAINT's tracker service. The tracker service then detects changes in the IP address associated with that asset ID, and updates all scan jobs and target groups to use the current IP address.

Follow these steps to use the asset tracker agent:

- Start your installation with the tracker service enabled:

SAINT Security Suite

```
cd /usr/share/saint/eSaint/saint_manager
./saint_manager.py --with_service tracker start
```

2. The first time the tracker service starts, it will generate the agent setup program containing its own public key and connect-back address. The program will be located in `/usr/share/saint/eSaint/saint_manager/bin/tracker_setup.exe`. Copy and run this program on all targets which are to be tracked. (The tracker agent is currently available for Windows only.)
3. A dialog box will inform you when installation is complete.
4. Schedule jobs or create target groups in the usual fashion, using each target's current IP address. The job or target group will be automatically updated whenever a change in a target's IP address is detected.

Once installed, the agent sends its asset ID to the tracker service every time the user who installed it logs in, and once every six hours if the user who installed it had administrator privileges. The agent uses 2048-bit RSA encryption to ensure the confidentiality of the asset IDs, and a challenge-response protocol to protect against replay attacks. Connections from the agent to the tracker service use port 6262/TCP.

Uninstalling the Asset Tracker Agent

To uninstall the asset tracker agent if it was installed with administrator privileges:

1. From the Windows control panel, open the *Programs and Features* dialog.
2. Highlight *SAINT Asset Tracker*.
3. Click on *Uninstall*.

To uninstall the asset tracker agent if it was not installed with administrator privileges:

1. Log in as the user who originally installed the asset tracker agent.
2. From the *All Programs* list, open the *Startup* folder.
3. Right click on *tracker*.
4. Click on *Delete*.

Asset Tracker Connect-back Address

When the tracker service generates the agent setup program, the address to which the agent will connect is hard-coded into the program. By default, the IP address of the SAINT machine's local interface is used. However, in some situations that might not be the correct address. For example, if the local interface is a private IP address which is mapped to a public IP address by the firewall, and the intended targets can only access the public IP address. In this case, you can

specify the correct connect-back IP address by editing `/usr/share/saint/eSaint/saint_manager/config/manager.ini` and changing the `connectback_addr` setting. (Delete the `.keys/tracker.key` file to force the tracker service to re-initialize the next time it restarts.)

Asset Tracker Scripts

In addition to automatically updating scan jobs and target groups, the tracker service allows you to plug in custom tracking scripts. This may be useful if you wish to track targets for purposes other than maintaining scans.

Any language may be used to write a tracker script, as long as the script file is executable by the operating system. The script should accept two command-line arguments. The first argument is the previous IP address of the target, and the second argument is the new IP address of the target. The script will be called with these two arguments whenever the tracker service detects a change in a target's IP address.

Once the script is complete, edit

`/usr/share/saint/eSaint/saint_manager/config/manager.ini` and set the `script_file` parameter to the full path of the script. Ensure that the `execute` bit is set on the script. If it is not or you aren't sure, run `chmod u+x <filename>`.

Standalone Usage

Besides running as a module within Security Suite, the asset tracker service can also run standalone. When running standalone, it can still support custom scripts, but cannot track targets in the database or automatically update jobs and target groups.

To run the tracker service standalone, copy

`/usr/share/saint/eSaint/saint_manager/src/services/tracker.py` and `/usr/share/saint/eSaint/saint_manager/bin/tracker_setup_win32` to the desired location. It may be outside the SAINT installation directory, or on an entirely separate machine.

Run the program as follows:

SAINT Security Suite

```
python tracker.py [-p port] [-t timeout] [-k key_file] [-d  
db_file] [-s script_file] [-l log_file] [-a agent_file] [-c  
connectback_addr]
```

All command-line arguments are optional. If no `script_file` is specified, then the tracker will simply log IP address changes and do nothing more.

User Guide

Introduction to SAINT®

What is SAINT®?

SAINT is an acronym for the **S**ecurity **A**dministrator's **I**ntegrated **N**etwork **T**ool. This product was first offered commercially in 2001 by the company derived from the original acronym. SAINT Corporation has since expanded this offering into two products: **SAINT Security Suite** and **SAINT Cloud**. Fundamentally, the key capability of both solutions is to non-intrusively detect security vulnerabilities on any remote target, including servers, workstations, networking devices, and other types of network hosts. It will also gather information such as operating system types and open ports. The graphical user interface provides access to data management, scan configuration, scan scheduling, data analysis, and reporting capabilities through a web browser.

What is SAINTexploit®?

SAINTexploit is the legacy product term for the penetration testing component of SAINT's product lines. Prior to version 8, this component was available as an integrated component of the "professional" edition of the product. As of version 8, this capability is now fully integrated in both Security Suite and SAINTCloud and is accessed simply via the *Exploit* menu option. It allows the user to verify the existence of vulnerabilities by exploiting them and gathering evidence of penetration. Unlike vulnerability and configuration scanning probes, which detect various types of vulnerabilities and configuration weaknesses, exploits run different probes which are meant to gain command execution access to targets. Detected vulnerabilities are displayed in the *Analyze* capabilities at the "record level of detail" and include a separate exploit column to highlight whether an exploit is available for the applicable vulnerability. Both solutions also provide pre-packaged "Pen Test" scan policies which automatically choose exploits based on the target's operating system and open services. This scan policy can be used in conjunction with interactive processes to achieve an in-depth penetration test. Information learned from initial scanning and analysis can be used to devise attack strategies to obtain a connection to vulnerable targets, and possibly initiate multiple attack methodologies (exploits, exploit tools, social engineering, etc.) to help you demonstrate the impact of the vulnerabilities and prioritize remediation efforts.

How does Scanning Work?

The scanning process begins by detecting all live targets within the given target list or range. The selected scanning policy then determines which core probes are run against each target. Results from the probes are used by the inference engine to schedule additional probes and to infer vulnerabilities and other information based on rule sets. Final scan results are then stored in the back end database to support data analysis and reporting through either the browser interface, command line Interface (CLI) or accessed via the application programming interface (API).

Deployment Options

There are five (5) deployment options available for the fully-integrated solution. Your individual installation, configuration and administration activities may vary, depending on your specific deployment option.

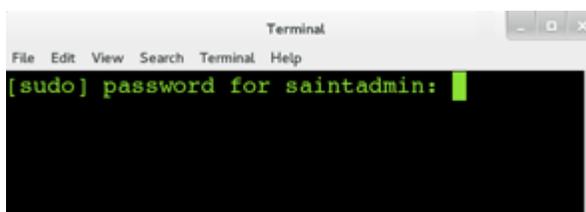
1. **Software Download** – The Security Suite download option is available for those that wish to control where and how the product is installed, configured and managed in their environment. The download options are available via the mySAINT customer portal.
2. **Virtual Appliance** – Security Suite is also available as a pre-configured virtual machine. Since the product only supports native installation on Linux-based hosts, a VM deployment option enables customers to deploy the product on Windows-based machines.
3. **SAINTbox®** – SAINTbox is a pre-configured appliance that provides an easy and affordable turnkey solution for getting started quickly and makes installation and updates easy.
4. **Cloud-based Software** – SAINT also offers a hosted scanning service via SAINTCloud. This service is provided through our hosted web servers as a shared multi-tenant environment. It is also available as a dedicated deployment for customers with larger capacity or special scanning requirements. The hosted service enables scanning TCP and UDP services on Internet-facing targets, based on the selected policy and host type fingerprinting executed during target discovery, as well as internal host scanning via secure VPN tunneling or remotely deployed scanners (i.e., distributed scanning nodes).
5. **Amazon Machine Image (AMI)** – Security Suite is also available through the AWS Marketplace as a pre-configured machine image. SAINT offers two deployment options for this AMI:

1. Non-preauthorized AMI for customers that require one deployment option that supports both direct access to the management console and scanning engine; and
2. Pre-authorized AMI for customers that wish to connect to an AMS-deployed scanning node that is configured to scan into AWS EC2 instances without prior approval of Amazon.

Start, Login, User Profile

Start

Start Security Suite by double clicking on the icon  and entering the administrative credentials to ensure processes execute with the necessary permissions on the installed host.



View the MAIN MENU and select the option for how you want to run this installation. These options allow you to start the product in a number of different ways, to support environments as diverse as standalone installations, network-based shared environments, or distributed multi-node architectures. See the [Administrator Guide](#) for a complete description for all of these options, as well as detailed instructions on how to setup and configure the software for various types of environments.

```

Terminal
File Edit View Search Terminal Help
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.
Continuing in 1 second...

```

The following describes starting SAINT Security Suite from the MAIN MENU:

- **Start and Launch Browser** – This is the most typical startup option for users that run the product from the installed host, such as from a desktop or laptop installation, or using the product directly on a server. When you close the browser, the background processes will continue to process scan requests until you choose to “stop” the software or restart or shut down the host machine. If Security Suite is currently running in background from a previous startup action, the only step required is to **Launch Browser**.
- **Start as a Background Process** – This option is typically selected when the software is installed on a shared resource, with user access done remotely via a desktop browser, using the localhost’s URL. This option starts all processes but does not open a browser on the installed host. Processes will remain open until a decision is made to “stop” the software or the installed host is rebooted or shutdown.
- **Start as a Remote Scanner Node** – This option starts the software on the installed host, and makes a secure connection to a separate installation that acts as a “manager” to support multi-node and load balanced scan requirements. This process requires additional installation and configuration actions by the system administrator, as described in the [Administrator’s Guide](#).

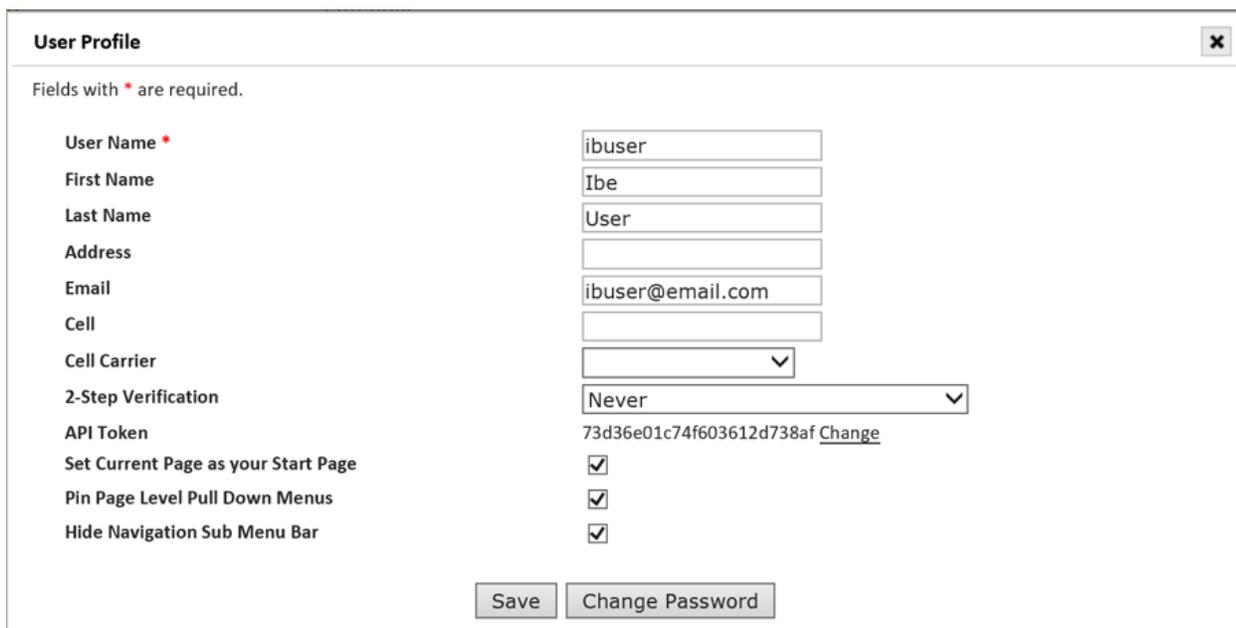
*NOTE: The default startup option is to **Start and Launch Browser**. However, the default option is updated automatically for subsequent start processes based on the selection made through this menu.*

Login

User account and Password credentials are case sensitive. Each installation comes pre-bundled with a default login account with administrative permissions to fully configure and administer the system. It is recommended that each user be given their own unique user account for ease of administration and user access control.

User Profile

Each user account contains a profile that stores information such as the user ID; access controls and permissions to system features and content; work address and e-mail address (to support automated notifications and report delivery workflows); and features to provide each user some level of customization to the system. An example of a user profile screen is shown below:



The screenshot shows a "User Profile" dialog box with a close button (X) in the top right corner. Below the title bar, it states "Fields with * are required." The form contains the following fields and options:

User Name *	ibuser
First Name	Ibe
Last Name	User
Address	
Email	ibuser@email.com
Cell	
Cell Carrier	
2-Step Verification	Never
API Token	73d36e01c74f603612d738af Change
Set Current Page as your Start Page	<input checked="" type="checkbox"/>
Pin Page Level Pull Down Menus	<input checked="" type="checkbox"/>
Hide Navigation Sub Menu Bar	<input checked="" type="checkbox"/>

At the bottom of the dialog, there are two buttons: "Save" and "Change Password".

The "Profile" link under the UserID displayed in the top right corner of the application is provided to access your profile information. Each user has write permission to edit the personal information related to the profile, configure system type configurations that are contained in this dialog; and the ability to change their password.

Change Password

Changing your password is done through the Profile option, or by contacting your Administrator. Follow these steps to change your password without Administrator assistance:

1. Open the *Profile* option under the UserID displayed in the top right corner of the application.
2. Select the *Change Password* button (Note: If the password button is grayed out, that means your account uses an authentication type which doesn't use locally stored passwords, such as Active Directory. In this case, the password would need to be changed from the Windows domain. See [Create a User](#) for more information.)
3. Enter your current password in the *Current Password* field to verify your identity
4. Enter your new password in the *New Password* field
5. Enter the new password again in the *Confirm New Password* field
6. Click *Save*
7. Close the dialog

Two-Step Verification

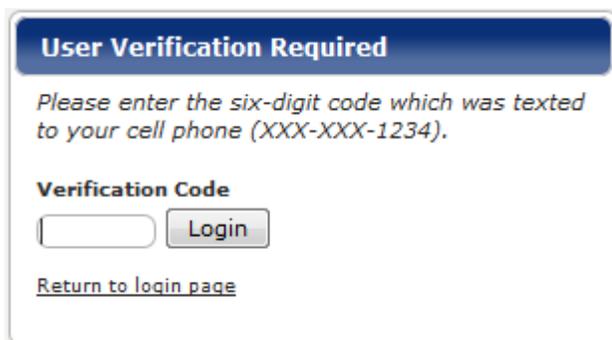
Although passwords are generally an accepted way of authenticating users, the use of passwords alone cannot prevent unauthorized access if a password is guessed or stolen. For increased security, users may add an additional layer of security to their accounts by enabling a two-step verification process. This process requires the user to have both the correct password and the correct cell phone for the account in order to be granted access to the system.

To enable two-step verification:

1. Click on the *Profile* link at the top right of any screen in the application.
2. In the *cell* setting, enter your cell phone number, including area code.
3. In the *2-Step Verification* setting, choose one of the following options:
 - **Always** – Require a login, password, and cell phone verification every time you log in.
 - **When logging in from new location** – Require a login, password, and cell phone verification only when you log in from a new IP address. When you log in from an IP address from which you have logged in before, require only a login and password.
 - **Never** – Require only a login and password.
4. Click on the *Save* button.

To use two-step verification once it is enabled:

1. At the login screen, enter your login and password.
2. If two-step verification is required from your location, you will see the following prompt. (The prompt shows the last four digits of your cell phone number. If this is not the correct number, contact your system administrator.)



User Verification Required

Please enter the six-digit code which was texted to your cell phone (XXX-XXX-1234).

Verification Code

[Return to login page](#)

3. Wait for a new text message to arrive from SAINT on your cell phone. The text message will contain a six-digit numeric code. (A new text message is sent each time you get to this step. Ensure you read the current message, since previous codes will not be accepted.)
4. Enter the code at the prompt.
5. Click on the *Login* button.

Set Default Start Page

Each user has control over what default page is displayed upon login. For example, one user may want to have the *Dashboard* tab displayed by default; while another user may want the *Report* tab to be the default. To set the default page:

1. Navigate to the page you want to be displayed by default when you log in
2. Open the *Profile* option in the top right corner of the application.
3. Select the checkbox for the “Set Current Page as your Start Page” option
4. Click *Save*
5. Close the dialog

Pin Page Level Pull Down Menus

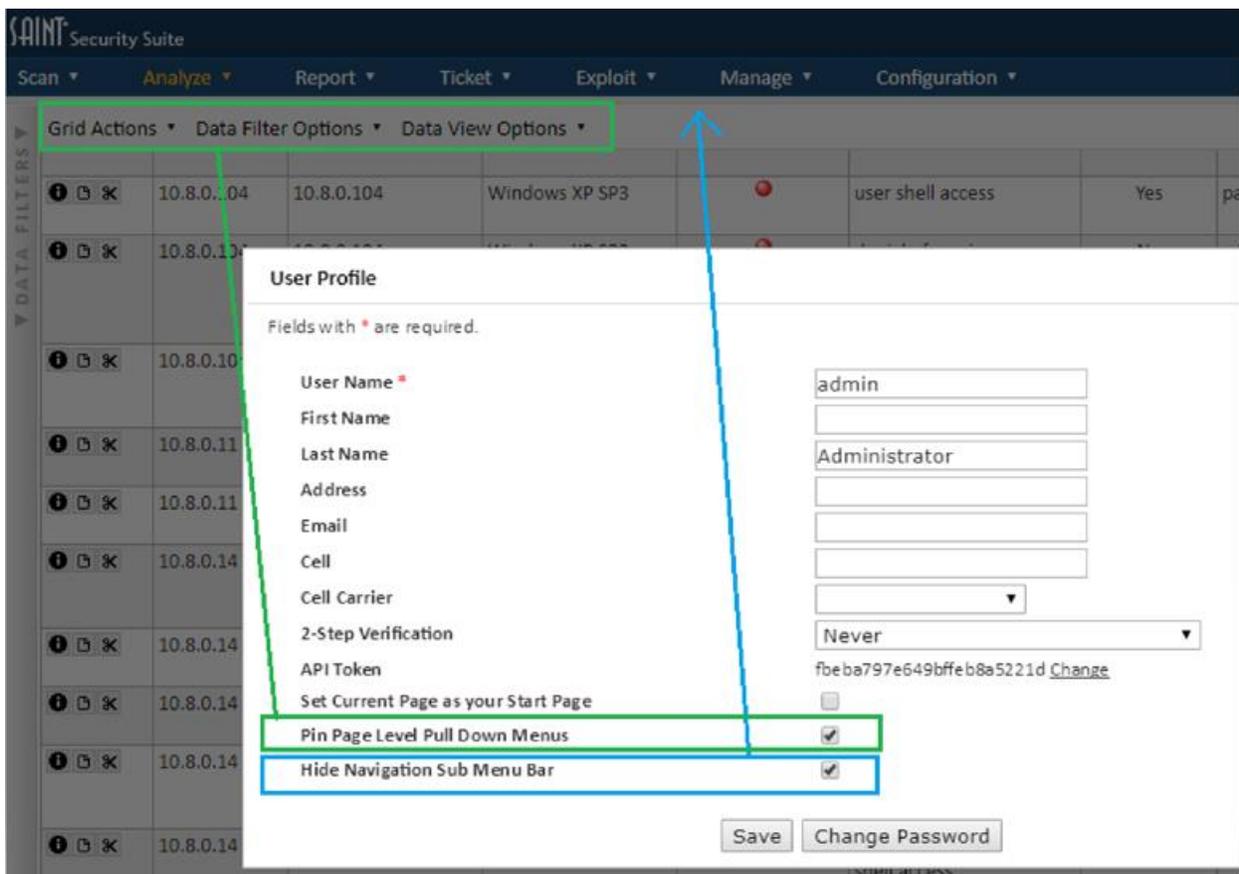
By the default, the Action options applicable to each page have a static position on each page, and scroll along with all other content as you scroll the pages up and down. This option

SAINT Security Suite

provides the capability to set the Actions menu bar to be pinned to the top level menu bar, and retain visibility as you scroll.

Hide Navigation Sub Menu Bar

By default, each main Menu option display, for convenience, a sub menu bar that includes all available page options for the selected menu. This hide option provides the capability to hide the sub menu navigation bar. The following illustrates the use of both the Pin and Hide options:



Access Controls

Security Suite and SAINTCloud feature a flexible object-based access control system. The system offers several benefits:

- Protects confidentiality and integrity.
- Allows users to perform all actions which are necessary for their job functions while preventing them from performing actions which are not.
- Allows users to share certain objects, such as reports, with selected users or all users.
- Allows multiple tenants to coexist on the same system without any visibility of other tenants' activities or even their existence.

Getting the maximum benefit from SAINT's access control system requires understanding how it works and configuring it properly, as well as creating an organized group structure. (See [Groups](#).)

Object-based Access Controls

Virtually anything that gets created during the course of vulnerability management, either by a user or system generated, is considered an object subject to security and access controls.

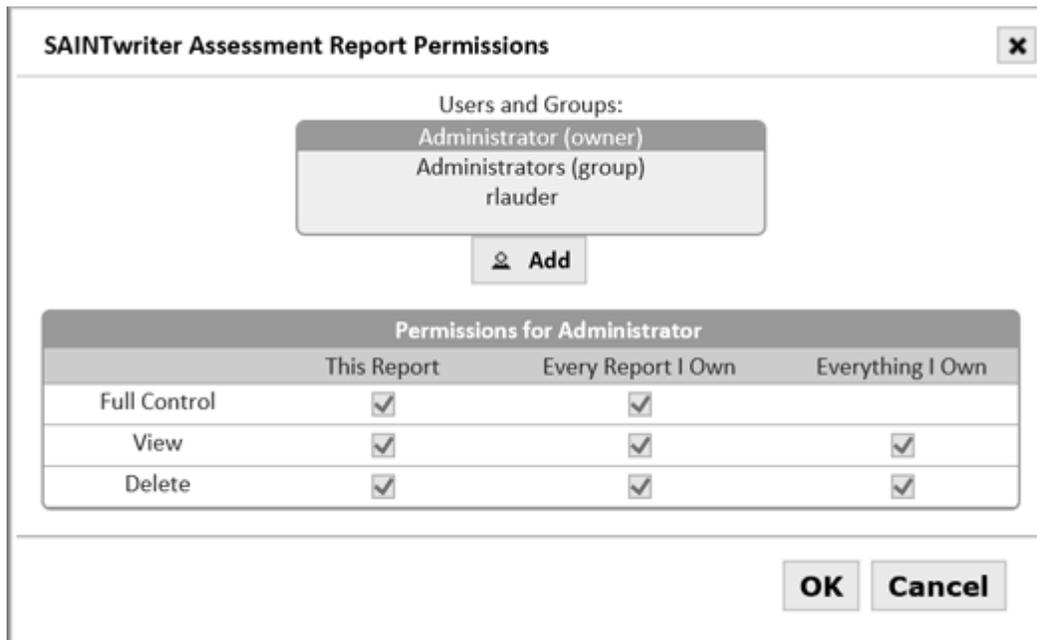
Objects include users, groups, scanner nodes, scan jobs, target groups, scan policies, reports, and many other types of content. As an object-based security design, the access control list is applied to individual objects. (Note: There are also a few access controls which are global, because they are applied to the system as a whole instead of individual objects. See [Assign Permissions to Users](#).)

Modifying Permissions

Only an object's owner or an administrator can modify the permissions on an object. To modify an object's permissions, follow the instructions below.

1. Find the desired object in the appropriate grid. For example, to set permissions on a report, click on the *Report* tab. Locate the desired object, using the grid's search boxes and other filtering as necessary. Click on the *Security* (padlock) icon on the desired object's row, or select the desired object's row and select *Security* from the Grid Actions dropdown menu without selecting any rows to modify the permissions on all of your objects instead of a specific object.

2. A permissions dialog will be displayed. For example:



3. The select box at the top of the dialog lists all the users and groups who already have some permissions on the object. The Administrator user and the Administrators group always appear in this list. The object’s owner (typically the user who created it), if not the administrator, also appears in the list, marked by the word “owner”.
4. Select the desired user or group from the select box to view or modify the permissions granted to that user or group. If the desired user or group doesn’t appear in the box, that means the user or group currently has no permissions on the object. In that case, click on *More Users*, select the desired user, and click *OK*.
5. The permissions table for the selected user or group will appear. The rows of the permissions table correspond to the possible actions on the object, and the columns correspond to the permission scope. (See [Permission Scope](#) below.) If the selected user is the Administrator user, the Administrators group, or the object’s owner, then the permissions cannot be unchecked. Those users always have full control over the object.
6. To modify the permissions which the selected user or group has on the object, check or uncheck the desired boxes in the permissions table, and click *OK*.

Permission Scope

The columns in the permissions table correspond to the permission scope. When setting permissions, there are three possible scopes. This makes it possible, for example, to share all of

your scan results with a co-worker without needing to remember to set permissions on every new scan job individually.

The three permission scopes are as follows:

Per object – The permission is only granted on the specific object. The specific object is the one which was selected from the grid when you opened the Permissions dialog, and is also indicated by the title bar of the Permissions dialog. If no object was selected, then this column is not shown.

Per object type – The permission is granted on all co-owned objects of the same type. For example, if you are modifying permissions for a report which you created, then the permission would be applied to all reports that you created.

Per owner – The permission is granted on all co-owned objects. For example, if you are modifying permissions for a report which you created, then the permissions would be applied to everything you create, including target groups, scan jobs, scan policies, etc.

Multi-tenancy

One of the benefits of SAINT's access control system is that it allows multiple tenants to co-exist on the same system without any visibility of other tenants' activities or even their existence. This is useful for managed service providers who want to provide a portal for their customers without disclosing any of one customer's data to another.

To create a tenant –

1. Create a new user. See [Create a User](#).
2. Remove the new user from the *Users* group. See [Edit a User](#).
3. *Optional*. Create a new group for the new tenant, and add the new user to the new group. See [Create a Group](#).
4. *Optional*. Enable the *create user* permission for the new user if you want the tenant to be able to create more users. See [Assign Permissions to Users](#).

Tenants are implemented as groups. For an administrator who manages multiple tenants, wherever data grids display users (e.g., job owner), there is the option to display the groups to which that user belongs. This will assist the administrator in filtering objects by tenant.

Configuration

SAINT includes a number of configuration options which control the way the system functions, scan run and exploits are executed. Many of these options are configurable in SAINT by users with Administrator permissions or those that have been granted edit permissions (see [Manage – Groups](#)) to modify Scan and Exploit configurations during job setup. The following describes each of these options in more detail.

Configuration Files

Behind the scenes, the software uses various configuration settings at job execution time, and passes them via job configuration files. For those using the command line interface, these files can also be modified manually. However, for most situations, SAINT's automated processes are the recommended method. Configuration files (both global and job specific) can be found in the `config` directory. The global configuration file is named `saint.cf`, and the job session configuration files are named `<session name>.cf`, where `<session name>` is the name of the scan being executed.

Global vs. Session Configuration

The global configuration file, `saint.cf` stores all configuration settings needed. These include global settings that are common to all scan jobs, such as settings for the management console and internal web server.

The settings found in the job-level `session` configuration file are used to control how a scan runs, such as the scan level, timeout values and password guesses. The job level configuration file is created whenever a Job is run. Note that the same variables found in the job's session configuration file are also contained in the global configuration file, under the line `Begin Session Configuration`, and in the `saintexploit.cf` file. However, values are only used to initialize new job session configuration files, and have no other effect.

Both the global and job level configuration files contain Perl variables corresponding to options shown in the Configuration tab, as well as additional variables controlled by the scan engine. Syntactically, lines beginning with a pound sign (`#`) are comments and do not affect program behavior, but do contain information but may be helpful when viewing or editing content.

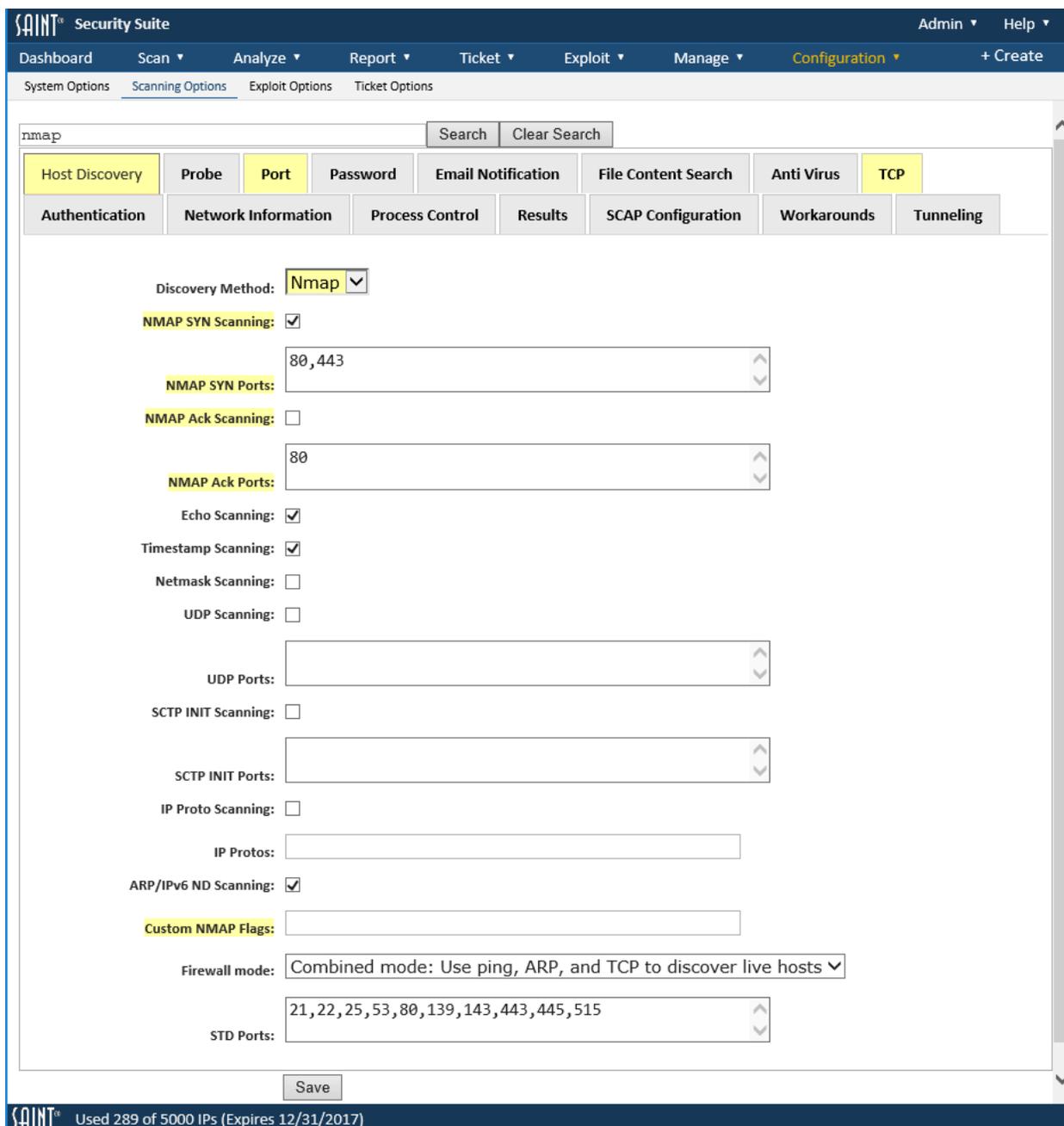
The sections below describe each configuration option and the corresponding variables in the configuration file.

Restoring to Default Options

- **All Options** – Clicking this option resets all configuration options back to “factor” default settings. Using this option will remove any prior customized changes you have made.
- **System/Scan/Exploit Specific Options** – Each configuration submenu provides an option to restore only the current displayed options (e.g., System only options; Scanning only options or Exploit-only options) to their factor default settings. As with the “All Options” this option will remove any prior changes you have made, but will be limited to the type of option selected.

Search Function

The configuration tab provides a search function to enable you to quickly locate configuration settings (variables) based on keywords. The search function will then highlight all Tabs where settings are located that either contain your search criteria in the setting’s title or is contained in the help text, since other variables may have relevance to your criteria. For example, locate where all settings are related to Nmap. As shown below, there are three tabs that contain references to Nmap – both Nmap specific configuration settings in Host Discovery, Port and TCP options, but also in the "Secs Before Dropping Connection Req" option (fw_timeout variable) since that variable has settings related to using Nmap.



Use the Clear Search button to clear the search field as an alternative to manually deleting or using the backspace key for the same action.

You can also enter partial words or strings, if you are unsure of the specific configuration names. For example, locate any configuration options for white listing content. SAINT provides support for white listing in its File Content Searches. Using only the string “white” found by filename and reverse_effect settings.

SAINT® Security Suite Admin ▾ Help ▾

Dashboard Scan ▾ Analyze ▾ Report ▾ Ticket ▾ Exploit ▾ Manage ▾ Configuration ▾ + Create

System Options Scanning Options Exploit Options Ticket Options

white Search Clear Search

Host Discovery	Probe	Port	Password	Email Notification	File Content Search	Anti Virus	TCP
Authentication	Network Information	Process Control	Results	SCAP Configuration	Workarounds	Tunneling	

FCS Enabled:

WCS Enabled:

FCS Dirs to Skip:

FCS File Types:

FCS Patterns:

Apply Luhn to Custom Patterns:

Blacklist Filename Regex:

FCS Whitelist Filename Regex:

FCS Whitelist Reverse Effect:

FCS NIX File Types:

FCS Objective:

Machine Search Timeout:

Restore default values? [\[All Options\]](#) or [\[Scanning Options\]](#)

SAINT® Used 289 of 5000 IPs (Expires 12/31/2017)

System Options

SAINT Security Suite admin Help + Create

System Options Scanning Options Exploit Options

Search Clear Search

Web Server Nodes API Password Policies Authentication Cisco FireSIGHT Cisco pxGrid Splunk License Notification Node Status Notification Agent Server Disputes ASV Passive Host Discovery Manager

Use TLS/SSL: Yes, except from localhost

Enable IPV6:

Enable IPV6:

Hosts Allowed to Connect: *

Server Port: 1414

Verbose: 0

TLS/SSL Key File: saint_manager/keys/saintweb.key

TLS/SSL Cert File: saint_manager/keys/saintweb.crt

TLS/SSL Cipher List: ALL

Enable SSV2:

Enable SSV3:

Enable TLSv1:

Enable TLSv1.1:

Enable TLSv1.2:

Enable TLSv1.3:

Save

Restore default values? [\[All Options\]](#) or [\[System Options\]](#)

SAINT Used 88 of 100 IPs. Using 1 of 2 agents. (Expires 10/18/2020) System time: 4:01 PM

Agent Server

The options described below control the behavior of agent-based scanning. In order to use these features, Agents must be enabled in your license key. See the [SAINT Agent Overview](#).

Enable Agent Scanning

This option specifies whether or not to run the service which allows agents to connect. It must be enabled in order to use agent-based features.

Server Port

This option specifies the TCP port on which the agent should listen for connections. The same port number must be specified when installing the agents in order for the connection to succeed.

Connection Strings

If this option is specified, each agent must provide one of the specified strings in order to connect to the manager. This prevents unauthorized agents from connecting. Use line breaks to separate the strings.

TLS/SSL Version

TLS/SSL protocol to use for remote connections. (TLSv1.1 and higher require Python 2.7.9 or higher and OpenSSL 1.0.1 or higher. TLSv1.3 requires OpenSSL 1.1.1 or higher.)

TLS/SSL Key File

The filename of the TLS/SSL key corresponding to the TLS/SSL certificate specified below.

TLS/SSL Certificate File

The filename of the TLS/SSL certificate which provides security between the manager and the agent. A self-signed certificate can be generated by clicking on the Generate Self-Signed SSL Files button.

Connection Timeout

The number of seconds the manager waits for a response from an agent before assuming the connection has been lost.

Server Address

The fully-qualified registered DNS host name of the manager. This is used as the subject name when generating the self-signed SSL files. It must be correct and resolvable by the agent in order for the connection to succeed. If the manager is not registered in DNS, an IP address may be used. In this case, the same IP address should be specified when installing the agent.

Web Server

SAINT delivers an embedded, proprietary web server with all product versions. This web server contains a number of configuration settings that control the communication between the application and server-based processes. While many of these configuration settings are controlled internal to SAINT, there are some that can be customized depending on local requirements, or are provided in the user interface to assist in troubleshooting possible issues. The options displayed in the configuration tab are described below.

[Use TLS/SSL](#)

Whether to enable TLS/SSL encryption for the web server. If TLS/SS is enabled, the URL to the web interface needs to begin with https. This setting only works for IPv4 communication.

SAINT Security Suite

Note that with this option, your browser will produce warnings because the default certificate is self-signed, until you either add the certificate to your browser's certificate store, or replace the self-signed certificate with one signed by a certificate authority. (See [TLS/SSL Key File](#) and [TLS/SSL Cert File](#) below.)

If you select *yes, except from localhost*, the web server will use TLS/SSL for connections from remote hosts, but not for connections from localhost. This avoids the certificate warnings when used locally, while still ensuring that network communication is encrypted.

Use TLS/SSL (0-No; 1-Yes; 2-Yes, except from localhost)

Enable IPv4

Allow the web interface to be accessed over IPv4.

Enable IPv4 (1-Yes; 0-No). The default is Yes.

Enable IPv6

Allow the web interface to be accessed over IPv6.

Enable IPv6 (1-Yes; 0-No). The default is No.

Hosts Allowed to Connect

This option defines the hosts that are authorized to connect to the 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.

Server Port

TCP/IP port that the SAINT web server listens on.

Verbose

This setting defines the level of verbose output for help in debugging or troubleshooting. You may be asked to change this setting by a SAINT engineer. However, it is not recommended that

these settings be changed in the normal course of use. The values are: (short request/responses; all socket activity; full request/responses; full debug).

```
verbose (0-short request/responses; 1-all socket activity; 2-  
full request/responses; 3-full debug).
```

TLS/SSL Key File

The path to the TLS/SSL private key file, relative to the `eSaint` directory, used by the web server and API services if [Use TLS/SSL](#) is enabled.

TLS/SSL Cert File

The path to the TLS/SSL certificate file, relative to the `eSaint` directory, used by the web server and API services if [Use TLS/SSL](#) is enabled.

TLS/SSL Cipher List

Colon-separated list of allowed TLS/SSL cipher suites to use if [Use TLS/SSL](#) is checked. See <https://www.openssl.org/docs/manmaster/apps/ciphers.html> for the correct format.

Enable SSLv2/SSLv3/TLSv1/TLSv1.x

These checkboxes specify which TLS/SSL protocols to allow for HTTPS connections if [Use TLS/SSL](#) is checked. Each HTTPS connection will use the highest selected protocol which is supported by the browser. TLSv1.3 requires OpenSSL 1.1.1 or higher to be installed on the Security Suite host. TLSv1.1 and TLSv1.2 require OpenSSL 1.0.1 or higher to be installed on the Security Suite host. If no supported protocols are checked, then TLSv1.2 is automatically allowed. Be aware that SSLv2, SSLv3, and TLSv1 are affected by known security vulnerabilities and should be avoided, but are still included for backwards compatibility with older browsers.

Node

SAINT's architecture provides support for multiple scanning engines (nodes), to support large-scale scanning requirements, distributed architectures and load balanced scanning. The following are configuration settings to control the connectivity and security for managing scanner nodes.

Port Number

TCP Port number that the "manager" uses to listen for connections from scanner nodes. The default is port 5252.

Allowed Nodes

Remote nodes that are allowed to connect. This can be a space or comma separated list of fixed IP addresses, CIDR blocks. You can also use * as a default condition without explicit allowances.

Connection String

Each remote scanner node must send this string when connecting to the manager. This helps ensure that only the correct nodes will connect. If this option is left blank, then no connection string is required when connecting a scanner node to the manager.

Max. Concurrent Scans

The number of concurrent scans allowed to run on each scan node. If a new scan is started when there are already this many scans running on the scan node, then the new scan is queued until one of the other scans finishes.

Poll Frequency

The number of seconds for each node to wait between requests for new tasks from the manager. Lower values cause more frequent requests, allowing a faster response from nodes when starting, stopping, or resuming scans. Higher values may be more appropriate when there are many nodes, to avoid overwhelming the manager with requests. The default setting of zero tells the manager to choose the optimal frequency based on the number of connected nodes. The chosen value starts at 1, increasing as more nodes connect and decreasing as nodes disconnect.

TLS/SSL Key File

Path to the TLS/SSL private key file, relative to the `saint_manager` directory. TLS/SSL is used to protect communications between the manager and remote nodes, if any.

TLS/SSL Cert File

Path to the TLS/SSL certificate file, relative to the `saint_manager` directory.

TLS/SSL Cipher List

Colon-separated list of allowed TLS/SSL cipher suites to use for communication with remote nodes, if any. See <https://www.openssl.org/docs/manmaster/apps/ciphers.html> for the correct format.

TLS/SSL Version

The TLS/SSL protocol to use for communications with remote nodes, if any. If *All* is chosen, each connection will use the highest available protocol which is supported by the browser. TLSv1.1 and TLSv1.2 require Python 2.7.9 or higher and OpenSSL 1.0.1 or higher to be installed on the application's host. TLSv1.3 requires OpenSSL 1.1.1 or higher to be installed on the application's host. Be aware that SSLv2, SSLv3, and TLSv1 are affected by known security vulnerabilities and should be avoided, but are still included for backwards compatibility with older browsers.

API

API Port

TCP Port number used to listen for API calls. The default port is 4242. The default port setting should only be modified if there is a port conflict with another application.

Allowed API Clients

Remote addresses allowed to connect to the API service. This can be a space or comma separated list of fixed IP addresses, CIDR blocks. You can also use * as a default condition without explicit allowances. The default value is null. If this value is left blank, only the localhost is allowed.

Use TLS/SSL

If this box is checked, then the HTTPS protocol is required for communicating with the API service.

TLS/SSL Cipher List

Colon-separated list of allowed TLS/SSL cipher suites to use if [Use TLS/SSL](#) is checked. See <https://www.openssl.org/docs/manmaster/apps/ciphers.html> for the correct format.

Enable SSLv2/SSLv3/TLSv1/TLSv1.x

These checkboxes specify which TLS/SSL protocols to allow for HTTPS connections if [Use TLS/SSL](#) is checked. Each HTTPS connection will use the highest selected protocol which is supported by the client. TLSv1.1 and TLSv1.2 require OpenSSL 1.0.1 or higher to be installed on the application's host. TLSv1.3 requires OpenSSL 1.1.1 or higher to be installed on the application's host. If no supported protocols are checked, then TLSv1 is automatically allowed. Be aware that SSLv2, SSLv3, and TLSv1 are affected by known security vulnerabilities and should be avoided, but are still included for backwards compatibility with older clients.

Memory Saving Mode

If enabled, the API service will handle each request in a child process. This prevents memory consumption from accumulating in the main API process, which could eventually lead to the kernel killing the process. This option should be enabled in use cases where many memory-intensive API resources are called, but should be disabled otherwise since forking the processes could potentially cause a slight decrease in performance.

Password Policies

Administrators can control various password policies through the system *Configuration* tab by editing the following password-specific System Options:

Minimum Password Length

This numeric value defines the minimum length of the password string that can be used when logging onto the software. The default value is 5.

Allowed Password Special Characters

These values define the non-numeric and non-alphabetic characters that can be used within a password string. The default values are `-_!@#$%^&*()+=?.,`

Total Stored Passwords

This numeric value defines the number of previous passwords that will be disallowed for reuse. For example, the default value, 5, restricts the user from re-using any of the last five passwords as a current or new password.

Failed Login Attempts

This numeric value defines the number of failed attempts before the system will lock the user out. If this occurs, the user must wait 15 minutes before he or she can log in, or notify a user with administrator rights to unlock the account.

Maximum Password Age

This numeric value specifies the number of days after which passwords expire. When this number of days have passed since the password was last changed, the user will be required to change the password the next time he or she logs in. The maximum password age requirement can be disabled by setting this value to zero.

Minimum Password Age

This numeric value specifies the number of days after which a password can be changed again. After a user changes the password, another password change will not be permitted until this number of days have passed. This prevents a user from defeating the [Total Stored Passwords](#) requirement by changing the password multiple times in succession. The minimum password age can be set to zero to allow password changes at any time.

Password Complexity

This setting specifies the character classes which passwords must contain at a minimum. If the new password does not contain the required character classes, the password change will be rejected. A strong password complexity policy greatly decreases the ability of an attacker to crack passwords because it exponentially increases the number of possible character combinations.

Options exist for specifying either the number of character classes (for example, “at least three character classes”) or the specific character classes (for example, “letter and number”) which must be represented. In the former case, new passwords must have at least the specified number of character classes represented, where the four possible character classes are uppercase letters, lowercase letters, numbers, and symbols (non-alphanumeric characters). For example, if the requirement is “at least three character classes,” the password “Saint1” would be accepted because it contains three character classes: an uppercase letter, lowercase letters, and a number. However, “saint1” and “Saint” would not be accepted because they contain only two character classes each.

For options that list specific character classes, at least one character in each of the required character classes must be represented. For example, if the requirement is “letter and number,” then “Saint1” would be accepted because it contains letters and a number. However, “Saint!” would not be accepted because, even though it contains three character classes, it does not contain a number.

If the password complexity is set to “none,” then no password complexity requirement is imposed.

Login Session Timeout

This numeric value defines the number of seconds allowed for user inactivity before a user’s session times out and is closed. Once this timeout is reached, the user must log back into the system to establish a new session and interact with the application. Changes to this configuration do not impact current user sessions. The new timeout value will take effect for users upon subsequent logins. The default value is 28,800 seconds (8 hours).

Authentication

SAINT offers the option of using an Active Directory server for authenticating users to the Security Suite. This allows users to use the same password to log into Security Suite as they do to log into the Windows domain. To enable this feature, use the settings described below, and set the authentication type for each desired user to Active Directory in the [Edit User](#) form.

Active Directory Server

This setting specifies the Active Directory server to be used for authentication. It may be an IP address or a registered hostname, but note that if SSL is enabled, this setting should match the common name of the server’s certificate.

Active Directory Port

This setting specifies the port number on which the Active Directory server listens for LDAP connections. The default value, 389, is normally correct and doesn’t need to be changed.

Active Directory SSL Port

This setting specifies the port number on which the Active Directory server listens for LDAPS connections. It is unused unless the SSL option is enabled below. The default value, 636, is normally correct and doesn't need to be changed.

Use SSL

This setting specifies whether or not to use SSL to encrypt the LDAP traffic to and from the Active Directory server. If this option is not chosen, then passwords will go over the network in clear text. If this option is chosen, then the Active Directory server's certificate must be installed on the application's host, and the `TLS_CACERT` setting in the `ldap.conf` file should be set to the path of the certificate. See <http://www.sans.org/reading-room/whitepapers/protocols/ssl-secure-ldap-traffic-microsoft-domain-controllers-33784> for more information about setting up SSL certificates for Microsoft domain controllers.

NetBIOS domain name

This setting is the NetBIOS name of the Active Directory server's domain. For example, MYCOMPANY. Unlike the fully-qualified domain name, it should not include any top-level domain extensions such as .local.

Create users

Configuring this option will automatically create a new user if Active Directory authentication succeeds for a login name which does not yet exist in the system. In other words, any time there is an attempt to log into Security Suite with a non-existent login name, the system will ask the Active Directory server whether the login and password are valid, and if they are, an account will be created and the login session will proceed using that account. This feature may be convenient for allowing new users onto the SAINT system without needing to manually create accounts for them. But it may be undesirable if only certain users from the Windows domain should be allowed into the system.

Active Directory domain

This setting specifies the fully-qualified domain name of the Active Directory server's domain (for example, mycompany.local) or the Base DN for the LDAP search (for example,

SAINT Security Suite

DC=mycompany,DC=local). It is used to search the server for information about the user when automatically creating new users. It is unused unless the *Create Users* option is enabled.

Cisco FireSIGHT

Security Suite provides the capability to export scan results to Cisco FireSIGHT. This allows the scan results to be viewed in Cisco FireSIGHT and used in Cisco FireSIGHT's impact assessment. (See [Export to Cisco FireSIGHT](#).)

The following options are used to configure Security Suite to communicate with Cisco FireSIGHT. These settings must be properly configured if you will be exporting results to Cisco FireSIGHT.

- Cisco FireSIGHT IP Address – This option specifies the IP address of Cisco FireSIGHT.
- Cisco FireSIGHT Port – This option specifies the TCP port on which the Cisco FireSIGHT Host Input API listens for connections. The default is 8307.
- Cisco FireSIGHT Certificate – Cisco FireSIGHT uses PKCS12 certificates for authentication of host input clients. To generate the certificate, log into the Cisco FireSIGHT web interface. Click on *System > local > registration > Host Input Client*. Enter Security Suite's IP address in the *hostname* field. Choose a passphrase for the certificate and enter it in the *password* field. Then download the certificate, and upload it into the *Cisco FireSIGHT Certificate* option in Security Suite.
- Cisco FireSIGHT Password – This should be set to the certificate passphrase you chose when generating the certificate described above.

Cisco pxGrid

Security Suite can be configured as a Cisco pxGrid client, allowing integration with the Cisco Identity Services Engine (ISE). This allows you to further protect your network by initiating a quarantine of high-risk assets directly from the Security Suite user interface. (See [Quarantines](#).)

Oracle Java Runtime Environment (JRE) is required on the Security Suite system in order to use the Cisco pxGrid client.

ISE Server

This setting specifies the host name or IP address of the Cisco ISE server.

User Name

This setting specifies the Cisco pxGrid client name. This must be unique for each client which connects to the Cisco ISE server. You do not need to create the client account on the server. It will be created automatically using the given name the first time a Cisco pxGrid action is performed. (It may need to be approved, however, if auto-registrations are disabled. See [ISE Server Configuration](#).)

ISE Server Certificate

This is where you need to paste the ISE server's certificate, in PEM format. The correct format begins with the line "-----BEGIN CERTIFICATE-----" and ends with the line "-----END CERTIFICATE-----". This certificate can be exported from the System Certificates page in ISE. Be sure to choose the certificate which is used by Cisco pxGrid. The Issued To hostname for this certificate must be registered in DNS and resolvable by the client.

Client Host name

This setting specifies the fully-qualified host name of the Security Suite host. This is used to generate the self-signed certificate as described below, so the host name should be registered in DNS and resolvable by the ISE server.

Client Certificate

This setting is the Security Suite host's certificate for authentication to the ISE server, in PEM format. The correct format begins with the line "-----BEGIN CERTIFICATE-----" and ends with the line "-----END CERTIFICATE-----". If this is a self-signed certificate, then besides being specified here, it must also be imported into the ISE server's Trusted Certificates page before the pxGrid persona is enabled. The Issued To hostname in this certificate must be the registered DNS hostname for the Security Suite host, and must be resolvable by the ISE server.

If you do not already have a certificate and want the client to use a new self-signed certificate, click on the *Generate* button beside this setting. This button will fill the Client Certificate text area with a newly generated self-signed certificate using the client hostname specified above. It will also fill the Client Key text area with the private key corresponding to the certificate.

Client Key

This setting is the private key corresponding to the above certificate, in PEM format. If you clicked on the *Generate* button above, then this setting is automatically filled and should not be changed.

ISE Server Configuration

After all of the above Cisco pxGrid client settings are complete, the ISE server must be configured for Cisco pxGrid. Under Administration > System > Deployment, edit the desired ISE node. Change it to a primary node if it is currently a standalone node. Under Personas, check the box beside pxGrid and click on *Save*.

Next, on the pxGrid Services page, click on *Enable auto-registration* if it is not already enabled. Otherwise, you will need to manually approve the client after the first time it attempts to connect. Even after the client is approved, the client's group may need to be changed to EPS before quarantine requests can succeed.

Splunk

The following describes the steps for configuration Splunk and Security Suite for ingesting scan results for use in Splunk.

Setup the Splunk Add-On

1. From the Splunk instance, download the *SAINT Add-on* for Splunk from Splunk.com
 - a. Click on the Splunk Apps Icon
 - b. Search for 'SAINT'
2. Install the Add-on from Splunk's Data-Input user interface and enable an HTTP Event Collector using the `saint8_scandata` sourcetype



- a. Select 'data inputs'
- b. Click on 'HTTP Event Collector'

- c. Click on 'New Token.'
 - d. Give the token a name
 - e. Click next
 - f. In the source type setting, click 'Select'
 - g. Choose 'Custom'
 - h. Choose 'saint8_scandata.'
3. Click *Review*
 4. Click *Submit*

IMPORTANT – Make a note of the token value it gives you which should look something like this: "0510E530-60C1-4BBB-8469-A294886547B8." You will need this when configuring Security Suite. Also, make a note of the HTTP Event Collector global settings by clicking on the *global settings* button on the HTTP Event Collector page. You will need to know if SSL Enabled is checked and the port number from there. These settings can be changed but they must match what you configure in Security Suite.

Configure SAINT for Splunk Integration

1. Login to your Security Suite installation
2. Click on the *Configuration* tab
3. Click on *System Options*
4. Click on the *Splunk* tab

The screenshot shows the SAINT Security Suite Configuration page. The top navigation bar includes 'Dashboard', 'Scan', 'Analyze', 'Report', 'Ticket', 'Exploit', 'Manage', 'Configuration', and '+ Create'. The 'Configuration' tab is active, and the 'Splunk' sub-tab is selected. The configuration form contains the following fields and options:

- Splunk server IP:
- HTTP Event Collector Token:
- HTTP Event Collector port:
- Use SSL:
- Splunk self-service cloud:
- Splunk non self-service cloud:

At the bottom of the form is a 'Save' button. Below the form, there is a link to 'Restore default values? [All Options] or [System Options]'. The footer of the page shows 'SAINT Used 289 of 5000 IPs (Expires 12/31/2017)' and 'System time 2:47 PM'.

5. Complete all fields, as they apply to your Splunk instance:
 - a. Splunk server IP – the fixed IP of the Splunk host.

- b. HTTP Event Collector Token – obtained when setting up Splunk add-on. Example: "0510E530-60C1-4BBB-8469-A294886547B8"
 - c. HTTP Event Collector Port: Collected in the Splunk global settings by clicking on the 'global settings' button on the HTTP Event Collector page. Security Suite default value is 8088
 - d. Use SSL – Check if the Splunk HTTP Event Handler is using SSL.
 - e. Splunk self-service cloud – Check if Security Suite will be forwarding data to a Splunk self-service Cloud instance.
 - f. Splunk non self-service cloud – Check if SAINT will be forwarding data to a Splunk non self-service Cloud instance.
6. Click *Save*

How to Use Security Suite with Splunk

Option 1

Click on [Configuration – Scanning Options](#) – Results tab to configure Security Suite to automatically transmit scan results to your Splunk installation. Check the “Export Results to Splunk” checkbox to configure Security Suite to transmit all scan results generated by Security Suite to your Splunk instance.

Option 2

Configure individual Jobs to automatically export/import scan results to your Splunk integration any time the Job is run. To transmit scan results by Job, navigate to [Step 4 – Advanced](#) when creating or editing a job in the job creation wizard, and click on the Results Tab. Check the “Export Results to Splunk”. Results when then be transmitted every time the specified Job is run.

Option 3

Export scan data from the [Analyze grid](#), and transmit the scan results into the pre-configured Splunk instance. Click on the *Splunk* option in the Grid Actions dropdown to choose how you wish to transmit the data shown in the data grid into the pre-configured Splunk instance. Click *Transmit Now* to automatically export the data to Splunk. Click *Save Export File* to generate a file which can be used to import data into Splunk using the JSON data source type.

Disputes

Enable Dispute Notifications

If this box is checked, an e-mail message will be sent to the dispute's creator when a dispute is resolved, and to the dispute resolver(s) when a dispute is opened or modified.

Dispute Resolver(s)

This option specifies the user or users who should receive a notification when a dispute is opened or modified if dispute notifications are enabled above. Both SAINT login names and e-mail addresses are accepted. If a login name is specified, the message will be sent to the e-mail address in that user's profile. Enter a comma-separated list to specify multiple recipients. If this option is left blank, notifications will be sent to all users who have Resolve Disputes permission (see [Global Permissions](#)) if any exist, or else to all Administrators.

From Email

This option specifies the From e-mail address for all PCI-related notifications. If left blank, the e-mail address of the user who initiated the event will be used.

From Email Display Name

This option specifies the From name for all PCI-related notifications. If left blank, the name of the user who initiated the event will be used.

Email Server

This option specifies the e-mail server to use for sending PCI notifications. If left blank, the registered MX for the recipient's domain will be used.

ASV

Note: This tab is only available to users with Attestation of Scan Compliance in their license.

ASV Certificate Number

This option specifies the ASV certificate number to put into the Attestation of Scan Compliance. The ASV certificate number is an eight-digit number (in nnnn-nn-nn format) issued by the PCI Security Standards Council.

Customer Attestations

This option specifies the conditions that the scan customer must accept when requesting an Attestation of Scan Compliance. The default conditions are based on PCI DSS requirements, but some ASVs may wish to reword them or add their own terms. Use a pipe character (|) to separate the conditions. Conditions which begin with an asterisk are required.

Enable Attestation Notifications

If this box is checked, an e-mail message will be sent to the requester when an Attestation of Scan Compliance is approved or denied, or to the attestation resolvers when an attestation request is opened or modified. This option is only used if Attestation of Scan Compliance is enabled in the license.

Attestation Resolver(s)

This option specifies the user or users who should receive a notification when a request for an Attestation of Scan Compliance is opened or modified, if attestation notifications are enabled above. Both SAINT login names and e-mail addresses are accepted. If a login name is specified, the message will be sent to the e-mail address in that user's profile. Enter a comma-separated list to specify multiple recipients. If this option is left blank, notifications will be sent to all users who have Issue AoSC permission (see [Global Permissions](#)) if any exist, or else to all Administrators.

Executive Summary Report Type

This option specifies the name of the report type to use when generating ASV Executive Summary reports for attestation requests. The default is SAINT's standard PCI Executive report type, but some ASVs may wish to use a custom report template with their own format and branding. If this setting is changed, be sure that the chosen report type complies with the executive summary reporting requirements in the ASV Program Guide.

Detail Report Type

This option is similar to the one above, but specifies the report type to use when generating ASV Detail reports.

AoS Report Type

This option is similar to the one above, but specifies the report type to use when generating Attestations of Scan Compliance.

License Notification

The license notification features described below provide visibility into the current status of the product license, and notification triggers for when you are close to the licensed capacity.

License Email Threshold

This threshold is the number of targets/scans left on the license before the notification is sent.

License Warning Email Address

This email address list is a space-separated list of email addresses to which license notifications will be sent.

License Warning Email Server

This email server is the hostname or IP address of the email server to use to send the email. If none is provided, the system will use the current default mail server.

License Warning Email Subject

This subject is the subject line that will appear on the license warning email messages.

Show License Key Status

If the license type is “metered” or “unique”, the status of the license will be shown on the GUI footer.

Passive Host Discovery

The passive host discovery feature attempts to continuously discover devices on the network by silently watching for traffic from new IP and MAC addresses, rather than actively probing a range of addresses. The discovered devices can then be easily imported into a scan job.

Enable Passive Host Discovery

Check this box and then restart the manager to activate the passive host discovery feature. When this box is checked, all connected scan nodes will monitor the chosen network interface and parse all IP and ARP packets. When previously unseen source IP or MAC addresses are found, those addresses are reported back to the manager, where they can be viewed and scanned. (See [Passive Host Discovery](#).)

Note that MAC addresses are only available for sources which are on the same LAN as the node. Furthermore, the traffic that can be seen on each node's network interface depends on the way the network switches are configured. Typically, the node will only be able to discover hosts which either send out broadcast requests on the node's local segment, or which have direct communication with the node.

Passive Host Discovery Networks

This option specifies which IP addresses to report. The value is a space- or comma-separated list of Class A, B, or C networks (such as 10, 172.16, or 192.168.1) or CIDR addresses (such as 10.0.0.0/8). This option is used as a filter by the packet capture engine. If it is left blank, no filter is used, and all addresses are reported. In this case, IP addresses which don't even belong to your organization could get reported, so leaving this option blank isn't recommended.

Passive Host Discovery Interface

This option specifies which network interface to monitor on the scan node. It is specified as an interface name returned by the "ifconfig" command, such as "eth0". If it is left blank, the lowest numbered configured interface, excluding the loopback interface, is used. If it is set to "any", then all interfaces are monitored.

Purge Offline Hosts After

This option is useful for removing stale entries from the passively discovered hosts table. The value specifies the number of days after which a host should be dropped if it has not been seen on the network. This prevents devices which are no longer on the network from being scanned again and again.

Manager

SAINI Security Suite

Scan ▾ Analyze ▾ Report ▾ Exploit ▾ Manage ▾ Configuration ▾

System Options Scanning Options Exploit Options

Search Clear Search

Web Server Nodes API Password Policies Authentication Cisco FireSIGHT

Infoblox

Purge Scans After Days:

Require Target Authorization: ▾

Scheduled scan grace time (minutes):

Maximum Analytics Processes: (Minimum number: 1)

Maximum Target Selection Hostname Resolution Time: (Minimum number: 1)

Maximum Overall Target Selection Hostname Resolution Time: (Minimum number: 1)

Save

Restore default values? [\[All Options\]](#) or [\[System Options\]](#)

Purge Scans After Days

This option can be used to automatically delete scans and their associated jobs and data after the specified number of days from the start date of the scan. Deletion is performed in a background process whenever the manager starts and every 24 hours thereafter. If this option is set to 0, then automatic deletion is not performed. *Note:* Regardless of this setting, on-demand deletion can be performed at any time by executing “python eSaint/saint_manager/src/modules/datastore/purge.py <days>” from the command line, where <days> is the number of days.

Require Target Authorization

This option allows you to require users to accept an agreement with an electronic signature before running a scan or exploit. This option may be useful if you are hosting a scanning platform for your customers, so you will have evidence that the scan activity was authorized in case you later receive abuse complaints from the target's owner. The form is presented after the user enters any new targets in the scan wizard or the exploit run form. When this option is enabled, a new menu option appears under the **Manage** tab called *Target Authorizations*, which allows you to view and download the authorization forms.

There are three options for this setting. *Always* will require target authorization for all new targets. *Local* will require target authorizations only for new targets being scanned or exploited from the local node. This option may be useful if you have some customers who own their own scan nodes for which authorization is not required. *Never*, which is the default, removes the target authorization requirement.

Target Authorization Agreement

This option only appears when the above option is enabled and allows you to specify the agreement text for target authorizations. This text is the terms and conditions that the user must accept before scanning or exploiting a new target.

Maximum Analytics Processes

The maximum number of analytics processes that can run at the same time, reduce it to save memory and processing power while scanning. New scan data is continuously analyzed by the manager during a scan and setting this value lower could save memory and processing power on systems that require it.

Maximum Target Selection Hostname Resolution Time

The maximum number of seconds to wait for hostname resolution when entering targets to scan by hostname or URL per target.

Maximum Overall Target Selection Hostname Resolution Time

The maximum number of seconds to wait for ALL hostnames to resolve when entering targets to scan by hostname or URL. For example: if this is set to 13 seconds, and a large hostname

target list is imported, SAINT will wait for this many seconds before ignoring the hostname resolution and add the targets regardless.

Infoblox

Two options are available:

- **Infoblox server IP or hostname** – The IP address or hostname of your infoblox server.
- **Infoblox API version** – The version of the API running on your Infoblox server. SAINT sets this to a lower version by default but if your server supports a higher version then you can set that here.

Scanning Options

The following configuration options define various characteristics and process controls over vulnerability, configuration and application scan activity.

The screenshot displays the SAINT Security Suite Configuration interface. The top navigation bar includes 'Dashboard', 'Scan', 'Analyze', 'Report', 'Ticket', 'Exploit', 'Manage', and 'Configuration'. The 'Configuration' tab is active, showing a search bar and a list of configuration categories: Host Discovery, Probe, Port, Password, Email Notification, File Content Search, Anti Virus, TCP, Authentication, Network Information, Process Control, Results, SCAP Configuration, Workarounds, and Tunneling. The 'Host Discovery' category is selected, showing the following settings:

- Discovery Method: Nmap
- NMAP SYN Scanning:
- NMAP SYN Ports: 80,443
- NMAP Ack Scanning:
- NMAP Ack Ports: 80
- Echo Scanning:
- Timestamp Scanning:
- Netmask Scanning:
- UDP Scanning:
- UDP Ports: [empty]
- SCTP INIT Scanning:
- SCTP INIT Ports: [empty]
- IP Proto Scanning:
- IP Protos: [empty]
- ARP/IPv6 ND Scanning:
- Custom NMAP Flags: [empty]
- Firewall mode: Combined mode: Use ping, ARP, and TCP to discover live hosts
- STD Ports: 21,22,25,53,80,139,143,443,445,515

A 'Save' button is located at the bottom of the configuration area. Below the configuration area, there are links to 'Restore default values? [All Options] or [Scanning Options]'. The footer of the page shows 'SAINT® Used 289 of 5000 IPs (Expires 12/31/2017)' and 'System time 2:28 PM'.

Host Discovery

These options determine the default behavior for discovery scans (SAINT or Nmap) and configuration settings for Nmap if that method is selected for host discovery. These settings can be defined globally, as well as overridden when setting up a scan Job.

Discovery Method

- **SAINT Firewall** – In order to avoid wasting time scanning hosts which do not exist or are unreachable, the scan engine attempts to discover live hosts at the start of a scan. The method used to discover live hosts varies depending upon whether a firewall is in place. Also, see the [Workarounds](#) section for additional Firewall rules/settings when using this discovery option.
Set this Flag to 0, to use SAINT's built-in discovery.
- **Nmap** – Default setting. This setting uses Nmap's Discovery engine. See the [Nmap](#) documentation for a complete list of Nmap options. Use caution when modifying these options, since certain settings may cause the port scan to miss ports in some environments, to use unintended protocols, or to scan unintended targets. Do not set any output options, since SAINT requires machine-readable output and therefore always includes that argument (-oM).

NMAP SYN Scanning (nmap_disco_syn)

Sends empty TCP packets with the SYN flag set. Live hosts will reply with either a RST or SYN/ACK TCP packet.

`Nmap_disco_syn` (0-No; 1-Yes).

NMAP SYN Ports (nmap_disco_synports)

Default is 443. An optional list of comma-separated ports may be supplied. If omitted, the default Nmap ports will be used.

NMAP Ack Scanning (nmap_disco_ack)

Sends empty TCP packets with the ACK flag set. Live hosts will reply with a RST packet. Some firewalls prevent hosts from replying to SYN requests to closed ports, but may still respond to ACK packets.

`Nmap_disco_ack` (0-No; 1-Yes)

NMAP Ack Ports (`nmap_disco_ackports`)

Default is 40. An optional list of comma-separated ports may be supplied. If omitted, the default Nmap ports will be used.

Echo Scanning (`nmap_disco_echo`)

One sends ICMP echo (type 8) request.

`Nmap_disco_echo` (0-No; 1-Yes)

Timestamp Scanning (`nmap_disco_timestamp`)

One sends timestamp (type 13) request.

`Nmap_disco_timestamp` (0-No; 1-Yes)

Netmask Scanning (`nmap_disco_mask`)

One sends Address Mask (type 17) request.

`Nmap_disco_mask` (0-No; 1-Yes)

UDP Scanning (`nmap_disco_udp`)

Sends UDP packets to the given ports. Empty packets will be sent to most ports.

`Nmap_disco_udp` (0-No; 1-Yes)

UDP Ports (`nmap_disco_udpports`)

Ports specified here will be included in the `config/nmap/nmap-payloads` and send the corresponding packets, which will be more likely to elicit a response.

SAINT Security Suite

SCTP INIT Scanning (nmap_disco_sctp)

Sends SCTP packet with the minimal INIT chunk. Live hosts will reply with an ABORT chunk if the port is closed or an INIT-ACK chunk if it is open.

Nmap_disco_sctp (0-No; 1-Yes)

SCTP INIT Ports (nmap_disco_sctpports)

An optional list of comma-separated ports may be supplied. If omitted, the default Nmap ports will be used.

IP Proto Scanning (nmap_disco_ip)

Sends an IP packet with the specified protocol number set.

Nmap_disco_ip (0-No; 1-Yes)

IP Protos (nmap_disco_ipprotos)

An optional list of comma-separated protocol list may be supplied. If omitted, the default Nmap protocols will be used.

ARP/IPv6 ND Scanning (nmap_disco_arp)

Uses NMAP to handle ARP requests instead of the host operating system. This is useful for scanning local LANs and may improve performance. If IPv6 targets are used, then ICMPv6 Neighbor Discovery is used instead of ARP.

Firewall mode: Firewall Flag

These options determine the default behavior for scans that use SAINT for host discovery. These settings can be overridden when setting up a scan Job. Each configuration setting and option is defined below:

- **No Firewall Support** – The No Firewall Support option is the default, and should be selected if no firewall is in place. With this option, SAINT attempts to send an ICMP echo request (ping) to each host. When the host does not respond, the scanner assumes the host is down and skips further probes.

- **Firewall Support – Use TCP Discovery** – If you are scanning targets that are behind a firewall from a system that is not behind the firewall, or in any other case where ICMP does not work, choose this or the ARP Ping Discovery options. This option causes the scanner to use TCP for discovering live targets. Each potential target in the specified target range will be scanned for a few standard TCP ports. If there is a response, either that the port is open or that the connection was refused by the target, then the host is considered to be alive. The ports scanned for this purpose are specified in the Standard Ports settings.
- **Extensive Firewall Support** – This option skips the discovery process altogether and does a complete scan of every target address, regardless of whether it is alive. Hence, Extensive Firewall Support can lead to a very slow scan, especially if a large target range was entered. Use this option only when the targets do not respond either to pings or to TCP requests to closed ports, and do not consistently have any of the standard ports open
- **ARP Ping Discovery** – With this option, the scanner will consider a potential target to be alive if the IP address can be resolved to a MAC address using the ARP protocol. The benefits of this method are that it still works even when ICMP pings and TCP ports are blocked, and it is the fastest discovery method. But it only works for targets that are on the same local network as the scanner.
- **Combined Firewall Support** – Choose this option if you do not know whether your targets are behind a firewall or if some targets may be behind a firewall while others are not. This option uses all of the above discovery methods. It is the slowest option, but also the most likely to succeed in discovering all live targets.

Firewall Flag (0=No Firewall Support; 1=Firewall Support - Use TCP Discovery; 2=Extensive Firewall Support; 3=ARP Ping Discovery; 4=Combined Firewall Support)

STD Ports (std_ports)

TCP Ports to scan to find live hosts, using SAINT's Discovery method set in Host Discovery, (discovery_method = 0). The firewall_flag value tells SAINT whether to expect the targets to be behind a firewall. If the firewall option is set to use TCP discovery and the primary target contains an IP address range or a subnet, then the scanner will scan each potential target for a few standard TCP ports and check whether or not there is a response, either that the port is

open or that the connection is refused. The `std_ports` values define ports to be scanned for this purpose.

Probe

Spider Depth (`spider_depth`)

Default level: 3 - SAINT's HTTP probe contains checks for vulnerabilities in many web applications which could be installed in non-standard locations on web servers. SAINT attempts to find these web applications by scanning pages which are linked from the root page, then scanning pages which are linked from those pages, and so on. This process is known as *spidering*. Increasing the depth allows a more thorough scan, but could cause an exponential increase in the time needed to complete the scan if a target has many links. Setting the depth to zero or unsetting Exhaustive flag at Job setup time tells the scanner to scan only the web root directory and not to follow hyperlinks. Setting the depth to one causes the scanner to also scan any pages linked from the root page. Setting the depth to two causes the scanner to also scan any pages linked from those pages, etc.

HTTP Limit (`http_limit`)

Default 10000 (Maximum number of pages); 0 - Unlimited. This option compliments the `spider_depth` setting to prevent scans from taking excessively long on sites that have many pages. In these cases, it is useful to limit the total number of pages scanned, in addition to controlling the depth. To limit the total number of pages scanned on each target, set the web page limit to the desired maximum number of pages. After the scanner has run the specified number of instances of `http.saint` and `https.saint` against a target, it will complete the scan and produce a warning message in the scan's status file to inform you that some pages weren't scanned. To allow an unlimited number of pages to be scanned, set this value to 0.

HTTP Form Limit (`http_form_limit`)

This setting is similar to the HTTP Limit described above, but limits the number of forms instead of the number of pages. To limit the total number of forms scanned on each target, set the limit to the desired maximum number of forms. After the scanner has run the specified number of instances of `http_form.saint` and `https_form.saint` against a target, it will complete the scan and produce a warning message in the scan's status file to inform you that some forms weren't scanned. The default is 10000. To allow an unlimited number of forms to be scanned, set this value to 0.

HTTP Delay (http_delay)

This setting specifies the number of milliseconds to wait between HTTP requests. The default is 0, meaning each HTTP request should begin as soon as the previous request is finished. This is typically the desired behavior since it minimizes the scan time. However, increasing this value may help if the default value causes a target to crash or become unresponsive.

Note that this setting only controls the delay within each probe instance, but there could be multiple probes making HTTP requests concurrently. To achieve the gentlest possible scan, also set the **Maximum Threads** to 1 to prevent probes from running concurrently.

HTTP User Agent (http_user_agent)

This setting specifies the User-Agent header to include in most HTTP requests. The default setting resembles the User-Agent header sent by a typical web browser, to make it appear to the target that SAINT's checks are coming from a real browser. However, it may be useful to change this in some cases. For example, some web application firewalls may allow you to whitelist custom HTTP headers, thus allowing a scan to proceed without interference.

Note that some vulnerability checks must use specific User-Agent headers in order to work as designed. These checks ignore this setting and always use the User-Agent header which allows the check to work.

Crawl Dynamic Content (crawl_dynamic_content)

In the early days of the World Wide Web, most web sites served static HTML content, which could be easily parsed by scanners to find links to other resources. However, modern web applications typically serve pages containing some amount of dynamic content. That is, in some cases the browser executes script embedded in the web page to create page elements, send data to and from the server, or handle mouse clicks and other user actions.

The Crawl Dynamic Content setting tells the scanner to execute the script embedded in each web page, as a web browser would do when loading the page. The scanner then records any HTTP requests which are triggered by the script execution, which may identify additional web resources, leading to improved vulnerability detection. However, since script execution takes time, enabling this option may slow down the scan. If this setting is disabled, embedded script

is not executed, but the scanner will still attempt to find links to other resources by parsing the static content.

Clicks Per Page (max_clicks_per_page)

In some cases, simply executing the embedded script as a browser would do when loading a page is insufficient for finding web resources. There could be some content which is only exposed after certain events such as mouse clicks. To ensure that the scanner finds such content, it needs to take it a step further and simulate the mouse clicks which would occur in a browser.

The Clicks Per Page setting specifies the maximum number of elements per web page on which to trigger a click event, if dynamic content crawling is enabled. Higher settings may uncover more web resources but may take more time. A value of zero disables the simulation of mouse clicks, but still allows the initial script execution on each page.

Dynamic Content Timeout (dynamic_content_timeout)

When dynamic content crawling is enabled, there could be situations where the scanner encounters script which takes a long time to run or gets stuck in an endless loop. The scanner aborts the script in this situation, to avoid slowing down the scan. The Dynamic Content Timeout setting specifies the number of seconds that the script is allowed to run on each page before execution is aborted.

Web Program Dirs (cgi_dirs)

The default web program directories are `/cgi-bin/` and `/scripts/`. This setting defines the set of standard web directories to scan that typically contain programs. These directories are specified in a comma-separated list. Each directory should start with a leading slash and end with a trailing slash.

Web Dirs to Skip (cgi_dirs_skip)

Default: blank – SAINT allows you to specify directories not to scan. This option is useful if a certain part of the web site should not be included in the scan. These directories are specified as a comma-separated list, and each directory should start with a leading slash. Each web page found during web crawling will be compared with every item on this list using a case-insensitive

comparison starting from the beginning, and if there is a match then the page is omitted from the scan.

Software Inventory

Setting this option ensures all scan policies include probes that retrieve a list of software installed on Windows-based targets. This configuration requires that applicable scan Jobs be defined with Windows Domain credentials (Step 4 in Job setup) or credentials to the targets have been previously defined in the Credentials Manager. The resulting software inventory can then be found in the Vulnerability List section of the Full Scan or Overview reports. Note that the software list is generated by enumerating the Uninstall key in the Windows registry. Therefore, only software registered with the operating system during installation will be included. Software placed on the system without running an installer program is typically omitted. Also, note that registered software incorrectly removed from the target system may still be included in the list after removal, due to orphaned registry keys.

Load Balancing

This setting specifies whether or not to run load balanced scans. With this option, the scan targets will be divided evenly among the available nodes, and the scan will be queued until at least two nodes are available. The minimum number of nodes and the set of nodes among which to run the scan can be customized when [creating the scan job](#).

This option can be overridden when creating the scan job.

Mobile Device Timespan

This setting affects the [mobile device](#) scan policy.

By default, a scanner deployed into an internal environment queries Active Directory servers for information about Exchange ActiveSync devices which have been changed in the past year, and uses that information to infer vulnerabilities on those devices. The default setting is intended to avoid reporting on many retired devices. However, this setting allows you to change the default time span to expand the search to include less frequently changed devices, or to limit it to more recently changed devices. Note that mobile device scanning requires Windows domain administrator credentials and the Active Directory server's SSL certificate. See [Authenticating to Windows Targets](#) for more information.

To change this setting, enter the new time span in days. Note that the last change date for a device is usually older than the last sync date.

Vulnerability Check Flags (vuln_check_flags)

This setting allows you to modify the behavior of certain vulnerability checks. It is a comma-separated list of one or more of the following options:

- `internalnetinfo_strict` – When checking for internal network information disclosure in SSL certificates, report the vulnerability for any internal IP address, with no exceptions. Without this flag, an exception is made for 192.168.168.168 since this is commonly used in default certificates and doesn't usually correspond to the real IP address.

Local Checks in Containers (internal_container_scan)

When SAINT runs a credentialed scan of a Linux target which hosts Docker or LXC containers, it enumerates the running containers and lists them as an informational item in the scan results. If this setting is enabled, it will go a step further and run local vulnerability checks inside of each running container. Each container will appear in the scan report as an additional host which was scanned, with the container name as the host name. This helps distinguish the vulnerabilities found in the container from the vulnerabilities found on the host itself. (It will not count as a separate target for licensing purposes.) Note that findings that come from scanning exposed container ports will still appear as if they are on the host, since it is the host which is exposing those ports.

Port

SAINT's portscan and vulnerability scan levels always include a TCP and UDP port scan. These port scans are important to the scan because their results usually determine which of SAINT's vulnerability checks to run.

Port scanning is pre-configured to cover two scopes: "heavy" and "common;" each of which can be controlled in the following settings. Ports included in a heavy port scan generally include a wide range of TCP and UDP ports, which is useful for detecting services running on either common ports or non-standard ports. The common ports include only commonly used ports, and is useful for quickly detecting services running on common ports. The port scan level setting controls which of the above two lists to use for the port scan.

Heavy TCP Ports (heavy_tcp_ports)

The ports included in heavy port scan generally include a wide range of TCP ports, which is useful for detecting services running on either common ports or non-standard ports.

Common TCP Ports (common_tcp_ports)

The common ports include only commonly used ports, and is useful for quickly detecting services running on common TCP ports. The Port scan level setting controls to use for the port scan.

Heavy UDP Ports (heavy_udp_ports)

The ports included in heavy port scan generally include a wide range of UDP ports, which is useful for detecting services running on either common ports or non-standard ports.

Common UDP Ports (common_udp_ports)

The common ports include only commonly used ports, and is useful for quickly detecting services running on common UDP ports. The Port scan level setting controls to use for the port scan.

SSH and Registry Ports (auth_test_ports)

This option allows you to specify the ports that the remote registry and SSH services run on in your network, by default this is '22,139' and for the most part you will not need to change port 139. If you run SSH on a non-standard port (other than 22) specify it here.

Use Heavy port ranges (allports)

Defines which TCP port scan list to use.

Allports (0 - common TCP ports; 1 - Heavy TCP Ports)

OS Type Ports (ostype_ports)

If the scan uses NMAP for TCP port scanning (see TCP options) and the Nmap Flag settings include the -O flag, then Nmap tries to determine the host type of each target during the TCP port scan. This takes advantage of the full port scan results to increase its chances of finding at least one open and one closed port, which improves the reliability of the host type guess. In all

other cases, SAINT uses Nmap and Xprobe2, if installed on the scanning platform, to determine the host type of the target by scanning a small number of ports. This port scan takes place in the `ostype.saint` probe, separately from SAINT's regular port scans executed by the `tcpscan.saint` and `udpscan.saint` probes.

The `ostype` configuration settings enable you to change the port numbers which are scanned for host type detection. By default, services which typically run from the Internet services daemon (`inetd`) are omitted because Nmap could reportedly crash some older implementations of `inetd`, so the ports to use at the heavy-plus level is set separately to include those ports.

Password

Security Suite includes checks for password policies for Windows targets. The password policy refers to the rules on the target system designed to enforce good password security practices.

The scanner attempts to identify login account names using finger and rusers on Unix systems, and netbios requests on Windows systems. For each login account name that the scanner identifies, it then checks each account to find out whether or not its password can be guessed.

NOTE ABOUT THE PCI SCANNING POLICY

Although password policy settings can be customized through this option, SAINT's PCI scanning policy setting are pre-defined for the following configurations based on the specified PCI DSS requirement:

- *DSS 8.5.9 - Change user passwords at least every [x] days.*
- *DSS 8.5.10 - Require a minimum password length of at least [x] characters.*
- *DSS 8.5.12 - Do not allow an individual to submit a new password that is the same as any of the last [x] passwords he or she has used.*
- *DSS 8.5.13 - Limit repeated access attempts by locking out the user ID after not more than [x] attempts.*

*The **length** refers to the number of characters in the password. Longer passwords are generally considered to be more secure than shorter passwords. **History** refers to the number of previous passwords which cannot be re-used. This prevents a user from defeating a password change requirement by re-using the same few passwords over and over again. **Maximum age** and **minimum age** refer to the range of days over which a password must remain before being*

changed again. The maximum age requires a user to change his or her password periodically, whereas the minimum age ensures that the user cannot defeat the password change requirement by immediately changing the password back to what it was before. Lockout refers to the number of failed login attempts which are allowed. After this number of failed attempts is surpassed, the account is disabled for a period of time to prevent brute-force password guessing attacks.

Password Guesses (password_guesses)

The number of guesses to try against each account is limited by the Password Guesses configuration setting.

- The default is two guesses.
- A value of zero (0) will disable password guessing. Any other value instructs the scanner to try the specified number of strings starting from the top of the list of password guesses.

Note that some systems lock out accounts after a set number of failed login attempts, usually three or greater. Setting *Password Guesses* higher than the default value of 2 will cause account lockouts on such systems, which could be a major inconvenience for the administrators and users of those systems.

First Guess – Fifth Guess (guess settings)

There are two ways the passwords guesses can be specified. The first option is to modify the Password Guess settings for each guess. SAINT supports up to 5 guesses. The default list of password guesses is:

1. (null password)
2. %l (password same as login name)
3. password (the word "password")
4. %b (login name backwards)
5. %l1 (login name followed by the digit "1")

Password Dictionary (password_dictionary)

The Dictionary option is the second option, which allows a more thorough password assessment. To use this option, type or paste a list of password strings, separated by line

breaks, into the text box, or click on the folder icon to populate the text box with one of the built-in password dictionaries. This option overrides the [First Guess through Fifth Guess](#) settings. All of the strings in the file are tried against each account, regardless of the [Password Guesses](#) setting.

Password Delay (password_delay)

If more than two guesses are desired, the Password Delay option can help you avoid lockouts by separating the login attempts by a specified number of seconds. Set the delay greater than the lockout counter resets time, in seconds. Note that using this setting with a dictionary attack could result in a scan which takes a very long time to complete.

Password Policy Length (pwpolicy_length)

This option allows you to customize the password policy checks to assess a target against your defined minimal string length. If a target system does not enforce a policy that is at least as strict as the specified settings, then a vulnerability is reported. Note that authentication is typically required in order to perform these checks.

Password Policy History (pwpolicy_history)

This option allows you to customize the password policy checks to assess a target against your defined value for the number of previous passwords that can't be re-used. If a target system does not enforce a policy that is at least as strict as the specified settings, then a vulnerability is reported. Note that authentication is typically required in order to perform these checks.

Password Policy Max Age (pwpolicy_max_age)

This option allows you to customize the password policy checks to assess a target against your defined value for the maximum number of days a user is permitted before changing their password. If a target system does not enforce a policy that is at least as strict as the specified settings, then a vulnerability is reported. Note that authentication is typically required in order to perform these checks.

Password Policy Min Age (pwpolicy_min_age)

This option allows you to customize the password policy checks to assess a target against your defined value for the minimum number of days before a user is permitted to change their password. If a target system does not enforce a policy that is at least as strict as the specified

settings, then a vulnerability is reported. Note that authentication is typically required in order to perform these checks.

Password Policy Lockout (pwpolicy_lockout)

This option allows you to customize the password policy checks to assess a target against your defined value for the number of failed attempts before password lockout. If a target system does not enforce a policy that is at least as strict as the specified settings, then a vulnerability is reported. Note that authentication is typically required in order to perform these checks.

E-mail Notifications

These configuration options support sending e-mail messages and content when scanning is completed. This configuration setting defines default mail server settings, addressing and content templates to be used for all scan jobs. E-mail notification settings can also be defined locally, at Job setup time, based on job-specific workflows.

Send Email (send_email)

The value is flag to define whether e-mail notifications are permitted for scan jobs.

Send_email (1-Yes; 0-No)

Mail Server (mail_server)

This configuration field stores the IP address of a mail relay server. If this option is left blank, the alert will be sent directly to the mail server for the recipient's e-mail domain. If that server cannot be resolved or reached for some reason, then an IP address for a mail relay server can be specified. If it is specified, then alerts will be sent through that server.

From Email (from_email)

This field stores the "from" e-mail address. If not value is specified, the default "From" e-mail address is root at the domain of the local host.

From Email Display Name (from_email_display_name)

You may also specify the default display name for the "from" e-mail address. The default display name is "SAINT".

Email Trend Length (email_trend_length)

Trend analysis reports will analyze and report the last one to ten data sets, or all data sets. The default trend value for e-mailed reports can be set in this field. The default value is zero.

Email Attachment Name (attachment_name)

Enter a default attachment name for attachments, if applicable. For example, "SAINT Scan Result".

E-mail Group Settings

These settings define the parameters for each e-mail you wish to execute at the conclusion of scan jobs. Each e-mail can include multiple comma-separated addresses.

- Email Address (E-mail_address) - You must provide one or more e-mail addresses to which the message will be sent.
- Send Report (Send_report) – Select the report template to be used for the e-mail group. For example, Executive Report.
- Report Format (Send_report_format) – Select the format of the report to be sent. For example, PDF.
- Note that since the HTML and Frameless HTML report formats are made up of multiple files, these reports are sent in a tar archive. To view the results from the mail client, extract the files and view index.html in a browser.
- Report Attachment Name (Send_report_attachment_name) – Enter a default attachment name. For example, "Last PCI Scan results".
- Report Subject (Send_report_subject) – Enter a default report subject for the e-mail group. When the subject is "default," the subject of the e-mail will be "Your SAINT scan has finished for session: <your job>."

File Content Search

File content checking, if enabled (default is Off), scans file systems or web sites to locate potentially sensitive information, such as credit card numbers, U.S. social security numbers, Mexican CURP codes, Canadian social insurance numbers, and default passwords. Report output for these types of results will then provide guidance, (e.g., result output, location, row number) for investigation and remediation. This capability also includes features to identify files and file types (e.g., .avi, .mp3), and find files of interest by matching their names as well as their contents, and potentially speeding up the (often lengthy) search process by quickly skipping

files known to be either safe (whitelist) or suspicious (blacklist) by their names alone. These configuration settings also include directories that should not be scanned or descended into, file types/extensions to search through, Perl style regular expressions used to match file content to, and a timeout value that sets the maximum scan time.

Note: This feature requires that the kernel supports the cifs filesystem. To determine this, you can do a `cat /proc/filesystems` and look for the word `cifs`.

FCS Enabled (`fcs_enabled`)

Default: Off. Set this field to On to enable file content scanning on the target's file system for the patterns specified by [FCS Objective](#). Authentication is required when using this option.

`Fcs_enabled` (0-Off; 1-On)

WCS Enabled (`wcs_enabled`)

Default: Off. Set this field to On to enable web content scanning. Use this option to search the content of web pages for the patterns specified by [FCS Objective](#) over HTTP or HTTPS. If both FCS and WCS are enabled, content scanning will be performed both on the file system and over HTTP or HTTPS.

Apply Luhn to Custom Patterns (`fcs_apply_luhn_to_custom_patterns`)

Default: Off. Set this field to On to enable application of the Luhn algorithm to custom search patterns for FCS on Windows and *NIX, and for WCS. The Luhn algorithm is a simple checksum formula used to validate a variety of identification numbers, including most credit card numbers. The Luhn algorithm is already applied to search results that match the PCN and Canadian CIN numbers FCS objectives. To enable custom search patterns, the pattern should be entered in FCS Patterns and the FCS Objective should be empty or contain 'custom'.

FCS Dirs to Skip (`fcs_disabled_dir`)

This configuration field contains target directories that are to be excluded for file content scanning. List all excluded directories here as a comma separated list.

This option only affects the file content search, not the web content search. Use the [Web Dirs to Skip](#) option if you wish to control which directories are included in the web content search.

FCS File Types (fcs_file_types)

This field contains the files and file types (e.g., .avi, .mp3) to be included in the file content scans on Windows systems by matching their names as well as their content. This option only affects the file content search, not the web content search.

FCS Patterns (fcs_patterns)

This field defines the file content patterns used in content scan probes if the *custom* keyword is present in [FCS Objectives](#), or if FCS Objectives is empty. SAINT's content scanning engine uses Perl regular expressions to perform these pattern searches. The default content scan parameters include patterns for common strings such as credit card data, social security numbers and others, as described above. Additionally, other patterns may also be included to support scanning for content that meets local needs. For example, patterns that match student IDs or patient IDs in publicly accessible systems that may expose sensitive information and should be identified and removed. The following illustrates one example of a complex pattern typical of this type of content:

`\b\d{4}-[A-Z]{2}-AA\d{4}\b` – pattern that matches a string that includes a combination of numbers, dashes and letters, as in an example student identifier of 2014-CS-AA0004

Use a Pipe (|) separator to append the additional pattern into the default string parameters:

`\b[1-6](?:\d[-]*){12,15}\b|\b\d{3}[-]+\d{2}[-]+\d{4}\b|\b\d{4}-[A-Z]{2}-AA\d{4}\b`

Blacklist Filename Regex (fcs_blacklist_filename_regex)

Enter file names in this field to define specific files that are known to be suspicious (blacklist) by their names alone, and should be included in content scan results, regardless of their content. Defining specific files can help focus scans and potentially speed up scan duration that can often be lengthy, based on target lists and content size.

FCS Whitelist Filename Regex (fcs_whitelist_filename_regex)

Enter file names in this field to define specific files that are known to be safe (white list) by their names alone, and should be excluded in content scan results, regardless of their content.

Defining specific files can help focus scans and potentially speed up scan duration that can often be lengthy, based on target lists and content size.

FCS Whitelist Reverse Effect (fcs_whitelist_reverse_effect)

Default: No. Checking this box reverses the affect of the white list scans, to ensure white listed files are included in content scanning.

Fcs_whiltelist_reverse_effect (0-No; 1-Yes)

FCS NIX File Types (fcs_nix_file_types)

This field contains the files and file types (e.g., .avi, .mp3) to be included in the file content scans on *NIX systems by matching their names as well as their content. This option only affects the file content search, not the web content search.

FCS Objective (fcs_objective)

This option specifies the type of information for which to search when FCS or WCS is enabled. It should be a comma-separated list of case-sensitive keywords without any spaces. The recognized keywords are as follows:

- PCN – Payment Card Number
- USA_SSN – USA Social Security Number
- CAN_SIN – Canadian Social Insurance Number
- MEX_CURP - Mexican CURP Code - unique identity code for both citizens and residents of Mexico
- custom – Patterns found in [FCS Patterns](#) setting

Machine Search Timeout (machinsearch_timeout)

Timeout value (in seconds) that sets the maximum scan time.

Anti-virus

Anti Virus Max Days Old (av_days_old)

Number of days since last run that anti-virus scans should be considered out-of-date?

TCP

Firewalls present some complications that require special attention by SAINT's TCP port scans. Therefore, a number of options have been created to help effectively scan through firewalls. Since some ordinary targets may have firewalls enabled by default, these options are used in all scans. However, they should only be changed if it is necessary to fine-tune the scanner for unusual firewall environments.

If Nmap is being used for your port scan and you wish to tune the port scan parameters, see the `use_nmap_tcp` configuration setting. The `fw_timeout` and `fw_loadlimit` and `fw_delay` options are only observed if Nmap is not available or the `use Nmap` option is not set, and possibly for some auxiliary port scans which use SAINT's native TCP scanner.

When using Security Suite for TCP port scans and modifying these values, keep in mind that the overall TCP port scan timeout (`fw_timeout`) may need to be modified accordingly. The scan engine calculates the maximum amount of time which the TCP port scan may require based on the current settings, and sets the overall port scan timeout to this value when the scan begins.

Secs Before Dropping Connection Req (`fw_timeout`)

This value defines the number of seconds before dropping connection requests. This allows the scanner to retry or give up on ports that are blocked by a firewall after a few seconds rather than hanging on them indefinitely. While the port scan proceeds, the scanner will measure the response time for any open ports it finds, and use those measurements to dynamically adjust the timeout setting to maximize performance.

Max Concurrent Requests (`fw_loadlimit`)

This value defines the maximum number of concurrent connection requests. This prevents the scanner from overloading the system with waiting connection requests.

Seconds Between Ports (`fw_delay`)

This value specifies the number of seconds to wait between each port during TCP port scans. It is usually only necessary to raise this when scanning through a firewall which detects port scans above a certain threshold and blocks further connections from the scanning host.

Note that this setting only controls the delay used during the port scan phase of the scan. If you also need to introduce a delay between HTTP requests in the later phases, see [HTTP Delay](#).

TCP Port Limit (tcp_port_limit)

This value specifies the maximum number of TCP ports we expect to find open on any target. If greater than this number of open TCP ports are detected, the port scanner assumes the ports aren't really open unless their output differs from the rest of the ports. This is useful for reducing false positives when a firewall is present which intercepts and accepts many or all TCP connection requests destined for the target.

UDP Timed-out Port Limit (udp_timedout_port_limit)

Due to the nature of the UDP protocol, UDP port scanners often can't distinguish between open ports and filtered ports, leading to false positives. To mitigate this, SAINT's UDP port scanner assumes that if many consecutive scanned ports time out, it's more likely that they're all filtered than open, so it doesn't report them. This value specifies the number of consecutive timed out UDP ports after which SAINT will make this assumption. If more than this many consecutive ports (from the list of ports being scanned) time out, then the ports aren't reported in the scan results.

Use NMAP TCP (use_nmap_tcp)

Nmap offers many advantages over SAINT's native port scanner, including support for SYN scans, advanced timing algorithms and additional configuration options. The performance benefits are also achieved when scanning through firewalls. Therefore, SAINT enables you to use Nmap for the main TCP and UDP port scan components of the vulnerability scan. SAINT's built-in scan engine will be for TCP port scans if this box is not checked..

Use_nmap_tcp (0-No; 1-Yes; Default: Yes)

Use NMAP UDP (use_nmap_udp)

Setting value to Yes uses NMAP for UDP scans.

Use_nmap_udp (0-No; 1-Yes.; Default: No)

NMAP for TCP Ports to scan (nmap_flags_tcp)

The Nmap TCP flag setting specifies the command-line arguments which are passed to Nmap for TCP port scans. These arguments allow you to control the scan type, timing aggressiveness, and more. Note that you do not need to specify the port range here. SAINT does that for you.

NMAP for UDP Ports to scan (nmap_flags_udp)

The Nmap UDP flag setting specifies the command-line arguments which are passed to Nmap for UDP port scans. These arguments allow you to control the scan type, timing aggressiveness, and more. Note that you do not need to specify the port range here. SAINT does that for you.

Max Connections Per Port (fw_count)

Default: 2 – Occasionally, due to problems or congestion on your network or the target's network, there may be some amount of packet loss during the scan. If a connection request to an open port is lost, then SAINT could miss the port. To mitigate this problem, it may be desirable to retry the connection for ports which do not respond. This option defines a maximum number of connection attempts and specifies the number of times SAINT should try to connect to each port in the event that there was no response to any previous attempts on that port. Since high numbered ports are less likely to be open than low numbered ports, it might not be worth the time it takes to retry the connection on every port.

Note: If Nmap is being used for your port scan and you wish to tune the port scan parameters, see the use_nmap_tcp configuration setting. The fw_count is only observed if Nmap is not available or the use Nmap option is not set, and possibly for some auxiliary port scans which use SAINT's native TCP scanner.

Retry Upon Timeout (fw_retry_port_max)

If Nmap is being used for your port scan and you wish to tune the port scan parameters, see the use_nmap_tcp configuration setting. The fw_retry_port_max is only observed if Nmap is not available or the use Nmap option is not set, and possibly for some auxiliary port scans which use SAINT's native TCP scanner.

Authentication

Use NTLMV2 (use_ntlmv2)

Microsoft Windows operating systems implement a number of different authentication protocols. In its default configuration, the system accepts both the older and the newer protocols. However, some targets may be configured to accept only NTLMv2 authentication, or equivalently, have the LMCompatibility registry setting set to level 5. To successfully authenticate to these targets, enable NTLMv2 authentication.

Use_ntlmv2 (0-No; 1-Yes; Default: No)

Workstation Name (workstation_name)

This value specifies the NetBIOS name to use for the SAINT host when authenticating to Windows targets.

Allow Insecure LDAP

This setting configures the scanner to allow unencrypted LDAP authentication. This should only be enabled if an Active Directory scan is needed (e.g., for the [mobile device](#) scan policy) and SSL is not enabled for the LDAP service or the SSL certificate is unavailable, and you wish to accept the risk of using insecure authentication. See [Authenticating to Windows Targets](#) for more information.

Cookie Lifetime (cookie_lifetime)

When you record your [web application credentials](#) using the standard or advanced authentication proxy, two things are saved: the authentication cookies for the current login session, and the HTTP requests which were used to establish that session. The latter can be used to generate a script which repeats the authentication steps and generates new cookies. This is useful in scans scheduled to run in the future, when the original cookies may have expired.

Whether to use the cookies saved by the proxy or to run the script which generates new cookies depends on the age of the scan job as compared to the Cookie Lifetime setting. This setting specifies the amount of time the cookies saved by the proxy can be considered valid, in minutes. If a scan begins before this amount of time has passed since the job was created, the

original cookies are used. Otherwise, the script will repeat the authentication steps to generate new cookies.

Ephemeral Encryption Key (use_ephemeral_cred_key)

When you enter default credentials during the authentication step of the scan job wizard, those credentials are encrypted using an AES-256 encryption key. Either of two different encryption keys can be used for this purpose: a permanent key which is stored on disk, or an ephemeral key which is stored only in the manager's memory. The default is to use the permanent key. That allows the scan to use the original credentials every time it runs, even for recurring scans and scans that run in the future. However, using the permanent key may be undesirable in some cases, such as when the local security policy requires encryption keys to be isolated from the data they are used to encrypt.

When the *Ephemeral Encryption Key* option is checked, the credentials are encrypted using the ephemeral key which is stored only in the manager's memory. This mitigates the issues surrounding storage of the encryption key on disk. However, the credentials will not be available after the manager restarts. Therefore, it is not a useful option for credentialed scans which run in the future.

Note that this option only pertains to default credentials which are stored with scan jobs, not to credentials stored in the [Credentials Manager](#).

Network Information

Target Netmask (target_netmask)

To test whether a host could be an amplifier for a smurf or fraggle attack, the scanner needs to know its network and broadcast addresses. On a Class C subnet, which is the most common type, the first three octets of these addresses are the same as the host's IP address, and the fourth octet is 0 and 255, respectively. In the general case, the network address is determined by setting all of the *host bits* (the bits *not* included in the netmask) to 0, and the broadcast address is determined by setting the host bits to 1.

By default, 255.255.255.0, 255.255.255.128, and 255.255.255.192 are all used as netmasks in the smurf and fraggle checks. If you know that your target network uses a different netmask, change the *Netmask* setting to the target's netmask. Be sure you know what you are doing if

you go below 255.255.255.0 (e.g. 255.255.254.0), or you could potentially scan a Class C network other than your own.

SNMP Communities (snmp_communities)

The Simple Network Management Protocol (SNMP) runs on routers and switches, as well as some printers, servers, and workstations, for the purpose of communicating configuration and status information. SNMP access is controlled using *communities*. A *community string* identifies the community, and can be thought of as the password for SNMP access.

SNMP access to targets is helpful because it provides configuration information that could be used for improved host type detection and vulnerability detection. The *SNMP Community Strings* configuration setting is a comma-separated list of community strings that the scanner uses to gain SNMP access. If the community strings on the targets are known, they should be placed in this variable. It is not necessary or recommended to include default strings such as "public" and "private". Passing these values is considered a security vulnerability in and of themselves, and the scanner already checks for them.

Performance Consideration: Each string listed in the SNMP community strings setting is tried for every SNMP-enabled target that is scanned. Thus, very long lists of strings may take more time and could cause the SNMP probe to time out. For improved efficiency, community strings which exist only on a certain device should be specified in the config/SNMP_communities.pl file instead of here. See that file for examples.

Process Control

Configuration settings in this section control various performance settings that affect the overall performance of SAINT probes and processes. These include probe timeout values and the number of open threads used for concurrent scanning of targets.

Timeout (timeout)

Default: (1) – Medium. Certain network probes will "hang" or continue to try to contact the remote host for a very long time with no response. To prevent this from slowing down the overall scan, each probe is run with a timeout value which tells the probe to terminate itself after the specified time period has elapsed. There are 4 timeout values, measured in seconds that can be controlled globally or at job setup time: Short, Medium, Long, and Extra Long

(default values defined below). By default, all SAINT probes are launched with the same timeout value, which is either the slow timeout, the medium timeout, or the fast timeout, except for a few probes which require more time, and are defined in other settings below. Which timeout to use is specified by using the setting defined globally or at Job setup. For example, if the selected timeout values are 15 (short), 30 (medium), 45 (long) and 60 (extra long), and the selected timeout is Medium, then all SAINT probes would be allowed 30 seconds to run, except for some of the longer probes which may be allowed 120 seconds or more.

When editing these settings, beware that reducing timeout values could lead to missed vulnerabilities. Timeouts are only intended to be used as a safeguard against hung probes preventing scan completion. Setting them too low could result in terminating probes which aren't hung, in which case one or more checks may never be executed, leading to unreliable results. To prevent this from happening, the scan engine will raise the timeout settings to the minimum acceptable value if you attempt to set them too low.

Short Timeout (short_timeout)

Default value: 30 seconds

Medium Probe Timeout (med_timeout)

Default value: 75 seconds (Default setting)

Long Timeout (long_timeout)

Default value: 180 seconds

Extra Long Timeout (extra_long_timeout)

Default value: 450 seconds

Max Threads (maximum_threads)

To increase the speed of a scan, SAINT scanners can run more than one probe at a time. The maximum number of probes that will run at a time is controlled by this setting. This value should be low for machines which are overloaded or which do not have much memory, but can be set higher to achieve faster scans on machines which have the resources available. Be careful with this value, because a value which is too high could cause the scanner to quickly use up large amounts of memory.

- The default setting is 0, which causes SAINT algorithms to choose an optimal value between 1 and 20 for each scan based on the processor speed and amount of available memory.
- To disable multitasking entirely, set this value to 1.

HTTP Connection Timeout (http_connection_timeout)

SAINT's HTTP and HTTPS probes include many checks, each of which establishes one or more individual connections to the target. The HTTP Connection Timeout setting specifies the number of seconds after which to close each connection if no response is received from the target. The default is 10 seconds. This setting allows you to tune your website scans with greater precision than you could using the overall probe timeouts discussed below. As with the overall probe timeouts, however, this setting is intended only to prevent hung connections from causing delays, and setting it too low could lead to missed vulnerabilities.

Individual Probe Timeouts

Due to the special nature of the TCP and UDP port scans, the timeout values for these probes are handled differently from other probes. The TCP port scan timeout is calculated during each scan based on the number of ports being scanned and the TCP port scan settings. Also, SAINT provides the capability to control the UDP port scan timeouts separately from other timeouts. For UDP port scans, it is a good idea to raise this value on slow networks to ensure that all open ports are detected, especially when using custom scan levels specifying more than the usual number of ports.

Other probes, such as the HTTP probe, SNMP probe, and NFS probe, also require more time. For this reason you can override the default timeout for any probe in the session configuration file. For example:

- HTTP Timeout (`http_timeout`) = 180;
- NFS Timeout (`nfs_chk_timeout`) = `long_timeout`;
- SNMP Timeout (`snmp_timeout`) = `extra_long_timeout`;

In this case, the timeout value for the *HTTP* probe is 180 seconds and the timeout value for the *nfs-chk* probe is equal to `$long_timeout`, which is the *Slow* timeout discussed above. The timeout value for the *snmp* probe is equal to the value of `$extra_long_timeout`, which is set in the session configuration file. The timeout value for any probe can be overridden by defining a new variable which is *probename_timeout*, where *probename* is the name of the probe (with dashes, if any, replaced by underscores).

As discussed above, when editing these settings, beware that reducing timeout values could lead to missed vulnerabilities. Setting them too low could result in terminating probes which aren't hung, potentially causing checks to be skipped. To prevent this from happening, the scan engine will raise the timeout settings to the minimum acceptable value if you attempt to set them too low. When editing the HTTP/HTTPS and HTTP/HTTPS Form timeouts, note that the HTTP Connection Timeout discussed above may be a better option than changing the overall probe timeouts.

Each of the probe timeout configuration options available for configuration globally or at job setup time include are listed below: are shown below:

- UDP Scan Timeout (Udpscan_timeout)
- NFS Timeout (Nfs_chk_timeout)
- SNMP Timeout (Snmpp_timeout)
- Smurf Timeout (Smurf_timeout)
- HTTP Timeout (http_timeout)
- HTTPS Timeout (https_timeout)
- HTTP Expect Timeout (http_expect_timeout)
- HTTPS Expect Timeout (https_expect_timeout)
- SMB Timeout (smb_timeout)
- Finger Timeout (finger_timeout)
- Win Login Timeout (win_login_timeout)
- Default Login Timeout (default_login_timeout)
- SSH Default Login Timeout (ssh_default_login_timeout)
- Telnet Timeout (telnet_timeout)
- TFTP Timeout (tftp_timeout)
- MSSQL Timeout (mssql_timeout)
- OS Type Timeout (ostype_timeout)
- DHCP Timeout (dhcp_timeout)
- Backupexec Timeout (backupexec_timeout)
- Win File Check Timeout (win_filechk_timeout)
- SSH Login Timeout (ssh_login_timeout)
- Win OVAL Check Timeout (win_ovalchk_timeout)
- Sovaldi Timeout (sovaldi_timeout)
- SXCCDFI Timeout (sxccdfi_timeout)
- SQLPLUS getsid Timeout (sqlplus_getsid_timeout)

- HTTP Form Timeout (`http_form_timeout`)
- HTTPS Form Timeout (`https_form_timeout`)
- FTP Default Login Timeout (`ftp_default_login_timeout`)
- Dictionary Login Timeout (`dictionary_login_timeout`)

Results

The following settings control what is done with the data after the scan completes, such as sending it to syslog or exporting it to other products.

Export Results to Splunk

Select this checkbox to automatically transmit all scan results to the Splunk installation configured in System Options. (See [Systems Options/Splunk](#)).

Export Results to Cisco FireSIGHT

Check this box to export the results to Cisco FireSIGHT automatically when the scan completes. The Cisco FireSIGHT settings must be properly configured in order for the export to succeed. (See [System Options/Cisco FireSIGHT](#).)

Syslog Level (`syslog_level`)

Besides receiving your scan results by e-mail, you may also wish to have your results sent to syslog. This has the advantage of allowing vulnerability alerts to be routed to the appropriate system through an existing syslog facility. When this option is enabled, your results will be sent to syslog when the scan finishes. Using this feature requires the syslog daemon already to be running on the host running Security Suite.

Options for sending scan output to syslog, and to indicate which events you would like to be logged, are as follows:

- Do not send results to syslog
- Log critical problems only
- Log critical problems and areas of concern
- Log all vulnerabilities
- Log all vulnerabilities and services

`Syslog_level` (Default: 0-do not send results to syslog; 1-critical problems only; 2-critical problems and areas of

concern; 3-all vulnerabilities; 4-all vulnerabilities and services

Syslog Format (syslog_format_type)

This setting controls the format of the syslog message. There are two options. The first option, *Custom Format*, allows you to specify your own message format. See [Syslog Custom Format](#) for further information. The second option, *LEEF*, can be used to export scan results to IBM QRadar via the syslog facility upon scan completion. Once exported, the scan results can be monitored in QRadar along with the rest of your organization's security events. If *LEEF* is chosen, the system's syslog function should be configured to send logs to QRadar for the facility and priority selected in the following options.

Syslog Priority (syslog_priority)

The priority is one of two syslog parameters used to determine how syslog handles the events. Valid values are as follows:

- emerg
- alert
- crit
- err
- warning
- notice (default)
- info
- debug

Syslog Facility (syslog_facility)

The facility is another syslog parameter used to determine how syslog handles the events. Valid values are as follows:

- auth
- security
- user (default)
- local0-local7

Syslog Custom Format (syslog_format)

The syslog entry format determines the format of the log messages. Each message will appear as specified, with keywords (e.g., “target”) replaced by the corresponding data. Possible keywords are: job_id, scan_id, session, target, service, severity, tutorial, text, cve, id, max_cvss, pci_compliance. This setting is only used if the Syslog Format setting above is set to *Custom Format*.

Save Files on Node When Finished (save_files_on_finish)

This setting determines whether the scan data, status file, and verbose output file are kept on the scan node after the scan finishes. It generally isn't necessary to keep these files on the node after the scan finishes, but they could be helpful for troubleshooting. If this box is checked, the files are saved permanently on the node. Otherwise, they are removed after they have been sent to the manager.

Save Files on Node When Stopped (save_files_on_stop)

This setting determines whether the scan data, status file, and verbose output file are kept on the scan node if the scan is stopped. If this box is checked, the files are saved permanently on the node. Otherwise, they are removed when a scan is stopped. *Warning:* This box must be checked in order for the scan to be resumed after it is stopped.

SCAP Configurations***Oval Results Format (oval_results_format)***

This configuration defines the system characteristics retrieved from OVAL scans.

```
Oval_results_format (0-No system characteristics; 1-System
characteristics (default); 2-Thin results)
```

XCCDF Header (xccdf_header)

This configuration option is provided to set the default Header information for SCAP Configuration scan output (from XCCDF profiles). The default setting is provided by SAINT, but can be changed here by changing the text in between the <title> and <organization> xml tags.
<title>XCCDF Results</title><organization>SAINT</organization>

SAINT Security Suite

Note: Do not change the Title and Organization open and closing XML tags, as this will result in an error generating the SCAP-required output.

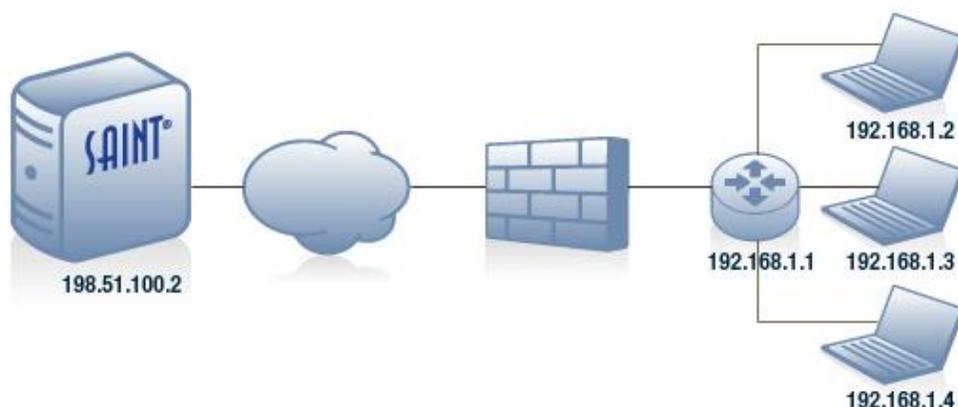
SCAP Scan Server Port

This configuration option is provided to define the local SCAP scan service listens on. The default is port 8383.

Tunneling

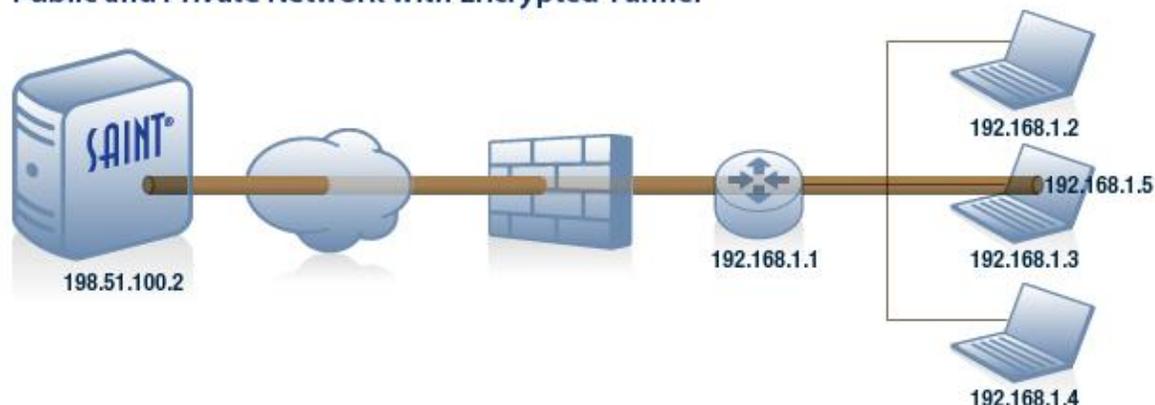
Tunneling allows SAINT's scanners to securely scan a private network from a public IP address by sending all packets through a designated host on the private network. For example, suppose 192.168.1.2, 192.168.1.3, and 192.168.1.4 are targets on a private network. The scanner, 198.51.100.2, is located on the Internet and cannot access the private network.

Public and Private Network



With SAINT's tunneling option, an encrypted tunnel is formed between the scanner and a chosen host on the private network. The tunnel uses Triple DES encryption with a 168-bit key. The chosen host bridges the tunnel with its physical network interface, forming a VPN. In this example, 192.168.1.3 is the chosen host. Now, the scanner can scan the targets on the private network through 192.168.1.3. The private IP address 192.168.1.5 is assigned to the scanner, so the scan probes originate from that IP address even though the scanner is not physically on the private network.

Public and Private Network with Encrypted Tunnel



Scanner IP Address

Setting this option tells the manager to establish a tunnel, and specifies the IP address to assign to the scanner on the private network. Any unused IP address in the private network's subnet may be used. Scans of targets on the private network will originate from this IP address.

Netmask

This option specifies the netmask of the private network's subnet. It should be the same as the netmask of the chosen host on the private network. This netmask determines which IP addresses should be accessed through the tunnel. For example, if the above option is 192.168.1.5 and this option is 255.255.255.0, then probes destined for any addresses beginning with 192.168.1 will be routed through the tunnel. Note that these options are for configuring the tunnel interface only, and do not imply that the entire subnet will be scanned. Only the targets selected in the scan wizard are included in the scan.

VPN Port

This option specifies the TCP port number to be used by the VPN tunnel. The scanner will listen for a connection from the chosen host on this port. Traffic on the specified port should be allowed outbound through the private network's firewall, and inbound through the scanner's firewall. The same port number should be entered when prompted by the VPN Tunnel Connector installer. If this option is left blank, a port number between 50000 and 60000 will be chosen at random.

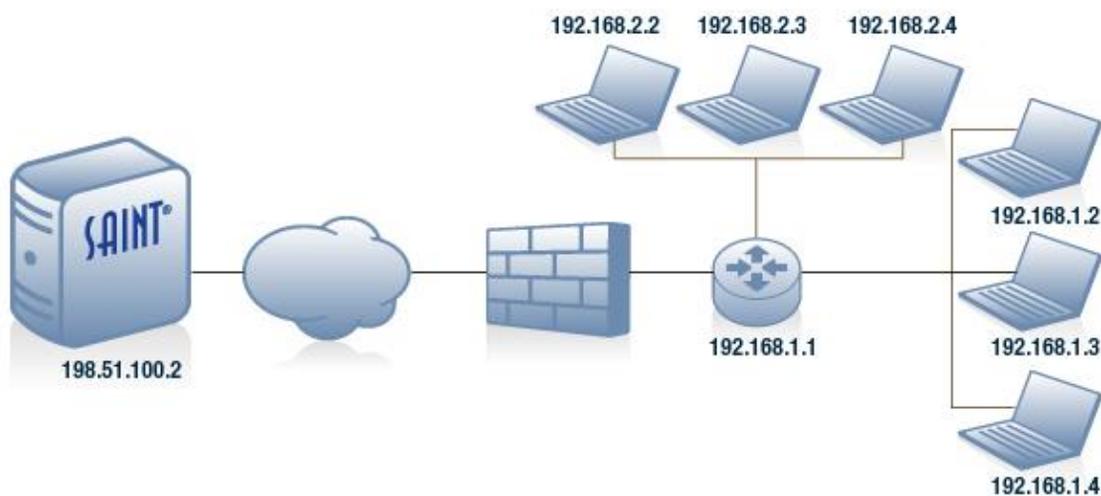
VPN Encryption Key

This option specifies the pre-shared VPN encryption key. It should be a 64-digit hexadecimal string, representing a 192-bit Triple-DES key and a 64-bit initialization vector. The same key should be entered when prompted by the VPN Tunnel Connector installer. If this option is left blank, a key will be generated at random.

Static Routes

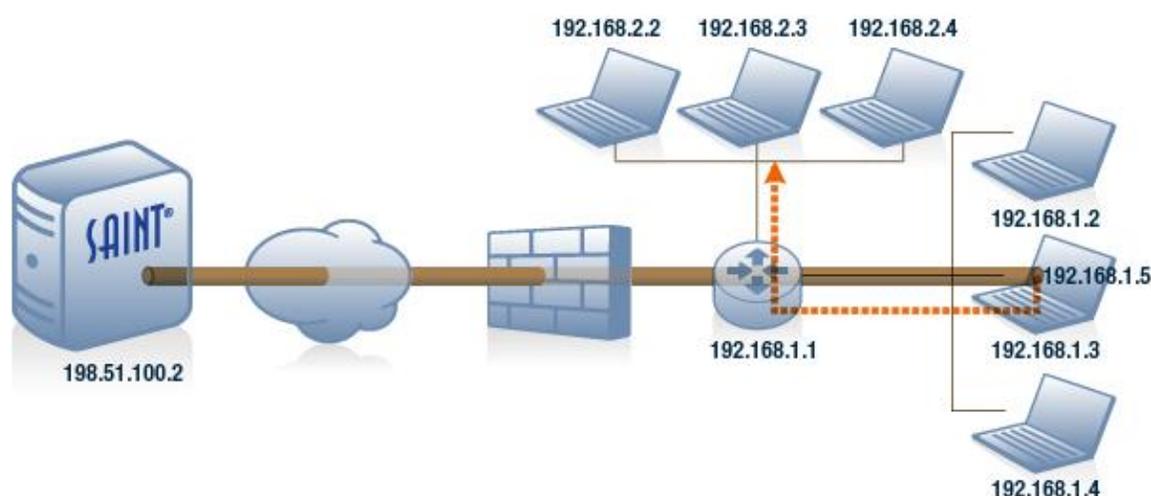
In some cases, the private network will extend beyond the chosen host's subnet. Referring to the previous example, now suppose that the 192.168.2 subnet also sits behind the 192.168.1.1 gateway router.

Public and Private Network with Additional Subnet



In this case, in order to scan targets 192.168.2.2, 192.168.2.3, and 192.168.2.4, a static route must be specified, which tells the scanner to reach those targets through the tunnel, routed through the 192.168.1.1 gateway.

Public and Private Network with Additional Subnet and Static Route



Static routes are specified as `<network>/<netmask>:<gateway>`. In the above example, that would be `192.168.2.0/255.255.255.0:192.168.1.1`. Multiple static routes may be specified in a list separated by semi-colons if necessary. For example:

```
192.168.2.0/255.255.255.0:192.168.1.1;192.168.3.0/255.255.255.0:192.168.1.1
```

Bridge Setup

The above scan configuration options are used to configure the scanner's side of the tunnel. However, establishing a tunnel also requires some steps on the targets' side of the tunnel. These steps are explained in a dialog box which appears after you set the above options in the scan wizard. To enable the tunnel:

1. Choose the host on the private network which will act as the bridge. Any physical Windows or Linux host on the private network may be chosen. Virtual machines might not work.
2. Select the operating system of the chosen host from the drop-down menu in the dialog box. Be sure to choose the correct architecture (i.e., 32-bit vs. 64-bit), since 32-bit compatibility mode may not work on 64-bit systems in this case.
3. If the chosen host's operating system is Linux, install the following packages if they are not already installed:
 - bridge-utils
 - tunctl (Red Hat/CentOS 5-6 only)
 - uml-utilities (Ubuntu only)

4. Click on the button in the dialog box to download the VPN Connector program. Note that the Linux program is customized with the correct VPN server address, port, and encryption key for your scan job, so it must be downloaded again for every new job. Since the program contains the encryption key, it is highly recommended that it be transferred securely. (A warning will be displayed if your HTTP connection is insecure. If you see this warning, see [use SSL](#) for instructions on enabling SSL encryption in the web interface.) When downloading the Windows version, be sure to save the parameters shown in the information box. You'll need these parameters during installation. See the next step.
5. Run the downloaded VPN Connector program on the chosen host. If you choose *Schedule Immediately* in the scan wizard, then the program must be run before clicking *Finish* in the scan wizard. Otherwise, it may be run any time before the scan is scheduled to begin. Note that there may be a momentary connectivity loss when the bridge is created.

Linux: The VPN Connector is a standalone executable program. Simply run the program on the Linux system.

Windows: The VPN Connector comes as a self-extracting executable which installs a Windows service, a desktop application allowing you to control and configure the service, and the TAP-Windows interface driver if not already installed. The installer will prompt you to enter the following parameters:

The screenshot shows a Windows-style dialog box titled "SAINT Scan Node Setup" with a close button (X) in the top right corner. The main heading is "Customer Information" and the instruction is "Please enter your customer information." The SAINT logo is in the top right. The form contains the following fields:

- Scanner IP address:** A text input field.
- VPN port:** A text input field containing "55555".
- Start service automatically?:** A checkbox that is checked.
- Encryption key:** A text input field.
- Network interface:** A dropdown menu.

At the bottom, there are three buttons: "Back", "Next" (highlighted with a blue border), and "Cancel".

At this step in the installation, enter the following information:

- **Scanner IP Address.** The public IP address of the scanner. If you chose the local node in step 2 of the scan wizard, this is normally the same IP address as the manager. If you chose a remote node, enter the public IP address of the remote node.
- **VPN Port.** The VPN port number which was shown in the information box below the download button when you downloaded the installer.
- **Start Service Automatically?** Whether you want the VPN Connector service to start automatically after installation and every time the computer starts. If you uncheck this box, use the [Windows VPN Connection Manager](#) to start the service before the scan runs.
- **Encryption Key.** The encryption key which was shown in the information box below the download button when you downloaded the installer.
- **Network Interface.** The network interface to bridge. Choose the network interface for the network which has the scan targets.

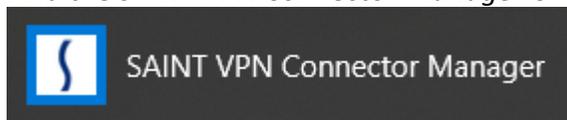
Upon execution, the connector program will first create the bridge interface and add the TAP interface and the primary Ethernet interface to the bridge. Note that there may be a momentary connectivity loss during this time, and on Windows the bridge interface may attempt to obtain new network configuration information using DHCP. After the bridge interface has been configured, the program will attempt to establish the tunnel connection. If the scanner is not yet listening for the connection, the connector program will retry periodically until the connection is accepted. Upon success, the program will output a message indicating that the connection has been established. If it is unsuccessful, see the error output from the scanner for a description of the problem.

If you are an advanced user and wish to set up the bridge yourself, run the connector program with the `-B` flag, which will skip the bridge setup and just attempt to establish the connection. If you wish to use a different Ethernet interface than the default, specify the desired interface using the `-e` flag. In Linux, use the interface's device name (e.g. `eth1`). In Windows, use the interface's GUID, which can be obtained from Local Area Connection > Properties > Configure > Details > Device class guid. Run the program with the `-h` flag to see the full list of command-line options.

Windows VPN Connector Manager

The Windows installer will install a desktop application which can be used to control, configure, and monitor the SAINT VPN Connector service. To use this application:

1. Find the *SAINT VPN Connector Manager* on the Windows start menu.

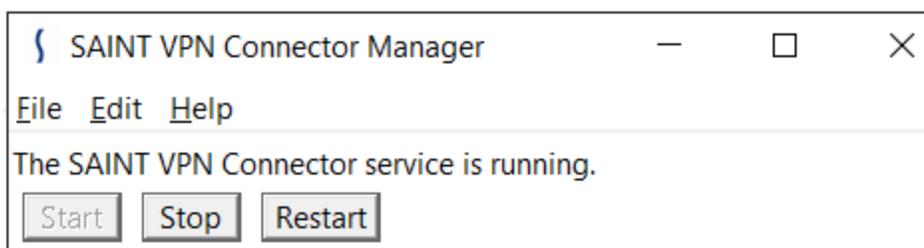


2. Right click on the *SAINT VPN Connector Manager* option and choose *Run as administrator*.



3. If you chose to run the service automatically when you installed it, then the service will already be running, and the *Stop* and *Restart* buttons can be used to stop or restart

it. When the service is stopped, you can use the *Start* button to start it.



4. Choose *Settings* from the *Edit* menu if you need to change the scanner IP address, VPN port, encryption key, or network interface.
5. Choose *Open Log* from the *File* menu to see the messages output by the VPN Connector service.

Workarounds

Skip Form Checks (skip_form_checks)

This options determines whether to skip checks against detected HTML form parameters. This option may be useful if excessive form submissions cause problems on the target. However, it will omit many generic web application checks such as SQL injection and cross-site scripting, so it should be used with caution.

Don't Use nslookup (dont_use_nslookup)

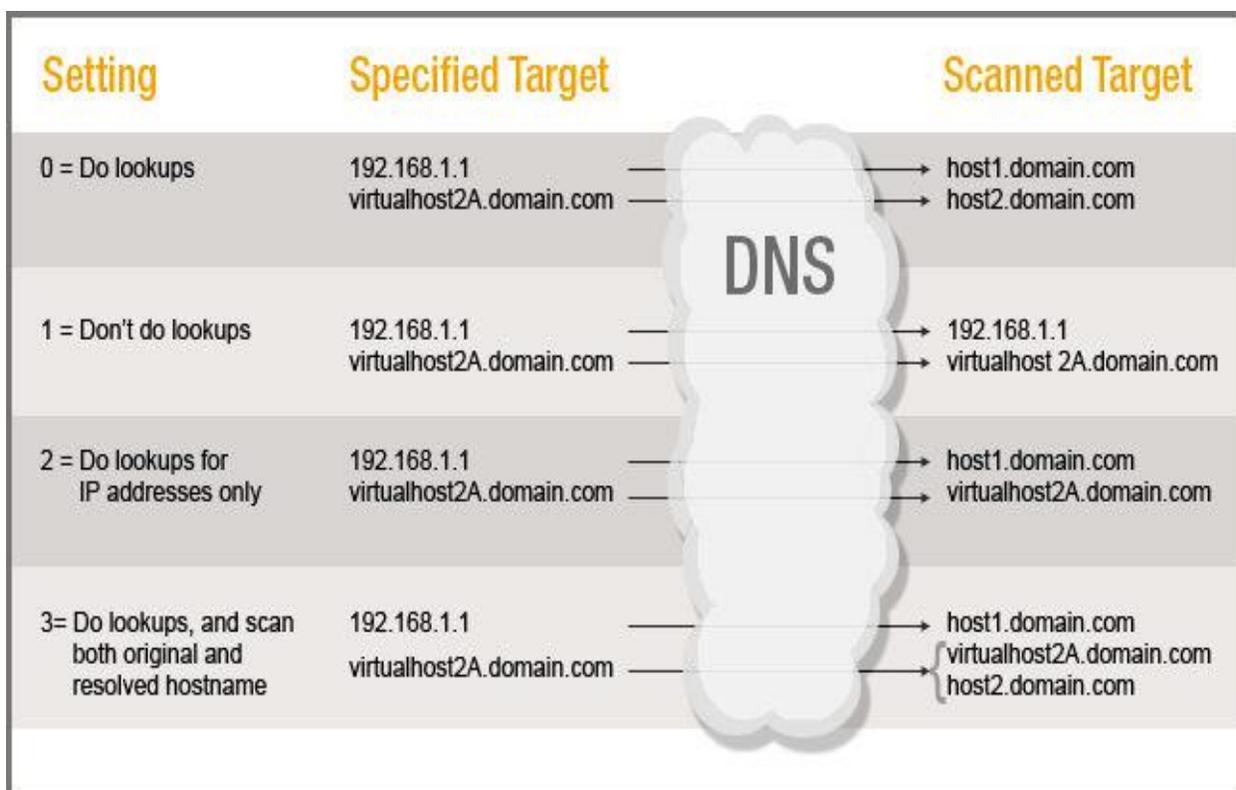
Check this box if DNS (Internet domain name service) is not available.

```
Dont_use_nslookup (0=Use nslookup; 1=(Default) Don't use
nslookup)
```

Disable Reverse DNS (disable_reverse_dns)

SAINT scanners attempt to determine the fully qualified host name (*host.domain*) of each primary target using reverse DNS. This ensures that the scan provides consistent results by always using each target's correct registered host name, if available. However, this behavior may be undesirable if you need to scan a target using a host name which is different from that target's registered host name, e.g., for scanning virtual web servers. This behavior may also be undesirable if reverse DNS service is slow or unavailable. The *Skip DNS Lookup* option controls whether the reverse DNS lookup is performed for primary targets. There are four available settings for this configuration option.

- 0 - Perform reverse DNS lookups on all targets. (Default setting).
- 1 - Disable reverse DNS lookups on any targets. This setting is useful if the DNS servers are slow or unavailable on the scanning host.
- 2 - Perform reverse DNS lookups on targets specified by IP address, but not on targets specified by host name. This is useful when scanning virtual web servers, because it allows IP addresses to be resolved into meaningful host names without affecting the name of the virtual web server.
- 3 - Perform reverse DNS lookups on all targets, and if a host name resolves to a different host name, to scan both host names. This is also useful for scanning virtual web servers, if a more thorough scan is desired.



Use Samba (*use_samba*)

If this option is enabled, scans will use the operating system's Samba tools (net and rpcclient) instead of SAINT's native SMB implementation for Windows checks. This may be useful if SAINT's protocol support is incompatible with the target, but may result in a slower scan. (Note: this setting has no effect on Windows file checks, which always use smbclient.)

Scan Failure Notification

SAINT Security Suite

Scan ▾ Analyze ▾ Report ▾ Exploit ▾ Manage ▾ Configuration ▾

System Options Scanning Options Exploit Options

Search Clear Search

Host Discovery	Probe	Port	Password	Email Notification	File Content Search	Anti Virus
Authentication	Network Information	Process Control	Results	SCAP Configuration	Workaround	
Scan Failure Notification						

Enable Scan Failure Email Notifications:

Email Server:

Scan Failure Notification Email Addresses:

From Email:

From Email Display Name: SAINT

Email Subject: SAINT

Report scan failure for the following reasons

Probe Crashes:	<input type="checkbox"/>
Probe Timeouts:	<input type="checkbox"/>
License Errors and Warnings:	<input checked="" type="checkbox"/>
Authentication Failures:	<input type="checkbox"/>
Scan Window Exceeded:	<input checked="" type="checkbox"/>
Scan Engine Errors:	<input type="checkbox"/>
Fatal Errors:	<input checked="" type="checkbox"/>

Enable Scan Failure Email Notifications

Sends an email to the listed email addresses if a scan fails for the selected reasons.

Email Server

The mail server address. (optional)

Scan Failure Notification Email Addresses

Space-separated list of email addresses to send the notification to.

From Email

The email address that the notification comes from. (optional)

From Email Display Name

The name of the email sender.

Email Subject

The subject of the email.

Report Scan Failure for the following reasons

- **Probe Crashes** – Message is included when a scan completes and probes crashed.
- **Probe Timeouts** – Message is included when a scan completes and probes timed out.
- **License Errors and Warnings** – Message is included when there are license issues during a scan.
- **Authentication Failures** – Message is included when authentication fails for any service that it is attempted on.
- **Scan Window Exceeded** – Message is included when a scan window is defined for a job and the scan is paused due to the window being exceeded.
- **Scan Engine Errors and Fatal Errors** – Message is included in rare cases where an issue prevents a scan from running.

Exploit Options

Network

Most exploits work by injecting machine code, known as a *payload*, into a vulnerable process. The payload runs a command shell which is redirected to a socket. A TCP connection to the command shell is then established, allowing command execution.

Exploit Timeout (exploit_timeout)

This value is the timeout value used when executing exploits. The Default value is 240 seconds.

Shell Type (shelltype)

There are two ways in which the shell connection can be established. Most exploits can use either of these two methods. Which one to use is specified by the port shelltype option.

- 0 – (Default) reverse port, is for the target to connect back to the manager. This method is useful when the target is behind a firewall which may deny some incoming connections, because the connection originates from the target.
- 1 – Bind port, is for the manager to connect to the target. This method may be preferable when Security Suite is behind a firewall which could deny the target's attempt to connect back.

Shell Port Start (shell_port_start)

The shell port is the TCP port upon which the command shell either listens for a connection (when using a bind port) or connects back to the manager (when using a reverse port). Most exploits allow the user to select the shell port that the payload will use. This is useful for working around firewall blocks which may only allow connections on certain ports.

Since only one process can bind to the same port on the same computer at a time, SAINT allows you to specify a range of shell ports. An unused port from this range is selected at random when you run an exploit, but can be overridden on the exploit's run form. During automated penetration tests, the exploits will use different port numbers within the range to avoid potential conflicts.

The shell_port_start field specifies the start of the range of shell ports.

Shell Port End (shell_port_end)

The shell_port_end field specifies the end of the range described above.

Shellcode Transfer Port Start (shellcode_transfer_port_start)

Some exploits need to connect back and retrieve shellcode from the manager. A range of ports, separate from the range described above, is used for such shellcode transfers. Again, an unused port from this range is selected at random when you run an exploit, and different port numbers from within the range will be used during automated penetration tests.

The `shellcode_transfer_port_start` field specifies the start of the range of shellcode transfer ports.

Shellcode Transfer Port End (`shellcode_transfer_port_end`)

The `shellcode_transfer_port_end` field specifies the end of the range described above.

Tunnel Port (`tunnel_port`)

Port used for tunneling.

Tunnel Local Port Start (`tunnel_localport_start`)

This port setting is the first port in the port range used by the localhost for tunneling.

Tunnel Local Port End (`tunnel_localport_end`)

This port setting is the last port in the port range used by the localhost for tunneling.

Local Ports per Tunnel (`localports_per_tunnel`)

Connect-back Address V4 (`connectback_addr`)

The connect-back address is used whenever an exploit needs to connect back to SAINT such as for reverse port exploits, exploit servers or file transfers. The default connect-back address used is the address of the system's network interface, which is acceptable in most cases. However, there may be cases where the target must use a different IP address to connect back to the manager. For example, due to Network Address Translation (NAT).

To set the connect-back address, enter the manager's IP address as recognized by the target. If it is the same as the manager's actual IP address, leave this setting blank, and the default will be used.

Connect-back Address V6 (`connectback_addr6`)

This connect-back address is used for the same purpose as the connect back address previous described, but specific to IPv6 environments.

Mail Server Domain (mail_server_domain)***FTPD Port (ftpd_port)***

SAINT installations contain an internal File Manager utility, for the purposes of file transfers during the execution of exploits. There are two configuration settings which affect the operation of this utility. The first is the FTP daemon port. When a file download request is made and the manager attempts to use FTP to transfer the file, it starts a listener on the specified port. The target system then connects to the port using its native FTP client and sends the file. Note that this setting has no effect if the target is a Windows system because the Windows FTP client only supports file transfers on port 21. SAINT may also use TFTP or SMB for some connections, in which case this setting has no effect.

Download Timeout (download_timeout)

This configuration option is the second setting that affects the operation of the File Manager utility. This value sets is the download timeout for file transfers. The File Manager will wait the specified number of seconds for a response from the target before giving up on a download request.

Credentials

Some exploits require authentication credentials to a service on the target host in order to work. This is typical if a vulnerability affects a specific function which is only available after a user has logged in. SAINT currently allows you to specify login credentials for the FTP, POP, and IMAP services, plus the IMAP post office name and the e-mail domain, if applicable. Enter a valid user name and password for any service to enable authenticated exploits for that service.

IMAP User (imap_user)

User ID for the imap login credentials. Default: guest

IMAP Password (imap_password)

Password for the imap login credentials.

IMAP Post Office (imap_post_office)

IMAP post office name of the target mail server. Default: imap

SAINT Security Suite

POP User (pop_user)

User ID for the POP login credentials. Default: guest

POP Password (pop_password)

Password for the POP login credentials.

FTP User (ftp_user)

User ID for the FTP login credentials. Default: anonymous

FTP Password (ftp_password)

Password for the FTP login credentials.

Exploit E-mail Notifications

Sometimes it will be beneficial to enable e-mail notifications for when a new exploit connection is received. In the cases where you are running a background exploit tool, such as the Flash Drive AutoPlay Tool, or performing any number of client exploits, you most likely won't get any connections instantly. The following configuration options are provided to configure e-mail notification options, specific to exploit execution.

Exploit Email Server (exp_notify_email_server)

This configuration field stores the IP address of a mail relay server. If this option is left blank, the alert will be sent directly to the mail server for the recipient's e-mail domain. If that server cannot be resolved or reached for some reason, then an IP address for a mail relay server can be specified. If it is specified, then alerts will be sent through that server.

Exploit Email Recipient 1 (exp_notify_to_email1)

Recipient email address to receive notifications from the execution of exploits.

Exploit Email Recipient 2 (exp_notify_to_email2)

Recipient email address to receive notifications from the execution of exploits.

Exploit Email Recipient 3 (exp_notify_to_email3)

Recipient email address to receive notifications from the execution of exploits.

Notify on New Connections (notify_on_new_connections)

Values: Yes/No. Default: No.

Ticket Options

The screenshot shows the SAINT Security Suite Configuration interface. The top navigation bar includes 'Scan', 'Analyze', 'Report', 'Ticket', 'Exploit', 'Manage', 'Configuration', and '+ Create'. The 'Configuration' menu is active, and the 'Ticket' sub-menu is selected. The 'Ticket Options' section is displayed, featuring a search bar and three tabs: 'General Ticketing', 'Ticket Notification', and 'Ticket Export Email'. The 'General Ticketing' tab is active, showing the following settings:

- Enable Ticketing: Always (dropdown menu)
- Autoclose Tickets: No (dropdown menu)
- Authentication Required to Autoclose:
- Auto-reopen Tickets: No (dropdown menu)
- Days Until Due: 30 (text input field)

A 'Save' button is located at the bottom of the form. Below the form, there are links to 'Restore default values? [All Options] or [Ticket Options]'. The bottom status bar indicates 'Used 3 of 100 IPs. Using 3 of 20 agents. (Expires 5/19/2021)'.

General Ticketing

Enable Ticketing

This option enables or disables generation of tickets as a result of vulnerabilities detected by a vulnerability scan. The default for `enable_ticketing` is for ticketing always to be enabled. If this setting is changed to *yes but allow override*, then tickets will be generated by default, but users can disable ticketing on a per-job basis by setting *Create Tickets* to no when creating or editing the job. (See [Select a Ticket Rule Set for a Job.](#)) Similarly, if this setting is changed to *no but allow override*, then tickets are not generated by default, but users can enable ticketing when creating or editing the job. If this setting is changed to *never*, then generation of tickets is always disabled. When *yes but export to another system* is set, tickets will not be created in SAINT but instead sent to another system via email. This allows tickets to be exported to third-party ticketing systems.

Autoclose Tickets

Open tickets can be closed automatically as a result of a vulnerability scan where the previously found vulnerability on a host does not recur. This option has 3 possible settings:

1. *No*: Default for autoclose_tickets - do not autoclose tickets.
2. *Yes, regardless of scan level*: Select this setting to auto-close tickets on a host where the vulnerability does not recur, regardless of the type of scan policy level. Note, different scan policies may find different vulnerabilities. Auto-closing tickets is most useful when you use a consistent scan policy across scans.
3. *Yes, only after Full Vulnerability scan*: Auto-close tickets on a host where the vulnerability does not recur, but only after a Full Vulnerability scan.

Authentication Required to Autoclose

This option can be *Off* (default) or *On*. If the setting is *On*, open tickets will only be auto-closed on hosts where primary authentication succeeded (e.g., registry login for Windows hosts, SSH login for *nix hosts). The default setting for autoclose_tickets_auth_required is *No*.

Auto-reopen Tickets

Closed tickets can be automatically reopened as the result of a vulnerability scan. The options are:

1. The default for auto_reopen_tickets is *No* - do not auto-reopen tickets.
2. *Yes, as New*: Auto-reopen tickets so they have the status of New with no assignee.
3. *Yes, as previous assignee*: Auto-reopen tickets so that, if they had a previous assignee, they will have the status of Assigned and the same assignee as before. If the closed ticket had no assignee, it will be reopened with status New and no assignee.

Days Until Due

Tickets are automatically assigned a due date at the time of ticket creation. The default for days_until_due is 30 days past the creation date.

Ticket Notification

Mail Server

The value for the `ticket_notify_mail_server` is the address of the relay mail server to be used for sending ticket-related notifications. This setting is optional. If the mail server is not provided, the system will try to determine the mail server for each recipient's domain.

From Email

The `ticket_notify_from_email` value is the From: email address that is used as the sender for ticket-related e-mail notifications. If this option is left blank, root is used as the user name.

From Email Display Name

The `ticket_notify_from_email_display_name` configuration setting is the display name of the sender, used for all ticket related e-mail notifications. The default value is "SAINT".

Enable Ticket Assignment Notification

The `enable_ticket_assignment_notify` setting indicates whether an e-mail notification should be sent to a user when the user is assigned tickets. The default is *Off*.

Days Before Ticket Due to Send Reminder

The *Ticket reminder days before due* configuration setting is the number of days before a ticket is due to send an e-mail reminder (blank=do not send reminder; 0=due today). The setting may also be a comma-separated list of numbers, e.g., '0,3,7' means to send a reminder on the due date, once within 3 days of the due date, and once within 7 days of the due date. The default is blank, so reminders are not sent.

Enable Past Due Ticket Reminders

The *Enable past due ticket reminders* configuration setting indicates whether a daily e-mail reminder should be sent to a user when tickets assigned to the user are past due. The default is *Off*.

Override Default Base URL

The *Ticket base URL* configuration setting contains the base URL to use for hyperlinks within ticket notification e-mails, e.g., <http://mysainthost:1414>. Security Suite's default base URL is set the first time the admin user logs in. This setting may be useful when hyperlinks in ticket notification e-mails must use the external host name or IP address instead of internal.

Ticket Export Email

This section describes how a user can configure SAINT to use a 3rd party ticketing system, rather than SAINT's integrated ticketing workflows, to send scan results via email-based records to manage response and remediation workflows. The configuration settings in this form will enable a user to configure the communication to the specific ticketing system, as well as a descriptive subject and body. This export workflow will work for any product (ZenDesk, ServiceNow, etc.) that accepts emails to generate a new ticket. Note that this process will send scan record information to generate a 3rd party ticket, but will not control or auto-update 3rd party tickets for status.

General Ticketing	Ticket Notification	Ticket Export Email
Mail Server: <input type="text"/>		
To Email: <input type="text"/>		
From Email: <input type="text"/>		
From display name: SAINT		
Email subject: %job_name% - Scan: %scan_date%: %host_name% - %desc		
Email body: <input type="text" value="%job_name% %scan_date%"/>		
Vulnerability tutorial: Do not send ▼		
Tutorial base URL: <input type="text"/>		

The options under this tab are used when exporting tickets to third-party ticket systems. (See [Enable Ticketing](#)).

Mail Server

Address of relay mail server (optional).

To Email

The email address used by the ticketing system to receive tickets.

From Email

The email address from which the ticket is sent. Default = root@

From Display Name

The display name of the from email address. Default = SAINT

Email Subject

The subject of the email (see [Macros](#) for formatting options). This field can be overridden by using [ticket rule sets](#).

Email Body

The email message (see [Macros](#) for formatting options).

Vulnerability Tutorial

Whether or not to send the tutorial as an attachment. Use the %tutorial_url% macro in the message body if you want a URL provided instead.

Tutorial base URL

When sending the tutorial as a hyperlink, this will override the default URL of the SAINT installation. This option may be useful when hyperlinks to SAINT should use the external host name or IP address instead of internal.

Macros

Macros are used to define where ticket fields should be added in the email. The following macros are available:

SAINT Security Suite

%job_name%	The name of the scan job.
%scan_date%	The date which the scan occurred on
%description%	The vulnerability description.
%host_ip%	The IP address on which the vulnerability was discovered.
%host_name%	The host name on which the vulnerability was discovered.
%sys_class%	The system class of the target host.
%sys_type%	The system type of the target host.
%service%	The service which the vulnerability was discovered on.
%cve_list%	A comma separated list of CVEs associated with the vulnerability.
%max_cvss_score%	The CVSS score of all CVEs associated with the vulnerability.
%check_id%	The SAINT check_id of the vulnerability.
%severity_color%	The SAINT severity color of the vulnerability (Red, Yellow, Brown)
%severity_category%	The SAINT severity category of the vulnerability (Concern, Critical, Potential)
%severity_description%	The SAINT severity description of the vulnerability

<code>%assigned_to%</code>	The firstname, lastname, and username of the assignee when using ticket rule sets.
<code>%due_on%</code>	The due date of the ticket.
<code>%created_on%</code>	The creation date of the ticket.
<code>%tech_details%</code>	The SAINT technical details showing evidence of the vulnerability's existence.
<code>%tutorial_url%</code>	A URL which can be used to access the relevant tutorial sections in the SAINT UI.
<code>!AssetTagName!</code>	AssetTagName can be replaced with the tag_name of any asset tag. For example, !CPE! could be replaced with <code>cpe:/o:microsoft:windows_7</code> if the asset associated with the vulnerability has that asset tag.

Email Subject Macro Example:

`%job_name%` - Scan: `%scan_date%`: `%host_name%` - `%description%`

My Test Job - Scan: 2018-12-06 08:38:51: 10.124.0.31 - Possible vulnerability in Microsoft Terminal Server

Email Body Macro Example:

[THEJOBNAME]`%job_name%`

`%scan_date%`

`%description%`

`%host_ip%`

`%host_name%`

`%sys_class%`

`%sys_type%`

`%service%`

`%cve_list%`

SAINT Security Suite

%max_cvss_score%
%check_id%
(%severity_category%) %severity_description%
[ASSIGNEE]%assigned_to%
%due_on%
%created_on%
%tech_details%
!CPE!

[THEJOBNAME]My Test Job

2018-12-06 08:38:51

SSL/TLS server supports short block sizes (SWEET32 attack)

10.124.0.3

10.124.0.3

WINDOWS

Windows 7 SP1

ftp

CVE-2016-2183,CVE-2016-2184

5.0

misc_tls_sweet32

(Critical) user shell access

[ASSIGNEE] Administrator (admin)

2019-01-05 05:00:00

2018-12-06

Server accepted SSLv3 64-bit block size cipher: TLS_RSA_WITH_3DES_EDE_CBC_SHA

cpe:/o:microsoft:windows_7

Data Filter Options

Many of the features in the user interface (Dashboards; Analyze; Reports; SCAP reporting) provide a Data Filter Options feature to allow the user to select the data context for display. Such as: selecting the scan data by Job(s) and/or selected Scan(s); constraining the data by selected Asset Tags or Custom Severity Sets; and showing or hiding results that have been

flagged as an Exclusion. The following example shows data filter options for analyzing detailed scan results.

The screenshot displays the SAINT Security Suite interface. The top navigation bar includes 'Dashboard', 'Scan', 'Analyze', 'Report', 'Ticket', 'Exploit', 'Manage', and 'Configuration'. The 'Analyze' tab is active, showing a table of scan results. The table has columns for 'Actions', 'IP', 'OS Type', 'Severity Level', 'Severity', 'Confirmed', 'Vulnerability Check ID', 'Description', and 'CVE(s)'. The table shows 10 rows of results, all with a severity level of 'High' (red circle) and a confirmed status of 'No'. The first row is for a Linux system with user shell access. The second row is for a Windows Server 2003 SP2 with administrator or root shell access. The third row is for a Windows Server 2003 SP2 with administrator or root shell access. The fourth row is for a Windows Server 2003 SP2 with administrator or root shell access. The fifth row is for a Windows Server 2003 SP2 with administrator or root shell access. The sixth row is for a Windows Server 2003 SP2 with root access via buffer overflow. The seventh row is for a Windows Server 2003 SP2 with user shell access. The eighth row is for a Windows Server 2003 SP2 with user file read access. The ninth row is for a Windows Server 2003 SP2 with user file read access. The tenth row is for a Windows Server 2003 SP2 with denial of service. The left sidebar shows 'Data Filters' with 'Data View' set to 'None' and 'Data Sources' set to 'Heavy Vuln Scan 10.8.0'. The bottom status bar shows 'Used 34 of 500 IPs (Expires 12/31/2018)' and 'Page 1 of 442'.

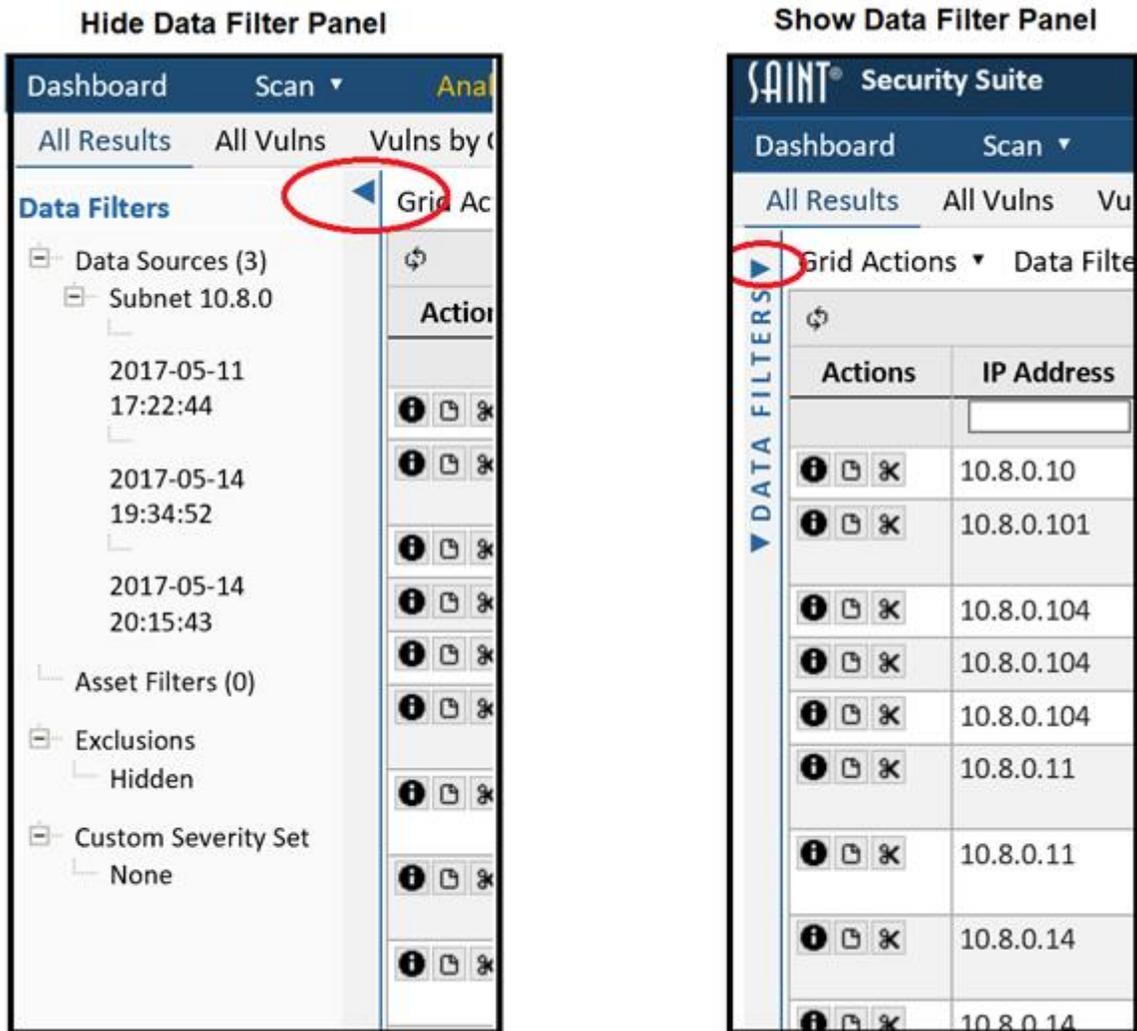
Actions	IP	OS Type	Severity Level	Severity	Confirmed	Vulnerability Check ID	Description	CVE(s)
ⓘ ⓧ	10.8.0.10	Linux	High	user shell access	No	misc_esxbuild	vulnerable VMWare ESXi Server 5.5 build: 1331820	CVE-2013-0242 CVE-2013-1752 CVE-2013-1914 CVE-2013-4238 CVE-2013-4332 CVE-2013-5211 CVE-2013-5973 CVE-2014-0076 CVE-2014-0160 More
ⓘ ⓧ	10.8.0.101	Windows Server 2003 SP2	High	administrator or root shell access	Yes	win_patch_ms17010	Windows SMB remote command execution (MS17-010)	
ⓘ ⓧ	10.8.0.101	Windows Server 2003 SP2	High	administrator or root shell access	No	win_patch_printspool1205	Windows print spooler remote code execution vulnerability (MS12-054)	CVE-2012-1851
ⓘ ⓧ	10.8.0.101	Windows Server 2003 SP2	High	administrator or root shell access	No	win_patch_ms11020	Windows SMB Server Transaction Vulnerability	CVE-2011-0661
ⓘ ⓧ	10.8.0.101	Windows Server 2003 SP2	High	administrator or root shell access	No	win_patch_netcomponent	Windows networking components remote code execution (MS12-054)	CVE-2012-1850
ⓘ ⓧ	10.8.0.101	Windows Server 2003 SP2	High	root access via buffer overflow	Yes	win_patch_ms12020	Microsoft Remote Desktop Protocol Remote Code Execution Vulnerability (MS12-020)	CVE-2012-0002 CVE-2012-0152
ⓘ ⓧ	10.8.0.101	Windows Server 2003 SP2	High	user shell access	No	win_dotnet14057iri	Microsoft .NET iriParsing vulnerability (MS14-057)	CVE-2014-4121
ⓘ ⓧ	10.8.0.101	Windows Server 2003 SP2	High	user file read access	No	win_patch_ssl	SSL and TLS Protocols Vulnerable Implementation (MS12-006)	CVE-2011-3389
ⓘ ⓧ	10.8.0.101	Windows Server 2003 SP2	High	user file read access	Yes	misc_pcamerica	pcAmerica point-of-sale system has default password	
ⓘ ⓧ	10.8.0.101	Windows Server 2003 SP2	High	denial of service	No	win_dotnet16019dos	Microsoft .NET Framework Stack Overflow Denial of Service Vulnerability (MS16-019)	CVE-2016-0033

Note that the data filters you set will be kept in memory and retained as you navigate throughout the product. For example, if you set the Exclusion filter on a page in the *Analyze* tab to “Show,” then results you see in Dashboards will reflect all results for the selected data sets, including those that have been flagged as Exclusions. If you are constraining results by Asset Tag “OS” = “Windows”, then the results will be limited to hosts that have an Asset Tag “OS” equal “Windows”.

Data Filters Context Panel

As shown in the example above, any page that displays scan results will also provide the capability to display the current data “context” defined by the selected data filters. In the example above, the current data is based on three scans conducted for can Job Subnet 10.8.0, with no Asset Tag filters or Custom Severity Sets, but does hide scan results previously flagged as an Exclusion.

The Data Filters panel can be controlled to show (for data context) or hide (to conserve screen space) it by clicking on the left arrow in the upper right corner of the panel.



Select Data Set

The *Select Data Set* option enables you to select one or more scan results (scans) produced by previously executed scan jobs, and set these data sets as the context across the application. As shown below, Job column values can be selected by the user, to include associated values such as Target Group, Scan Policy, User Group or User (job owner). Clicking on a job displays the list of scans executed for the job, to include the date/time the scan was completed; job title, and the number of vulnerabilities found during the scan. You may choose one or more jobs to merge entire collections of scan results into a single result for analysis. Or, you may select one, multiple, or all scans executed within a single job to view scan results.

The selector also provides the capability to set the number of scans to retrieve to support trend analysis. In the *Scans* panel, you can enter one (1) in the “__ most recent scans” option to

always use the most current scan run data for the selected job(s); or enter a number greater than one if you want to use more than one scan result for a selected job to support trend analysis.

Select Scans
✕

Jobs
1 of 3 selected

	Job	Target Group	Policy
<input type="checkbox"/>	RHEL scan	saint-data	Heavy/Vulnerability S
<input type="checkbox"/>	Windows scan	saint-data	Heavy/Vulnerability S
<input checked="" type="checkbox"/>	Subnet 10.8.0	saint-data	Heavy/Vulnerability S

Scans
3 of 3 selected
 5 most recent scans

	Date/Time ↕	Job	# Vulns
<input checked="" type="checkbox"/>	2017/05/14 20:15:43	Subnet 10.8.0	2492
<input checked="" type="checkbox"/>	2017/05/14 19:34:52	Subnet 10.8.0	2494
<input checked="" type="checkbox"/>	2017/05/11 17:22:44	Subnet 10.8.0	2491

⌕ ✕ View 1 - 3 of 3

⌕ View 1 - 3 of 3

OK
Cancel

Note that you are not restricted on the type of results you can select for analysis. This means that you can select multiple types of scans (e.g., full vulnerability scan; an XCCDF configuration policy scan; and a Pen Test policy scan), and produce a single output in both the *Dashboard* and *Analyze* grids. This can be beneficial in displaying raw output, but note that results may not be useful in computing particular types of dashboards more directed at vulnerability counts, or other risk-specific areas.

Understanding the Content Counts

The following is an example of a user view choosing all jobs in the job selector to gain visibility of all scans executed for those jobs. The grid counts describe jobs and scan results as follows:

Jobs:

View x – x of x – These grid counts mean there are 15 total jobs in the current display, and 15 total jobs in the system. Currently, this grid is not designed to “page” rows by a limited row count per page, so all jobs are available for sorting and use within the single page.

Scans:

View x – x of x – These grid counts mean that there are 14 total scans completed or being executed (ready; queued; in progress), and 13 are visible and available for selection for analysis. The one indicates that the user has selected a single scan result for display.

In a more practical example, a user has selected to view all completed scans run for two recent Jobs that used the PCI scan policy. Two scans were completed. The user chooses to select the first job for analysis.

Hide/Show Exclusions

The Hide/Show Exclusion option in the Date Filter Options provides the capability to show results in dashboards and analysis based on all scanned results (Show Exclusions) or filtered to show and compute results based on results that do not have a Vulnerability that is currently flagged as an Exclusions (Hide Exclusions). Click the applicable option in the Data Filter Options dropdown to toggle the results for "what if" analysis based on vulnerabilities that have or have not been flagged as exclusions.

The following screen shots show a series of data results to illustrate this feature: 1) showing all scan results; 2) filtering the records in the Exclusions column to "Yes" to show only records with the Exclusion flag; 3) removing the Exclusion constraint at the Column level and using the Data Filter option to Hide only records set as an Exclusion; and 4) all results but filtered in the data's Exclusions column to see the records that have the Exclusion flag set to "Yes". Note the total record count at the top right of the data grid, as this flag is filtered. See the [Exclusions](#) section for more information about how to set exclusions on vulnerabilities.

SAINT Security Suite Admin Help

Dashboard Scan Analyze Report Ticket Exploit Manage Configuration

All Results All Vulns Vulns by CVSS Vuln Count by Host Exclusions Vuln DB Custom Severities + Create

Data Filters

- Data View
 - None
- Data Source (1)
 - PCI Subnet 10.8.0
 - 2017-05-22 12:07:09
- Asset Filters (0)
- Exclusions
 - Visible
- Custom Severity Set
 - None

Grid Actions Data Filter Options

Page 1 of 361

View 1 - 10 of 3,608

Actions	IP Address	System Type	Severity Level	Severity	Vulnerability Check ID	Description	CVE(s)	Exclusion
[D] [K]	10.8.0.10	Linux	[Red Circle]	user shell access	misc_esxbuild	vulnerable VMWare ESXi Server 5.5 build: 1331820	CVE-2013-0242 CVE-2013-1752 CVE-2013-1914 CVE-2013-4238 CVE-2013-4332 CVE-2013-5211 CVE-2013-5973 CVE-2014-0076 CVE-2014-0160 More	No
[D] [K]	10.8.0.101	Windows Server 2003 SP2	[Red Circle]	administrator or root shell access	win_patch_printspool1205	Windows print spooler remote code execution vulnerability (MS12-054)	CVE-2012-1851	No
[D] [K]	10.8.0.101	Windows Server 2003 SP2	[Red Circle]	administrator or root shell access	win_patch_ms11020	Windows SMB Server Transaction Vulnerability	CVE-2011-0661	No
[D] [K]	10.8.0.101	Windows Server 2003 SP2	[Red Circle]	administrator or root shell access	win_patch_netcomponent1	Windows networking components remote code execution (MS12-054)	CVE-2012-1850	No

SAINT Security Suite Admin Help

Dashboard Scan Analyze Report Ticket Exploit Manage Configuration

All Results All Vulns Vulns by CVSS Vuln Count by Host Exclusions Vuln DB Custom Severities + Create

Data Filters

- Data View
 - None
- Data Source (1)
 - PCI Subnet 10.8.0
 - 2017-05-22 12:07:09
- Asset Filters (0)
- Exclusions
 - Visible
- Custom Severity Set
 - None

Grid Actions Data Filter Options

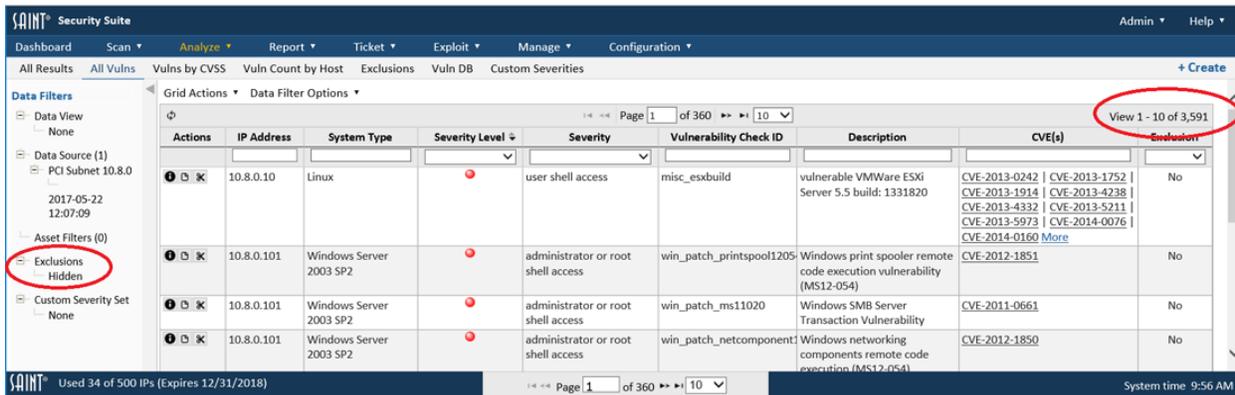
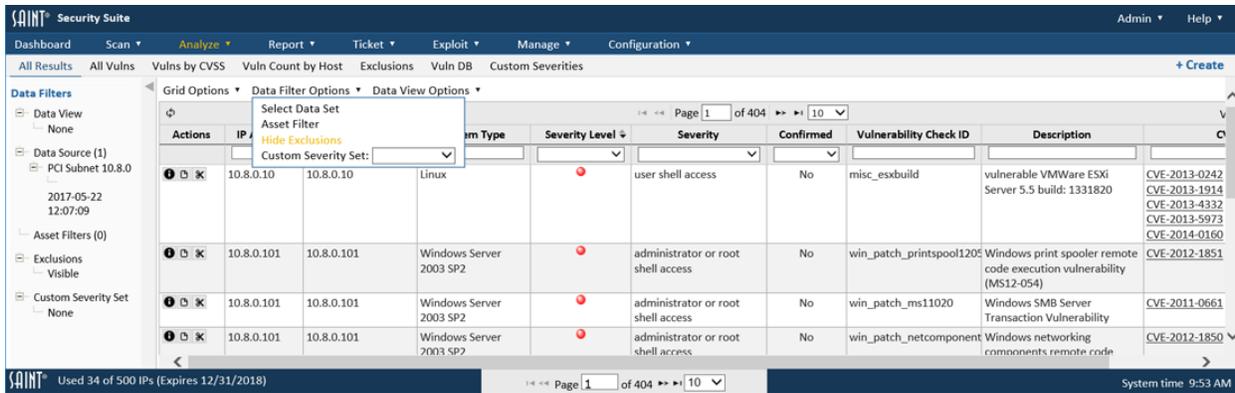
Page 1 of 2

View 1 - 10 of 17

Actions	IP Address	System Type	Severity Level	Severity	Vulnerability Check ID	Description	CVE(s)	Exclusion
[D] [K]	10.8.0.10	Linux	[Yellow Circle]	information gathering	misc_tls_heartbleed	TLS heartbleed memory disclosure vulnerability	CVE-2014-0160	Yes
[D] [K]	10.8.0.10	Linux	[Yellow Circle]	information gathering	misc_tls_heartbleed	TLS heartbleed memory disclosure vulnerability	CVE-2014-0160	Yes
[D] [K]	10.8.0.10	Linux	[Yellow Circle]	information gathering	misc_tls_heartbleed	TLS heartbleed memory disclosure vulnerability	CVE-2014-0160	Yes
[D] [K]	10.8.0.10	Linux	[Yellow Circle]	information gathering	misc_tls_heartbleed	TLS heartbleed memory disclosure vulnerability	CVE-2014-0160	Yes
[D] [K]	10.8.0.101	Windows Server 2003 SP2	[Yellow Circle]	susceptibility to malicious content	win_dotnet1	Microsoft .NET Common Language Runtime Could Allow Remote Code Execution	CVE-2009-0090 CVE-2009-0091 CVE-2009-2497	Yes
[D] [K]	10.8.0.11	Windows Server	[Yellow Circle]	susceptibility to malicious	win_dotnet1	Microsoft .NET Common	CVE-2009-0090 CVE-2009-0091	Yes

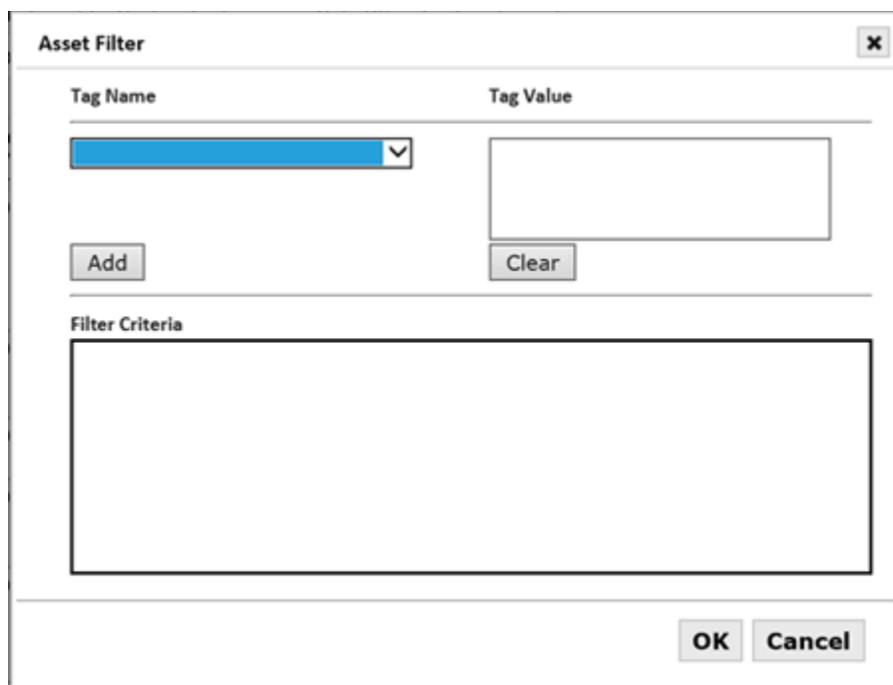
SAINT Used 34 of 500 IPs (Expires 12/31/2018) Page 1 of 2 System time 9:58 AM

SAINT Security Suite



Asset Filter

This option in the Data Filter dropdown provides the capability to filter the results in the analyze and dashboard grid and Report content based on Asset Tags. Click this option to view the Asset Filter dialog, as shown below:

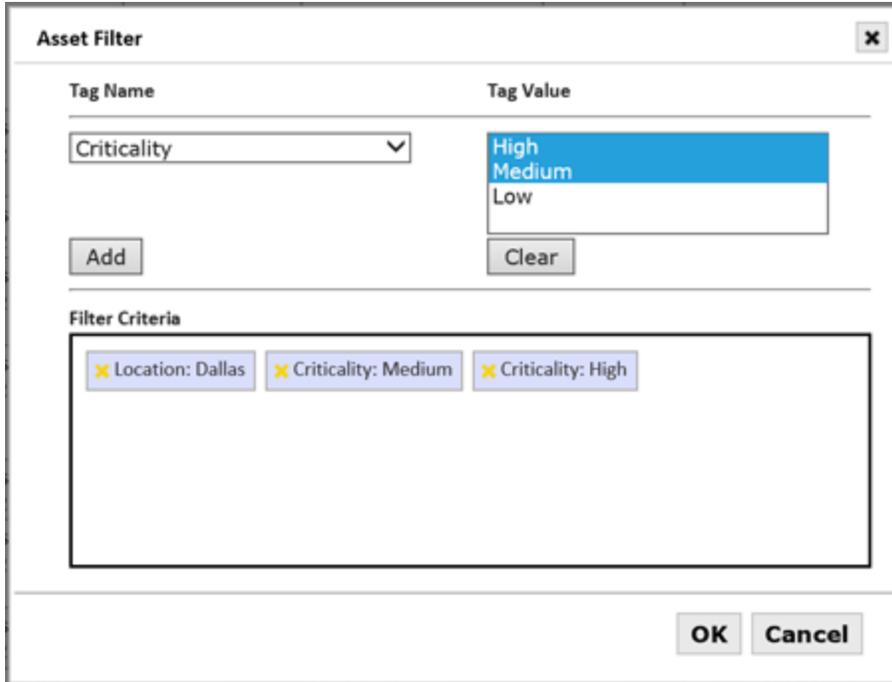


The screenshot shows a dialog box titled "Asset Filter" with a close button (X) in the top right corner. The dialog is divided into three main sections. The top section is labeled "Tag Name" and "Tag Value". Under "Tag Name", there is a dropdown menu with a blue background and a downward arrow. Under "Tag Value", there is a text input field. Below these fields are two buttons: "Add" on the left and "Clear" on the right. The middle section is labeled "Filter Criteria" and contains a large, empty rectangular box. The bottom section of the dialog contains two buttons: "OK" and "Cancel".

To filter the content:

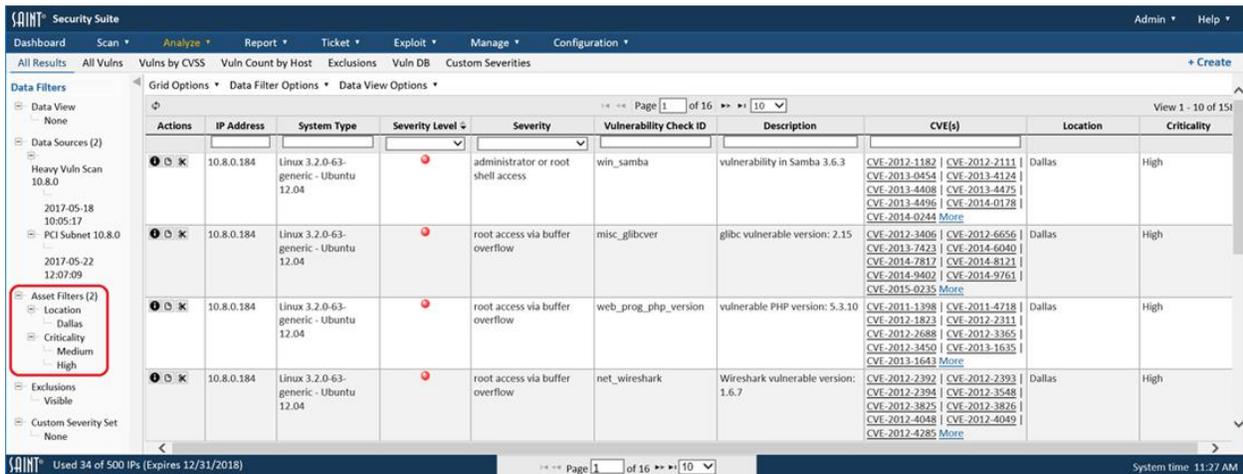
- Select a Tag Name for the tag(s) to be displayed (e.g., Criticality)
- Click on the tag value. Use *control-click* to select multiple options, as in the example below, to see results for both Criticality High and Medium.
- Click the *Add* button to add the filter to the *Filter Criteria* box
- Repeat steps 1-3 to add additional Tag criteria.

In this example, we will filter the scan results to location=Dallas and assets that have been tagged as Criticality High or Medium:



Click *OK* to save the filter criteria.

Close the Asset Filter dialog to view the results constrained by the chosen filter(s).



Custom Severities Set

The Custom Severity Set filter option provides the capability to display and compute vulnerability results based on the severities defined locally, rather than by external sources

such as SAINT's Severity categories or NIST's CVSS scores. The Custom Severity Set drop-down menu option is available from any page used to display or compute scan results. For example, in the following screen shots, Severity codes of Severe, High, Medium, Low and Acceptable have been previously defined as the "Internal Severity Standards" using the [Custom Severities](#) data management page found under the Analyze tab. The Dashboard displays computed results, data drill-down and charts based on the vulnerabilities associated with the selected Severity Set. The Analysis tab then provides a more detailed view, displaying the custom severity codes for individual vulnerabilities that are associated with:

The screenshot shows the SAINT Security Suite Dashboard. On the left, the 'Data Filters' sidebar has 'Custom Severity Set' set to 'Internal'. The main dashboard area shows a summary of 19 Critical and 66 Potential vulnerabilities. A 'Custom Severity Counts' dropdown is highlighted with a red circle, showing 238 High, 84 Medium, and 0 Low vulnerabilities. A 'Total Vulns by Custom Severity' pie chart is also highlighted with a red circle, showing 238 (72.9%) High, 84 (25.9%) Medium, and 7 (2.1%) Low vulnerabilities. Below the summary are two tables: 'Concern Severity Details' and 'Concern Severity Details' (repeated), showing individual vulnerability entries with their IP addresses, severity levels, and associated CVEs.

The screenshot shows the SAINT Security Suite Analysis tab. The 'All Results' section is active, displaying a table of vulnerabilities. The 'Custom Severity' column is highlighted with a red box, showing values like 'High' for several entries. The table includes columns for Actions, IP Address, System Type, Severity Level, Severity, Vulnerability Check ID, Description, CVE(s), and Custom Severity. The 'Custom Severity Set' in the sidebar is also highlighted with a red box, set to 'Internal'.

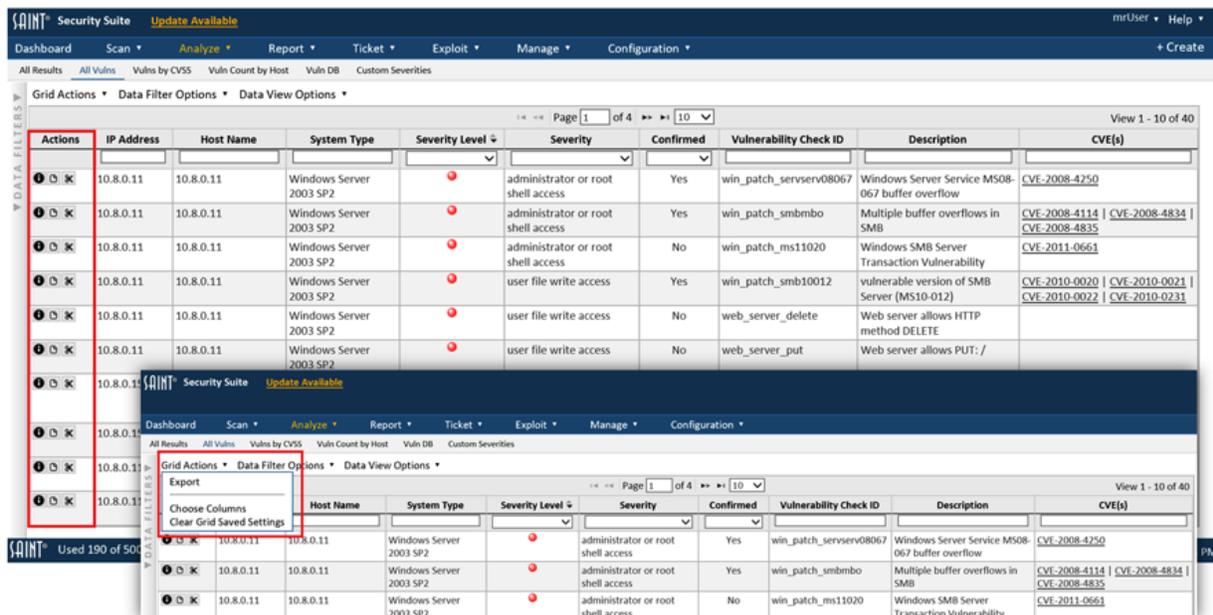
Actions	IP Address	System Type	Severity Level	Severity	Vulnerability Check ID	Description	CVE(s)	Custom Severity
🔍 📄 🗑️	10.8.0.184	Linux 3.2.0-63-generic - Ubuntu 12.04	High	High	win_samba	vulnerability in Samba 3.6.3	CVE-2012-1182 CVE-2012-2111 CVE-2013-0454 CVE-2013-4124 CVE-2013-4408 CVE-2013-4475 CVE-2013-4496 CVE-2014-0178 CVE-2014-0244 More	High
🔍 📄 🗑️	10.8.0.184	Linux 3.2.0-63-generic - Ubuntu 12.04	High	High	net_wireshark	Wireshark vulnerable version: 1.6.7	CVE-2012-2292 CVE-2012-2292 CVE-2012-2394 CVE-2012-3548 CVE-2012-3825 CVE-2012-3826 CVE-2012-4048 CVE-2012-4049 CVE-2012-4285 More	High
🔍 📄 🗑️	10.8.0.184	Linux 3.2.0-63-generic - Ubuntu 12.04	High	High	misc_glibcver	glibc vulnerable version: 2.15	CVE-2012-3406 CVE-2012-6656 CVE-2013-7423 CVE-2014-6040 CVE-2014-7817 CVE-2014-8121 CVE-2014-9402 CVE-2014-9761 CVE-2015-0235 More	High
🔍 📄 🗑️	10.8.0.184	Linux 3.2.0-63-generic - Ubuntu 12.04	High	High	web_prog_php_version	vulnerable PHP version: 5.3.10	CVE-2011-1398 CVE-2011-4718 CVE-2012-1823 CVE-2012-2311 More	High

Grid Actions

Action Types

The following is an example analysis page that illustrates the types of actions that can be taken on data displayed the grids throughout the product. There are two methods for effecting actions on content in the product.

- For grid actions on individual rows, these actions are presented as graphical icons with text displayed when you mouse over the icon. Row level actions such as “get detail”, “set exclusion”, “view tutorial”, “delete”, and “security” effect change on the selected row.
- The second method is to select one or more rows, and use the top level “Grid Actions” dropdown menu to effect changes on the grid or selected rows, such as, “Choose Columns”, “Clear Grid Saved Settings”, “Export”, “Delete selected rows” and changing “Security”. The “All Results” and “All Vulnerabilities” grids also have the option to generate a Full Scan report by selecting “Report” from the “Grid Actions” dropdown menu. This report only shows vulnerabilities as filtered in the grid and uses visible grid columns to populate the report vulnerability list and modify the report in other ways.



Icon Descriptions

The following describes these and other actions:

Icon	Grid Option
	Reload/Refresh grid content
	Column selector
	Clear grid's saved settings
	New – add new record
	Upload (input) content
	Edit selected record; Rename custom policy; Bulk update tickets
	Delete selected record
	Enable selected record
	Disable selected record
	Tool icon used in Exploit Tools setup and execution
	Disconnect
	Exploit connections log
	Export CSV
	Export XML
	Send mail
	Information about selected record
	Run selected exploit
	Re-run
	Tutorial
	Set/View exclusion
	Copy; Clone a rule set
	Permissions
	Search
	Quarantine

Using the Results Grids

Many of the results you will see throughout the user interface (UI) rely on lists of data. Whether that is a list of scan jobs, scan results, exploit results or reports, the use of these list views are presented in much the same manner as a spreadsheet. There are instances where some features or functions are unique to a specific tab or page. In those instances, help will be found in the applicable section of this documentation. However, this section is intended as a primer on the basic layout and features found consistently across the UI and to provide a single location for presenting how these grids function.

The following shows an example of a data grid for the *Analyze* tab, and shows the results of a recent scan job.

Actions	IP Address	System Type	Severity Level	Severity	Description	CVE(s)	Exploit	Exclusion
	10.8.0.11	Windows Server 2003 SP2		administrator or root shell access	Windows Server Service MS08-067 buffer overflow	CVE-2008-4250	CORE EDB-16362 EDB-6824 EDB-6841 EDB-7104 EDB-7132 SAINTEXPLOIT-954	No
	10.8.0.11	Windows Server 2003 SP2		administrator or root shell access	Multiple buffer overflows in SMB	CVE-2008-4114 CVE-2008-4834 CVE-2008-4835	CORE	No
	10.8.0.11	Windows Server 2003 SP2		administrator or root shell access	Windows SMB Server Transaction Vulnerability	CVE-2011-0661		No
	10.8.0.11	Windows Server 2003 SP2		user file write access	vulnerable version of SMB Server (MS10-012)	CVE-2010-0020 CVE-2010-0021 CVE-2010-0022 CVE-2010-0231	CORE EDB-15266	No
	10.8.0.11	Windows Server 2003 SP2		user file write access	Web server allows HTTP method DELETE			No
	10.8.0.11	Windows Server 2003 SP2		user file write access	Web server allows PUT: /			No
	10.8.0.150	Windows Server 2008 R2		administrator or root shell access	Windows http.sys range header parsing vulnerability (MS15-034)	CVE-2015-1635	CORE EDB-36773 EDB-36776	No
	10.8.0.150	Windows Server 2008 R2		user shell access	default device password (ftp:ftp)	CVE-1999-0507 CVE-1999-0508		No

As shown in the example, results can contain text; numbers; images that may portray color and text alternatives that highlight a key data point; Boolean values (yes/no) that communicate whether a result is true/value, exists or does not exist; and also hyperlinks from a displayed value to an internal or external reference. Each grid may also contain buttons or icons on the row to offer additional information about a row's content; as well as additional options that effect the selected row, as described in the [Grid Actions section](#).

View a Record's Details

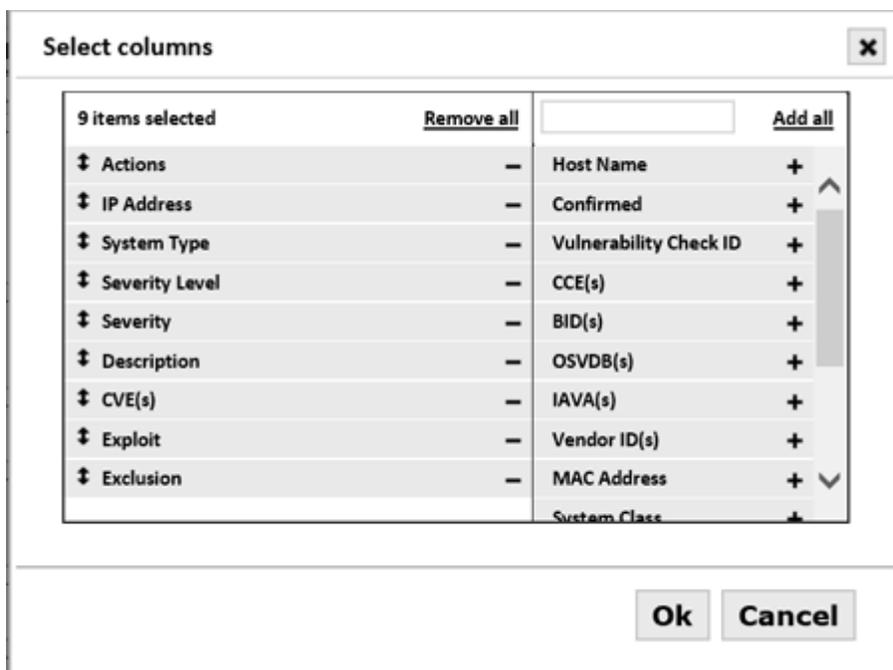
Some results grids only show a subset of the total number of available fields/columns for data being displayed. In most instances, there are two methods for viewing all information for a record. First, you can click on the Information (i) action of the record you wish to view. Alternatively, you can double click on the record to see further details.

Column Selector

The results grids provide default column values based on the information relevant to the chosen tab. However, you can choose the columns to be displayed by clicking the column selector in the Grid Actions dropdown menu. The column selector will then display the columns currently selected in the left side of the pop-up, and other available columns (if applicable) in

the right column. Use the (-) sign to remove a column from the grid and the (+) sign in the right column to add columns. You can also add all columns quickly by clicking on the *Add all* option.

You can also click and hold your mouse button on a column in the left column and drag it up/down to reorder the columns (drag a column up to move it to the left in the grid; drag a column down to move it to the right in the column order.)



Column Sorting

You can also sort data in a data grid (ascending and descending order) by clicking on a column heading. Clicking the heading again will re-order the data in the opposite sort order.

Column Search and Filtering

The grid feature also provides the capability to filter data content by a value found in a specified column. There are two ways to filter data.

The first method is to select a value from a column's drop down list. The example below shows filtering scan results for the selected scan data, by vulnerabilities based on "privilege elevation."

Page 1 of 4				
Severity Level	Severity	Description	CVE(s)	Exploit
	Critical Problems administrator or root shell access user shell access user file write access Areas of Concern susceptibility to malicious content privilege elevation information gathering Potential Problems check it out for possible vulnerabilities do you want this accessible on the Internet?	MS08-	CVE-2008-4250	CORE EDB-16362 EDB-6824 EDB-6841 EDB-7104 EDB-7132 SAINTEXPLOIT-954
		in	CVE-2008-4114 CVE-2008-4834 CVE-2008-4835	CORE
	administrator or root shell access	Windows SMB Server Transaction Vulnerability	CVE-2011-0661	
	user file write access	vulnerable version of SMB Server (MS10-012)	CVE-2010-0020 CVE-2010-0021 CVE-2010-0022 CVE-2010-0231	CORE EDB-15266

The second method is to simply type a value in the column search field. The following example filters the scan results to display only hosts and vulnerabilities based on issues with the "buffer" as in buffer overflows:

View 1 - 4 of 4			
Description	CVE(s)	Exploit	Exclusion
buffer			
Windows Server Service MS08-067 buffer overflow	CVE-2008-4250	CORE EDB-16362 EDB-6824 EDB-6841 EDB-7104 EDB-7132 SAINTEXPLOIT-954	No
Multiple buffer overflows in SMB	CVE-2008-4114 CVE-2008-4834 CVE-2008-4835	CORE	No
Windows DNS Server RPC Management Interface Buffer Overflow	CVE-2007-1748	CORE EDB-16366 EDB-16748 EDB-3737 METASPLOIT SAINTEXPLOIT-942	No
Possible buffer overflow in Active Directory			No

Some columns have optional search operators next to the search field. Entering a value in the search field and selecting an operator allows further control of filtering. The following example filters the scan results to display only records with CVSS score greater than "8".

Page 1 of 5 >> >> 10

Click to select search operation.

Vulnerability Check ID	Description	CVE	CVSS Score
win_patch_servserv08067	Windows Server Service MS08-067 buffer overflow	CVE-2008-4250	> 8
win_patch_smbmbo	Multiple buffer overflows in SMB	CVE-2008-4834	> greater
win_patch_smbmbo	Multiple buffer overflows in SMB	CVE-2008-4835	>= greater or equal
win_patch_ms11020	Windows SMB Server Transaction Vulnerability	CVE-2011-0661	= equal
			<= less or equal
			< less

Navigating through Results Pages

Every grid displays the total number of results retrieved for a given result; as well as the total number of rows per page, and number of pages that contain the results. Each grid provides a convenient method for managing large data sets by displaying only a limited number of records per page, and providing page navigation arrows to navigate between pages. All results grids also give you control over the total number of results to display on a page by selecting the total number of pages from the drop down list to the right of the paging arrows, as shown in the example below.

The screenshot shows the SAINT Security Suite interface. At the top, there is a navigation bar with tabs for Dashboard, Scan, Analyze, Report, Ticket, Exploit, Manage, and Configuration. Below this is a sub-navigation bar with options like All Results, All Vulns, Vulns by CVSS, Vuln Count by Host, Vuln DB, and Custom Severities. The main area contains a grid of vulnerability results. The grid has columns for Host Name, Severity Level, Severity, Vulnerability Check ID, Description, CVE, and CVSS Score. The grid shows three rows of results for host 10.8.0.11. A blue toolbar is visible at the bottom of the grid, containing page navigation controls and a system time indicator.

Note that the bottom blue toolbar is persistent, in that it is always visible to you as you scroll up and down with the grid. The top grid paging controls are contained within the grid header. However, the blue toolbar enables paging without having to scroll to the top or bottom of a grid to locate the controls.

Scan

The *Scan* menu contains the primary interface for creating and managing scan activity. This includes creating target groups to centrally manage the collection of “like” hosts to be targeted for scanning; managing Assets (discovered/scanned hosts); viewing the extensive list of vulnerability checks for individual SAINT scan policies; adding custom checks to those policies as well as adding custom policies; creating and managing credentials that can be applied to scan jobs on a recurring basis; and creating scan jobs for immediate use or scheduled at a pre-defined time, or setting up recurring scans based on a defined job.

As shown below, the Scan Jobs page provides a data grid to enable you to view, sort, search, and manage scan Jobs and the Scans executed from these jobs. You can obtain information about specific records or perform other actions such as running existing jobs, or using the options from the Grid Actions drop-down to perform actions as reloading the grid content (refresh), creating a new Job, and identifying what columns you wish to view or resorting the view. Refer to the [Using the Results Grid](#) section for more detail on the definition and usage of these options.

Actions	Job #	Job Name	Owner	Last Run	# Scans	Target Group	# Targets	# Schedules
<input type="checkbox"/> [Info] [Run] [Refresh] [Delete] [Add]	7	Remote lab vulns	admin	2017-07-03 11:28:56 (Completed)	2	saint-data	256	0
<input type="checkbox"/> [Info] [Run] [Refresh] [Delete] [Add]	6	Web App scan	admin	2017-06-30 08:51:11 (Completed)	1	saint-data	1	0
<input type="checkbox"/> [Info] [Run] [Refresh] [Delete] [Add]	5	HR Group Vuln scan	admin	2017-06-30 11:44:45 (Completed)	2	saint-data	5	1
<input type="checkbox"/> [Info] [Run] [Refresh] [Delete] [Add]	4	Exec group vuln scan	admin	2017-06-30 11:30:17 (Completed)	2	saint-data	3	1
<input type="checkbox"/> [Info] [Run] [Refresh] [Delete] [Add]	3	Data Center 1 Discovery	admin	2017-06-30 08:17:51 (Completed)	1	saint-data	256	0
<input type="checkbox"/> [Info] [Run] [Refresh] [Delete] [Add]	2	vers81519vulns	admin	2017-07-03 11:42:11 (Completed)	3	saint-data	5	0
<input type="checkbox"/> [Info] [Run] [Refresh] [Delete] [Add]	1	vers8_15_19	admin	2017-06-28 14:17:39 (Completed)	1	saint-data	256	0

Jobs Tab

A **job** is a main object for setting up and executing scans. Jobs can be associated with target groups during job setup, or can be run outside of a target group. A job can be run as single scans, or can be configured for recurring, continuous scans based on the job’s defined targets,

policies, credentials, configurations, notification workflows and schedule. As with target groups, *Manage Jobs* main display presents all available jobs in a list view in a results grid.

With the applicable role-based permissions, you can sort this list, perform column searches, see detailed information about a record in the display, or take other actions such as adding/removing columns, refreshing the display to dynamically update the content with any new content since you entered the grid, and take other actions related to creating, editing and deleting content. The following describes these features in more detail.

Single and Multi-Node Scan Support

For installations that are using only a single scan engine (local scanner node), such as standalone installations or shared installations that are scanning reasonably small environments, you will enter targets into the *Enter Target(s)* tab named local node. SAINT's architecture also provides support for multiple scanner node deployments to support large environments or distributed scan needs. The scan job setup process for this type of implementation will be a bit different, in that the target setup process will display both the local node (or whatever custom name your administrator has chosen for it), and a + (add) option to choose other available nodes to scan specific targets or to be used as part of a load balanced scan process. The following describes the job setup process for either a single or multi-node deployment.

Create a New Job

For quick, uncredentialed scans, scan jobs can be run by entering a job name and selecting the applicable scan policy in Step 1; entering a target in Step 2; and clicking the FINISH button to run the job "immediately" in the *Summary* tab. This three-step process then uses pre-defined configuration settings to execute the scan on the target hosts. Scans can also be set up with more advanced configurations; with multiple targets or based on targets already defined in a target group or by asset tags; target credentialed/authentication; specific scan configuration settings and notification work flows; as well as based on scheduled or recurring scan needs. The job wizard provides a step-by-step approach to setting up these options. Each is described in more detail in the following sections.

To create a scan job, click on the *Create* option (upper right corner of the screen) from any page, or select *Grid Actions > Create Job* from the Jobs grid on the Scan page. The job creation wizard will be displayed to walk through the steps for creating a scan job:

Step 1 – Scan Info

Name and Description

Enter a name for the new job. Enter a detailed description to communicate the purpose of the job and other details pertinent to the job.

Category and Scan Policy

Scan policies control the types of probes and checks that are executed for defined targets.

These policies are categorized for ease of management and include subject-matter groups such as compliance, platform and type of scan.

1. Select a scan policy by first selecting a category from the *Select Policy Category* drop down list.
2. Select a policy for the category by clicking on the policy name in the *Select Policy* drop down list. Then, click *Next* to enter the host targets to be scanned

Each category and their applicable policies are described below.

Information Gathering

- **Discovery** – This is the least intrusive scan. SAINT identifies hosts which are alive and fingerprints their host type. If desired, the live hosts can then be pre-selected when

creating a new job after the discovery scan finishes, using the *Choose Targets from a Previous Scan* option in step 2.

- **Port scan** – For this policy, SAINT will identify live hosts and check for services listening on TCP or UDP ports. The range of ports to check is determined by the ports to scan settings on the *Options* page.
- **Web Crawl** – For this policy, SAINT detects web directories on the targets. It does so by first scanning ports for web services, and then finding directories by following HTML links starting from the home page.
- **Content Search** – For this policy, SAINT searches files on Windows and Linux/Mac targets for credit card numbers, social security numbers, or any other specified patterns. See the SAINT [Configuration section](#) for more information on configuring SAINT's file content searching feature. Authentication is required for this policy and if scanning a Linux/Mac target, SSH must be enabled.
- **Anti-virus (AV) information** – For this policy, information is collected about installed AV software, such as last scan date, enabled, definition file dates, and other information useful for auditing requirement 5 of the PCI DSS. Information is currently gathered for Windows versions for many of the most popular AV software products in use today, such as: Vipre Business Agent, McAfee, Symantec, AVG, F-Secure, MS Forefront, Kaspersky, and Trend Micro. Note that some results are only reported if they are considered vulnerabilities while others are always reported. For example, if available, the last scan date is always reported while a check to determine if updates or the AV software itself is enabled, only gets reported if it's disabled. Authentication is needed to run this scanning policy. Facts containing the string '(Master)' mean that an anti-virus server/manager/admin is installed on the target. For more information, see [Configuration options](#); also see the knowledge base on the mySAINT customer web site.
- **Auth Test** – For this policy, SAINT performs authentication against the targets using the credentials specified in either the credentials manager or the Windows/Linux/Unix/Mac input boxes under the *Authentication* tab. User can generate reports from this test by selecting the Auth Test report template from the report creation wizard.
- **Software Inventory** – This policy generates a list of software installed on Windows targets. Authentication is required. The software list retrieved during the scan is displayed in the Vulnerability List section of the Full Scan or the Overview reports. Note that the software list is generated by enumerating the Uninstall key in the Windows registry. Therefore, only software which was registered with the operating system during installation will be included. Software which was placed on the system without running an installer program is typically omitted. Furthermore, registered software

which was incorrectly removed from the system may still be included in the list after removal.

Vulnerability

- **Full Vulnerability Scan** – For this policy, SAINT will check for services listening on TCP or UDP ports. Any services detected will then be scanned for any known vulnerabilities. This scan policy includes SAINT's entire set of vulnerability checks, and is the scan policy that should be used in most situations.
- **Windows Patch** – For this policy, SAINT checks for missing Windows patches. Since most of the checks for Windows patches require authentication, Windows domain authentication is recommended with this policy.
- **Win Password Guess** – This policy conducts password guess checks against Windows targets using the password guess and password dictionary configuration options. Authentication is recommended so SAINT can enumerate accounts.
- **Microsoft Patch Tuesday** – This policy checks for the latest published Microsoft patch Tuesday vulnerabilities (second Tuesday of each month). This policy and associated content is typically updated via SAINTexpress by noon Wednesday, following publication of Bulletins from Microsoft.
- **Web (OWASP Top 10)** – This policy checks for vulnerabilities in web servers and web applications, such as SQL injection, cross-site scripting, unpatched web server software, weak SSL ciphers, and other OWASP Top 10 vulnerabilities. It also enables file content checks. Authentication is recommended or required for some of the checks included in this policy. SAINT OWASP Top 10 Coverage is detailed in the table below. [More information about OWASP Top 10.](#)

OWASP	Examples	SAINT ID	Authentication
A01:2021-Broken Access Control	Direct URL Access	web_prog_cgi_directurlaccess	Web authentication recommended
A02:2021-Cryptographic Failures	Unencrypted Content	misc_checkmachine	Operating system authentication required
		misc_webcontentsearch	Web authentication recommended
	Cleartext password transmission	web_security_clearbasicauth web_security_clearpass	Authentication not required

	TLS/SSL weak algorithms and invalid certificates	misc_cipher_* misc_tls_*	
	Session cookies without "secure" flag	web_security_httpssecure	
A3:2021-Injection	SQL Injection	web_prog_sql_*	Web authentication recommended
	Command Injection	web_prog_cgi_cmdinject	
	CRLF Injection	web_prog_cgi_responsesplit	
	SSI Injection	web_prog_cgi_ssiinject	
	XPath Injection	web_prog_cgi_xpathinj	
	Cross-site scripting	web_prog_cgi_xssgeneric web_prog_cgi_xsstored	
A04:2021-Insecure Design	Insecure design	This item cannot be detected by a vulnerability scan.	
A05:2021-Security Misconfiguration	Software patches	web_server_*	Operating system authentication recommended
	Default passwords	net_password pass_httpbasic pass_webapp	Authentication not required
	Error Message Information Leakage	web_security_errorinfo	
	Missing or Incorrect Security Headers	web_security_mimesniff web_security_clickjack web_security_httponly web_security_sslcache	
	XXE vulnerability	web_service_xxe	Web authentication recommended
	Vulnerable Server Software	web_server_*	

A06:2021-Vulnerable and Outdated Components	Vulnerable Development Frameworks	web_dev_* win_dotnet*	Operating system authentication recommended
	Vulnerable Libraries	web_lib_*	Web authentication recommended
A7:2021-Identification and Authentication Failures	Weak Passwords	net_password pass_httpbasic pass_webapp	Authentication not required
	Cleartext Password Transmission	web_security_clearbasicauth web_security_clearpass	
	Session IDs in URL	web_security_urlrewriting	
	Session Fixation	web_security_sessionfixation	Web authentication required
A08:2021-Software and Data Integrity Failures	Insecure deserialization	web_dev_jvaserialobject	Web authentication recommended
A09:2021-Security Logging and Monitoring Failures	Security Logging and Monitoring Failures	This item cannot be detected by a vulnerability scan.	
A10:2021-Server-Side Request Forgery	Server Side Request Forgery	web_prog_cgi_ssrf	Web authentication recommended

- **Operating System Password Guess** – This policy includes all SAINT password guessing features designed to guess the operating system password. This policy includes checks for default FTP passwords, as well as dictionary-based password guessing via Telnet, SSH, and FTP. Authentication is recommended to ensure user account enumeration.
- **Mobile Device** – This policy queries Active Directory servers for information about mobile devices (for example, phones and tablets) which use Exchange ActiveSync, and uses that information to infer vulnerabilities on those devices. The devices which are discovered in this manner will be listed in the scan results as separate targets although those targets aren't actually scanned. In order for this policy to succeed, OpenLDAP must be installed on the scanning host, and the scan must run with Windows domain administrator credentials (see [Step 3 – Authentication](#)). The target list must include at

least one Active Directory server, and the SSL certificate for that Active Directory server should be installed and configured on the scanning host. (See [Authenticating to Windows Targets.](#))

- **Network Device** – This policy checks for vulnerabilities in routers, switches, and other networking devices.
- **Log4j** – This policy scans for vulnerabilities in the Log4j Java library. It includes checks for remote Log4j attack vectors, a filesystem search for vulnerable versions of Log4j, and checks for other software which is known to include vulnerable versions of Log4j. Windows or Linux authentication is recommended for a thorough scan.

Legacy

- **Normal** – For this policy, SAINT collects information from the DNS (Domain Name System), tries to identify the operating system, and tries to establish what RPC (Remote Procedure Call) services the host offers and what file systems it shares via the network. The policy also includes probes for the presence of common network services such as finger, remote login, FTP, WWW, Gopher, e-mail, and a few others. With this information, SAINT finds out the general character of a host (file server, diskless workstation) and establishes the operating system type and, where possible, the software release version.
- **SQL/XSS** – For this policy, SAINT checks for SQL injection and cross-site scripting vulnerabilities on web servers. This includes both generic tests, where SAINT finds HTML forms and tests all parameters for SQL injection and cross-site scripting, and checks for known SQL injection and cross-site scripting vulnerabilities.

PenTesting

- **Discovery** will discover live hosts in the selected address range, and then stop. This level does not require a license key. It is useful for figuring out which IP addresses to put in your key. The discovery method depends on the selected Host Discovery option.
- **Information Gathering** will discover live hosts, try to determine their operating system types, and scan their ports.
- **Single Penetration** will include all of the above steps and then proceed to run remote exploits for the detected operating system and services, starting with those least likely to cause crashes, until one succeeds in establishing a shell connection.
- **Root Penetration** is similar to single penetration but continues until the maximum privilege level is reached on the target. The maximum privilege level is root on a Unix or Linux system and administrator on a Windows target. The root penetration level also runs local exploits if the available remote exploits result in a connection without maximum privileges.

- **Full Penetration** will run all available exploits for the detected operating system and services. This level is the best choice if the objective is to exploit as many vulnerabilities as possible. However, if the objective is to obtain evidence of penetration, such as files or screen captures from the target, then this level is not the best choice because a successful connection could be severed if a later exploit causes a crash.
- **Web Application** will search the target for Web applications, and run all available exploits against those applications. This level is the fastest way to find exploitable Web application vulnerabilities such as SQL injection.

The PenTest job setup also provides a step for entering credentials to authenticate to the targets. However, the login and password are not typically needed for the exploits themselves. For the purpose of penetration testing, authentication is helpful for determining operating system differences, such as service pack levels or Linux varieties, more precisely than would be possible using unauthenticated methods. This information also aids the pen test engine in choosing the correct arguments when running exploits, and may improve the success rate.

Compliance

- **PCI External** – This scan policy, when run by an Approved Scanning Vendor (ASV) in accordance with the ASV Program Guide, satisfies the quarterly external scan requirement outlined in PCI DSS section 11.2.2. It is similar to the Vulnerability Scan policy, but includes all 65535 TCP ports and only common UDP ports, enforces a spider depth of at least 5, enables certain low severity checks which are normally disabled, and reduces the restrictiveness of certain other checks.
- **PCI Internal** – This scan policy satisfies the quarterly internal scan requirement outlined in PCI DSS section 11.2.1. Unlike the PCI External policy, it does not include all 65535 TCP ports.
- **FISMA** – This scan policy provides support for security controls related to continuous monitoring, as well as performing risk assessments. Selecting this scan policy ensures that probes scan for the entire set of vulnerability checks, with the *Exhaustive* option. SAINT also provides a pre-configured report template that describes the supported controls and reports results at a summary and detailed level.
- **HIPAA** – This scan policy provides support to HIPAA security requirements related to both risk analysis and overall risk management. Selecting this scan policy ensures that probes scan for the entire set of vulnerability checks, with the *Exhaustive* option. SAINT also provides a pre-configured report template that describes the supported controls and reports results at a summary and detailed level.

- **NERC CIP** – The NERC CIP compliance scanning policy reports the results of an exhaustive vulnerability scan on selected hosts. SAINT also provides a NERC CIP report template to use the results of this scan policy that describes the applicable NERC CIP security controls, as well as a pre-formatted report with executive level graphs/charts and detailed level scan results.
- **SOX** – The SOX scan policy runs all available vulnerability checks against selected targets, and supports financial organizations’ internal risk management strategies, as well as facilitating provisions in Section 404 of the Sarbanes-Oxley Act, requiring a management report annually on the effectiveness of internal controls for financial reporting and that external auditors confirm management’s assessment.
- **IAVA** – This compliance policy executes a full port scan for all vulnerabilities reported in the Information Assurance Vulnerability Alert (IAVA).
- **NESA** – The NESA report template provides a background on the Information Assurance Standards specified by the United Arab Emirates National Electronic Security Authority (NESA) and reports all available information, including charts, tables, hosts, vulnerabilities, services, users, shares, and technical details.

Host-Based

These scan policies require an agent to be installed on the asset being scanned. See [Managing Agents](#) and [Host-based Assessments](#) for more information.

Custom Policies

- SAINT provides the capability through the *Scan Policies* page to create new checks, enable/disable existing checks and create custom policies based on local requirements. Custom scan policies can then be viewed by selecting *custom* from the *Select Policy Category* drop down list, and then the applicable policy from the *Select Policy* drop down list. See the section on [Scan Policies](#) for more information on creating a custom scan policy.

Scan Policy Options

The following options can be used to modify some of the scan policies described above.

- **Exhaustive** – During the course of a scan, there are certain cases where it seems unlikely that there would be any benefit to running a certain instance of a probe, but it may still be worthwhile to do so for the sake of being as thorough as possible. Examples include checking for default router passwords on non-standard telnet ports, checking for web application vulnerabilities in non-standard directories, and checking for proxy vulnerabilities on non-standard HTTP ports. The exhaustive scanning option allows you to control what SAINT does in these cases. Enabling this option results in a more thorough scan, but may cause the scan to take more time but will take extra steps to be

as thorough as possible. This option affects the vulnerability, PCI and custom scan policies.

- **Allow Dangerous Tests** – By default, SAINT takes a conservative approach and does not run checks which could have harmful side effects, but this makes it impossible to confirm certain vulnerabilities. However, if an extreme scan is run, the scan may include "dangerous" checks, in which attacks designed to crash services are launched in order to confirm that the target is or is not vulnerable. These tests may help SAINT eliminate false alarms by verifying the existence of certain vulnerabilities but can cause services on the target hosts to crash as a result. Another side-effect of dangerous tests is that successful detection of a vulnerability could cause other vulnerabilities to be missed. That is, if a test crashes a service on the target, then any further tests against that service will come up negative. Targets should be re-scanned after the known vulnerabilities have been fixed in case there are other vulnerabilities that were missed because the service crashed. This option affects the vulnerability and custom scan policies.

Step 2 – Targets

Create New Job

1 Scan Info
Basic setup and scan policy selection.

2 Targets
Select scan targets.

3 Authentication
Select credentials.

4 Advanced
Additional options.

5 Finish
Create schedules and select ticket rule set.

Step 2: Select Scan Targets

Enter Scan Targets

Local Node

Enter target(s) ? Selected Target(s)

Node Information
Description: SAINT Built-In Scanner
Status: Active

More Options...

Remove All

Enter Target Restrictions

Enter target(s) ? Target Restrictions(s)

Previous Next Finish

1. By default, Security Suite and SAINTCloud provide access to a single scanning engine (aka "local node"). SAINT also provides support for a multi-scanner (aka multi-node) architecture. When defining hosts to scan, step two of the wizard will display the primary scanner as the highlighted tab (as shown above) as well as providing the capability to select this or other scan nodes on which to run the scan from the tabs in the Enter Scan Targets area. If the desired node is not shown, choose the "+" tab and select it from the drop-down menu. (If the "+" tab is not shown, then all allowed nodes are already shown.)

To run a scan on multiple nodes, select the desired scan nodes one at a time, and enter the targets to be scanned by each node under the corresponding tab

Optional – Check the *Load Balance* box if a load balanced scan is desired. With this option, the targets will be divided evenly among all available nodes, and the scan will be queued until at least two nodes are available. Click on the *Configure* button to customize the minimum number of nodes and the set of nodes among which to run the scan.

2. Enter the targets (desktops, servers, routers, etc.) to be scanned for this job. By default, this is done individually through the *Enter Target(s)* field, but other options are available by clicking on *More Options*. See [Target Entry Options](#) for more information about these other options. SAINT allows target selection in one or any combination of several formats:
 - Host names – one or more host names. SAINT must be able to resolve the host names, either using a DNS server or the `/etc/hosts` file or an error will result.
 - IP addresses – one or more IP addresses.
 - Subnets – one or more class C subnets, represented as only the first three octets. SAINT will expand the subnet to include every IP address beginning with the given three octets.
 - IP address ranges – one or more IP address ranges. Each range consists of a beginning and ending IP address, separated by a dash. SAINT will expand the range to include the starting and ending addresses and every address in between.
 - URLs – one or more URLs, such as `http://hostname:port/path`. SAINT will scan the target specified in the hostname portion of the URL, specifically including the web program(s) found on the specified port and path.

- CIDR network addresses – a network address followed by a slash and a prefix length. For example: 192.30.250.0/18.
- Previous Scan – use the host information collected from previous scans to select hosts to scan.
- Passively Discovered Hosts – Scan devices which have been recently seen on the network, if [Passive Host Discovery](#) is enabled.
- Target Groups – select a pre-defined Target Group to quickly load the target list, or create a target group at scan run time based on the live hosts discovered during the scan.
- Asset Tags – defined assets to be scanned by Asset Tags assigned in the Asset table.
- Active Directory – configure the scanner to connect to an AD server to collect host information.
- Amazon Web Services (AWS) – connect to AWS instances
- Azure – connect to hosts residing in Microsoft Azure
- Imported File – import host lists from an imported file
- Docker images – Scan Docker images from a registry or repository.
- Infoblox – Import targets from Infoblox.

Note: All of these with the exception of Subnets can be used with both IPv4 and IPv6 addresses. Most of SAINT's vulnerability checks work on IPv6 targets, as long as any system tools which the check uses (Samba, rpcinfo, Telnet, etc.) are also IPv6-compatible. Only the Linux version of SAINT is IPv6-compatible. Note that IPv6 addresses must be specified by IP address, not by host name. The required Perl modules for running IPv6 exploits are Socket6 and IO-Socket-INET6. Both are available from www.cpan.org. Also, note that IPv4 and IPv6 addresses can be scanned together in the same job, with the exception of Subnet target.

Note: Targets can be removed from the list at any time in the job setup, by selecting the “x” pinned to a target shown in the selected targets box.

Optional – Target restrictions can also be set by entering the target(s) in the *Target Restriction* field. This can be useful, for example, if you must exclude specific IP addresses, hostnames, Internet domains, IP address ranges, subnets, or CIDR blocks from the scan.

- Click *Next* to manually configure other job settings OR click FINISH to use pre-defined scan configuration settings and either a) save the job without executing a scan at this time or b) choosing when to run the job once the job is saved.

Step 3 – Authentication

Optional – Use this tab if you wish to run an authenticated scan and you have the knowledge of a login and password to the targets.

Create New Job

1 Scan Info
Basic setup and scan policy selection.

2 Targets
Select scan targets.

3 Authentication
Select credentials.

4 Advanced
Additional options.

5 Finish
Create schedules and select ticket rule set.

Step 3: Authentication and Credentials

Default Credentials

Enter default credentials for this scan. These credentials will be used on each host to attempt authenticated scans against certain services.

Microsoft Windows Domain (Admin):	+ Set	Oracle Server:	+ Set
Windows Domain (non-admin):	+ Set	Microsoft SQL Server:	+ Set
Unix, Linux, MacOS, etc.:	+ Set	MySQL Server:	+ Set
HTTP Basic:	+ Set	SNMP Version 3:	+ Set
Amazon Web Services (AWS):	+ Set	Web Application:	+ Set
Microsoft Azure:	+ Set		

Credentials Manager

The credentials manager allows you to securely store credentials on a per-host basis. By default, these credentials will be used in place of any default credentials entered above when appropriate.

Use stored credentials if available [Manage stored credentials](#)

Previous Next Finish

Scans can be executed without providing account credentials (i.e., authentication) to the target hosts. However, providing authentication credentials does enable scan probes to access the registry, file attributes, or package lists on remote targets, and provide a much more in-depth scan. There are three benefits to authentication. First, an authenticated scan can detect additional vulnerabilities, such as client vulnerabilities and missing hotfixes, which could not otherwise be detected by probing network services. Second, an authenticated scan is sometimes able to check for fixes whose presence could not otherwise be determined, thereby reducing false alarms. Third, an authenticated scan may be able to gather additional information related to the targets, such as user lists, software inventory, or mobile devices

which sync with the target. Besides authentication to operating systems, authenticating to specific services offers additional benefits. For example, authenticating to web servers allows access to pages within web applications that may be affected by vulnerabilities such as SQL injection or cross-site scripting. Authenticating to database services allows inspection of objects within the database system for security weaknesses. Authenticating to the SNMP service will allow SAINT to collect certain system properties when SNMPv3 is being used.

Default Credentials

This Authentication option enables you to enter a single user/password combination for each authentication type on all targets.

1. Click on the *+ Set* button for the required platform. For example, Microsoft Windows Domain (Admin).
2. Enter the username and password.
3. Optional – confirm the password by re-entering it in the *Confirm Password* field.
4. Optional – For Windows Domain Admin credentials, you can also click on the *Check Login* button to verify the credentials before continuing. If a "Service unavailable" message is displayed, this typically means the target host was offline or is blocking the Windows services used for authentication.
5. Click *Save*.

Further details about the usage for each supported platform's credentials are described in the [Credentials Manager section](#) of this document.

Default credentials are stored with scan jobs using AES-256 encryption with either a permanent or ephemeral encryption key. See [Ephemeral Encryption Key](#) for more information.

Manage Stored Credentials

The *Credentials Manager* allows you to store credentials securely on a per-host basis, by a comma-separated list or by associating the credentials to a pre-defined target list in a target group. The scan engine automatically uses any stored credentials to speed up the scan setup time, and will use a combination of manually entered credentials and the credentials manager if both are used.

- Click on the *Manage Stored Credentials* button to open the *Credentials Manager* grid to view or edit the current list of stored credentials or create a new credentials file for use in the job.

Refer to the [Credentials Manager](#) for more information about creating and storing credentials for each supported platform.

Click *Next* to complete the authentication step.

Step 4 – Advanced

The scan configurations displayed in the Advanced tab are set either by scan default values, locally modified in the global *Configuration* tab, or modified at job-level through this step.

As shown, these configurations enable you to control such settings as discovery controls; port settings; e-mail and report delivery settings; anti-virus and content search settings; and a wide-variety of others. This section will highlight some of the most frequently modified configuration settings. Refer to the [Configuration Tab](#) section for a detailed description of each option.

Host Discovery

SAINT's scanning engine can perform host discovery two ways: using SAINT's proprietary discovery engine, or with Nmap. The SAINT method is simpler to configure, while Nmap allows for more customization.

SAINT Discovery Configuration

In order to avoid wasting time scanning hosts which do not exist or are unreachable, the scanner attempts to discover live hosts at the start of a scan. The method used to discover live hosts varies depending upon whether a firewall is in place.

- **No Firewall Support** – The *No Firewall Support* option is the default, and should be selected if no firewall is in place. With this option, the scanner attempts to send an ICMP echo request (ping) to each host. When the host does not respond, the scanner assumes the host is down and skips further probes.
- **Firewall Support** – If you are scanning targets that are behind a firewall from a system that is not behind the firewall, or in any other case where ICMP does not work, choose one of the *Firewall Support* options. With these options, the scan engine does not rely on ICMP for discovering live targets. Instead, there are two alternate options.
 - **TCP Discovery** – This option causes the scanner to use TCP for discovering live targets. Each potential target in the specified target range will be scanned for a few standard TCP ports. If there is a response, either that the port is open or that the connection was refused by the target, then the host is considered to be alive.
 - **ARP Ping Discovery** – With this option, the scanner will consider a potential target to be alive if the IP address can be resolved to a MAC address using the ARP protocol. The benefits of this method are that it still works even when ICMP pings and TCP ports are blocked, and it is the fastest discovery method. But it only works for targets that are on the same local network as the scanner.
- **Combined Firewall Support** – If you do not know whether your targets are behind a firewall, or if some targets may be behind a firewall while others are not, then choose the *Combined Firewall Support* option. This option uses all of the above discovery methods. It is the slowest option, but also the most likely to succeed in discovering all live targets.
- **Extensive Firewall Support** – This option skips the discovery process altogether and does a complete scan of every target address, regardless of whether it is alive. Hence, *Extensive Firewall Support* can lead to a very slow scan, especially if a large target range was entered. Use this option only when the targets do not respond either to pings or to TCP requests to closed ports, and do not consistently have any of the standard ports open.

See the [Workarounds](#) section for more information on configuring the standard port. The firewall support options are intended only to work around discovery issues, and do not allow the scanner to scan targets behind firewalls which perform network address translation, or IP address masquerading. Hosts behind such firewalls will still be invisible from the outside and thus cannot be scanned from the outside.

Nmap Discovery Configuration

- **TCP SYN Scan** – Sends empty TCP packets with the SYN flag set. Live hosts will reply with either a RST or SYN/ACK TCP packet. An optional list of comma-separated ports may be supplied. If omitted, the default Nmap ports will be used.
- **TCP ACK Scan** – Sends empty TCP packets with the ACK flag set. Live hosts will reply with a RST packet. Some firewalls prevent hosts from replying to SYN requests to closed ports, but may still respond to ACK packets. An optional list of comma-separated ports may be supplied. If omitted, the default Nmap ports will be used.
- **ICMP Echo/Timestamp/Address Mask** – Sends ICMP Echo (type 8), Timestamp (type 13), or Address Mask (type 17) request.
- **UDP Ping** – Sends UDP packets to the given ports. Empty packets will be sent to most ports; however, ports specified in the `config/nmap/nmap-payloads` will send the corresponding packets, which will be more likely to illicit a response.
- **SCTP INIT Ping** – Sends an SCTP packet with the minimal INIT chunk. Live hosts will reply with an ABORT chunk if the port is closed, or an INIT-ACK chunk if it is open. An optional list of comma-separated ports may be supplied. If omitted, the default Nmap ports will be used.
- **IP Protocol Ping** – Sends an IP packet with the specified protocol number set. An optional list of comma-separated protocol list may be supplied. If omitted, the default Nmap protocols will be used.
- **ARP/ND Ping** – Uses Nmap to handle ARP requests instead of the host operating system. This is useful for scanning local LANs and may improve performance. If IPv6 targets are used, then ICMPv6 Neighbor Discovery is used instead of ARP.

Port Settings

Use Heavy Port Ranges – Check this box to include all ports defined in the heavy ports lists (TCP and UDP). Leave this box unchecked to run scan using only ports listed in common ports lists (TCP and UDP).

These configuration options provide granular port setting control for “All” ports or specific TCP and UDP ports. Each text box in this tab display the current defined list of ports and port ranges for TCP and UDP port for heavy scans, common port scans, OS types and authentication tests. The boxes are designed to fit inside of the confines of the *Port* tab. However, you can use the up/down arrow in each text box to scroll through the list and make changes. Or, click and hold the mouse pointer on the lower right corner of a text box and drag it out to make an individual box larger and easier to view/edit the content.

E-mail Notifications

These configuration options define whether you wish to send an e-mail alert and content to e-mail recipients once a scan has been completed for the job being defined. Use the fields in the upper section of the tab to do the following:

- First section:
 - Set the e-mail notification flag by clicking the *Send E-mail* checkbox
 - Define a local mail server (blank uses the recipient's default mail configuration)
 - Define the e-mail address that will display as the e-mail's "From" address
 - Define an e-mail "display name" for the from addressee
 - Set a trend length if you wish to send trend reports in the job notifications. The default 0 uses all scans for the job to build trends.
 - Define a default name and attachment. You can also be more granular and define specific report names in individual e-mails if you intend to send multiple reports.
- Lower sections subdivided by horizontal lines:
 - Each section provides the capability to define individual e-mail notifications. Each with their own comma separated e-mail addressee list; report name, subject, report type (e.g., executive report) and report format (e.g., PDF).

Click *Next* once you have completed any *Scan Configuration* options, to continue the *job setup*.

Step 5 – Finish

Step five is the last step in setting up a scan job, and enables you to define the job schedule; select a Scan Window, if applicable, and apply a pre-defined Ticket Rule Set, if applicable.

Once all final decisions are made to control the scan activity and post-scan ticket generation/update, you must click the *Finish* button to save the changes and execute any changes you've made – either during job creation time or editing an existing job to adjust these settings.

Scheduling

These options include running the scan now (immediately); scheduling the scan to run at a specific date/time (schedule once); and schedule continuous scanning (schedule recurring) for this job, based on defined date(s), day(s) of the week and frequency. Each option is described in detail below:

Schedule Immediately

Select this option to send the job to the scan queue immediately after finishing the job setup. This option will be displayed in the *Schedule(s)* window to confirm your selection.

Schedule Once

Select this option to display the *One-Time Schedule* dialog, and configure the job to run on a specified date/time.

1. Enter the date to run the job
2. Enter the time to run the job
3. Click *Add*

This option will now be displayed in the *Schedule(s)* window to confirm your selection.

Schedule Recurring

Select this option to display the *Recurring Schedule* dialog, and configure the job to start on a specified date/time; set when the job should run; and (optionally) when the recurring job should end.

Recurring Schedule

Repeat: Daily Repeat Every: 1 days

Begin Date

July 2017

S	M	T	W	T	F	S
25	26	27	28	29	30	1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31	1	2	3	4	5

Scan Time

Schedule Ends:

Never

After 2 Occurrences

Before End Date

Save

1. First, select the period to repeat the recurring scan (daily, weekly, monthly)
2. Use the *Repeat Every [number]*. Set the number of [days, weeks, months] to set how frequently the job should run within the day, week, or month setting.
3. For weekly scans, define the days you wish to run the scan during the week.
4. For monthly scans, use the radio button for *Day [number] of the Month* to define the recurrence based on a calendar date. For example, “Day 15 of the Month” runs the job on the 15th day of each month. Alternatively, you can also choose the radio button for “The [1st-5th] [Sunday-Saturday]” option to set the job to run on a specified day during the month. For example, run the job on the “Second Tuesday” of each Month, to support a Microsoft Patch Tuesday assessment.

5. Set the *Begin Date* to define when the job should start for the first time.
6. Set the *Scan Time* by sliding the hour and minute bars to the applicable hour and minute, using a 24-hour time clock.
7. Next, define when the job schedule should end. The first option is to *Never* end the recurring schedule. This radio button is selected by default. Setting this value ensures the job runs, as defined, until you edit the schedule and choose to modify or disable (stop) the schedule. A second approach is to run the job for a pre-defined number of times. Choose the radio button for the *After [number] Occurrences*. A third option for defining the end of the schedule, is by a defined date. Use the radio button for *Before End Date* to display the *End Date* calendar and select the month/date/year you wish to end the scheduled job.
8. Click the *Add* button once you have defined all of the settings for the recurring job.

The following shows an example of a recurring job schedule to run scans on the second Wednesday of every month for 6 months, to validate patches applied after each Microsoft Patch Tuesday bulletin release:

Recurring Schedule ✕

Repeat: Monthly Repeat Every: months

Day of the month
 The Second Wednesday

Begin Date

July 2017

S	M	T	W	T	F	S
25	26	27	28	29	30	1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31	1	2	3	4	5

Scan Time

Time

Hour

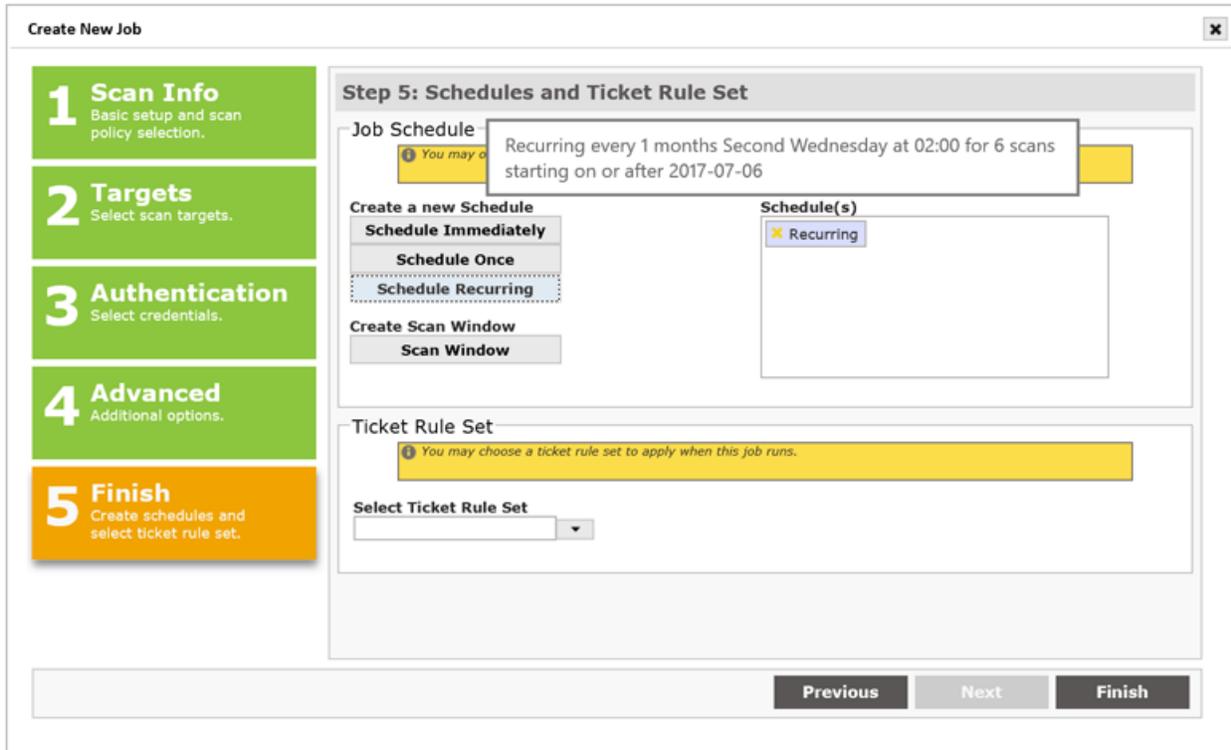
Minute

Schedule Ends:

Never
 After Occurrences
 Before End Date

Save

The *Schedule(s)* window is displayed to confirm your selection:



Click the *Finish* button to save your job and send it to the job's queue for its schedule execution.

Return to the *Job* grid and click the *Refresh* icon. You will now see the new job in the display, along with the current status of execution:

Dashboard Scan Analyze Report Ticket Exploit Manage Configuration									
Scan Jobs Schedules Assets Policies Credentials Manager Benchmark Scanning									
Grid Actions									
Scans Jobs									
Page 1 of 1 20 View 1 - 1 of 1									
Actions	Job #	Job Name	Owner	Last Run	# Scans	Target Group	# Targets	# Schedules	
	1	First Scan	admin		0	saint-data	1	1	

Click on the *Scans* tab to view the ongoing status of the current scan for the Job:

The screenshot shows the SAINT Security Suite interface. At the top, there is a navigation bar with the following items: Dashboard, Scan (selected), Analyze, Report, Ticket, Exploit, Manage, and Configuration. Below this is a secondary navigation bar with Scan Jobs, Schedules, Assets, Policies, Credentials Manager, and Benchmark Scanning. The main content area is titled 'Grid Actions' and has two tabs: 'Scans' (selected) and 'Jobs'. Below the tabs is a table with the following columns: Actions, Scan #, Job Name, Start Time, End Time, # Targets, # Results, Status, and Progress. The table contains one row for a scan job with the following data: Scan # 1, Job Name 'First Scan', Start Time '2017-07-06 10:55:39', # Targets 1, # Results 1, Status 'Running', and Progress '17%'. The table also includes a search icon, pagination controls (Page 1 of 1), and a view selector (View 1 - 1 of 1).

Actions	Scan #	Job Name	Start Time	End Time	# Targets	# Results	Status	Progress
	1	First Scan	2017-07-06 10:55:39		1	1	Running	17%

Scan Window

The Scan Window feature provides the capability to set a time period (scan window) during which recurring scheduled scans can run. The scan window start time/date is the time a scheduled scan will resume (if scheduled scan is currently paused) and the scan window end time/date is the time a scheduled scan will pause (if scheduled scan is currently running). The defined scan window time frames are used to send signals to the scheduled scan process to ensure scheduled scan processes do not run during times outside of the scan window range. The following are example use-cases:

Use-case 1 – I want to schedule a daily scan job to run only between 9 p.m. and 3 a.m. the next day. In this case, the scheduled scan job will start at 9 p.m. and run until 3 a.m. unless it completes before then. If it does not complete by 3 a.m., the scheduled scan job will pause and resume when the next allotted start scan window is reached (i.e., daily at 9 p.m.) If it completes the night before, a new scan will start at 9 p.m. and will run with the same settings as the previous scheduled scan.

Use-case 2 – I want to run a weekly scheduled scan job to run only on Saturday starting at 9 p.m. and pause (if not yet completed) on Monday at 6 a.m. for a scan job that may take a long time due to the size and complexity of the targets. In this case, the scheduled scan job will start on Saturday night at 9 p.m. and more time must be allocated for this large job to minimize the possibility that it will not complete within the scan window and overlap with the next scan window. If it does not complete by 6 a.m. on Monday, the scheduled scan job will pause and will only resume when the next scan window is reached.

Create a Scan Window

1. Create a scan window for the job by clicking on the *Scan Window* button in Step five of the job wizard. If you are editing a job that has an existing scan window, this option will display *Edit/Delete Scan Window* to view and modify the existing window.

The following dialog will be displayed to define the Scan Window Start (resume) Time Period and Scan Window End (pause) Time Period.

Scan Window

Scan Window Start Time
 12 00 PM

Scan Window Start Date
 Only 01 01
 Every Day
 Every Monday
 Day 1 every month
 First Monday of every month

Scan Window End Time
 12 00 PM

Scan Window End Date
 Only 01 01
 Every Day
 Every Monday

Save Remove Scan Window

2. As described in the example use-cases, define when you want the scans to be allowed to run. Remember to complete both a Start and End period for the scan window.
3. Click *Save* to create the new scan window and return to the finishing steps of the job setup.

View, Edit, Delete a Job's Scan Windows

To view the current settings of a scan window, click on the Edit (pencil) icon for the job in the Manage Job's grid, and navigate to Step 6 of the wizard. Notice that the scan window option has changed to Edit/Delete Scan Window. This verifies the job has a defined scan window. Click on the *Scan Window* button to display the current settings. You can now edit the settings and re-save, to change the scan window and re-run the job. Or, you can click the *Remove Scan Window* button to delete the scan window and continue using the job without a defined scan window.

Select a Ticket Rule Set for a Job

As defined in the Ticketing section, you can create one or more rules for determining ticket assignments based on parameters such as: a target list, host operating system platforms, type of vulnerability, severity of a vulnerability or even ranges of CVSS score. These rules are packaged in a parent Rule Set and then used at Job creation time to ensure tickets generated as a result of vulnerabilities detected during a job's scans are assigned to the proper individual for remediation.

[Ticket Rule Sets](#) are made available, based on the user's permission settings, via a drop-down list in Step five of the job creation wizard. Selection of a Rule Set is optional. Select an applicable Ticket Rule Set only if you wish to automatically assign remediation tickets generated from the job's scans.

Besides choosing a ticket rule set here, if *allow override* is chosen in the [Enable Ticketing](#) setting, this is also where generation of tickets can be enabled or disabled for the job. Under *Create Tickets*, choose *yes* or *no* to enable or disable ticket generation for this job, respectively. The third option, *When vulnerability matches a rule*, can be used to cause tickets to be created only for vulnerabilities which match one or more rules in the selected rule set.

Once all settings have been defined for the Job, click the *Finish* button to save the job and send it to the queue for schedule execution.

Target Entry Options

Besides the default method of specifying targets individually, there are also several options available to assist in selecting or importing multiple targets in a single step. These options are described in the following sections.

Free-form Target Entry

Free-form target entry allows you to copy and paste an existing list of targets rather than entering them one at a time. This may be useful if you already have your target list saved in an external document. To use free-form target entry:

1. From either the *Create/Edit Target Group* dialog or step 2 of the scan job wizard, click on *More Options...* under the *Enter Target(s)* box.
2. Click on *Free-form Target Entry* to open the free-form target entry dialog, which is shown below:

Free-form Target Input [X]

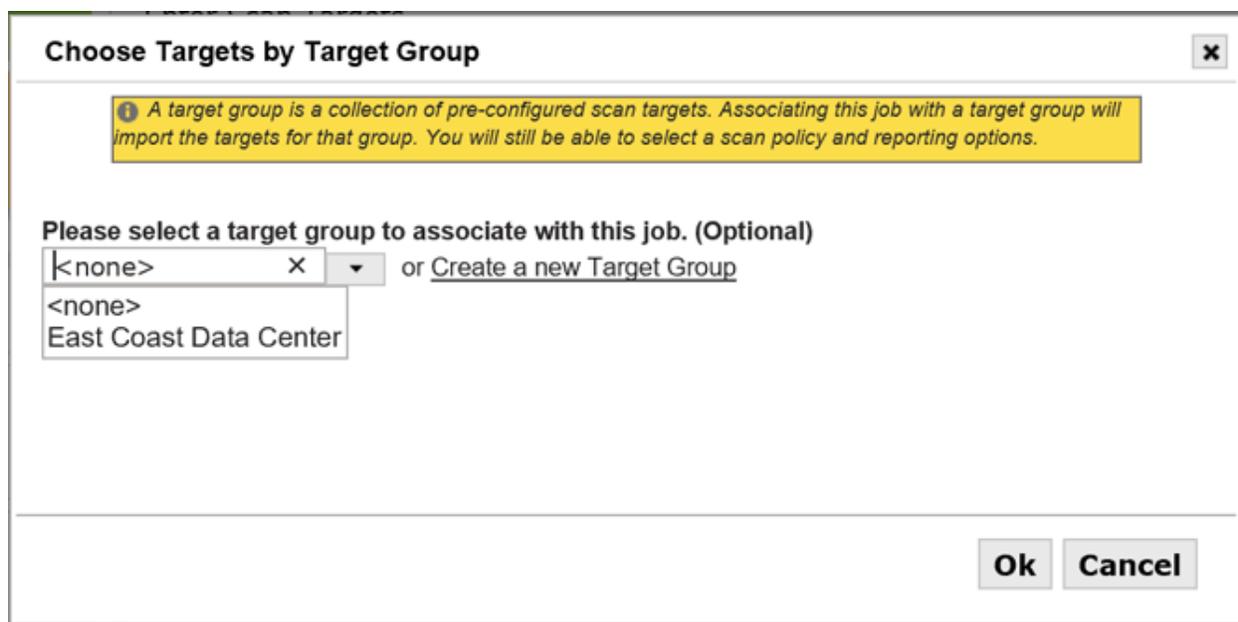
Enter any number of targets in any combination of [valid formats](#). Entries must be separated by commas or whitespace (spaces, tabs, or linebreaks).

[Add] [Cancel]

3. Enter the targets by hand, or copy and paste the target list into the text area. Targets must be separated by spaces, line breaks, or commas. The same target formats are allowed here as when entering targets individually. Mouse over the *valid formats* link for information about the acceptable target formats.
4. Click on the *Add* button. This will populate the *Selected Target(s)* box with the targets you entered.

Choose Targets by Target Group

Target Groups provide the capability to pre-store a collection of hosts or host ranges to decrease the time it takes to set up scans. For example, a Target Group has been defined in the example below for a range of internal addresses for hosts to be scanned in a data center. Rather than remembering the IP range, the group was defined ahead of time and selected at job setup time.



Also note that you can create Target Groups at job run time by selecting the “Create a new Target Group” option, and giving the Target Group a name. The live hosts discovered for the target(s) entered in the job target list will be used to populate the new Target Group upon scan completion.

Choose Targets by Asset Tag

Choose Targets by Asset Tag to display the following Asset Filter dialog:

Asset Filter [X]

Tag Name	Tag Value
<ul style="list-style-type: none"> CPE OS Class OS Type Function Criticality Availability Location Owner Business Cost 	<input type="text"/> <input type="button" value="Clear"/>

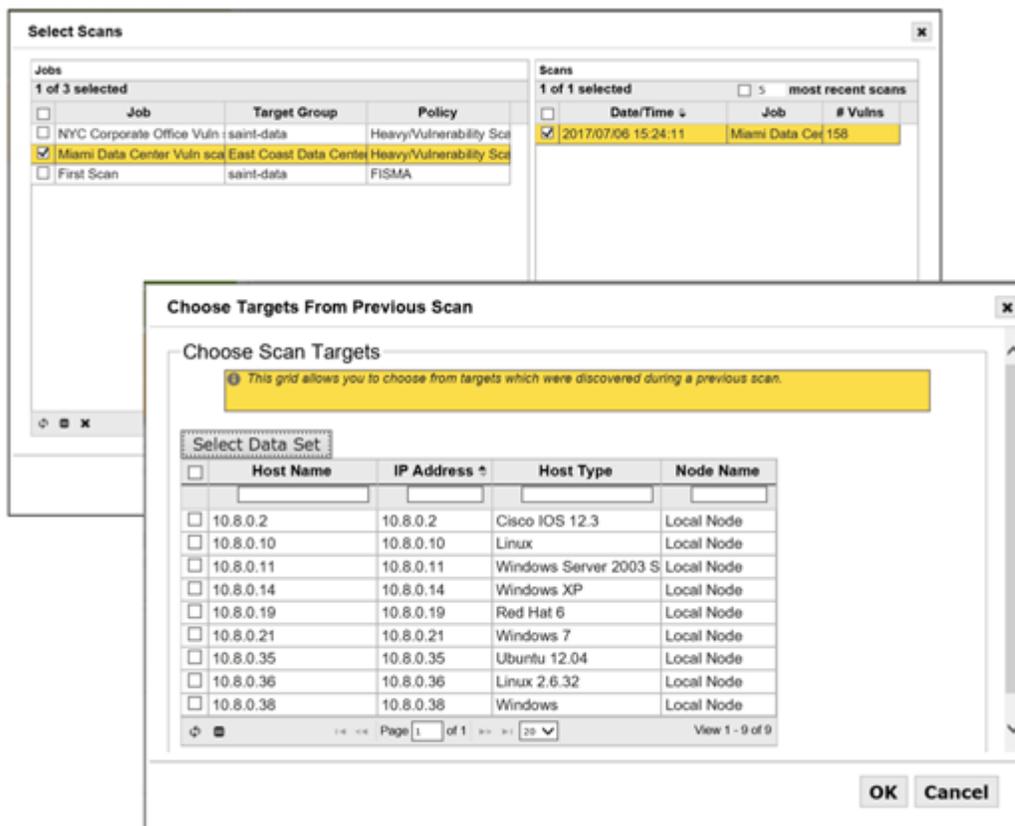
1. Select a Tag Name for the tag(s) to be displayed.
2. Click on the Tag Value. Use Control-Click to select multiple options.
3. Click the *Add* button to add the filter to the Filter Criteria box.
4. Repeat steps 1-3 to add additional criteria for the Target list.
5. Click *OK* to save the criteria and add the Asset Tags to the Target List, as shown below:

Choose Targets From a Previous Scan

When creating a job or target group, besides allowing you to enter new targets, the job wizard also supports creating target lists from hosts that have already been scanned. This may be convenient if you want to scan just a subset of the targets from an existing job. You can also run a scan using the *Discovery* policy initially to find live targets, and then select targets from that scan to populate the target list for a heavier scan.

To choose targets from a previous scan:

1. From step two of the scan job wizard, click on *More Options...* under the *Enter Target(s)* box.
2. Click on *Choose Targets From a Previous Scan* to open the list of previous targets, which is shown below:



3. Optional – Click on the *Select Data Set* button to choose the scans from which to select targets, and click *OK*.
4. Check the box beside each target you wish to add. Or, click on the box at the top-left corner of the grid to add all visible targets. Use the filter boxes in the second row of the grid to narrow down the displayed targets as desired. If there are many targets, use the paging buttons at the bottom of the grid to view additional targets.
5. Click on the *OK* button. This will populate the *Selected Target(s)* box with the targets you selected.

Choose Passively Discovered Hosts

If the passive host discovery option is enabled (see [Passive Host Discovery](#)), this option allows you to easily scan the devices which have been recently seen on the network.

To scan passively discovered hosts:

1. From step two of the scan job wizard, click on *More Options...* under the *Enter Target(s)* box.

- Click on *Choose Passively Discovered Hosts*. The following dialog box will appear:

Choose Targets From Passively Discovered Hosts ✕

Choose Scan Targets

i This grid allows you to choose from hosts which were discovered passively.

Scan all passively discovered hosts
 Scan hosts which haven't been scanned in last 90 days from scan date
 Select hosts to scan

- Click on the button for one of the three options:
 - Scan all passively discovered hosts – This option will dynamically generate the target list every time the scan job runs, to ensure that all recently seen devices are scanned.
 - Scan hosts which haven't been scanned in last N days from scan date – This option will also dynamically generate the target list every time the scan runs. All passively discovered hosts which have not been scanned in the chosen number of past days, including hosts which have never been scanned, will be included.
 - Select hosts to scan – Selecting this option will open a grid allowing you to select one or more hosts to scan from the current list of passively discovered hosts.
- Click on the *OK* button. This will populate the *Selected Target(s)* box with the option you selected.

Import Targets From Active Directory

To assist with the scanning of Windows domains, import target lists from an Active Directory server (typically a domain controller). This allows scan jobs to automatically include every computer which exists in the domain controller's directory under a specified domain. It is also possible to customize the search to reduce the list down to those computers which have specific properties in the directory.

To import targets from Active Directory:

- From step two of the scan job wizard, click on *More Options...* under the *Enter Target(s)* box.

2. Click on *Import Targets From Active Directory*. That opens the dialog shown below.

Import Targets From Active Directory [x]

Active Directory Server Address

Active Directory Port
 Use SSL

ⓘ Credentials will be sent in clear text!

Active Directory Domain

Examples: company.local or DC=company,DC=local

Login (including domain)

Example: DOMAIN\Administrator

Password

▣ Advanced Options

OK Cancel

3. Enter the IP address of the Active Directory server.
4. Check the *Use SSL* box if you want the LDAP request to go over SSL. (i.e., LDAPS) **Warning:** If you choose not to check this box, your credentials will be sent to the Active Directory server in plain text. If you check this box, then the certificate of the Active Directory server must be installed on the system running SAINT. See <http://www.sans.org/reading-room/whitepapers/protocols/ssl-secure-ldap-traffic-microsoft-domain-controllers-33784> for further instructions.
5. Optional – enter the LDAP port used by the Active Directory server. In most cases, the default is the correct port, and this field shouldn't be changed.
6. Enter the Active Directory domain. This can either be formatted as a Windows domain (such as *company.local*), or an LDAP Base DN (such as *DC=company,DC=local*).
7. Enter the Active Directory login (including the domain name) and password.
8. Optional – Click on the *Advanced Options* button.

- a. Modify the search filter if desired. The filter should be formatted as defined in [RFC 4515](#). The default filter searches for all computers in the specified domain.
 - b. Leave *Resolve Targets to IP Addresses* checked if you want the targets to appear as IP addresses in your target list, or uncheck this box if you want the targets to appear as fully-qualified host names in the Active Directory domain. **Warning:** If you uncheck this box, it may be necessary to configure the scan node to use the Active Directory server as its DNS server in order for it to resolve the host names.
9. Click on the *OK* button. This will perform the Active Directory search and populate the *Selected Target(s)* box with the resulting targets.

Import from a File

This option provides the capability to import target lists from an external file. Use the *Browse* button to select a plain text file containing a comma or whitespace (spaces, tabs, linebreak) separated list of targets. Once the file name is displayed in the form field, click the *Import* button to import the list to populate the target list in step 2two of the wizard.

This feature also provides the capability to create a Target Group at job runtime, by entering the title of the new Target Group field, and checking the “Create Target Group” checkbox in the highlighted area above the import form.

Import AWS EC2 Instances

To assist in scanning your Amazon Web Services (AWS) environment, import EC2 instances from a chosen region into your scan jobs. These instances are resolved to their current IP addresses every time the scan runs, to ensure that the correct targets continue to be scanned even if their IP addresses change. There is also an option to include all newly created instances in future scans, to ensure that the entire environment continues to be scanned as it expands over time.

To import AWS EC2 instances:

1. From step two of the scan job wizard, click on *More Options* under the Enter Target(s) box.
2. Choose *Import AWS EC2 instances* from the pop-up menu.
3. Enter your AWS Access Key ID and AWS Secret Access Key. (To obtain an AWS access key, log into the AWS console, and go to *Identity & Access Management* on the AWS console home page, or *Services > Security & Identity > IAM*. Create a user, or select an

existing user and choose *User Actions > Manage Access Keys > Create Access Key*. (The IAM user must have at least **AmazonEC2ReadOnlyAccess** permissions.)

Optional: Check the *Remember* box to save the AWS Access Key ID and AWS Secret Access Key entered above in your user profile. This will cause these fields to be automatically completed in the future.

4. Choose the desired AWS region from the drop-down menu.
5. Click on the *Import* button. This brings up a grid displaying information about all EC2 instances found in the specified region.
6. All instances which are accessible from the selected scan node are selected by default. If you want to exclude any of these instances from the scan, deselect them by clicking on the corresponding checkboxes. (*Note: For an instance to be accessible from the selected scan node, it must either have a public IP address or be in the same VPC as the scan node.*)
7. *Optional.* If you are creating a recurring scan job, check the radio button beside *Scan selected instances* **and** *any running instances not shown above* to ensure that your entire EC2 environment continues to be scanned as it expands over time. If this button is checked, then SAINT will check the selected AWS region for new EC2 instances every time the scan runs, and will add those of which are accessible from the selected scan node to the target list.
8. Click on the *Import* button. The selected instances, identified by their region and instance ID, will appear in the *Selected Target(s)* box.

Import Microsoft Azure Instances

To create an Azure user, log into <https://portal.azure.com> and go to *Azure Active Directory > Users > New User*. Enter a name and username and click *Save*. Then go to *Subscriptions* and click on your subscription. Go to *Access Control (IAM) > Add Role Assignment*. Add the *Reader* role to the user you just created and click *Save*. Log in as the new user and change the password.

In the scan Job wizard, enter the Azure Subscription ID, Azure UserID and Azure User's Password.

Click the *Import* button to configure the scan Job to connect to Azure and scan the host(s) associated with this subscription.

Scan Docker Images

To assist with the scanning of Docker container images, SAINT allows you to specify an image in a Docker registry, a repository on a remote host running SSH, or a local repository on the scanner. When you use any of these options, the scanner will download and temporarily run the specified image on the scanner. While the container is running, the scanner will scan its IP address (which is typically a private IP address visible only to the scanner) and run local checks inside the container. The scanner will remove the temporary container and any downloaded files when the scan completes.

In order for a Docker image scan to work, Docker must be installed on the scanner, and the image must be compatible with the scanner's kernel and architecture. Furthermore, the Docker image must be able to run persistently by default. An image that runs a single command and then exits will not stay running long enough to be scanned.

To scan Docker images:

1. From step two of the scan job wizard, click on *More Options...* under the *Enter Target(s)* box.

2. Choose *Scan Docker Images*. The following dialog will appear:

Docker Image Scan

Choose a Docker image to scan. The scanner will download and run the image in a temporary container to scan it. The image must be compatible with the scanner's kernel and architecture.

Docker Image Source
Default registry (DockerHub)

Docker Registry Login

Docker Registry Password

Repository

Tag
latest

OK Cancel

3. Choose the source of the Docker image:
 - a. Default registry (DockerHub) – The image is in a repository located at hub.docker.com. A login and password for the registry is required.
 - b. Other registry – The image is in a repository located at a Docker registry other than the default registry. The IP address or hostname of the registry server is required in addition to the login credentials for the registry.
 - c. Remote repository (SSH server) – The image is located in a repository on a remote host which is running SSH. The IP address or hostname of the remote host and the host's SSH credentials are required. The image will be exported on the remote host and transferred using the SCP protocol.
 - d. Local repository (on scanner) – The image is located in a local repository on the scanner.
4. Enter the repository name and the tag name. If the tag name is omitted, the latest image in the repository is used. If a registry was selected in the previous step, you may either enter the repository in user/repository format or just the repository name. If just the repository name is entered, the user name will be prepended automatically.

5. Click on the *OK* button and continue through the scan wizard.
6. If you chose “Remote repository (SSH server)” above, click on the *Set* button beside Unix/Linux/Mac in step 3 of the scan wizard, and enter the SSH credentials for the remote host.

Infoblox

SAINT Security Suite can import “USED” targets from Infoblox while creating a scan job, and automatically grab new targets before each scan run. (See [Configuration](#))

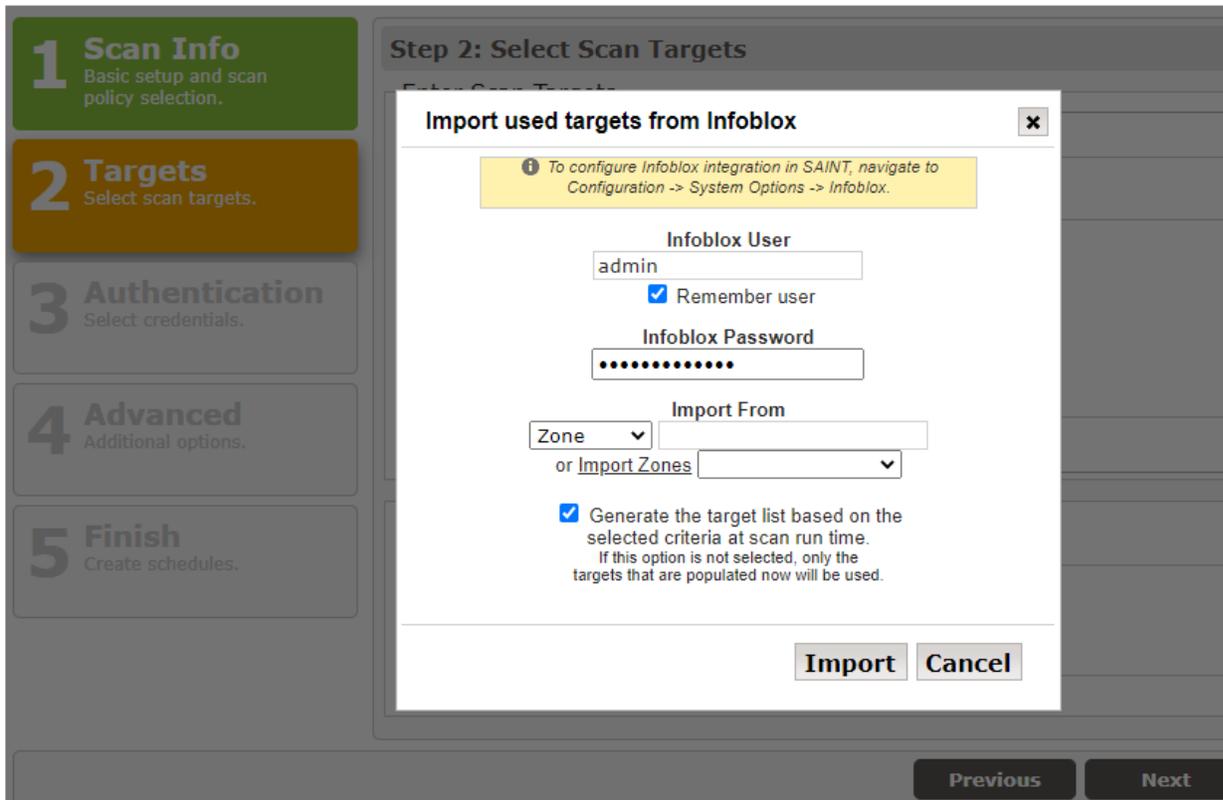
Importing Targets

After the Infoblox configuration is completed, the option to import targets from Infoblox will be available during job creation. Click on the “More Options” link in step #2 of the job creation wizard.

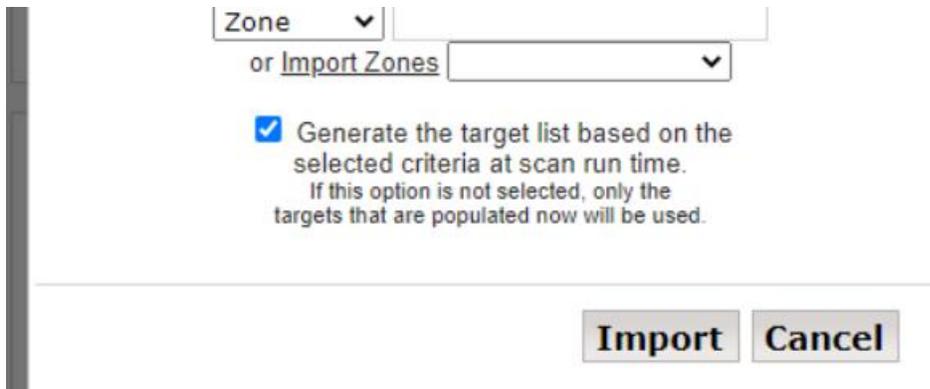
Create New Job

This will open a form, allowing targets to be imported by subnet, IP range, or zone.

Create New Job



When it comes to zones, there is an option that will populate the zone list after the credentials have been entered. Users can also input the zone into the field next to the *Zone* field.



While importing targets from Infoblox, there is an option to save the criteria that gets used before each scan run. If this option is enabled, then the target list will be expanded to include new targets found based on the subnet, zone, or range before each scan starts within the job.

View Job Details

The Action column of the Jobs tab provides an option to view basic information (name, description, target group, target lists, and scan policy) about each job, as well as detailed about job schedules, execution history and status files. Click the *Information* option (“i” icon) on the job row that you wish to view. An example of this display is shown below:

The screenshot shows a window titled "Job Details" with a close button (x) in the top right corner. The main content area is divided into several sections:

- Job Information** (highlighted in yellow):
 - Job Name:** Miami Data Center Vulr
 - Description:** Miami Data Center Vuln scan
 - Target Group:** East Coast Data Center
 - A **Save Changes** button with a pencil icon is located below the Target Group field.
- Targets** (expandable section)
- Scanning Configuration** (expandable section)
- Schedules** (expandable section)
- Execution History** (expandable section)

A **Close** button is located in the bottom right corner of the window.

Clicking on the section headings in this window will expand the selected section and provide further details such as the Target List, scan Schedules and the Execution History that displays details about scans that have been run for the job.

Host-Based Assessments

Starting a Scan

There are currently three scan policies which can be used with the Agent: Local Checks, OVAL Definitions, and Configuration Benchmark.

1. Local Checks

- a. Windows
 - i. Patch checks
 - ii. Application checks
 - iii. Firewall status
 - iv. Software inventory
 - v. Open ports
 - b. Linux/Mac OS
 - i. Patch checks
 - ii. Application checks
 - iii. Open ports
2. OVAL Definitions (Windows/Linux/Mac OS)
 - a. All OVAL definition content found at the CIS OVAL Repository may be used.
 - b. Content from other sources will work as well.
 3. Configuration Benchmark (Windows/Linux/Mac OS)
 - a. Perform configuration scans using benchmarks available from USGCB, DISA, CIS, and others.

To start a Host-based Assessment, load up the job creation wizard by using the '+ Create' button at the top right of the UI and clicking on *Scan Job*. You can also access the wizard by navigating to Scan > Grid Actions > Create Job.

Select the *Host-based Assessment* from the *Select Policy Category* dropdown. Now, from the *Select Policy* dropdown, you can choose Local Checks, OVAL Definitions, or Configuration Benchmark.

**If performing an OVAL Definitions or Configuration scan, benchmark/OVAL content must first be downloaded or imported from Scan > Benchmark Scanning. From this page you can import one of the predefined benchmarks or OVAL Definitions, or import your own.

Step 1

Create New Job ✕

1 Scan Info
Basic setup and scan policy selection.

2 Targets
Select scan targets.

3 Authentication
Select credentials.

4 Advanced
Additional options.

5 Finish
Create schedules and select ticket rule set.

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

Select Policy

- Local Checks SAINT Scanning Agents to perform
- Configuration Benchmark checks. It also performs information
- gathering tasks such as checking firewall status, reporting open ports, and more.

Create New Job ✕

1 Scan Info
Basic setup and scan policy selection.

2 Targets
Select scan targets.

3 Authentication
Select credentials.

4 Advanced
Additional options.

5 Finish
Create schedules and select ticket rule set.

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

Select Policy

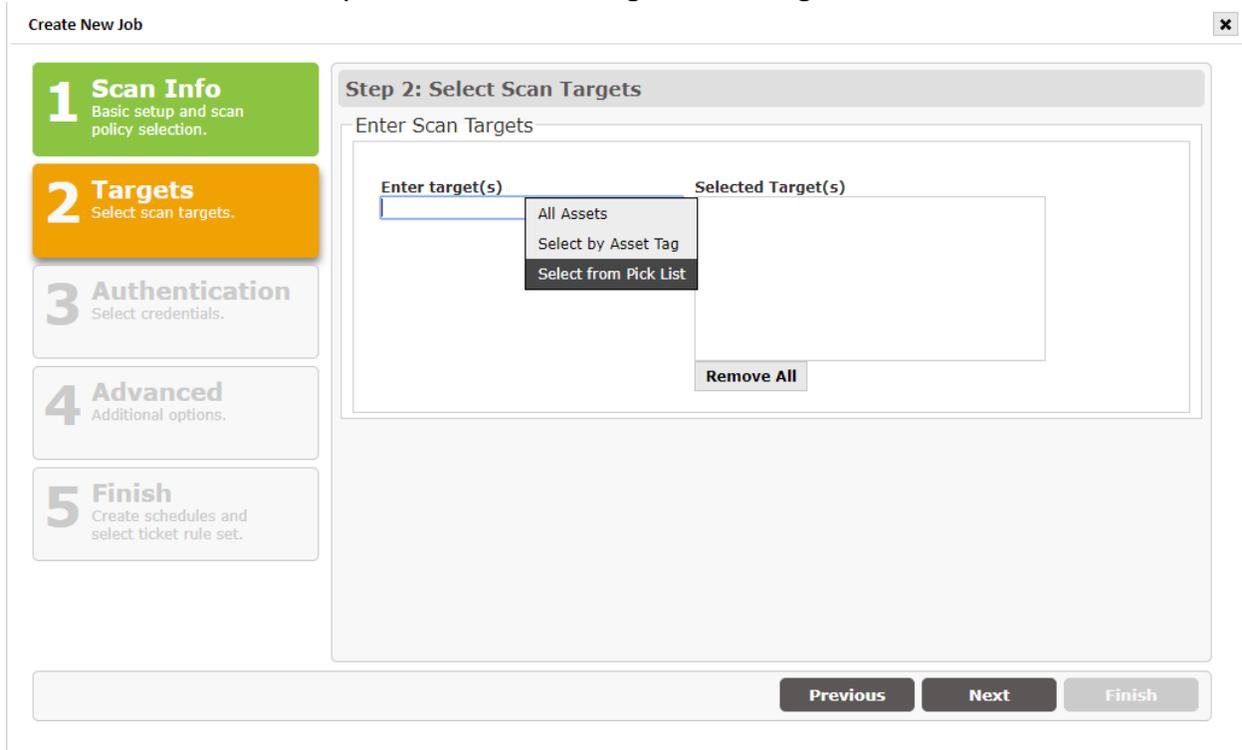
Select Benchmark

Select Profile

Step 2

After selecting a policy, click on Next to get to the target selection step. Click on the *Enter target(s)* text box and there will be three options:

1. All Assets - This will allow all agents to perform scans
2. Asset Tag - This will perform scans against assets that only have certain tags
3. Pick List - This lets you select individual agents from a grid



Step 3

The last step is to schedule the scan. The scan will initiate from a given start time, or immediately, and await connections and data from agents for the number of hours specified in the *Duration* field.

Create New Job
✕

1 Scan Info
Basic setup and scan policy selection.

2 Targets
Select scan targets.

3 Authentication
Select credentials.

4 Advanced
Additional options.

5 Finish
Create schedules and select ticket rule set.

Step 5: Schedules and Ticket Rule Set

Job Schedule

ⓘ You may opt not to create a schedule for this job at this time.

Create a new Schedule

Schedule Immediately

Schedule Once

Schedule Recurring

Schedule(s)

✖ Immediate

Scan Duration

12 Hours

Ticket Rule Set

ⓘ You may choose a ticket rule set to apply when this job runs.

Select Ticket Rule Set

Previous

Next

Finish

Checking Scan Progress

The progress of each Agent can be checked during and after a scan by clicking on the orange *Details* link in the progress column. The progress percentage is determined by the number of completed scan tasks divided by total number of scan tasks across all agents in the scan.

Security Suite										
Scan ▾ Analyze ▾ Report ▾ Ticket ▾ Exploit ▾ Manage ▾ Configuration ▾										
Scan Jobs Schedules Policies Credentials Manager Benchmark Scanning										
Grid Actions ▾										
Scans Jobs										
⊕ Page 1 of 1 20 ▾										
Actions	Scan #	Job Name	Start Time	End Time	# Targets	# Results	Status	Progress		
	8	Local Checks Job	2018-11-08 16:34:28		1	41	Running	60% Details	Loc	
	7	CIS Win10	2018-11-08 14:46:19	2018-11-08 14:52:42	1	254	Finished	100%	CIS	
	6	scap 1.0 test	2018-11-08 13:49:49	2018-11-08 13:52:13	1	254	Finished	100% Details	Cor	
	5	1.2 Benchmark Local	2018-11-08 13:47:32	2018-11-08 13:48:54	1	3	Finished	100% Details	Cor	
	4	1.2 Benchmark Local	2018-11-08 13:41:35	2018-11-08 13:42:51	1	3	Finished	100% Details	Cor	
	3	1.2 Benchmark Local	2018-11-08 13:33:01	2018-11-08 13:34:28	1	3	Finished	100% Details	Cor	
	2	1.2 Benchmark Local	2018-11-08 13:12:14	2018-11-08 13:13:41	1	3	Finished	100% Details	Cor	
	1	LocalChecksTest	2018-11-08 13:02:48	2018-11-08 13:05:42	1	138	Finished	100% Details	Loc	

Clicking *Details* will bring up a dialog containing the status of each scan task for each agent.

Host-based Scan Details

Task	Task Status	Start Time	Agent GUID
<input type="text"/>	<input type="text"/>		<input type="text"/>
<ul style="list-style-type: none"> ▣ Scanning ▣ rscnb018.example.com 			
win_open_ports	sent	2018-11-08 16:34:56	db41ce4bde5941109e6e5e6f7bf523b5
win_fw_status	done	2018-11-08 16:34:54	db41ce4bde5941109e6e5e6f7bf523b5
win_filechk	sent	2018-11-08 16:34:56	db41ce4bde5941109e6e5e6f7bf523b5
win_registry	sent	2018-11-08 16:34:56	db41ce4bde5941109e6e5e6f7bf523b5

View 1 - 4 of 5

The status categories are:

- a. Scanning – Agent is in the process of performing scan tasks
- b. Finished – Agent has finished scanning
- c. Hasn't checked in – Scan is running but the Agent has not been seen yet
- d. Didn't check in – Scan is complete, but the Agent never connected
- e. Partially Scanned – Some of the scan tasks were completed, but others did not finish.

This could occur due to stopping a scan or the scan ending.

The scan tasks are the various probes which run on each Agent. They have three states:

1. New – task is waiting to be started on the Agent
2. Sent – task has been started on the Agent
3. Done – task has been completed and results returned

Edit Jobs and Save As

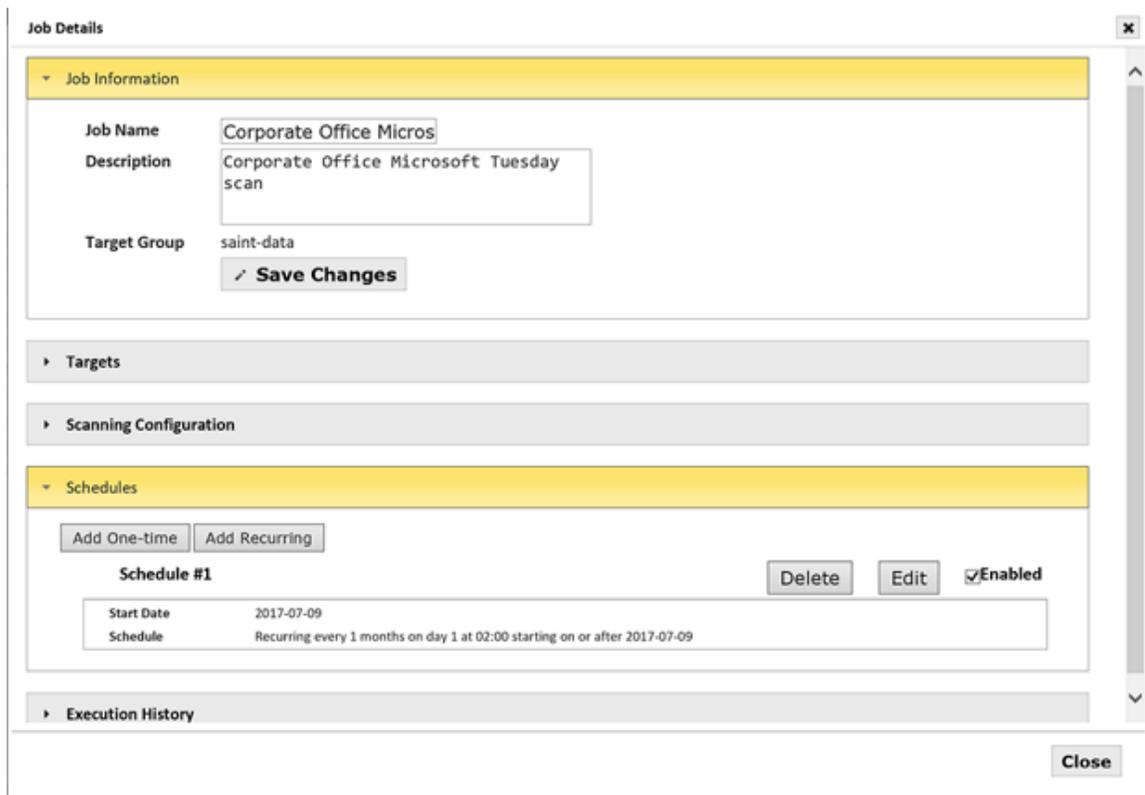
The scan job creation wizard is also used to support editing the settings of an existing job. This can include editing the job Name, Description, Target lists, Targets to Exclude, the Policy, detailed Configurations and Email notifications, Authentication and running the edited job Immediately or adding a new scan schedule. The only limitation is removing (deleting) an existing schedule. You must use the process described in the [Edit Job Schedules](#), to edit, enable or disable a job's schedule from the scan queue. Note that editing settings such as the target list, target exclusions, scan policy, authentication settings and others can dramatically affect the scan results from previous scans associated with the Job and future scans. So care should be taken when editing an existing job to ensure the integrity of the intended purpose of the job (such as trend analysis or performing a specific assessment like content scanning or a compliance analysis) is not compromised. Follow these steps to edit an existing job:

1. Navigate to the Scan page's *Job* tab.
2. Click on the *Edit* option (pencil icon) for the job to be modified. The job creation wizard will be displayed with the existing job settings populated in each step.
3. Navigate to the applicable steps and scan setting, as you did during job creation, and update the required settings.
4. When all changes have been made, navigate to Step five and click *Finish*. A confirmation dialog will be displayed to ask whether you wish to save the changes for the existing job or "save as" a new job. Once you have made your selection, the changes will be saved and executed, as applicable.

Edit Job Schedules

The *Job Details* dialog provides support for editing the name and description, as well as managing the schedules defined when the job was created (see [Step 5 – Summary](#) of the job creation process for more details). The following describes the steps for viewing a job's information and editing this information.

1. Click the *Edit* option (pencil icon) on the job row that you wish to edit.
2. Edit a job's name and description can be done by clicking in the applicable text box and typing in the revised text. Click the *Save Changes* button once you've completed the changes.
3. Expand the *Schedules* section of the *Job Details* to view the current schedules defined for the job.



4. Editing Job Schedules through this feature supports the following options:
 - a. **Add One-time** – click this option to add an additional scan that will run once, based on the job definition. The *Run Once* dialog will be displayed to define the date and time to run the job.
 - b. **Add Recurring** – click this option to add a new recurring scheduled scan for the job. The [Recurring Schedule](#) dialog, also used in the job creation wizard will be displayed to define the settings for the new recurring job schedule.
 - c. **Delete** – click *Delete* to remove the currently selected schedule.
 - d. **Edit** – click *Edit* to view the selected schedule and edit when scheduled scans should run for that schedule.
 - e. **Enable** – Check this box to activate the selected schedule and run scans for the job based on the schedule’s settings. Uncheck this box to cancel any further scans being run based on the selected schedule.
Note: there may be existing scan activity currently underway if your revisions are being done at the time a job schedule is to be executed. Individual scans can be stopped by navigating to the [Scan](#) grid and clicking the *Stop* button on the applicable scan.

Copy Jobs

Owners of jobs, and users with “Copy” permissions to applicable job(s), may copy existing jobs and use them as a starting point for a new job. For example, a job owner may use an existing job to perform similar scans across a number of host environments, as different jobs. Or, an administrator may develop a job with a number of customized configuration settings and then permit other users to copy that job to use in their own work, such as using the copied job to enter their own targets for managing their own scans while taking advantage of previous efforts in configuring a job template for consistency across teams. To copy a job:

1. Navigate to the *Jobs* tab.
2. Click on the *copy* action button beside the job to be copied (If the *copy* action button is not visible, click on the *more options* button to display it.)
3. A dialog box will be displayed to choose whether you also want to copy the existing job’s Schedule(s) and Credential settings. Check each box, if applicable, then click the *Copy* button to close this dialog.
4. A new job will be created in the grid, using the title “Copy of [*name of the copied job*]”
5. Click the *edit* button beside the newly created job, to open the job’s setup wizard, perform applicable modifications, such as giving the job a new name, modifying target lists, etc. and then save the new settings for execution.

Permission settings to support the Copy function

Scan jobs can include a host of content and settings that are not globally accessible by all users of the product. Such as the scanning engine (node) being used to scan, the hosts being scanned, the credentials being used for credentialed scanning, specific configuration settings, etc.

Therefore, the owner of a job must ensure that the users being permitted to View and Copy a job have the applicable permissions required to view, copy and execute the intended capability of the copied job. The following is a synopsis of the permissions settings to be considered for the “copy job” feature:

- The owner of a job has all permissions required, by default, to copy a job. If the owner of a job wants to make a copy of the job click the *Copy* button in the Action column of the Scan Jobs grid. A copy of the job, named “Copy of [*name of the copied job*]” will appear on the Scan Jobs page.
- If the user of the copied job does not have permission to scan from the scanner node associated with the copied job, then scan permission is granted as a result of the “copy”

permission. However, the user does not have full visibility of the scanner node. It will be displayed as "Unknown node".

- A user who is not the owner of the job, who has "Copy" permission on the job, may click the *Copy* button in the Action column of the Scan Jobs page to make a copy of the job.
- The user who copies another user's job becomes the owner of the new copy of the job. The original owner still owns the original job.
- If owner of the job edits a job in the Scan Wizard, a dialog will be displayed when the *Finish* button is selected, to "Save" the edited job or "Save as" a new job, that includes all of the previous job's settings and modifications.
- The owner of a job may grant permission to another user to "copy" the job. The original owner must first grant the new owner "View" permission on any Credentials Manager credentials needed by the job, if the owner wishing to allow the user to use those credentials from the original job.
- If the job uses a custom scan policy, and the custom scan policy contains custom checks, the original owner must grant the new owner "view" permission on the custom checks.
- If a user who is not the owner of a job has "modify" permission on a job, that user may edit the job in the Scan Wizard. When that user clicks *Finish*, the option to "Save A Copy" of the job will not be displayed unless that user also has "copy" permission on the job.

Delete Job

Delete a single Job:

1. Click the *Delete* option (trash can icon) on the job row that you wish to delete.
2. Confirm the delete action.

Delete multiple jobs at once:

1. Click the checkboxes in the leftmost column on the job rows that you wish to delete.
2. Click on *Delete Jobs* under the *Grid Actions* menu above the grid.
3. Confirm the delete action.

Export Job

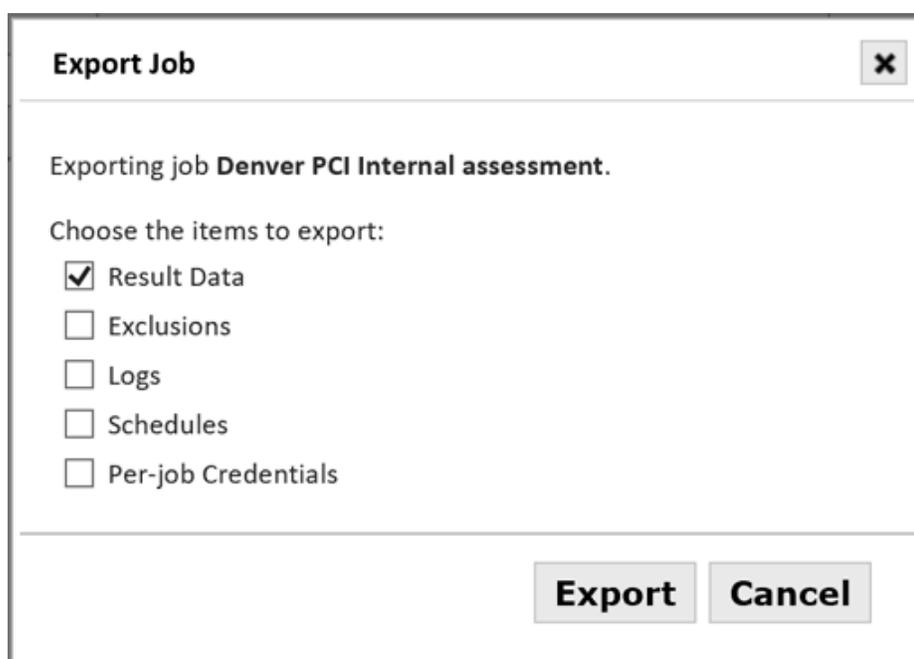
To assist with the management of jobs, jobs can be exported and imported. The export format is a gzip-compressed data file which can be easily saved, transferred, backed up, and re-imported at a later time to the same installation or a different installation. This may be useful in

situations where scanning and reporting are to be performed on two separate installations, or in situations where scan data is considered too sensitive to store permanently in the database.

Only the user who created the job or a member of the Administrators group may export a scan job.

To export a scan job:

1. From the *Scan* tab, click on the *Export* icon (box with diagonal arrow) on the job row that you wish to export. (If the *Export* icon isn't visible, click on the *More Options* button on the desired job row to show it.) This opens a dialog box as shown below, which exports the job with all scan runs. Alternatively, to export the job with only a single scan run, go to *Scans* tab and click on the *Export* icon on the desired scan row.



2. In the dialog box, check the items which you want to export:
 - Check **Result Data** if you want the scan results to be available in the dashboard, analyze, or report screens after importation.
 - Check **Exclusions** if you want any excluded vulnerabilities to remain excluded after importation. (See [Exclusions](#).)

- Check **Logs** if you want the status file and verbose output to be available after importation. (See [View Current Status of a Running Scan](#) and [View Verbose Output](#).)
 - Check **Schedules** if you want any one-time or recurring scan runs scheduled for the future to run after importation.
 - Check **Per-job Credentials** if you want any credentials which were entered in the create job wizard to be used when running the job after importation. Note that this does not include credentials stored in the credentials manager. (See [Authentication](#).) *Warning: since the destination SAINT installation may have a different encryption key than the source installation, passwords are not encrypted in the export file.*
 - Note: if none of the above are selected, the job name, description, target list, and configuration will still be exported.
3. Click on the *Export* button.
 4. Save the export file. The interface for saving the file varies with different browsers.
 5. *Optional* – After the export dialog closes, click on the *Delete* icon (trash can) on the grid row if you wish to delete the job or scan run from the database. The job can be restored later from the saved export file.

Import Job

To import a scan job which was exported as described above:

1. From the *Jobs* tab, click on the *Import* option from the *Grid Actions* dropdown list. This opens an Import Job dialog box.
2. In the dialog box, choose the file which was saved in step 4 above. The interface for choosing the file varies with different browsers.
3. Click on the *Import* button.
4. Wait for the import process to complete. A message will appear in the dialog box indicating whether the import was successful.

All imported jobs will be owned by the user who imported them, regardless of the original owner.

Export Jobs

The Export Jobs option from the Grid Actions menu allows you to choose multiple jobs by age, job name, or owner username to export to a location on the SAINT host, or to download locally to your computer. The number of days may be set to '0' to export all the jobs. The job name

and owner username may be specified with wildcard characters where '*' matches zero or more characters and '?' matches one character. Just like when exporting an individual job, you have options for which job-related data to export for multiple jobs. Once the export is complete, you also have an option to delete the jobs that you just exported.

Export Jobs ✕

Export jobs older than days

Items to export

- SCAP Reports
- Result Data
- Exclusions
- Logs
- Schedules
- Per-job Credentials

Filter by Job Name ?

Filter by Job Owner Username ?

Download Export File

Server Export Location

Scan Tab

The *Scans* tab on the Scan page provides basic information about individual scans executed for a job. This information is similar to the job, but is focused on the actual scan that produced results you analyze in *Dashboards*, *Analyze* grids and *Reports*. Click the *Information* option ("i" icon) on the scan row that you wish to view.

Scan Details

Denver PCI Internal assessment (SCANID 39)

▼ Scan Details

Job Name: Denver PCI Internal assessment
 Scan ID: 39
 Scan Policy: PCI
 Start Time: 2017-07-12 11:33:34
 End Time:

▼ Execution History

Agent/Node	Start Time	End Time	Status	Status File	Verbose Output	Results data
Local Node	2017-07-12 11:33:34		Running (0%)	View Status File	View Verbose Output	View Results

Close

Scan Status

While a scan is running, the *Status* column indicates whether the scan is ready to run, running, paused, finished or stopped. Paused scans are denoted by “Paused” to indicate manual interaction to temporarily pause a scan, or “Pause Window” to indicate a scan is currently paused because a [Scan Window](#) was defined for the recurring scheduled scan Job and the current scan is currently active but the time is not within the defined scanning Window. The *Progress* column provides an estimate of the percentage of scan phases and probes that have completed. Both of the above indicators are automatically refreshed periodically, but they can be manually refreshed by clicking on the refresh icon at the bottom left corner of the grid. Note that the progress indicator is only an estimate, because the execution time of the scan phases and probes vary, and the total number of phases and probes is unpredictable.

To view a more detailed account of the scan progress, click on the *Information* (“i”) icon of the desired scan, expand the *Execution History* section, and click on *View Status File*. This will open a dialog providing a continuously updated log of probes which have started or finished.

If the Status column shows “Error,” then the scan was unsuccessful on at least one scan node. Click on the *Information* (“i”) icon for the unsuccessful scan and expand the *Execution History*

section to find out which node had the error. Then click on the *View Verbose Output* link on that node's row to see information about the error.

Scan Details

The scan details define what job a scan is based on including the scan policy, when the job was first started and ended (if applicable), and the current status.

Execution History

The scan execution history shows the start and end times of the executed scan, from the defined job. This information describes which scanner node was used (for standalone installations this will be the local node), the start and end times of the scan, the current status for each scanner used in the job, a link to the status file for the scan, expanded status details describes a "verbose output," and a hyperlink to go directly to the scan results in the *Analyze* tab. The example shown above describes the current status of a scan being run on the built-in scanner local node. Note that running scans on multiple nodes will provide a visual status of scan progress on each node used in the scan.

View Current Status of a Running Scan

The *Scan Details Execution History* provides a hyperlink to view the status file content that shows the current state of a scan, ongoing progress of individual scan processes by date/time stamp, affected hosts and ports, and other useful information as a scan progresses toward completion. This information can also be useful to determine if particular hosts have been scanned or were unavailable at the time the host was assessed. The following is an example of a status file, and some of the information you may see during your own scans.



View Verbose Output

Viewing verbose output is done in the same manner as viewing the status file. While the status file focuses on the status of scan activity, the verbose output provides insights into the underlying results. For example, in the screen shot below we see host information and vulnerability results described for a target being scanned. While not a complete record, this information can be useful in gaining some insight into intermediate results for a scan.

```

Stdout File
weak RSA public key
weak https cache policy
web server allows MIME sniffing
Services:
  SSH
  WWW
  WWW (Secure)
  ideafarm-door (902/TCP)
  irdmi (8000/TCP)
10.8.0.101:
Information:
  Administrators: WIN2003PATCHED\Administrator, SAINTTEST\Domain Admins
  OS=[Windows Server 2003 R2 3790 Service Pack 2] Server=[Windows Server 2003 R2 5.2]
  Users: Administrator (500), Guest (501) (disabled), HelpServicesGroup (1000), SUPPORT_388945a0
  Windows services: Wireless Configuration, Automatic Updates, Windows Management Instrumentatio
  lockout duration = 30m, reset = 30m, threshold = 0
Critical Problems:
  Microsoft .NET Framework Stack Overflow Denial of Service Vulnerability (MS16-019)
  Microsoft .NET Framework hash collision denial of service vulnerability (MS14-053)
  Microsoft .NET iriParsing vulnerability (MS14-057)
  Microsoft Remote Desktop Protocol Denial of Service Vulnerability (MS11-065)
  Microsoft Remote Desktop Protocol Remote Code Execution Vulnerability (MS12-020)
  SSL and TLS Protocols Vulnerable Implementation (MS12-006)
Ok

```

View Results

The *View Results* hyperlink provided in the job details is a convenient, one click link to view scan results in a grid display in the *Analyze* tab and set the focus of the analysis on the selected job.

Pausing and Stopping Scans

While a scan is running, two additional action buttons appear to allow you to control the scan: *Pause and Stop*. The *Stop* button causes the scanner to immediately cease all scanning activity and terminate the scan process. At that point, a *Resume* button appears. Pressing the *Resume* button causes the scan to re-enter the scan queue and reload the scan's state into a new process so it can continue scanning where it left off.

The *Pause* button is a gentler alternative to *Stop*. It tells the scan process to refrain from initiating any new probes, but doesn't terminate the scan process. The *Continue* button can then be used to tell the process to resume scanning. Note that while a scan is paused, the process remains alive and thus it continues to use system resources. Also, note that the pause function only stops initiating new probes and doesn't terminate probes which are already

running, so it could take several minutes after pausing a scan before all scanning activity fully ceases.

Delete Scan

Delete a single scan:

1. Click the *Delete* option (trash can icon) on the scan row that you wish to delete.
2. Confirm the delete action.

Delete multiple scans at once:

1. Click the check boxes in the left most column on the scan rows that you wish to delete.
2. Click the *Delete Scans* under the *Grid Actions* menu above the grid.
3. Confirm the delete action.

Export Scan

Use the *Export* icon (box with diagonal arrow) to export the desired scan run. See [Export Job](#) for further information.

Request Attestation of Scan Compliance

If the scan ran using the PCI scan policy and completed successfully, then the scan results can be used to request an Attestation of Scan Compliance. *Note: this option only appears if Attestation of Scan Compliance is enabled in your license. Furthermore, this feature does not include ASV attestation services. You should have your own certified ASV staff members in order to use this feature as intended.*

To request an Attestation, go to the *Scan -> Scan Jobs* page and click on the *Scans* tab. Then click on the checkmark icon for the desired scan. (If the checkmark does not appear, then the scan is incomplete, the scan did not run using the PCI scan policy, or attestations are not included in your license.) This brings up a five-step attestation request wizard, as shown below.

Request Attestation of Scan Compliance x

1 Scan Scope

2 Scan Results

3 Special Notes

4 Customer Identity

5 Customer Attestation

Scan Scope

Targets
 The scan included the following targets: 198.51.100.10.

Related Hosts
 The following targets were not included. If any of these targets belong in scope, please add them to the target list and run the scan again.

Related Host	Relationship
www.example.com	198.51.100.10 redirects to this host

I attest that all targets which belong in scope were included in the scan.

Previous
Next
Submit

Each step must be completed before you can advance to the next step. However, you can return to previous steps at any time. The steps are as follows:

1. **Scan Scope** – This step will display the scan scope and ask you to confirm that the scope is correct. It will also inform you if any possible scoping discrepancies were detected.
2. **Scan Results** – This step shows whether or not the scan detected any vulnerabilities which cause PCI failure. If there are vulnerabilities which cause PCI failure, click on the *Go to failing vulnerabilities* button to see what they are. (This exits the wizard, but you can re-enter the wizard at any time.) Then, you can either fix the failing vulnerabilities and run the scan again, or click on the X icon beside the failing vulnerabilities to submit disputes. (See [Create a Dispute](#).)
3. **Special Notes** – This step shows whether the scan detected any conditions that require special notes according to the ASV Program Guide. If there are special notes, click on the *Edit Special Notes* button to view the special notes and enter declarations for them.
4. **Customer Identity** – This step is where you enter the name, address, phone number, and other information to appear in the *Scan Customer Information* section of the Attestation of Scan Compliance. Click on the *Add New Identity* button to enter this information, or select an existing identity from the drop-down menu.

- Customer Attestation** – This step is where you make several attestations and agreements required by the ASV Program Guide, the PCI Security Standards Council, and the ASV solution. All of the required boxes must be checked before the attestation request can be submitted. (The text can be customized using the [Customer Attestations](#) system option.)

When you have completed the five steps in the wizard, click on the *Submit* button. This will notify the ASV staff (as defined by the [Attestation Resolver\(s\)](#) system option) that action is required, and cause an open attestation request to appear on the PCI Attestations page. (See [PCI Attestations](#).)

Job-Scan Tree Tab

Grid Actions ▾

Scans Jobs **Job - Scan Tree**

Page 1 of 1 20 View 1 - 1 of

Actions	Job Name	Job #	Scan #	Last Run ↓	Start Time	End Time	Status	Progress	Scan Policy
▶	My Job C	3							Port Scan
▶	My Job F	6							Full Vulnerability Scan
▶	My Job X	7							Full Vulnerability Scan
▶	My Job D	4		2019-05-22 15:02:14 (Completed)					Port Scan
▶	My Job D	4	11		2019-05-22 15:00:04	2019-05-22 15:02:14	Finished	100%	Port Scan
▶	My Job D	4	8		2019-05-21 15:00:03	2019-05-21 15:02:17	Finished	100%	Port Scan
▶	My Job P	9		2019-05-21 14:25:52 (Completed)					Port Scan
▶	My Job P	9	7		2019-05-21 14:23:36	2019-05-21 14:25:52	Finished	100%	Port Scan
▶	My Job B	2		2019-05-21 14:02:35 (Completed)					Port Scan
▶	My Job Y	8		2019-05-21 13:26:06 (Completed)					Single Penetration
▶	My Job Y	8	5		2019-05-21 13:14:58	2019-05-21 13:26:06	Finished	100%	Single Penetration
▶	My Job E	5		2019-05-21 12:25:08 (Completed)					Full Vulnerability Scan
▶	My Job A	1		2019-05-21 11:37:59 (Completed)					Full Vulnerability Scan
▶	My Job U	11		2019-04-22 12:37:18 (Completed)					Windows Server 2019 \
▶	My Job Q	10		2019-03-13 16:04:28 (Completed)					Network Device

The *Job-Scan Tree* tab provides a grid that combines the functionality of both the *Jobs* and *Scans* tabs. To set this as the default tab whenever navigating to *Scan* or *Scan Jobs* from the navigation bar, use the checkbox in the *Grid Actions* pull-down menu labeled *Default Tab*. For information on the features of the *Jobs* and *Scans* tabs, see the documentation sections [Jobs Tab](#) and [Scan Tab](#).

Using the Job-Scan Tree Tab

To display all the scans for a given job, click the solid right arrow to the left of the job name. To expand or collapse every job, use the *Expand All* or *Collapse All* options, which are in the *Grid Actions* pull-down menu. The grid will automatically refresh every three minutes and its current state will persist, so jobs will not have to be re-expanded; this is also true when sorting,

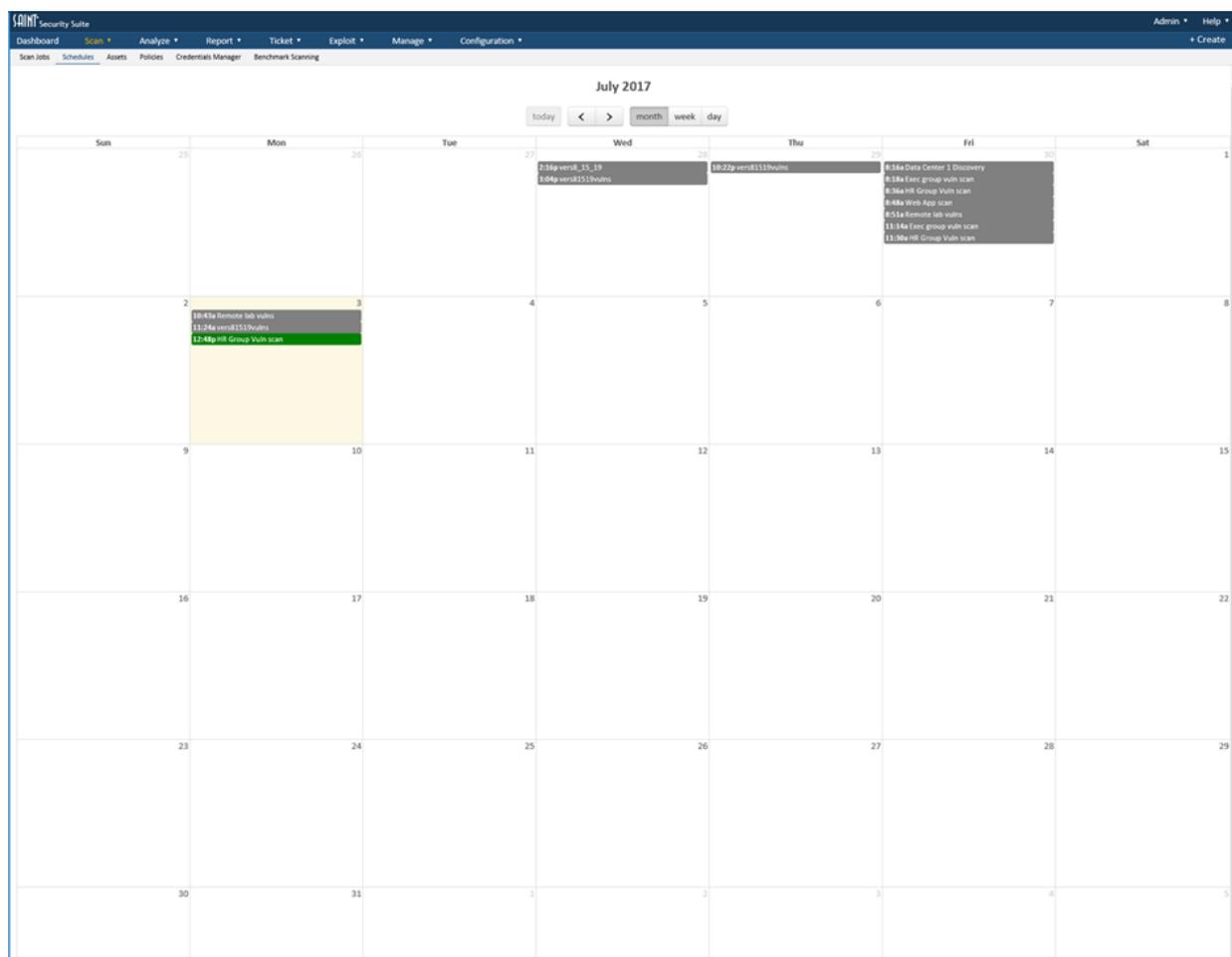
searching, refreshing the grid, and changing the number of records currently in view. To refresh a single job, use the *Refresh Job* icon in the *Actions* column next to the job name.

Additional Functionality in the Job-Scan Tree Tab

This grid also allows you to delete both jobs and scans at the same time. Any row that is checked, which is done by using the checkbox column on the left side of the grid, will be deleted when choosing *Delete Selected* from the *Grid Actions* pull-down menu.

Schedules

The *Schedule* pages provides the same information as the Schedules and Execution History sections of the View Job Details dialog, but in calendar format. It allows you to view your past scans, running scans, and upcoming scans for a given day, week, or month.



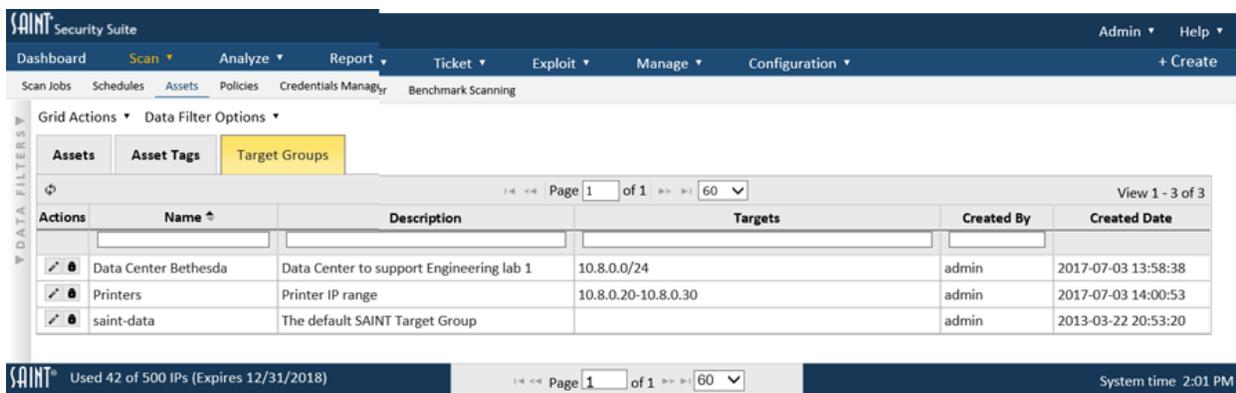
To select the time period for which to show the scan schedule, use the *Month*, *Week*, and *Day* buttons at the top of the screen to switch between calendar layouts. Then use the forward and backward buttons to move to the desired, month, week, or day. Alternatively, use the *Today* button to skip to the current day, week, or month.

On the scan schedule, gray blocks represent past scans, green blocks represent running scans, and blue blocks represent scheduled scans. Click on any block to [view the job details](#). On the daily and weekly views, the size of gray and green blocks corresponds to the duration of the scan job for long-running scans.

To create or delete scan jobs, choose [Manage Jobs](#) from the *Scan* Menu.

Target Groups

The main purpose of this feature is to create a logical collection of “like” scan targets, to reduce the time to set up scan jobs and insert target lists to be scanned. Unlike an asset “tag”, where a tag is associated with an existing host (collected from a scan job's execution) for the purposes of tracking, analyzing, remediating and reporting; a Target Group is simply a method to identify a logical collection of hosts to scan. For example, a Target Group = Servers with a Target list of 192.168.1.1 – 192.168.1.50 describes a range of IP addresses that a job will scan for when the “Servers” target list is selected for job’s target list. Live hosts found from this scan will then be appended to the Asset table for management. **Targets become Assets once they have been acquired from a scan and stored in the Asset table.** If Assets are selected for scanning by their Asset Tag, for example Location=Data Center, then a scan job will scan only the Assets currently in the Asset table that have this tag.



Create Target Group

1. Click the *Target Groups* tab under Assets.
2. Click on *Grid Actions > Create Target Group* option to display the Target Group creation form.
3. Enter a unique name for the target group.
4. Enter a description of the collection of scan targets.
5. Define the targets for the group.

Single Node Target Groups

For installations that are using only a single scan engine (local scanner node), such as standalone installations or shared installations that are scanning reasonably small environments, enter targets into the Enter Target(s) area. Targets can be specified by IP address, hostname, URL, subnet, or CIDR address. IP addresses can be either IPv4 or IPv6. Additional options for selecting or importing target lists are available by clicking on the *More Options* link. See [Target Entry Options](#) for more information about these other options.

Create Target Group [X]

Fields with * are required.

Name *

Description

Local Node

Enter target(s) ?

Selected Target(s)

Remove All

Node Information
Description: SAINT Built-In Scanner
Status: Active

[More Options...](#)

Create

Multi-Node Target Groups

For environments deploying multiple scanner nodes, you can also create target groups that include targets that span across the enterprise, and specify the distributed scanner that can access individual targets and report findings back to the installation acting as the central manager. For example, creating an target group for all Cisco routers, and associating individual routers in each subnet to the scanner node that is deployed in the subnet that can access the target. For those environments, the *Create Target Group* dialog will display the primary (local node) scanner as a named tab, with a plus (+) symbol over a second tab to associated target groups to other available scanners.

Enter targets that will be scanned across multiple nodes, by entering each target list under their associated node. For example,

- A. Enter targets that will be scanned by the local node.
- B. Click the + button beside the *Local Node* tab to view a list of additional nodes you have permission to scan from.

- C. Click on the name of the next node you want to use in setting up your target group to

display that node's target list fields.

D. Enter the targets to be scanned by the additional node.

E. Continue this process for any additional nodes and targets, as needed.

6. Click *Create* to create and save the new target group. The new target group will be displayed in the target group list.
7. View the details of a new target group later by double clicking on a row, or select a row and click on the *edit* (pencil) icon.

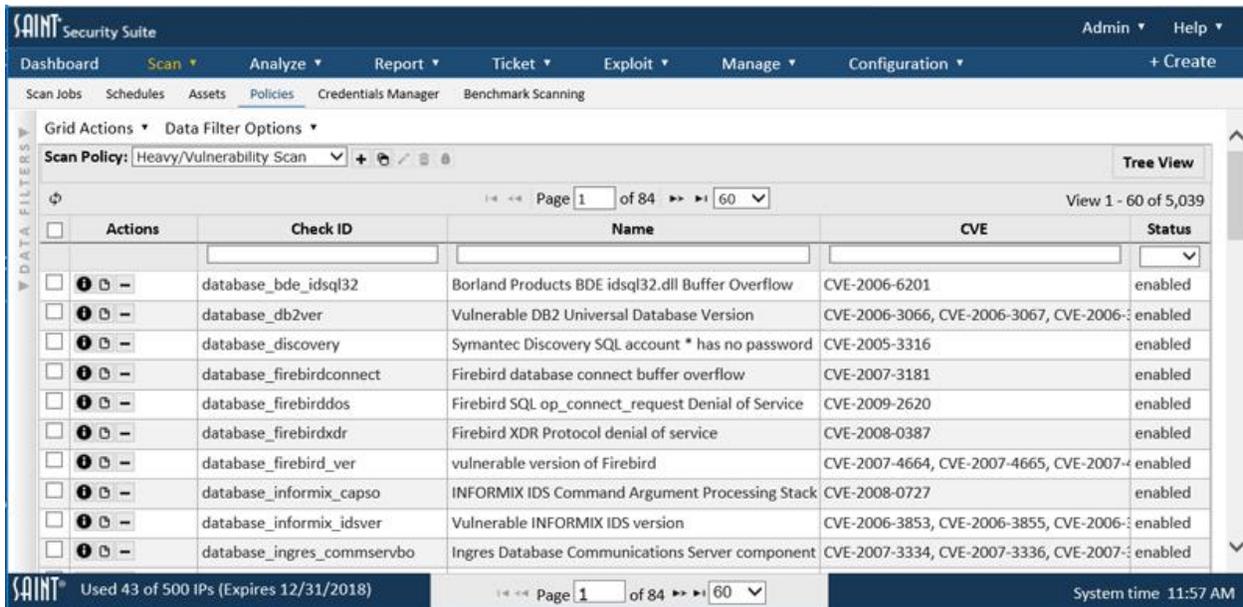
Edit Target Group

1. Click the *Target Group* tab from the Asset page..
2. Double click the target group's record or single click and click the *Edit* option (pencil icon) on the target group row that you wish to edit.
3. Type or copy/paste in the values to be changed.
4. Click *Save*.

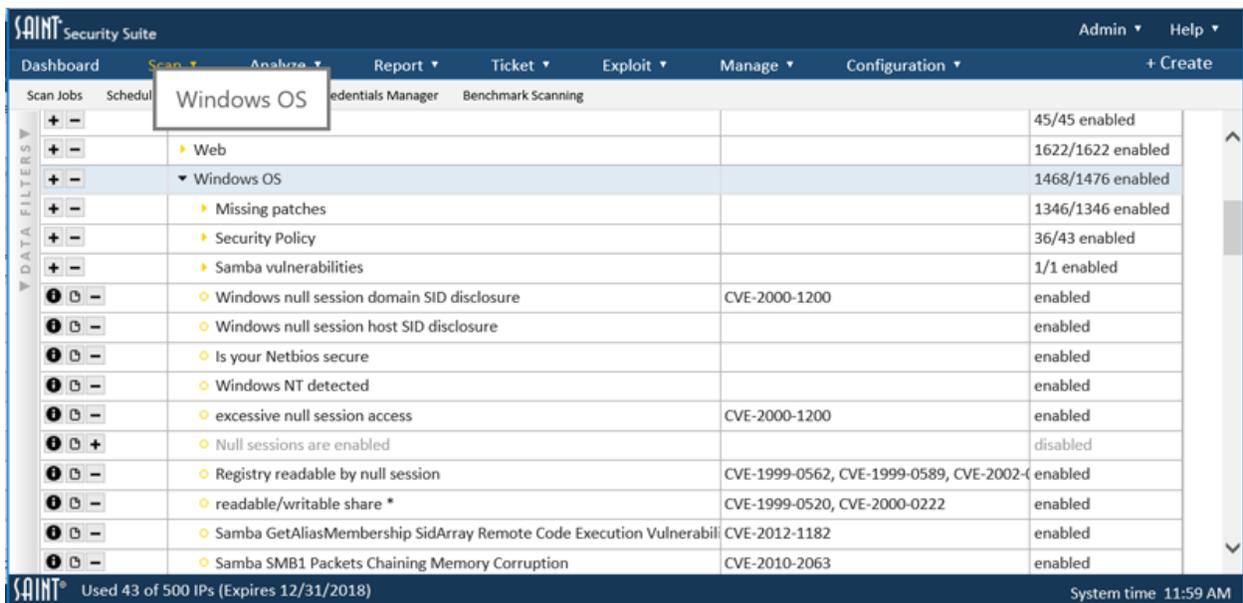
Scan Policies

The *Scan Policy* grid shows all checks by the scan policy visible in the grid's header row. This grid shows all vulnerability checks, to include a descriptive name, associated CVEs, and whether the checks are currently enabled for the policy. This page also provides the capability to select a Custom Severity Set and view the relationship between those defined custom severities and the vulnerability checks within the selected Scan Policy. Note: The Custom Severity column is hidden by default. It can be added by selecting it from the grid's column selector. This view will facilitate such actions as enabling/disabling checks for creating a custom policy; and creating new checks that may be needed for local requirements or for vulnerabilities that may not be available in SAINT's current check repository.

SAINT Security Suite



Use the *Tree Grid* button (upper right corner of the grid) to view checks in a hierarchical view, by various categories, such as by “Database” and “Vendor”. This list also shows the total number of checks, by category. Clicking on each level of the hierarchy will provide more detail, with the actual checks displayed in the lowest level, as shown below in the example:



Click the *Flat View* button to return to the flat view. In the *Flat View*, inside the *Grid Actions* menu, you can export the list of checks and indicate whether each is enabled or disabled by

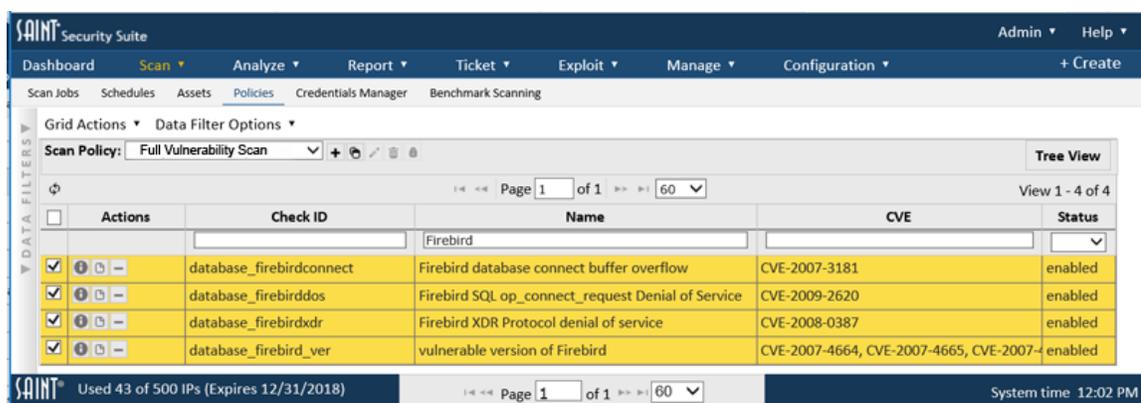
clicking *Export Policy Checks*. You can select CSV or XML format, and the default filename for the export will be the name of the selected Scan Policy with all special characters replaced by underscores.

Creating a Custom Policy

There are instances where you may wish to create a policy that disables some checks, while retaining others. This can be done by:

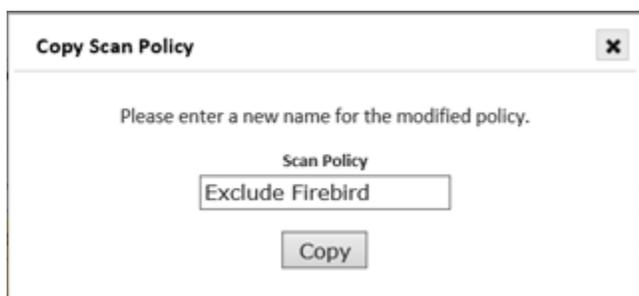
1. Using the check boxes to select the checks on which to act
2. Select the applicable *Enable* or *Disable* option

In the example below, we've performed a column search for checks for "Firebird" for "SAINT's Full Vulnerability Scan" policy. Once that list is present, we've checked all of these checks, to take the required steps to disable them and create a custom policy that excluded the execution of these checks.



Actions	Check ID	Name	CVE	Status
<input checked="" type="checkbox"/>	database_firebirdconnect	Firebird database connect buffer overflow	CVE-2007-3181	enabled
<input checked="" type="checkbox"/>	database_firebirddos	Firebird SQL op_connect_request Denial of Service	CVE-2009-2620	enabled
<input checked="" type="checkbox"/>	database_firebirdxdr	Firebird XDR Protocol denial of service	CVE-2008-0387	enabled
<input checked="" type="checkbox"/>	database_firebird_ver	vulnerable version of Firebird	CVE-2007-4664, CVE-2007-4665, CVE-2007-4	enabled

3. Once you located and clicked in the checkbox for the vulnerability check(s), click the *Disable* option from the *Grid Actions* dropdown to give the new policy a name.



Copy Scan Policy [X]

Please enter a new name for the modified policy.

Scan Policy

Exclude Firebird

Copy

4. *Optional*. Enter a comma-separated list of ports or port ranges in the *Extra Ports* box at the top of the grid, and click on the *Save* button. *Example: 8000-8002,8080*

If specified, these ports will be added to the scan policy. This is only necessary for detecting vulnerabilities on non-standard ports. The standard ports for the enabled vulnerability checks are automatically included. If this field is left blank, only the standard ports for the enabled vulnerability checks are included.

The default for these ports is TCP. To add a UDP port, append `"/UDP"`. *Example:*
`111/UDP`

This custom policy will now be available, as shown in this example:

Create New Job

1 Scan Info
Basic setup and scan policy selection.

2 Targets
Select scan targets.

3 Authentication
Select credentials.

4 Advanced
Additional options.

5 Finish
Create schedules and select ticket rule set.

Step 1: Scan Job Information

Name & Description

Please enter a unique name for this job.
an excluding Firebird

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

Select a Scan Policy

Select Policy Category: Custom

Select Policy: Exclude Firebird

Scan Policy Options

Exhaustive Scan ?

Allow Dangerous Tests ?

Previous Next Finish

Custom Vulnerability Checks

Although SAINT's check repository contains thousands of vulnerability checks, there may be reasons to add custom vulnerability checks, such as site-specific security guidelines which define misconfigurations for which there isn't already a check.

SAINT allows you to create custom vulnerability checks without requiring any programming knowledge. All associated information, such as the severity level, CVE, and tutorial, is created

along with the check. Once created, a custom check will run at the default vulnerability scan level, and can also be selected when creating custom scan levels.

Create a Custom Check

1. Select the *Create Custom Check* option from the Policy's Grid Action dropdown to open the *New Custom Check* dialog (shown below).

The screenshot shows a dialog box titled "New Custom Check" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Vulnerability ***: An empty text input field.
- Check Category ***: A dropdown menu with "Databases" selected.
- Severity**: A dropdown menu with "root access via buffer overflow" selected.
- CVE**: Two empty text input fields.
- Check Type**: A dropdown menu with "Registry Key" selected.
- Check Rule**: A text input field containing "Registry key HKEY_LOCAL_MACHINE" followed by an empty space.
- exists**: A dropdown menu with "exists" selected.
- Impact**: A text input field with up and down arrow icons on the right.
- Background**: A text input field with up and down arrow icons on the right.
- Problem**: A text input field with up and down arrow icons on the right.
- Resolution**: A text input field with up and down arrow icons on the right.
- References**: A text input field with up and down arrow icons on the right.
- Create**: A button at the bottom center.

2. Complete each required field (*) and optional fields, as necessary to define the check details.

- **Vulnerabilities Title** – This is the short vulnerability description which will appear if the vulnerability is detected.
- **Category** – This selection determines where the vulnerability will appear in the vulnerability hierarchy. Top-level categories are indicated by three asterisks (***) . Subcategories are indicated by two dashes (--).
- **Severity** – This is the severity level of the vulnerability.
- **CVE** – This is the CVE name for the vulnerability, if any.

The next step in creating the check is to create the rules which determine when to report the vulnerability. If the rule is true for a target, then the vulnerability will be reported on that target. There are several rule templates, each of which uses a different check methodology. To create the rule, choose the radio button beside the desired rule template, and fill in the template. The available rule templates follow:

- **Registry key exists/doesn't exist** – Fill in the path to the registry key. Note that the hive HKEY_LOCAL_MACHINE is already there, so start with the top-level key under that, such as SYSTEM or SOFTWARE. Use a backslash to delineate sub-keys.
- **Registry value equals/not equal/less than/greater than x.y in key** – Fill in the registry value, operand, and registry key. Note that a numerical comparison is performed on the operand, which is typically a version number. When entering the key, start with the top-level key under the HKEY_LOCAL_MACHINE hive.
- **File in folder is dated earlier than date** – Fill in the file name, folder name, and date. The folder name should start with the root (either slash or backslash is accepted) and the same character should be used to delineate sub-folders. The date should be in Month/Date/Year format, with a four-digit year.
- **File in folder is less than version x.y** – Fill in the file name, folder name, and version number. The folder name should start with the root (either slash or backslash is accepted) and the same characters should be used to delineate sub-folders. Note that determining the file version requires the file to be downloaded, which could slow down the scan if the file is large.
- **Received string from port (and version equals/not equal/less than/greater than x.y)** – Fill in a string and a port number, or an asterisk or the string <any> to run the check against every port. If the data received from the specified port matches the string, the vulnerability is reported. If the second variation of this template is used, then the %version% substring within the string is a placeholder

for a version number to be extracted from the network data, and then a numerical comparison is performed on that version number.

- **URL contains string (and version equals/not equal/less than/greater than x.y)** – Fill in the URL and string. Note that the `http://target/` portion of the URL is already there, so specify the URL beginning with the first character beyond the slash following the target, or leave the field blank to specify the home page of the target. The URL will be requested from the server using a GET request, and the vulnerability is reported if the string is found in the resulting page. If the second variation of this template is used, then the `%version%` substring within the string is a placeholder for a version number to be extracted from the resulting page, and then a numerical comparison is performed on that version number.
3. Optional - Impact, Background, Problem, Resolution, References – Complete these paragraphs to create the Remediation Tutorial for the vulnerability. HTML tags can be used in these fields to create hyperlinks or formatted text.
 4. Click on the *Create* button to create the check.

Running Custom Checks

Custom checks are run the same way as built-in checks. That is, they will be included in scans run at the Vulnerability scan level, and can also be selected when creating custom scan levels. The custom check will appear in the vulnerability hierarchy in the category that was specified when creating the check.

Viewing and Editing Custom Checks

Custom checks are stored and associated with the scan policy they were created for. Whether part of an existing SAINT policy or a custom policy. Custom checks can be viewed and edited using the following steps.

1. Click on the main *Scan* menu – Policies page.
2. Select the applicable scan policy from the policy drop down list in the top of the vulnerability checks grid to view all vulnerability checks for the selected scan policy.
3. Locate a specified custom check by searching the CheckID field, check name or associated CVE, or use the custom column (already displayed or chosen from the grid's column chooser). Selecting the *Yes* value for the custom column will constrain the records to only custom checks for the selected policy.

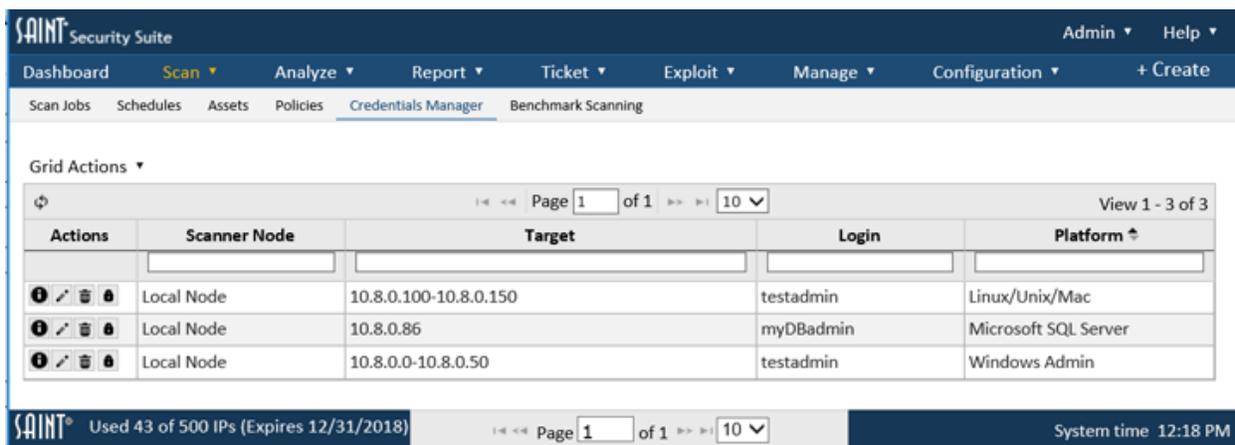
4. Click on the *details* (i) option for the custom check to view current details about the check, relate to vendor references, severity and authentication requirements.
5. Click on the *edit* (pencil) option to view the specific details about the custom checks settings and tutorial content, and make any required modifications.
6. Click *Save* to save changes made to any of the settings or content.

Delete a Custom Check

To delete a custom check, simply click on the *Delete* (trashcan) option on the row of the check to be deleted; then confirm the delete action.

Credentials Manager

The credentials manager allows you to store user credentials securely, and then use them later in scan jobs to authenticate to targets. When selected, a credential “file” is packaged up and passed securely to the scanning engine to support authenticated scans for more in-depth results.



Authenticating to various Platforms

Windows Targets

For authentication to Windows targets, use an account with administrative privileges on the domain for the Windows Admin credentials. It is not necessary to specify the domain; the scanner will authenticate to the target’s domain by default, or a local account if the target is not a member of a domain. If you wish to authenticate using an account in a different domain

than the target, specify the login as *domain\username*. (Note that the separator is a backslash, not a forward slash.) To use a local account even if the target is a member of a domain, specify the account name as "local:login", where login is the login name. Do not put a space after the colon.

The Windows Admin credentials are used to detect Windows updates, registry settings, and program versions, as well as enumerating users, shares, services, and software. If the scan uses the [mobile device](#) scan policy, these credentials may also be used to authenticate to Active Directory servers using LDAP to search for mobile devices which may have vulnerabilities. To enable LDAP authentication, in addition to providing Windows Admin credentials, the SSL certificate for the Active Directory server should be installed on the scanning host, and the TLS_CACERT setting in the ldap.conf file should be set to the path of the certificate. See <http://www.sans.org/reading-room/whitepapers/protocols/ssl-secure-ldap-traffic-microsoft-domain-controllers-33784> for more information about setting up SSL certificates for Microsoft domain controllers. If SSL is not enabled for the LDAP service or the SSL certificate is not available, and you wish to accept the risk of using insecure authentication to the Active Directory server, then enable Allow Insecure LDAP under the Authentication tab of the scan options.

The Windows Non-Admin credentials are used to evaluate file share access controls. Use an account with typical user privileges. As with the Windows Admin credentials, it is not necessary to specify the domain.

If you wish to verify that the Windows Admin login and password are correct, enter the same password in the *Confirm Password* field beside the login and password boxes. Clicking on this button will display a green Login OK message within a few seconds if authentication to the target was successful using those credentials. If there are multiple primary targets selected, the first one will be used for this test. Targets must be specified individually, not as ranges, CIDR blocks, or subnets, in order to use this feature.

Keep in mind that detection of Windows updates should be used as a baseline assessment only. The scanner detects Windows updates using simple checks for the presence of registry keys and file time stamps, which cannot always account for updates that have been incorrectly installed, uninstalled, rendered ineffective due to incorrect order of installation, or other unusual situations. For a more thorough evaluation of Windows updates, it would be advisable to use one of several available patch management tools.

Configuring Windows Targets for Authenticated Scans

Windows Vista introduced more restrictive security settings than previous versions of the Windows operating system. That is good from a security perspective, but creates some challenges for scanners. In order for authenticated checks to work on modern Windows operating systems, the following conditions must be true:

1. Samba 3.0.23d or higher must be installed on the host running Security Suite.
2. OpenSSL 0.9.7 or higher must be installed on the host running Security Suite
3. The Remote Registry service must be running on the target host. This service is not started by default. If it is not running, the scanner will attempt to start it before running any credentialed checks, and stop it after the scan is finished.
4. File and Printer Sharing must be allowed through the Windows firewall. To enable this setting, go to the Control Panel, choose Windows Firewall, and click on Change Settings. Under the Exceptions tab, check the box beside File and Printer Sharing.
5. If the target is not a member of a domain, either one of the following must be true:
 - The scanner must authenticate to the target using the built-in Administrator account. This account is disabled by default so it must first be enabled. (An account which is not the built-in Administrator account does not have sufficient privileges to perform most checks, even if it is in the Administrator's group.)
 - OR, the following registry value is set:
Key:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system\
Value Type: DWORD value
Value Name: LocalAccountTokenFilterPolicy
Value Data: 1
This setting grants sufficient privileges for running a scan to any user in the Administrator's group.
6. Ensure that no Windows security policies are in place that block access to these services. Two common problems are the SEP configurations that block off the scanners even after the scanner is authenticated and a network access model that sets network access to "Guest only" permissions.

Linux, Unix, or Mac

For authentication to Linux, Unix, and Macintosh targets, any active user account on the system may be used. The SSH service must be running on the remote target in order for authentication

on Linux, Unix, and Macintosh targets to function. If you choose not to authenticate, the scan engine will still conduct its full set of unprivileged vulnerability checks, omitting only those few which require authentication.

SSH Private Key

Optional – You also have the option to use SSH public key authentication to Linux, Unix and Macintosh targets. To use public key authentication, paste the private key into the `ssh_private_key` text area. The private key should correspond to a public key contained in the `authorized_keys` file on the target host. If the private key requires a passphrase, enter it in the *Password* field.

New Credential [X]

Fields with * are required.

Target Group: Credentials Type*:

Login*: Password: Verify Password:

Local Node

Enter target(s): ? Selected Target(s):

Node Information
Description: SAINT Built-In Scanner
Status: Active

Oracle Database Servers

For authentication to Oracle Database servers, a fully privileged account such as SYS or SYSTEM should be used. The scanning system must meet the requirements for the Oracle Instant Client in order for Oracle authentication to succeed. The Oracle instant client, which enables Oracle Database account checks and exploits, is included with Security Suite and supported on Linux with glibc 2.3 or higher (x86 or x86_64) and Mac OS X 10.4 or higher (x86). Oracle

authentication allows the scan to detect local Oracle vulnerabilities such as users or roles with ANY privileges or users with the DBA role. Note that Oracle authentication is not necessary to check for Oracle security patches. Windows or Linux/Unix authentication is required for that.

Oracle SID

Besides specifying the Oracle login and password, it is also possible to specify the SID of the database instance to be scanned. Enter this value when creating the credentials for an Oracle target.

New Credential [X]

Fields with * are required.

Target Group: None
Credentials Type *: Oracle

Login *:
Password:
Verify Password:

SID:

Local Node

Enter target(s):

Node Information
Description: SAINT Built-In Scanner
Status: Active

Selected Target(s):

Remove All

Create

The SID is needed in order to authenticate to the database. If the SID is omitted, the scanner will attempt to determine the SID of the remote database; however, determining the SID of the remote database is not always possible. Therefore, it is advisable to specify the SID if known. The SID can be specified even if the login and password are not, in order to assist the password guessing attempts.

Microsoft SQL Server

Authentication to Microsoft SQL Server allows scanning for local database vulnerabilities such as privilege elevation through stored procedures and privilege elevation through web tasks. Authentication to Microsoft SQL Server requires the database to be configured to use mixed-mode authentication, and to allow remote connections using TCP. A fully privileged account such as "sa" should be used. (Security Warning: The Microsoft SQL Server password will be sent over the network using weak encryption.)

Note that Microsoft SQL Server authentication is not required in order to detect whether SQL Server patches have been applied. Windows authentication should be used for that.

MySQL Databases

Authentication to MySQL databases allows scanning for local database vulnerabilities, such as users having excessive privileges. The mysql client program must be installed on the Security Suite host in order for this feature to be used. Also, authentication to MySQL requires the database to be listening over the network, and for access to be allowed from the Security Suite host. A fully privileged database account such as "root" should be used to authenticate.

Note that MySQL authentication isn't required for determining vulnerabilities in the MySQL software itself. Those vulnerabilities are inferred without authentication from the MySQL version number found in the network response from the MySQL service. Unix/Linux authentication may be helpful for reducing false positives however.

SNMP Version 3

For collecting certain system properties from SNMP services using version 3 SNMPv3 credentials may be supplied.

New Credential

*Fields with * are required.*

Target Group: None
 Credentials Type*: SNMPv3

Login*: Password: Verify Password:

SNMP Version 3 Passphrase:

Password Protocol: MDS SHA
 Passphrase Protocol: DES AES

Local Node

Enter target(s): ? Selected Target(s):

Node Information
 Description: SAINT Built-In Scanner
 Status: Active

These fields correspond to the following snmpget tool arguments:

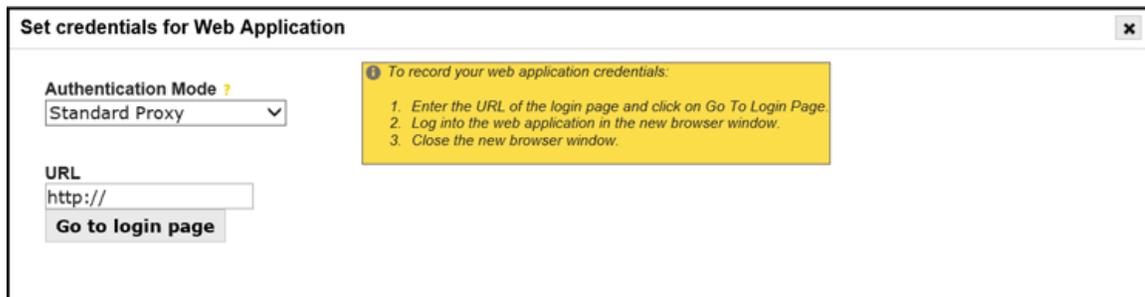
- Login: -u (securityName)
- Password: -A (authKey)
- Password Protocol: -a (authProtocol)
- Passphrase: -X (privKey)
- Passphrase Protocol: -x (privProtocol)

Web Applications

SAINT also supports form-based authentication to web applications. However, instead of simply specifying the login and password directly on the Scan page, you must either record the login steps or specify the POST parameters to be sent to the application.

To authenticate to a web application using form-based authentication:

1. Open the [New Job wizard](#) and proceed to step three of the wizard.
2. Click on the *Set* button beside *Web Application*. A dialog box will appear.



3. Optional. Choose the *Authentication Mode*. There are three modes:
 - a. The **Standard Proxy** is the default mode. It uses URL rewriting to send HTTP requests through SAINT to record your login steps. It doesn't require any configuration changes to your browser.
 - b. The **Advanced Proxy** records your login steps without modifying URL references. This may improve usability on more complex sites, but requires you to make configuration changes to your browser.
 - c. The **Manual** mode allows you to specify a browser cookie. Choose this option if you already know the session ID of an authenticated session on the site.
 - d. The **POST Data** mode allows you to specify your application credentials as form parameters without using a proxy. However, this only works for applications that use single-step authentication.

Note: If you choose an option other than Standard Proxy, skip to the appropriate instructions below.

4. Enter the URL of the login page for your web application.
5. Click on the *Go to login page* button. This will open a pop-up window with the login page for your web application.
6. Log into the web application.
7. After you have successfully logged in, close the pop-up window. Your session cookie will be displayed.
8. Click on the *Save* button.

Note that web authentication only works if the application uses HTTP cookies for tracking sessions. Also, note that the authentication steps are saved as well as the session cookies. Scheduled scans will generate an authentication script which reproduces the

authentication steps, rather than saving the session ID itself. That is because the session ID will usually expire after a certain amount of idle time.

Note: the authentication script may be unable to correctly reproduce the authentication steps if the steps are very complex.

Advanced Proxy

The Advanced Proxy uses an HTTP proxy service to capture your login steps. This helps avoid URL rewriting errors which may be unavoidable when using the standard proxy. However, it requires you to modify your browser's configuration to send all HTTP requests through the proxy service. It also requires you to import a CA certificate into your browser's certificate store. That is because the proxy service must decrypt TLS sessions in order to record the authentication steps. Therefore, the proxy service creates and signs a certificate for each TLS server, allowing itself to negotiate a TLS session with your browser on behalf of the server. The CA certificate tells your browser to accept these server certificates.

To use the advanced proxy, first follow steps 1 through 3 above, and choose *Advanced Proxy* in step 3. Then follow the instructions shown in the yellow box on the right side of the dialog box. Click on the *Save* button after completing the steps. *Note:* be sure to choose a proxy port which is allowed through your firewall.

Manual Web Authentication

Besides carrying out the authentication steps, it is also possible to enter an existing session ID for an authenticated web application session directly. This may be desirable, for example, if you already have an authenticated session and don't want to bother repeating the steps, or if the authentication steps are too complex to work in the standard proxy mode and you don't have an unfiltered port to use for the advanced proxy mode.

To use manual web authentication, first follow steps 1 through 3 above, and choose *Manual* in step 3. Then continue as follows:

4. In the *Post-authentication Landing Page* box, enter the full URL of the page which you normally arrive at after authentication.
5. In the *Cookie* box, enter your session ID as an HTTP cookie value, i.e., as a list of name=value pairs, separated by semi-colons. For example: sid=123456; uid=789

6. Click on *Save*.

POST Data

In cases where a web application uses a single form submission to send login credentials, this option allows you to specify the POST data and action URL directly, without using a proxy. This may be more reliable than using the Standard Proxy, and more convenient than using the Advanced Proxy. The wizard helps you determine the form parameters and action URL for your application's login page, so you can still use this option even if you don't already know this information. Once your credentials are saved as POST data, this data will be sent to the specified action URL at the start of every scan run, and the resulting session cookie will be used throughout the scan.

To specify your credentials as POST data, first follow steps 1 through 3 above, choosing POST Data in step 3. Then continue as follows:

1. Enter the URL of your web application's login page in the *Login Form URL* box.
2. Click on the *Load* button to automatically initialize the remaining fields based on the content of the specified login form.

OR

Fill in the remaining fields manually. Click on the *Add Row* button if more parameter rows are needed. Click on the minus icon beside any parameter row to delete that row.

3. Enter any missing parameter values such as the login name and password. (Click on the *Add Row* button if the needed parameter names are not already present.)
4. The *POST Data* field shows you the raw POST data which will be posted to the action URL. It is automatically updated as you modify the parameter names and values, so you do not need to modify this field by hand.
5. *Optional* – In the *Successful Login Response Pattern* input, enter a string which the application always returns after a successful login. The scanner will search for this string to verify that authentication is successful. If this string is specified but is not matched in the response page after the POST data is submitted, the scan will not run, and the scan's status will be set to "Error".
6. Click on the *Save* button.

HTTP Basic Authentication

HTTP Basic authentication refers to web servers hosting password-protected directories. HTTP Basic authentication typically results in a pop-up dialog box prompting the user to enter a login and password, as shown in the example image below.

Note that HTTP Basic authentication is not the same as form-based authentication, where the user is prompted to enter a login and password directly into a web page.

When entering HTTP Basic authentication credentials, be aware that the password will possibly be sent over the network without encryption.

Create a Credentials File

New Credential [Close]

*Fields with * are required.*

Target Group: None [v] Credentials Type*: HTTP Basic [v]

Login*: [] Password: [] Verify Password: []

Local Node

Enter target(s): [] ?

Node Information
Description: SAINT Built-In Scanner
Status: Active

Selected Target(s): []

[Remove All]

[Create]

1. Navigate to the *Credential Manager* page from the main Scan menu.
2. Click *Create Credential* from the Grid Actions dropdown list.
SAINT will display a dialog window.

3. Optional – Select a target group. This will automatically populate the target selection.
4. Select the credentials type.
5. Enter the login and password.
6. Optional – Select the scan node on which to apply the credentials from the tabs above the *Enter Target(s)* box. If the desired node is not shown, choose the “+” tab and select it from the drop-down menu. (If the “+” tab is not shown, then all allowed nodes are already shown.) To apply the credentials on multiple nodes, select the desired scan nodes one at a time, and enter the targets for each node under the corresponding tab. To apply the credentials on all nodes, enter the targets under the *All Nodes* tab.
7. Type targets into the *Enter Target(s)* box one at a time. Targets can be specified by IP address, URL, Subnet, or CIDR address. Note that IP addresses can be either IPv4 or IPv6.
8. Click *Create*.

Credentials File Format

platform|target|username|password

Platform may equal any of the following:

- 'B' = windows/linux/mac
- 'W' = windows
- 'L' = linux
- 'O' = oracle
- 'X' = windows non-admin
- 'M' = Microsoft SQL Server
- 'Y' = MySQL
- 'H' = HTTP basic authentication
- 'S' = SNMP Version 3

Example Files:

W|127.0.0.1|user|pass

B|127.0.0.4|admin|pw

L|127.0.0.10|root|abc123

L|127.0.0.5|somekey:someuser|x4y5z6

S|127.0.0.1|somekey~~~~SHA~~~~DES:someuser|abc456

Note that the passwords will be encoded and never displayed in plain text.

Edit a Credentials File

1. Navigate to the *Credential Manager* page from the main Scan menu.
2. Click the *Edit* (pencil) action for the credential record to be edited.
An edit dialog window will be displayed.
3. Change the applicable fields (e.g., target, login ID, password)
4. Click *Save*

You will now see the edited version of the save credentials in the *Credentials* grid.

Delete a Credentials File

1. Navigate to the *Credential Manager* page from the main Scan menu.
2. Click the *Delete* (trashcan) action for the credential record to be deleted.
A message will be displayed to confirm the delete operation..
3. Click *OK* to confirm and delete the stored credentials.

You will now see the deleted credential record is no longer displayed in the *Credentials* grid.

Benchmark Scanning

Benchmark scanning provides the capability to assess scan targets against various industry-standard best-practices and security states such as platform configurations, patch levels, software inventory, and status of known vulnerabilities tracked by standards bodies such as CIS, NIST, DISA, Red Hat, AIX, Cisco, and others. For example, the configuration benchmarks are security configuration baselines that allow a user to assess a host's platform configurations to ensure their security settings map to industry best-practices.

The following shows an example list of the current configuration baselines available for comparison against your host environment.

Name	Platform	Version	URL
USGCB 1.2 Windows 7	USGCB/T	1.2	https://usgcb.nist.gov/usgcb/content/scap/oval510/Win7-2.0.5.1.zip
USGCB 1.2 Windows 7 Firewall	USGCB/T	1.2	https://usgcb.nist.gov/usgcb/content/scap/oval510/Win7-Firewall-1.3.0.1.zip
USGCB 1.2 Windows Vista	USGCB/T	1.2	https://usgcb.nist.gov/usgcb/content/scap/oval510/WinVista-3.0.5.1.zip
USGCB 1.2 Windows Vista Firewall	USGCB/T	1.2	https://usgcb.nist.gov/usgcb/content/scap/oval510/WinVista-Firewall-2.1.0.1.zip
USGCB 1.2 Windows XP	USGCB/T	1.2	https://usgcb.nist.gov/usgcb/content/scap/oval510/WinXP-3.0.3.1.zip
USGCB 1.2 Windows XP Firewall	USGCB/T	1.2	https://usgcb.nist.gov/usgcb/content/scap/oval510/WinXP-Firewall-2.1.0.1.zip
CyberESI Suspicious Files	CyberESI	1.1	feeds.cyberesi.com/scap/generic/CyberESI-SCAP-SuspiciousFiles.zip
Microsoft Windows 2008 DC	DISA	1.1	iaase.disa.mil/stigs/Documents/u_windows_2008_dc_v6r1.28_stig_benchmark.zip
USGCB Redhat 5	USGCB/T	1.1	https://usgcb.nist.gov/usgcb/content/scap/USGCB+hel5desktop-1.2.5.0.zip
AIX 5.3	DISA	1.1	iaase.disa.mil/stigs/Documents/u_aix_5.3-v1r2_stig_benchmark.zip
AIX 6.1	DISA	1.1	iaase.disa.mil/stigs/Documents/u_aix_6.1_v1r3_stig_benchmark.zip
Sun Solaris 9	DISA	1.1	iaase.disa.mil/stigs/Documents/u_solaris_9_sparc-v1r4_stig_benchmark.zip
Microsoft Windows 2008 MS	DISA	1.1	iaase.disa.mil/stigs/Documents/u_windows_2008_ms_v6r1.28_stig_benchmark.zip
Microsoft Windows 2012/2012 R2 MS	DISA	1.1	http://iaasecontent.disa.mil/stigs/zip/jul2016/U_Windows_2012_and_2012_R2_MS_V2R5_STIG_SCAP
Microsoft Windows 2012/2012 R2 DC	DISA	1.1	http://iaasecontent.disa.mil/stigs/zip/jul2016/U_Windows_2012_and_2012_R2_DC_V2R5_STIG_SCAP
Internet Explorer 10	DISA	1	iaase.disa.mil/stigs/Documents/u_microsoft_ie10_v1r3_stig_benchmark.zip
Internet Explorer 9	DISA	1	iaase.disa.mil/stigs/Documents/u_microsoft_ie9_v1r5_stig_benchmark.zip
Microsoft Windows 2003 DC	DISA	1	iaase.disa.mil/stigs/Documents/u_windows_2003_dc_v6r1.36_stig_benchmark.zip
Microsoft Windows 2003 MS	DISA	1	iaase.disa.mil/stigs/Documents/u_windows_2003_ms_v6r1.36_stig_benchmark.zip
Sun Solaris 10	DISA	1	iaase.disa.mil/stigs/Documents/u_solaris_10_sparc_v1r7_benchmark.zip

The capabilities supported on this page enable a user to download the latest policies and profiles, using the download option under the Actions column of a data grid, create scan jobs, and execute the selected assessment against hosts associated with the applicable platform. Additionally, the software also provides a configuration [Policy Editor](#) to modify selected configuration profiles and create custom benchmarks to support local requirements.

For those that require the use of this capability for NIST compliance, SAINT provides an SCAP Version column to assist in determining content compliance with the latest standards. Refer to the [SCAP section](#) of this user guide for comprehensive help on SAINT's support to the SCAP program and running scans using this content.

SAINT's benchmark scanning capability requires Oracle Java 8 to be installed on the scanning system. See [System Requirements](#) for more information.

Target Settings

Due to the type of scan assessments performed in benchmark analysis, the hosts must have certain configurations enabled to ensure a thorough and accurate assessment. The following settings must be configured on hosts assessed by these profiles:

*For Linux/Unix (*nix) targets*

1. Ensure SSH is installed on the target and is running.
2. If using the root account to scan (recommended) make sure root log in is enabled in SSHD:

- a) Open `/etc/ssh/sshd_config`
 - b) Set `'PermitRootLogin no'` to `'PermitRootLogin yes'`
 - c) Restart SSH
3. Make sure iptables / firewall allows communication to/from the SAINT 8 host.

For Windows targets

1. Configure firewall rules for ws-management and ensure port 139 is not blocked; and enable and configure ws-management on the hosts.
2. Configure the needed Firewall Rules via the group or local policy, or whatever other means are used on your network. For example:
 - a) Open the local policy editor
 - b) Add a firewall rule using the predefined type - Windows Remote Management Service (WS-Management)
 - c) Add a firewall rule using the port type - TCP 139
3. From the network and sharing center, make sure a network other than “public” is being used. WinRM does not work over “public”.
4. The Remote management (WinRM) ws-management service must be running and configured on the host. It is pre-installed on all versions of Windows operating systems, except XP, but is not running by default. Reference: ws-management reference: <http://msdn.microsoft.com/en-us/library/aa384372%28v=vs.85%29.aspx> .
To configure WinRM:
 - a) Open control panel > Administrator tools > Services
 - b) Start the Windows Remote Management Service (WS-Management) (default port 5985)
 - c) Right click cmd and Run as Administrator
 - d) Type `winrm qc`
 - e) Enter `y` twice; this enables WinRM in its default configuration
5. Additional steps may be required to get port 139 and 5985 unblocked/filtered from the network on the target host. These may include:
 - a) Enabling file and printer sharing
 - b) Starting the netbios over TCP/IP service
 - c) Making changes to the Windows Firewall Domain Profile if the target is Windows XP:
 - i. Enable Windows Firewall > Domain Profile > Allow file and print sharing exception
 - ii. Enable Windows Firewall > Domain Profile > Allow local port exceptions

- d) The user account used to perform SCAP scans must have a password associated with that user account unless it is a SSH account using a SSH key.

MICROSOFT WINDOWS TROUBLESHOOTING TIPS:

- Incorrect password
- Attempting to log in as a user who is not a member of the Administrator's group. Only Administrators are able to login via WS-Management.
- The target machine is configured to disallow the "Negotiate" authenticate method. To view permitted authentication methods on the target, run the command: `winrm get winrm/config/Client/Auth`
- In certain situations, when the target machine is joined to a domain, logging in using a local machine account is disabled. This problem has been observed after upgrading from Windows Management Framework 1.0 to 2.0, for example, on a Windows 2008 Server machine (not R2). To enable local account logins in this situation, you must create the `LocalAccountTokenFilterPolicy` registry value:

Key Path: `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System`

Value Name: `LocalAccountTokenFilterPolicy`

Type: `DWORD`

Value: `1`

- If WinRM has been configured and port 5985 still appears to be filtered on the target, which can be checked by running `nmap -p5985` from the scanner, then a Group Policy Object (GPO) may have prevented the WinRM listener from being set up correctly. This can be checked by running the following command on the target as administrator:

```
winrm enumerate winrm/config/listener
```

If you notice something similar to the following,

```
Listener[Source="GPO"]
```

```
.
```

```
.
```

```
.
```

```
ListeningOn=null
```

Then the GPO needs to be updated before reconfiguring WinRM on the target. To do this:

1. Set the IP filters in the GPO setting: *Allow automatic configuration of listeners*, to an asterisk (*)

2. Reload the GPO on the target
3. Shut down the ws-management service
4. Run winrm qc again as administrator

For CIS-hardened Windows Systems

----- WinRM Auth Setup -----

The following should be performed after you have applied the L1 GPO before you scan and also after you have applied the L2 GPO before you scan.

Ensure that your account is part of the Administrators group.

Ensure that your account is part of the Remote Management Users group.

Ensure that Administrators have Full Control over WinRM:

```
$]winrm configSDDL default
```

- Ensure Administrators have FULL control.

```
$]wmimgmt
```

- Right click WMI Control -> properties
- Security Tab -> Security button
- Ensure Administrators have FULL control.

GPO -> Computer -> Local Policies -> User Rights Assignment

'Deny access to this computer from the network' should only be 'Guests'

'Access this computer from the network' should include 'Administrators'

'Allow log on locally' should include 'Administrators'

GPO -> Computer -> Administrative Templates -> Windows Components -> Windows Remote Management -> WinRM Service

'Allow remote server management through WinRM' = 'Enabled' Set IPv4 to *

'Allow Basic authentication' = 'Disabled'

'Allow unencrypted traffic' = 'Disabled'

'Disallow WinRm from storing RunAs credentials' = 'Enabled'

GPO -> Computer -> Administrative Templates -> Windows Components -> Windows Remote Shell

'Allow Remote Shell Access' = 'Enabled'

The firewall must be enabled for the PASS state scans so make sure you have a firewall rule:

```
$]netsh advfirewall firewall add rule name="WinRM-HTTP"  
dir=in localport=5985 protocol=TCP action=allow
```

You may also need to allow the WinRM program through the firewall and / or run winrm qc again.

When using a local admin account the following key must be set to 1 before performing a scan.

This setting likes to reset on occasion so it's a good idea to check it before scanning.

[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]

LocalAccountTokenFilterPolicy

You will get an error code 5 if this has been set to 0 on the target.

Test that you can access WinRM from your scanner by running:

```
nc -z -w1 10.7.0.34 5985;echo $?
```

the output should be '0'

Vulnerability/Patch and Inventory Scanning

1. Click on the *Import Policy* button under the Actions column for the applicable profile. This step will validate the current benchmark and update it, if applicable, to ensure your scan uses the most current profile.
2. Once the download step is complete, click the *Run* (right arrow) button in the Actions column to create a new scan job and run the imported profile against targets defined in the job.
3. Refer to the [Create a New Job](#) section for more detail on setting up a scan job.

Note: Use the *Info* (i) button in the Action column to view the XML content for any profile on this tab.

Configuration Scanning

1. Click on the *Import Policy* button under the Actions column for the applicable profile. This step will validate the current benchmark and update it, if applicable, to ensure your scan uses the most current profile(s).
Note: Some platforms may have multiple profiles, based on the authoritative source's defined levels of security baselines. For example, the Microsoft Windows 2008 DC benchmark 9 distinct profiles based on the various security configuration levels.
2. Once the download step is complete, you can view the configuration settings of a selected profile by clicking on the *Edit* (pencil) icon beside the applicable profile.
3. Click the *Run* (right arrow) button in the Actions column to create a new scan job and run the imported profile against targets defined in the job. For benchmarks with

multiple profiles, use the *Run* (right arrow) button in the Profiles dialog window to select the applicable benchmark profile.

4. Refer to the [Create a New Job](#) section for more detail on setting up a scan job.

Note: Use the *Info* (i) button in the Action column to view the XML content for any profile on this tab.

Creating Custom Configurations

SAINT provides the capability to modify configuration benchmarks to create custom benchmarks for local use. To view or modify a profile, click on the *Edit* (pencil) icon for the applicable profile. This profile Editor can be used for modifying any profile listed in this tab, including SCAP benchmarks. Refer to the [Configuration Benchmark Policy Editor](#) section for more information about this process.

Passive Host Discovery

The Passive Host Discovery grid displays targets on the network which have been discovered by silently watching for traffic from new IP and MAC addresses, rather than actively probing a range of addresses. The grid indicates when each host was last seen and last scanned.

Note: This feature is disabled by default. To enable and configure it, see [Passive Host Discovery](#).

The screenshot displays the SAINT Security Suite interface. At the top, there is a navigation bar with the following menus: Scan, Analyze, Report, Ticket, Exploit, Manage, Configuration, and a + Create button. Below the navigation bar, the 'Passive Host Discovery' tab is active. The main content area shows a grid with the following columns: Actions, IP Address, Node Name, Last Seen, and Last Scanned. The grid contains several rows of data, including IP addresses like 192.0.2.1, 192.0.2.100, 192.0.2.101, 192.0.2.104, 192.0.2.110, 192.0.2.121, 192.0.2.135, 192.0.2.136, and 192.0.2.147, all identified as 'Local Node'. The 'Last Seen' column shows various timestamps from 2019-09-05 to 2019-09-09. The 'Last Scanned' column is currently empty. The interface also includes a 'Grid Actions' dropdown and pagination controls showing 'Page 1 of 2' and 'View 1 - 20 of 38'. At the bottom, a status bar indicates 'Using 0 of 10 agents. (Expires 12/31/2020)' and 'System time 3:39 PM'.

Scanning Passively Discovered Hosts

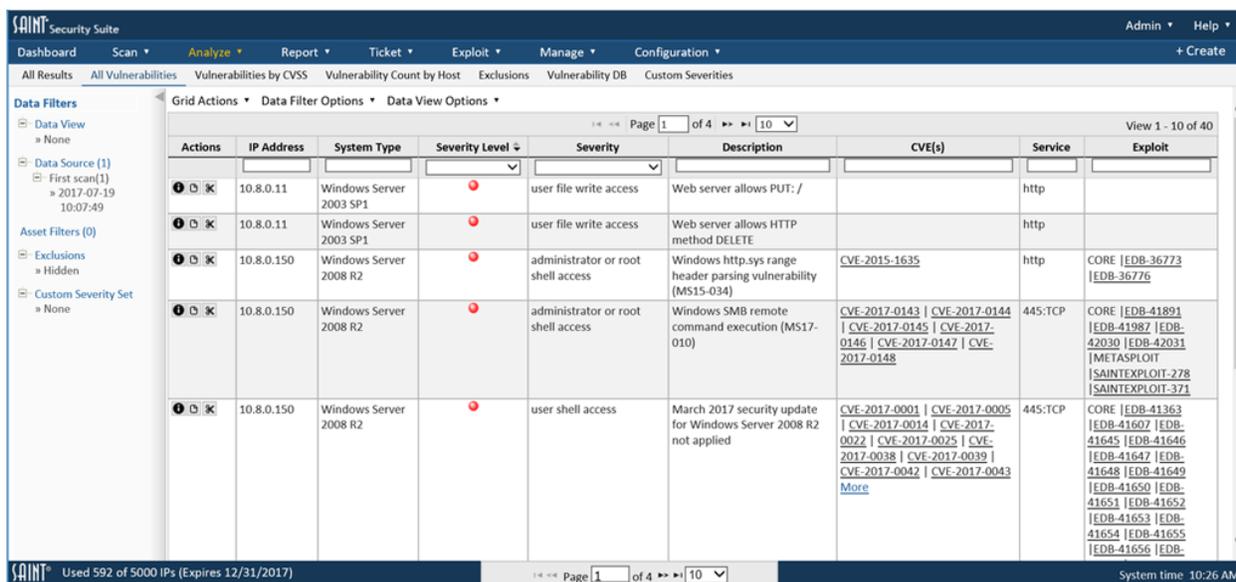
After hosts have been discovered, they can be easily scanned by choosing Scan Hosts from the *Grid Actions* menu. This brings up a dialog box with the following three options:

- Scan Selected Hosts – This option will scan the targets which are currently selected in the grid. (This button is disabled if no targets are currently selected.)
- Scan By Interval – This option will scan all passively discovered hosts which have not been scanned in the chosen number of past days, including hosts which have never been scanned, regardless of whether they are selected in the grid. If this option is chosen, the target list will be dynamically generated every time the scan job runs. This allows you to create a recurring scan job which regularly scans all new devices seen on the network.
- Scan All Hosts – This option will scan all passively discovered hosts, regardless of whether they are selected in the grid. As with the previous option, this option will cause the target list to be dynamically generated every time the scan job runs. This allows you to create a recurring scan job which regularly scans all devices which have been recently seen on the network.

Click on the button corresponding to the desired scan option. This opens the scan job setup wizard. Proceed with the scan job setup as described in [Create a New Job](#) but skip the target entry step.

Analyze

The capabilities under the *Analyze* menu enable you to view detailed scan results, perform analysis, make decisions on other actions, and export scan results for external use.



These analytics provide a wide variety of features to facilitate on-line analysis, such as dynamic selection of one or more data sets; column selection; sorting and filtering; basic column-level searching; advanced sorting; and exporting content. The analytics pages also provide a number of predefined views of the data based on some of the most common ways to look at raw vulnerability results—from all results including services and informational items, to just results with specific vulnerability severity codes, to rolled-up aggregate counts by Host.

You can also set your own data context with the [Data Filters](#) options; control data grid displays from option under the [Grid Actions](#) dropdown menu and record level Actions; and create your own pre-defined views using the Data View Options capabilities. The Data Filters you define will always be visibility for data context in the left Data Filters column. The arrow displays on the top right side of the Data Filters board can be used to Hide this column to give you more usable screen space for analysis or Show it for context while performing analysis.

The list of pre-defined views are displayed dynamically, based on the type of scan results selected. For example, selecting an exploit-related scan (penetration testing; individual exploits or tool) will display views that customize the list of available columns specific to exploit scans. Selecting a vulnerability or configuration scan will display views customized for these types of content. Each view is described below.

All Scan Results

This view shows vulnerability results for the selected data set(s) at the host level of detail, for all vulnerability severity levels, to include services and facts coded as “informational” only. This view also shows an aggregation of all related CVEs, for each vulnerability, with hyperlinks from the CVE to the associated external source. You can also see all available column values for a record by double clicking the row. You can also view the full tutorial about the vulnerability by clicking on the tutorial button in the row's Action column.

View All Facts

The *View all Facts* option is available only in the *All Scan Results* view, and displays all scan information recorded during the selected scan—not just vulnerability, service and information items determined by interrogating the host.



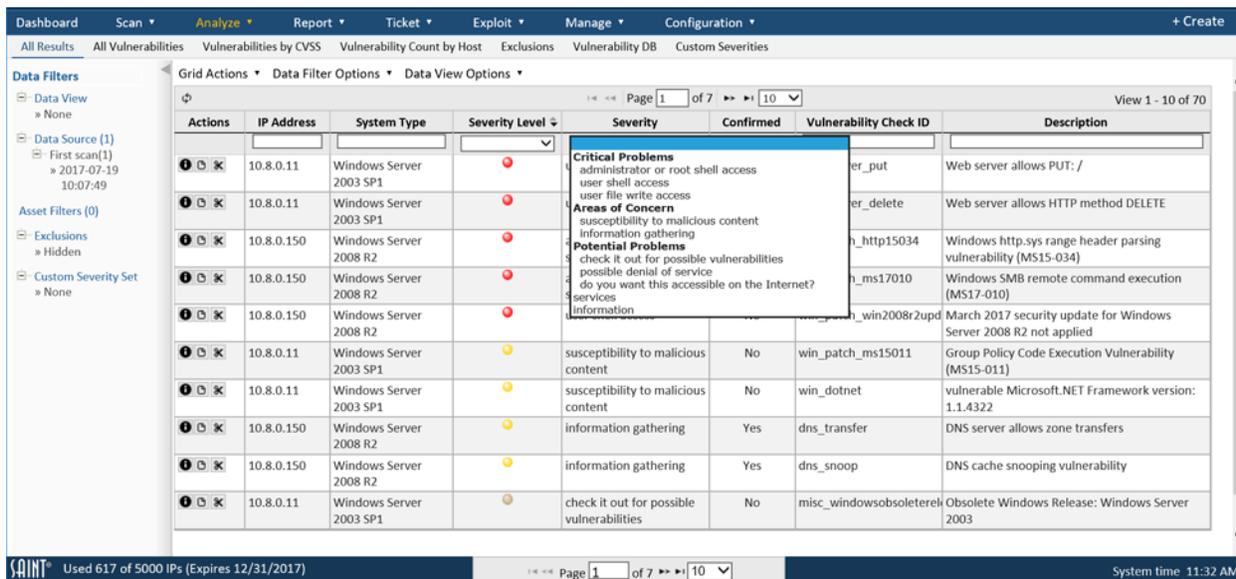
This level of detail is not applicable to day-to-day risk and vulnerability analysis, but can be beneficial in troubleshooting and false positive investigation, as they include codes that are recorded at scan run time and can have an effect on how scan probes and checks are executed. Some of the more common codes follow:

- Severity = “a” (available)
- Severity = “i” "full user list"
- Severity “r”, “y” and “b” (red, yellow, brown) are "number of vulnerabilities"
- Severity “g” (Green) is "number of services"
- Severity = “u” (unavailable) is sometimes useful for troubleshooting by SAINT’s Support engineers.
- Severity = “n” (network or broadcast address) is only used for legacy Smurf and Fraggle checks and are rare seen anymore, but may be included in the results.
- Severity “b” (bad, unable to resolve) and “x” (look into further) may be in the results data and may require further investigation by SAINT Support to make a determination of cause or affect.

Note that your SAINT support engineer may ask for this information or refer to it during an on-line troubleshooting call. Therefore, having access to this information directly through the user interface can save time whenever they are asked to assist in an issue.

All Vulnerabilities

This view shows vulnerability results for the selected data set(s) at the host level of detail, excluding services and facts coded as “informational” only. As with the *All Scan Results* view, this view also shows an aggregation of all related CVEs for each vulnerability associated with the SAINT Vulnerability Check; hyperlinks from the CVE to the associated external source; access to the summary view of all vulnerability columns; and the tutorials. The following shows an example of this page, with the Severity column being used to select a Severity type of filtering results:



Vulnerabilities by CVSS

This view shows vulnerability results for the selected data set(s) at the host level of detail, excluding services and facts coded as “informational” only. This view is different than the All Vulnerabilities page in that it shows all vulnerability records at the vulnerability, CVE and CVSS score level of detail. This view makes it easier to sort by CVSS score, search and filter by CVSS or export this level of detail quickly without additional view customization.

Total Vulnerabilities by Host

This view provides a one-click approach to answering one of the most commonly asked questions – what are my most vulnerable hosts? This view shows both the total number of vulnerabilities by severity level, and the aggregate total. If you are using the asset tagging features in [Asset Management](#), these tags will also be available as columns to align these asset metrics with scan results. The following shows an example of this use-case:

Actions	Host Name	Function	Criticality	Availability	Location	Business Impact	Business Cost	Critical Problems	Areas of Concern	Potential Problems	Total Vulnerabilities
	10.8.0.1	Infrastructure	High	High	Miami Data Center	High	\$5M	0	0	0	0
	10.8.0.11	Sales	Medium	High	Corporate Office	Medium	\$1M	2	2	13	17
	10.8.0.12	Sales	Medium	High	Corporate Office	Medium	\$1M	0	0	0	0
	10.8.0.150	Customer Data	High	High	AWS East Region	High	\$10M	3	2	14	19
	10.8.0.2	Infrastructure	High	High	Miami Data Center	High	\$5M	0	0	4	4

All Exploits

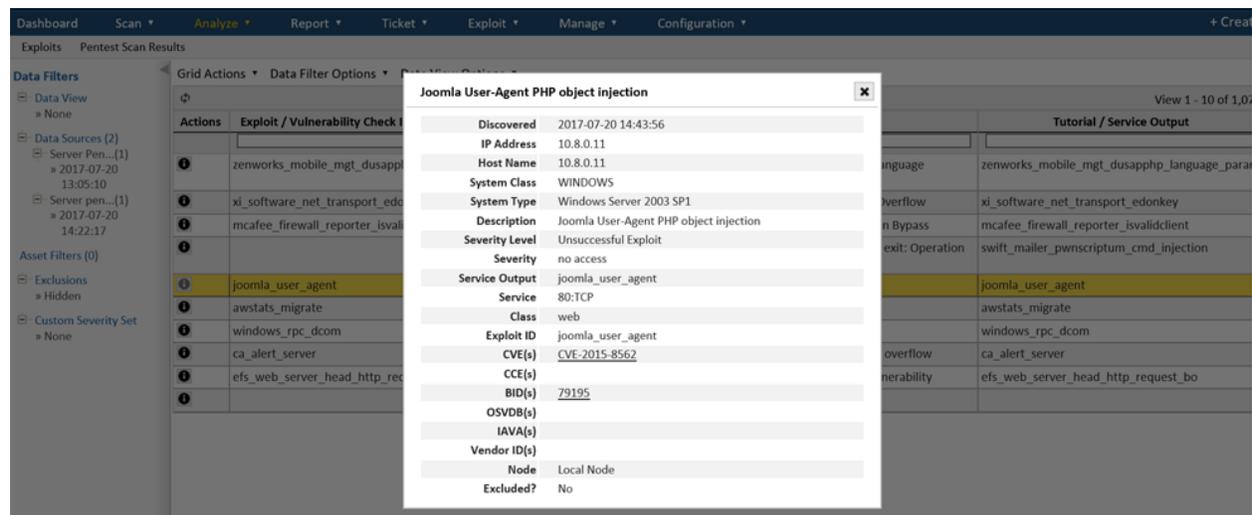
This view is provided for viewing and assessing the results of running individual exploits or tools. The default view provides the raw results at the host level of detail, including unsuccessful exploits as well as exploits executed on the host(s). As with other views, the results grid allows you to search and filter by any displayed column, to include the exploit-specific severity levels that define the type of exploit (remote admin; remote user; client access; privilege elevation) or if you just want to see what hosts had a successful exploit run on it.

Actions	IP Address	System Type	Severity Level	Severity	Exploit ID	Description	CVE(s)
	10.8.0.150	Windows Server 2008 R2		remote user access	smb_login	Windows password weakness (netbank:netbank)	CVE-1999-0503
	10.8.0.150	Windows Server 2008 R2		remote user access	smb_login	Windows password weakness (testadmin:testadmin)	CVE-1999-0503
	10.8.0.150	Windows Server 2008 R2		remote user access	smb_login	Windows password weakness (testuser:testuser)	CVE-1999-0503

All Pen Test Scan Results

This view is provided for viewing and assessing the results of the automated penetration test scan policy – executed as a scan job. It is similar to views for individual exploits; however, it provides a subset of columns specific to pen test analysis, as well as a *View all Pen Test Facts* feature to investigate both returned exploit information and details about all facts returned

during the test, as well as links to tutorial information for individual exploits, as shown in the following example:



Using the Results Grid

Scan results selected from the *Data Set* selector are presented in the data grid, based on default settings upon installation. Many of these settings are also available for customizing as you are performing your analysis. The following describe the various controls available in this grid to support data presentation, as well as ad hoc analysis and exporting.

View External Source References

External source references, such as CVE, BID, OSVDB and vendor references like Microsoft Bulletins and Red Hat advisories can be selected from the column selector and displayed in the grid. These coded references also contain a hyperlink to allow you to click on the reference and launch the external source’s detail page about the vulnerability.

Report

There are times when you will need to generate a quick report from the filtered data in a results grid, rather than navigating to the Report features and building a report through the report wizard. The “All Results” and “All Vulnerabilities” grids have the option to quickly generate a “Full Scan” report by selecting “Report” from the “Grid Actions” dropdown menu. This report feature will generate a report using the vulnerabilities results, as filtered in the grid

and the Data Filter options, using the visible grid columns, with the following exceptions and considerations:

- The System Class, CCE(s) and Vendor ID(s) columns are not currently supported in report output.
- The “Severity” column is displayed as “Severity Level” in reports.
- If “Custom Severity” and SAINT’s “Severity Level” columns are used in a grid, the report includes report graphs for both.
- If only the “Custom Severity” column is used, the report will exclude SAINT’s “Severity Level”.
- Host List columns will vary from the standard Full Report template, based on which severity-related columns are visible in the grid.

IMPORTANT: Note that report widths have inherent limitations due to document and print sizes. Therefore, there may be cases where the visible data grid columns and content exceed readability when generating a report. It may be necessary to limit or modify the columns used in order to produce a report that is both legible and beneficial to the report purpose.

Export to CSV or XML

Exporting the raw scan results simple. Click the *export* option from the Grid Actions dropdown, then choose CSV or XML from the pop-up menu and save the file.

The export feature will export all columns and vulnerability records for the selected context (data set(s)) to the selected path. An example XML output is shown below:

SAINT Security Suite

```
<?xml version="1.0" encoding="UTF-8"?>
- <report>
  - <ipaddr>
    <![CDATA[10.7.0.2]]>
  </ipaddr>
  - <hostname>
    <![CDATA[10.7.0.2]]>
  </hostname>
  - <hosttype>
    <![CDATA[Windows 2000 SP2]]>
  </hosttype>
  - <severity>
    <![CDATA[Critical Problem]]>
  </severity>
  - <category>
    <![CDATA[administrator or root shell access]]>
  </category>
  - <confirmed>
    <![CDATA[No]]>
  </confirmed>
  - <description>
    <![CDATA[SQL Server account sa has no password]]>
  </description>
  - <cve>
    <![CDATA[<a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-1209" target="_blank">CVE-2000-1209</a>]]>
  </cve>
  - <iava>
    <![CDATA[]]>
  </iava>
  - <macaddr>
    <![CDATA[]]>
  </macaddr>
  - <service>
    <![CDATA[1433:TCP]]>
  </service>
  - <exploit_available>
    <![CDATA[]]>
  </exploit_available>
```

Export to Cisco FireSIGHT

Through our partnership with Cisco, you can configure the Security Suite manager to communicate with Cisco FireSIGHT and export scan results into the data correlation engine. This allows the scan results to be viewed in Cisco FireSIGHT and used in Cisco FireSIGHT's impact assessment.

To export scan results to Cisco FireSIGHT, first configure Security Suite to communicate with Cisco FireSIGHT. (See [System Options/Cisco FireSIGHT](#).) Then, from the *All Scan Results*, *All Vulnerabilities*, or *Vulnerabilities by CVSS* grids, click on the export option from the Grid Actions dropdown list. Then click on *FireSIGHT* from the pop-up menu. This will open a dialog box which tells you whether the export was successful.

Scans can also be configured to export results to Cisco FireSIGHT automatically when the scan completes. See [Export Results to Cisco FireSIGHT](#) for further instructions on this feature.

Export to Splunk

In addition to automatically transmitting scan results to Splunk when scans have completed, scan results can also be exported manually in a format that can be imported into Splunk. This option is available from the All Scan Results; All Vulnerabilities; and Vulnerabilities by CVSS grids. Click on this *Export* option through the *Grid Actions* drop-down to choose how you wish to transmit the data shown in the data grid into the pre-configured Splunk instance. Click *Transmit Now* to automatically export the data to Splunk. Click *Save Export File* to generate a file which can be used to import data into Splunk using the JSON data source type. An error message will be displayed if the Splunk configuration settings have not been configured in the Configuration – System Options page or the target Splunk instance is unavailable. See [System Options/Splunk](#) for further instructions on this feature.

View a Record's Details

In addition to viewing a vulnerability record's displayed columns, you can also quickly view the full details of a vulnerability record by clicking on the *Fact* icon (i) in the Action column. You can also view all of a record's detail by double clicking on a highlighted row.

View a Tutorial

SAINT develops and maintains its own tutorial categories and articles about vulnerabilities. These tutorials contain information such as impact, background, problem and resolution information. Some articles also contain a *more information* section that can include links to external references to aid in your research and remediation activities.

You can view the tutorial articles for any vulnerability records by clicking on the *Tutorial Information* (📖) icon in the far right column. An example of a tutorial is shown below:

Tutorial
x

|<
<<
>>
Article 1 of 1

Multiple vulnerabilities fixed in Malware Protection Engine 1.1.13704.0

Impact	Vulnerabilities in Microsoft Malware Protection Engine lead to Denial of Service, and arbitrary code execution, when processing a crafted malformed file.
Background	The Microsoft Malware Protection Engine is the processing engine for several pieces of Microsoft malware protection products including Windows Live OneCare , Microsoft Windows Defender , Antigen for SMTP Gateway and Antigen for Exchange , Forefront for Exchange Server , and Forefront for SharePoint .
Problem	<p style="margin: 0;">05/26/17 CVE 2017-0290</p> <p>Microsoft Forefront Endpoint Protection, Microsoft Forefront Endpoint Protection 2010, Microsoft System Center Endpoint Protection, and Windows Defender prior to engine build number 1.1.13704.0 have a vulnerability which could lead to an arbitrary code execution. The vulnerability exists when the Microsoft Malware Protection Engine does not properly scan a specially crafted file, leading to memory corruption.</p> <p><u>Verify</u> that the Microsoft Malware Protection Engine version is 1.1.13903.0 or later.</p>
Resolution	Windows Live OneCare, Microsoft Windows Defender, Antigen for SMTP Gateway, Antigen for Exchange, Forefront for Exchange Server and Forefront for SharePoint have built-in mechanisms for automatic detection and deployment of updates.
More Information	For further information, see Microsoft Security Advisory 4022344 , Microsoft Security Bulletins 07-010 , 08-029 .

Note that some tutorials contain more than one article, due to the scope and magnitude of a vulnerability. In instances where a tutorial contains more than a single article, you can page through the tutorial by using the left (back) and right (forward) arrows to navigate through the articles.

Exclusions

The scan engine reports all vulnerabilities found, whether confirmed by clear evidence or inferred as a result of other information obtained during the scan. For example, for some vulnerability checks, the presence of TCP wrappers, a packet filter, a firewall, back-ported

patches or other security measures on a target host could cause the scanner to return a false alarm. For other vulnerabilities, it is impossible to determine with certainty whether or not the vulnerability in fact exists, merely by probing it remotely. Unconfirmed vulnerabilities usually fall into the brown level, but it is also possible for a red or yellow vulnerability to be a false alarm. If, after further investigation, it is determined that a vulnerability does not exist, then the vulnerability is a false alarm. In other scenarios, you may know the existence of a vulnerability, but local policies or decisions dictate that you need to tag the vulnerability in a special way and exclude it from current or future analysis or reporting. SAINT supports these types of scenarios by allowing you to set an exclusion flag on the vulnerability, and determine whether the vulnerability should be specific to a host, all hosts, a selected scan job or for all future scan jobs. While this feature can be a helpful way to minimize your analysis time and focus on risks you deem the most important, a periodic review of the tutorials that correspond to excluded vulnerabilities is recommended in order to confirm that they should remain excluded, or to determine if there is a new vulnerability with the same description that may impact your decisions for exclusions.

The exclusions features are found on pages under the *Analyze* menu, and contain two primary functions: 1) Use the *Exclusions* option (scissors icon) to create an exclusion or view exclusion information specific to a selected row; 2) Use the *Exclusions* column in the analysis grids to determine whether individual rows have exclusions set for them; 3) use the *Exclusions* page option under the *Analyze* menu to view and manage all exclusions set in the system; and 4) Use the *Exclusions are Included/Hidden* option in the *Data Filters option* dropdown to hide or unhide exclusion records.

Create an Exclusion

1. To exclude a vulnerability, click on the *Set Exclusions* (scissors) option in the *Actions* column of the vulnerability to be excluded. In the example, we will exclude sunrpc vulnerability for the current scan job and a specific host.

Vulnerability Exclusion



*Fields with * are required.*

- Set exclusion in all jobs
- Set exclusion in this job only
- Set exclusion for all targets
- Set exclusion for host.example.com only

Apply this exclusion to new scans until

Description

Comment

2. By default, the exclusion will only be applied to the current job. Choose “Set exclusion in all jobs” if you want the exclusion also to be applied to other jobs. Note: If the logged-in user is not an administrator, then the exclusion will only be applied to the user’s own jobs and jobs to which the user has exclude results permissions. (See [Modifying Permissions](#).)
3. By default, the exclusion will only be applied to the current target. Choose “Set exclusion for all targets” if you want the exclusion also to be applied to other targets.
4. By default, the exclusion will be applied to new scans (including those from new jobs if all jobs was chosen in step 2) until someone deletes the exclusion. If you would prefer to automatically stop applying the exclusion to new scans on a predetermined date, click on the *Apply this exclusion to new scans until* box and choose a date.

5. Enter detailed comments to describe the reason for the exclusion and any other relevant information that will be useful later in your overall risk strategy.
6. Click the *Create* button to save the exclusion.

Show/Hide Excluded Vulnerabilities

Although a vulnerability can be flagged as an exclusion, it can still be displayed or hidden dynamically while performing analysis.

Show

To show excluded vulnerabilities in the displayed results, the Show/Hide option is a toggle option under the *Data Filters Option* dropdown list. Show Exclusions will be displayed when Exclusions are hidden. Hide Exclusions will be displayed when Exclusions are currently being displayed in scan results and calculations. The Data Filters column (left-most column) will display the current state of this filter.

In the following example, all vulnerabilities are shown, to include all that have been flagged as exclusions:

Actions	IP Address	System Type	Severity Level	Severity	Description	Exclusion	Exclusion Comment
	10.8.0.188	Ubuntu 14.04		check it out for possible vulnerabilities	sunrpc services may be vulnerable	Yes	Compensation controls on this host enviro
	10.8.0.21	Windows 7		susceptibility to malicious content	Windows SMB Client vulnerabilities (MS11-019)	Yes	Exclude this Win7 vulnerability for initial c
	10.8.0.21	Windows 7		authenticated denial of service	LSASS Denial of Service vulnerability (MS17-004)	Yes	DoS vuln's are being excluded on this sub
	10.8.0.188	Ubuntu 14.04		susceptibility to malicious content	GnuTLS vulnerable version: 2.12.23	Yes	GnuTLS vulnerability will be deferred on t
	10.8.0.188	Ubuntu 14.04		administrator or root shell access	Windows account nobody has no password	No	
	10.8.0.188	Ubuntu 14.04		user file write access	Web server allows HTTP method DELETE	No	
	10.8.0.188	Ubuntu 14.04		user file write access	readable/writable share at UBUNTU14/testshare	No	
	10.8.0.188	Ubuntu 14.04		user file write access	Web server allows PUT: /	No	
	10.8.0.188	Ubuntu 14.04		privilege elevation	vulnerability in Samba 4.3.11	No	
	10.8.0.188	Ubuntu 14.04		privilege elevation	Over-the-network SMB packet vulnerabilities in Windows system (MS10-054)	No	

In this example, there are 548 total vulnerability records displayed for the scan – including those having been flagged as an exclusion. You can use the column search feature to locate specific excluded vulnerabilities or to merely sort the list in ascending or descending order for

exclusions (yes/no). Click on the *exclusion* (scissors) option for an exclusion record, to view the information previously defined for the exclusion. The *Vulnerability Exclusion* dialog will display in the same manner as for creating an exclusion.

Hide

To perform analysis without excluded vulnerabilities, choose the *Hide Exclusions* option in the Data Filters dropdown list. The display is refreshed again, hiding all excluded vulnerabilities. View the total record count at the bottom of the grid to see how many vulnerability records have been affected by the exclusions. In our example, the record count is now down to 544, as a result of hiding multiple exclusions affecting three different hosts:

Actions	IP Address	System Type	Severity Level	Severity	Description	Exclusion	Exclusion Comment
	10.8.0.188	Ubuntu 14.04		administrator or root shell access	Windows account nobody has no password	No	
	10.8.0.188	Ubuntu 14.04		user file write access	Web server allows HTTP method DELETE	No	
	10.8.0.188	Ubuntu 14.04		user file write access	readable/writable share at UBUNTU14/testshare	No	
	10.8.0.188	Ubuntu 14.04		user file write access	Web server allows PUT: /	No	
	10.8.0.21	Windows 7		administrator or root shell access	Windows print spooler remote code execution vulnerability (MS13-001)	No	
	10.8.0.21	Windows 7		administrator or root shell access	Windows print spooler remote code execution vulnerability (MS12-054)	No	
	10.8.0.21	Windows 7		administrator or root shell access	Windows SMB Server Transaction Vulnerability	No	
	10.8.0.21	Windows 7		administrator or root shell access	Windows print spooler remote code execution vulnerability (MS16-087)	No	
	10.8.0.21	Windows 7		administrator or root shell access	May 2017 security update for Windows 7 not applied	No	

Remove an Exclusion

Exclusions can also be removed in order to facilitate changes to the environment, organization decisions, compliance requirements and risk strategies.

One method is to locate the exclusion within an *Analysis* grid, selecting the affected job and vulnerability. This method is typical when managing exclusions at low levels of detail (job, host). Use the following steps to remove exclusions directly within the *Analysis* grid:

1. Select a scan job (and/or specific scan) that is affected by an exception.
2. Select the *All Vulnerabilities* view to limit your display to vulnerability records.
3. Use the *Column Chooser* to include the *Exclusions* column in your display grid.

4. Use the column sort feature to sort your view by Exclusions = “yes”.
5. Click on the *Set Exclusions* (scissors) option on the vulnerability exclusion record to remove.

SAINT will display the *Vulnerability Exclusions* dialog.

Vulnerability Exclusion



<<< *This Vulnerability is already set as an Exclusion* >>>

- Set exclusion in all jobs
- Set exclusion in this job only
- Set exclusion for all targets
- Set exclusion for host.example.com only

Apply this exclusion to new scans until

someone deletes it

Description

sunrpc services may be vulnerable

Comment

Remove

6. Click the *Remove* button.

The exclusion flag will be removed, leaving the vulnerability record intact for future analysis. Note that deleting an exclusion configured to impact “all jobs and selected host target” or “all jobs and all host targets” will remove this condition and not set exclusions for subsequent scans.

The second method for removing exclusions is to perform the delete within the Exclusions page found under the *Analyze* menu. Refer to the next section (below) for steps for viewing all exclusions in the system and editing or deleting as required.

View Exclusions

The previous section described how individual exceptions are created, and can be used or hidden while performing detailed analysis. This section describes how to view all exclusions that have been created in the system, and the features available for editing details or deleting exclusions without having to locate them within affected scans.

First, click on the *Exclusions* page under the *Analyze menu* to display a list of all current exclusions:

Actions	Created By	Created At	Job	All Jobs?	Target	All Targets?	Tutorial	Description	Comment
	admin	2017-07-20 16:27:16		Yes	10.8.0.188	No	GnuTLS vulnerabilities	GnuTLS vulnerable version: 2.12.23	GnuTLS vulnerability will be deferred on this target. It is being decommissioned.
	admin	2017-07-20 16:28:31		Yes		Yes	Windows updates needed	LSASS Denial of Service vulnerability (MS17-004)	DoS vuln's are being excluded on this subnet due to other compensating controls.
	admin	2017-07-20 16:33:37	Vuln scan	No	10.8.0.21	No	Windows updates needed	Windows SMB Client vulnerabilities (MS11-019)	Exclude this Win7 vulnerability for initial remediation. Revisit on next rescan.
	admin	2017-07-20 16:44:51	Vuln scan	No	10.8.0.188	No	sunrpc vulnerabilities	sunrpc services may be vulnerable	Compensation controls on this host environment remediate against this issue.

You can now view, sort, and search exclusion content in the same manner you would with other grids in the system. This display shows useful information, such as the author of the exclusion and when it was created, as well as the scope of the exclusion, such as individual or all host targets, and whether the exclusion is specific to a job or spanning all jobs. Additional columns may also be available through the column chooser, depending on your current display.

Use the *Edit* (pencil) option to view the current settings of the exclusion and modify the comments or end date.

Use the *Delete* (trashcan) option to delete the exclusion. Note that deleting an exclusion configured to impact “all jobs and selected host target” or “all jobs and all host targets” will remove this condition and not set exclusions for subsequent scans.

Quarantines

In some cases, if a critical vulnerability is detected on a host, it may be desirable to quarantine that host from the rest of the network as a protective measure. This capability exists on networks which use Cisco ISE for authentication of devices to network resources, and can be initiated using the Cisco pxGrid service. After a target is quarantined, it will be unable to access the network, thus preventing any compromise of the target from affecting the rest of the network.

Creating a Quarantine Policy in ISE

Before a target can be quarantined, you must create a quarantine profile in ISE. The steps below only provide a basic overview. Please consult the ISE documentation for the full details.

1. (ISE 1.x only) Change the service status to *Enabled* under Administration > System > Settings > Adaptive Network Control.
2. Create a new authorization profile called *Quarantine* of type ACCESS_ACCEPT under Policy > Policy Elements > Results > Authorization > Authorization Profiles.
3. Under Policy > Authorization, insert a new rule above the *Basic_Authenticated_Access* rule. In the Conditions box, choose Create New Condition > Select Attribute > Session > EPStatus. In the next box, choose *Quarantine*. In the Authz Profile box, choose Standard > Quarantine. The final rule should read: “if Session:EPStatus EQUALS Quarantine then Quarantine”.

Quarantine or Unquarantine a Target

1. Locate the desired vulnerability record on any of the Analyze grids.
2. Click on the Quarantine icon (exclamation point inside a triangle) in the *Actions* column for that record. (This icon only appears if the Cisco pxGrid client has been configured in SAINT. See [Cisco pxGrid configuration](#).)
3. A dialog box reports the current status of the vulnerable target as reported by ISE.
 - a. If the target is currently unquarantined, click on the *Quarantine* button to request that it be quarantined.

- b. If the target is currently quarantined, click on the *Unquarantine* button to request that it be unquarantined.
 - c. If the target does not have an active session with the ISE server, then no action can be taken.
4. The quarantine or unquarantine request will take effect the next time the target authenticates to ISE. Until then, the status reported in the dialog box will remain unchanged, and the request can be cancelled by re-opening the dialog box and clicking on the *Keep Quarantined* or *Keep Unquarantined* button.

Disputes

While the exclusion feature discussed in the previous section is useful for informally excluding certain findings, SAINT also includes a vulnerability dispute feature for situations where a more formal approval process and audit trail are required. This feature is primarily designed to satisfy the reporting requirements in the ASV Program Guide, but it can also be used for other purposes as needed. Disputes can be created by any user who has *dispute results* permission on the scan job, but can only be resolved by a user who has *resolve disputes* permission on the system.

Create a Dispute

To dispute a vulnerability, go to the *Analyze -> All Results* or *Analyze -> All Vulnerabilities* page, and click on the Dispute button (X icon) in the Actions column for the vulnerability. This opens the dispute dialog containing three expandable sections: *Dispute Information*, *Evidence*, and *Response*:

Dispute



▼ Dispute Information

Vulnerability Description
Windows SMB remote command execution (MS17-010)

Dispute Type
-- Select Type --

Explanation

▶ Evidence

▶ Response

Create

Select the dispute type from the drop-down menu, and explain why you disagree with the vulnerability finding in the *Explanation* box. If you have evidence files to support the dispute, expand the *Evidence* section by clicking on the triangle beside the *Evidence* section header:

Dispute
✕

▶ Dispute Information

▼ Evidence

<i>Evidence File</i>	<i>Date Obtained</i>	<i>How Obtained</i>
<input type="button" value="Browse..."/> No file selected.	<input type="text" value="2018-08-29"/>	<input type="text"/>
<input type="button" value="+ Add Row"/>		

▶ Response

Click on the *Browse* button to select the evidence file to upload, and specify the date the file was obtained, and a brief explanation of how it was obtained. Click on the *Add Row* button if you have more than one evidence file.

When you are finished, click on the *Create* button.

Bulk Disputes

Sometimes the same explanation and evidence apply to several disputed vulnerabilities. In these cases, it is faster to create one dispute covering all the disputed vulnerabilities rather than creating a separate dispute for each one. To create a dispute covering multiple vulnerabilities, go to the *Analyze -> All Results* or *Analyze -> All Vulnerabilities* page, and check the boxes beside the desired vulnerabilities. Then choose *Dispute* from the *Grid Actions* menu. Fill out the dispute form as described in the previous section.

View Disputes

To view a list of disputes, go to the *Analyze -> Disputes* page. This page displays a grid showing all disputes in the system which you have permission to view or resolve. Disputes can be

filtered by their status using the drop-down menu at the top of the *Status* column, to help resolvers find the disputes that require a resolution.

To view a dispute, click on the Details button (“i” icon) beside the desired dispute. This brings up a dialog containing two tabs:

View Dispute ✕

Dispute Information	Vulnerability Information
Description	October 2017 security update for Windows Server 2008 R2 not applied
Type	False Positive
Explanation	This is a false positive.
Evidence	1.png
Status	Approved
Response	This is a false positive.
Create Time	2018-08-29 12:08:54
Create User	kline
Update Time	2018-08-29 12:08:54
Resolve Time	2018-08-29 12:44:08
Resolve User	asv

The *Dispute Information* tab shows the information about the dispute itself, including links to any evidence files. The *Vulnerability Information* tab shows information about the disputed vulnerability. If more than one vulnerability is being disputed, use the pager buttons to page through the vulnerability information.

Each dispute also has action buttons allowing you to edit the dispute, delete the dispute, or view the dispute’s activity log.

Resolve a Dispute

Once created, a dispute can only be resolved by a user who has both *View Results* permission on the scan job and *Resolve Disputes* permission globally. (Global permissions are set from the *Permissions* tab when editing the user or group on the *Manage Users and Groups* page. See [Access Controls](#) for more information about permissions.) Before resolving a dispute, review the dispute information, evidence files, and associated vulnerability information as described in

the previous section, and decide whether to approve the dispute, deny the dispute, or request additional information from the user who created the dispute.

To resolve the dispute, go to the *Analyze -> Disputes* page and click on the *Edit* button (pencil icon) beside the desired dispute. Alternatively, go to the *Analyze -> All Results* or *Analyze -> All Vulnerabilities* page and click on the *Dispute* button (X icon) beside the vulnerability. This opens the dispute dialog. Click on the triangle beside the *Response* section header to expand the response section:

Click on *Approve*, *Deny*, or *Request More Information*, and enter a response explaining your decision. If you are approving the dispute, the response will go into the PCI Comment column of the analyze grids as well as the ASV Summary report, so ensure that it is clear and brief. If you are requesting more information, be sure to state what information is needed. The dispute status will change to pending until someone modifies the dispute, at which time it will change back to *open*. When you are done, click on the *Update* button. The dispute status will then be changed to reflect your decision. Furthermore, if you approved the dispute, then the PCI status will change to *Pass* and the PCI Comment will show your response.

Delete a Dispute

Disputes can be deleted either by clicking on the *Delete* button inside the dispute dialog, or the delete button (trash can icon) on the *Analyze -> Disputes* page. Deleting the dispute will cause the PCI and PCI Comment fields to return to their original values if the dispute had previously been approved.

Vulnerability DB

The Vulnerability database page provides access to SAINT's vulnerability database, to allow you to view information about all of the vulnerabilities SAINT currently supports. This grid provides full support to select the columns to be displayed, column order, column sorts, as well as filtering the displayed results based on any available column, such as: SAINT's unique check ID, keyword column searches, CVEs, CVSS score, SAINT's severity category or your organization's custom severities. In the following example, this grid displays all vulnerability checks (by Check ID), as well as the user's custom severities associated with their FISMA custom severity set. This particular custom severity assignment sets all checks associated with the check category of "database" to be a Medium custom severity. Note: Each check_id may be associated with multiple CVEs with varying CVSS scores, and Custom Severities. Therefore, the CVSS score and Custom Severity code is the HIGHEST score computed for those instances.

Actions	CVE	Check ID	Name	CVSS	Severity Level
	CVE-1999-0002	rpc_mountd	mountd may be vulnerable	10	
	CVE-1999-0003	rpc_tooltalkbo	tooltalk version may be vulnerable to buffer overflow	10	
	CVE-1999-0005	mail_imap_bo	imap version may be vulnerable to buffer overflow	10	
	CVE-1999-0006	mail_pop_qpop	vulnerable pop3 version: Qpopper*	10	
	CVE-1999-0006	mail_pop_two	pop version may be vulnerable to buffer overflow	10	
	CVE-1999-0008	rpc_nisd	nisd may be vulnerable to buffer overflow	10	
	CVE-1999-0009	dns_bindbo	buffer overflow in BIND	10	
	CVE-1999-0009	dns_potential	DNS may be vulnerable	10	
	CVE-1999-0010	dns_bindbo	buffer overflow in BIND	5	
	CVE-1999-0010	dns_potential	DNS may be vulnerable	5	
	CVE-1999-0011	dns_bindbo	buffer overflow in BIND	10	
	CVE-1999-0011	dns_potential	DNS may be vulnerable	10	
	CVE-1999-0013	shell_ssh_fsecure	F-Secure SSH is vulnerable	7.5	
	CVE-1999-0013	shell_ssh_ssh	SSH is vulnerable	7.5	
	CVE-1999-0017	ftp_bounce	FTP server can do ftp bounce	7.5	
	CVE-1999-0018	rpc_statd	rpc.statd is enabled and may be vulnerable	10	

Tree View

This option rolls up vulnerability checks into categories, such as databases, DNS, mail and passwords.

CVE View

This option displays a view of all supported CVEs, including their associated CVSS score, SAINT check ID, SAINT severity level, and any custom severities that have been associated with listed CVEs. From the *Grid Actions* menu, click *Export* to create a file in either CSV or XML format which contains all the CVEs that can be identified by SAINT.

Custom Severities

This feature provides the capability to create one or more sets of custom severity codes, and assign them to vulnerabilities, similar to how SAINT and the industry uses other ways to categorize or classify the severity of vulnerabilities, such as: the CVSS scoring system (1-10); PCI (Pass/Fail); SAINT Severity Levels (Red-Critical; Yellow-Area of Concern); SAINT Severity

categories (Denial of Service; Privilege Elevation). Some use-cases can include, but are not limited to:

- Regulatory compliance – create custom severity codes for a regulatory compliance area (e.g., FISMA) that mandates risk management based on a specified list of severities, such as High, Medium, Low for classes or groups of risks/vulnerabilities.
- Local standards – maybe your organization has an internal method for classifying risks. For example, you define a custom severity set of “Local” and create custom severities by categories defined in your internal risk management framework (e.g., Critical; Important; Routine). Then you assign risks related to the types of checks related to various areas of interest, such as: web servers, web applications and passwords are deemed Critical; risks related to Windows OS are deemed Important; risks related to Print Services are deemed Routine.
- Classifying high visibility vulnerabilities – in this use-case, you could create a Custom Severity set, and create severities based on the level of risk or severity you deem appropriate for high visibility vulnerabilities that hit the news. For example, assign a High Visibility Severity code of Urgent for individual checks related to vulnerabilities such as: Poodle, Heartbleed and Bash.

The screenshot shows the SAINT Security Suite interface. The top navigation bar includes 'Dashboard', 'Scan', 'Analyze', 'Report', 'Ticket', 'Exploit', 'Manage', 'Configuration', and '+ Create'. The 'Analyze' menu is active. Below the navigation bar, there are several tabs: 'All Results', 'All Vulnerabilities', 'Vulnerabilities by CVSS', 'Vulnerability Count by Host', 'Exclusions', 'Vulnerability DB', and 'Custom Severities'. The 'Custom Severities' tab is selected.

Under the 'Grid Actions' dropdown, there are two tabs: 'Severity Sets' (highlighted in yellow) and 'Severities'. Below the tabs, there is a 'New set:' field with a 'Create' button. Below this is a table with the following columns: 'Actions', 'Set Name', 'Created By', 'Creator Groups', and 'Created At'.

Actions	Set Name	Created By	Creator Groups	Created At
 	Internal	admin		2017-07-20 18:39:46

At the bottom of the interface, there is a status bar showing 'SAINT® Used 632 of 5000 IPs (Expires 12/31/2017)', a pagination control 'Page 1 of 1', and 'System time 6:43 PM'.

Add Custom Severity Sets

1. Enter a name in the *New Set* field in the *Severity Sets* tab
2. Click the *Create* button to add the new set to the existing list.

Controlling Permissions to Custom Severity Sets

User access control and permissions can be managed for individual custom severity sets.

Permissions can be defined and managed by performing the following steps:

1. Click the *Security* action button beside the Custom Severity Set to be managed.
2. Select a user or group in the current panel or use the *Add* button to select the applicable user(s) and/or group(s) to include in your permissions.
3. Use the check boxes in the Permissions for [user] section to define the View, Modify, Delete permission for the selected custom severity set or others, as specified in the permissions dialog.
4. Click *OK* to save the permissions settings.

Edit/Delete Custom Severity Sets

1. To edit the title of an existing Custom Severity Set, click in the cell of the applicable Set Name, and edit the name as needed. Click outside of the cell when done to retain the changes.
2. To Delete a Custom Severity Set, click the *Delete* action button in the Actions column. This action will display a second prompt to verify that you want to delete the Custom Severity set.

WARNING: Deleting a custom severity set will also delete all custom severities associated with the custom severity set AND all vulnerability assignments that have been made based on the assignment rules that may exist for the set.

Add Custom Severity Codes

After a Custom Severity Set has been defined, the next step is to create one or more custom severity codes that will be used to assign severities to vulnerabilities.

1. Click on the *Severities* tab in the Custom Severities grid to view the Severities grid, as shown below:

Default View

Dashboard Scan Analyze Report Ticket Exploit Manage Configuration + Create

All Results All Vulnerabilities Vulnerabilities by CVSS Vulnerability Count by Host Exclusions Vulnerability DB Custom Severities

Grid Actions ▾

Severity Sets Severities

Assignments View

Page 1 of 1 15

Actions	Severity Set	Severity Code	Severity Rating	Color	Description	Created By	Created At
	Internal	Low	3	#acd918	Minimal risk. Assess for impact.	admin	2017-07-20 18:41:21
	Internal	Medium	2	#d98f0f	Remediate after most critical	admin	2017-07-20 18:40:37
	Internal	High	1	#810000	Most critical	admin	2017-07-20 18:40:09

SAINT® Used 632 of 5000 IPs (Expires 12/31/2017) Page 1 of 1 15 System time 11:53 AM

2. Select *Create Severity* from the Grid Actions dropdown to display the New Severities creation window.
3. The next step is to define the various attributes of the Severity Code. This detail includes the severity code to the applicable Severity Set; the sort/priority order for the severity in relationship to other codes defined for the set; a short description that defines the code; and a color to associate to the code for applicable charts and graphs.

New Severity [X]

Severity Set
Internal ▾

Severity Code
High

Severity Rating (A lower value is more severe)
1

Description
Vulnerabilities deemed most critical to operations and must be remediated.

color
#e81e1e

Create

4. Click the *Create* button to save the new Custom Severity code.

At this stage in the process, there are no vulnerability assignments associated with the new severity code. Vulnerability assignments are done once a new custom severity code has been defined and associated with a custom severity set.

There are two ways to view custom severities. 1) The Default View provides a quick view of the Severity Codes and the details used to create them. This view is the fastest and simplest way to view and make modification to the attributes about a custom severity. 2) The Assignment View provides the details associated with vulnerability criteria assigned to each custom severity. This

view is the fastest and simplest way to view and make modifications to the criterion used to map each severity to the target vulnerabilities. Each view and their usage are described below.

Default View

The screenshot shows the SAINT Security Suite interface. The top navigation bar includes 'Dashboard', 'Scan', 'Analyze', 'Report', 'Ticket', 'Exploit', 'Manage', 'Configuration', and '+ Create'. The main content area is titled 'Custom Severities' and contains a table with the following data:

Actions	Severity Set	Severity Code	Severity Rating	Color	Description	Created By	Created At
	Internal	Low	3	#acd918	Minimal risk. Assess for impact.	admin	2017-07-20 18:41:21
	Internal	Medium	2	#d98f0f	Remediate after most critical	admin	2017-07-20 18:40:37
	Internal	High	1	#810000	Most critical	admin	2017-07-20 18:40:09

The interface also shows a status bar at the bottom with the text 'SAINT® Used 632 of 5000 IPs (Expires 12/31/2017)' and 'System time 11:12 AM'.

Edit a Custom Severity Code

1. Click on the *Edit* action button on the row of the applicable severity code to display the detailed information for modification.
2. Modify the settings for the Severity Set, Severity Code, Sort Order, Description or Color, as needed.
3. Click the *Update* button to save changes.

Delete a Custom Severity Code

Click on the *Delete* (trash can) action button on the row of the applicable severity code. This action will display a second prompt to verify that you want to delete the Custom Severity.

Warning: Deleting a custom severity code will also delete all vulnerability assignments that have been made based on the assignment rules that may existing for the code. Do you wish to continue?

Assign Custom Severity Codes to Vulnerabilities

Once Custom Severity Sets and their applicable Severity Codes have been created, they can be assigned to vulnerabilities. Unlike exclusions, where vulnerabilities exclusions must be

investigated and determined based on the actual occurrence on a host, and the policy and configuration of a scan job, custom severities can be pre-assigned to vulnerability definition, much like a CVSS score or PCI pass/fail standard.

1. Click the Custom Severities Assignment option (links icon) in the Action column for the corresponding Severity Code, as shown below, to display the assignment options.

Assignments View							
Page 1 of 15							
Actions	Severity Set	Severity Code	Severity Rating	Color	Description	Created By	Created At
  	Internal	Low	3	#acd918	Minimal risk. Assess for impact.	admin	2017-07-20 18:41:21
  	Internal	Medium	2	#d98f0f	Remediate after most critical	admin	2017-07-20 18:40:37
   	Internal	High	1	#810000	Most critical	admin	2017-07-20 18:40:09

This selection will display a grid that shows all assignment criteria currently defined for a Custom Severity, and Grid Actions for adding Custom Severity Assignment rules:

Assignment Criteria - High							
Grid Actions							
Page 1 of 10							
Actions	CVSS Min	CVSS Max	CVE	Check Category	Check Id	Priority	
 	6	10				1	

Custom Severities can be assigned to vulnerabilities in a number of ways.

- CVSS Score or Ranges – assign a severity code to vulnerabilities based on a range of CVSS scores (e.g., CVSS scores 7-10 are assigned high severity)
- Individual or a collection of CVEs
- SAINT check categories (e.g., Passwords)
- SAINT check IDs – Check IDs are identifiers for individual probes used for assessing a target and finding a vulnerability. A vulnerability, as defined in a check, is different than a CVE, as defined by MITRE and published by NIST. CVEs are based on unique instantiations (e.g., enumerations) of a vulnerability, so a Check ID can be associated with one or more related CVEs. For example, the win_samba vulnerability check contains all of the code needed to assess a target against a vulnerability related to Samba 3.x that allows remote attackers to execute arbitrary code via a crafted RPC call. This check covers that

vulnerability—including all of its variants—as defined in related CVEs. Two such examples are: CVE-2012-1182 (CVSS 10.0) related to the RPC code generator in Samba; and CVE-2014-2393 (CVSS 2.9) related to the push_ascii function in smb in Samba. The benefit of assigning a severity code at the check id level is ensuring consistency across the environment in the way you identify the risk of the actual vulnerability, not every instantiation or variant, as defined by CVEs.

- To assign a custom severity to one or more vulnerabilities, click on the *Create Assignment Criterion* option in the *Grid Actions* dropdown. An assignment dialog will be displayed to set your criteria, as shown below:

- Choose the type of criterion to be used from the *Assign to* dropdown list. (e.g., Check Category)
- Next, select or enter the specific criterion related to the chosen type. (e.g., Check Category > Passwords)
- Click the *Save* button to save each severity code assignment.

The following shows two criteria assigned for vulnerabilities to be associated with the “High” custom severity. In this example, all vulnerabilities that have a CVSS score of 6-10, or are associated with SAINT’s “Password” checks will be assigned custom severity = “High” for the “Internal” custom severity set.

Actions	CVSS Min	CVSS Max	CVE	Check Category	Check Id	Priority
<input type="checkbox"/>	<input type="text"/>					
<input type="checkbox"/>				pass		4
<input type="checkbox"/>	6	10				1

Assignments View

The default view for the severities displays all severity sets and their associated custom severities. Click on the *Assignments* view to see all details, including all current vulnerabilities assignment criteria, as shown in the following example:

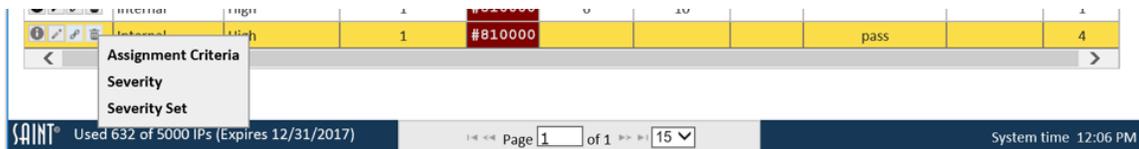
Actions	Severity Set	Severity Code	Severity Rating	Color	CVSS Min	CVSS Max	CVE	Check Category	Check Id	Priority
	Internal	Low	3	#acd918	0	2.9				3
	Internal	Medium	2	#d98f0f	3	5.9				2
	Internal	High	1	#810000	6	10				1
	Internal	High	1	#810000				pass		4

Remove a Custom Severity Code Assignment

Custom Severity code assignments can be removed at any time, based on your access and permissions to the associated Custom Severity Set.

1. From the Assignments View, click the *Delete* (trash can) option for the Assignment Criteria to be removed.

This selection will display three options to control specifically what assignments will be deleted. At this point, you can delete just the selected Criteria; the Severity and all associated Criteria; or even the entire Severity Set and all associated Criteria.



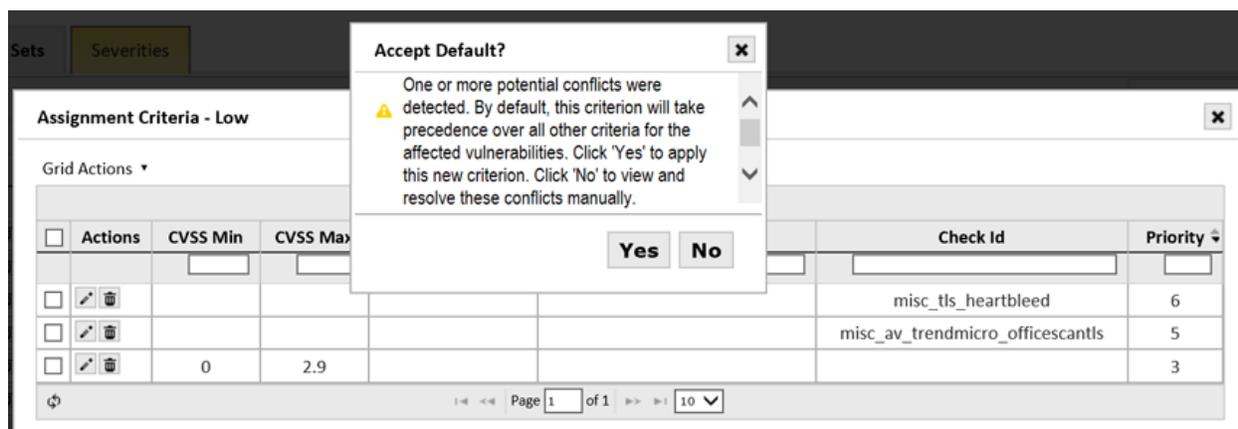
2. Click on *Assignment Criteria* to remove the assigned custom severity from all impacted vulnerabilities.

Warning: Removing a custom severity code's assignment will remove the assignment rule from the Custom Severity code's Checks Criteria, as well as all current and future vulnerability scan records. Once the Submit button is selected, this action cannot be undone.

3. Click *OK* in the confirmation box to delete. Click *Cancel* to close the box without deleting.

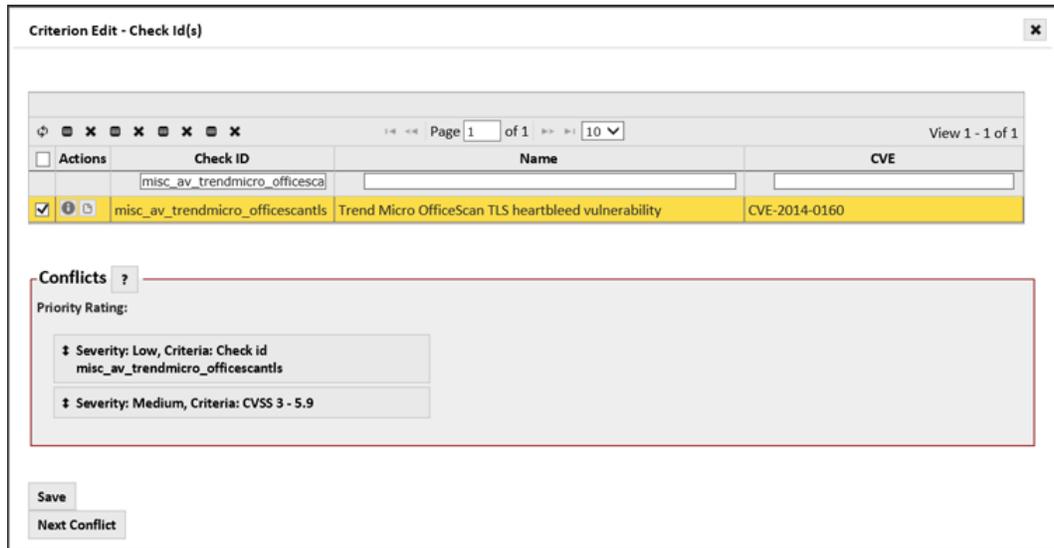
Priority Handling

You will note that when a custom severity is assigned to vulnerabilities, a numeric value is set for the Priority field. The Priority defines the order which assignment rules are applied to vulnerabilities in the event of a conflict. By default, if a conflict occurs, the most recently created assignment rule will take precedence over other assignment rules.

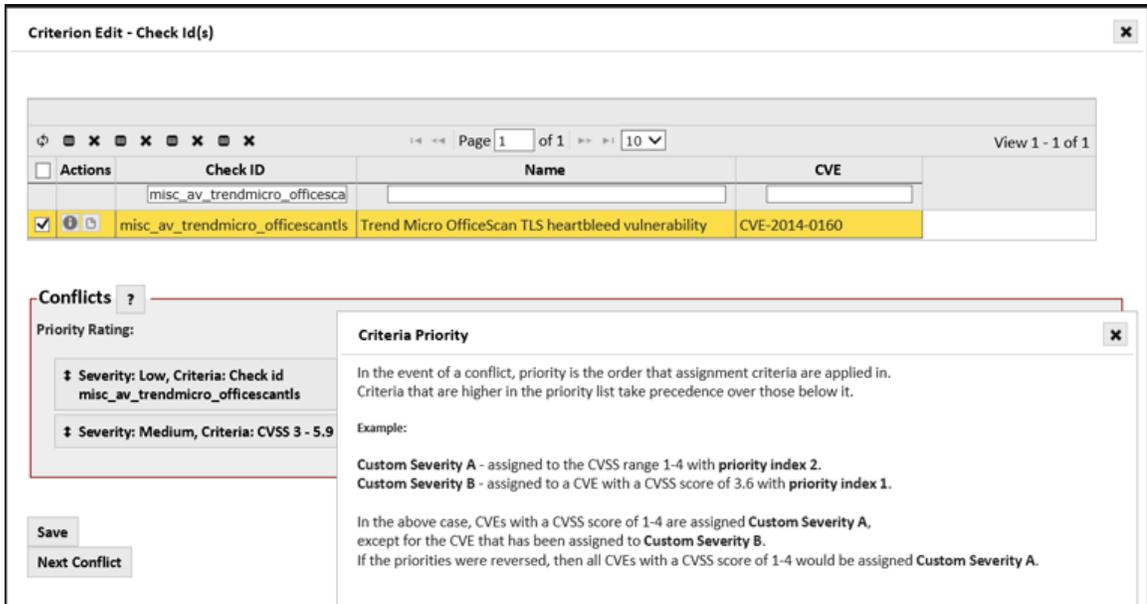


1. When creating assignment rules, if a conflict occurs you will be prompted on whether or not you want to accept the default or if you want to adjust the priority settings. In this use case, there are two choices:
 - a. Click *Yes* to use your current assignment as the top priority over any previous assignment rules.
 - b. Click *No* to save the assignment and bring up the conflict resolution UI.

If you click *No*, a Criteria Edit screen (shown below) will display to allow you to review the conflicting rule and determine if it is OK or if you wish to change the order of priority for the conflicting rules.



2. Use the up/down arrows in the Priority Ratings list to move the assignment criteria to define the order of priority within this Custom Severity Set.
3. Click on the Conflicts ? to view details about the conflict and help in taking actions to ensure accurate usage of the assigned criteria.

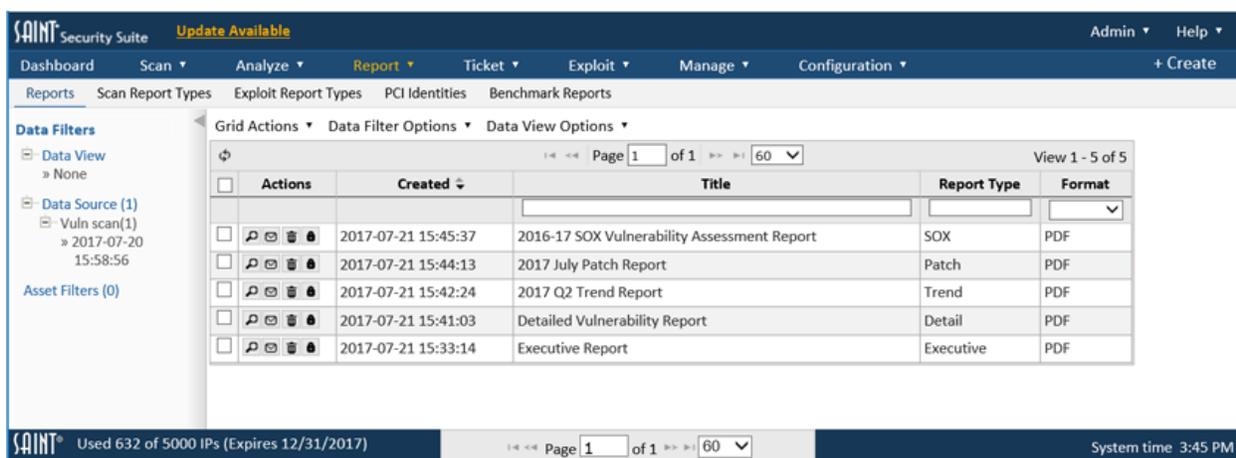


4. Once you have made your decisions, click *Save* to update the vulnerability data and close the screen. Or,
5. Click the *Next Conflict* button, if shown, to move to the next criterion conflict for resolution.

Reporting

The report menu provides access to a wide variety of canned vulnerability report types—compliance reports applicable to many of today’s industry standards and security controls; and capabilities for creating customized reports and re-usable report types tailored to your specific needs. These reports can be generated, displayed, and saved in numerous report formats such as HTML, PDF, XML, and CSV.

Reports can then be viewed, printed and e-mailed by selecting the applicable option for a report record, as well as viewing and modifying report permissions, or deleting reports that are no longer needed.



The screenshot shows the SAINT Security Suite interface. The top navigation bar includes 'Dashboard', 'Scan', 'Analyze', 'Report', 'Ticket', 'Exploit', 'Manage', and 'Configuration'. The 'Report' menu is expanded, showing options for 'Reports', 'Scan Report Types', 'Exploit Report Types', 'PCI Identities', and 'Benchmark Reports'. The 'Reports' sub-menu is active, displaying a table of reports. The table has columns for 'Actions', 'Created', 'Title', 'Report Type', and 'Format'. The reports listed are:

Actions	Created	Title	Report Type	Format
[Print] [Email] [Delete]	2017-07-21 15:45:37	2016-17 SOX Vulnerability Assessment Report	SOX	PDF
[Print] [Email] [Delete]	2017-07-21 15:44:13	2017 July Patch Report	Patch	PDF
[Print] [Email] [Delete]	2017-07-21 15:42:24	2017 Q2 Trend Report	Trend	PDF
[Print] [Email] [Delete]	2017-07-21 15:41:03	Detailed Vulnerability Report	Detail	PDF
[Print] [Email] [Delete]	2017-07-21 15:33:14	Executive Report	Executive	PDF

The interface also shows a sidebar with 'Data Filters' and 'Asset Filters (0)'. The bottom status bar indicates 'Used 632 of 5000 IPs (Expires 12/31/2017)' and 'System time 3:45 PM'.

The report menu provides access to give components:

1. Reports page for viewing existing reports
2. Scan Report Types page (templates) for accessing details of pre-defined and custom scanning report templates
3. Exploit Report Types page for accessing details of pre-defined and custom exploit report templates
4. PCI Identities page for managing the identity information for users and organizations that must report under PCI
5. Benchmark Reports page for generating and accessing reports created from benchmark assessments

Selecting Data for Reports

There are two ways to select data for reporting:

- Option 1 – use the *Select Data Set* option in the [Data Filters Option](#) dropdown, by Job and associated scans. The selected scan results can be constrained further by the Asset Filter to report on a subset of the scanned hosts by their associated Asset Tags.
- Option 2 – select a pre-configured data View from the Data View Options dropdown that already contains the Job(s), Scan(s) and Asset tag filters to be used for the report(s). Selecting a Data View will override any existing settings in the Data Selector or Asset Filter and set values stored by the View.

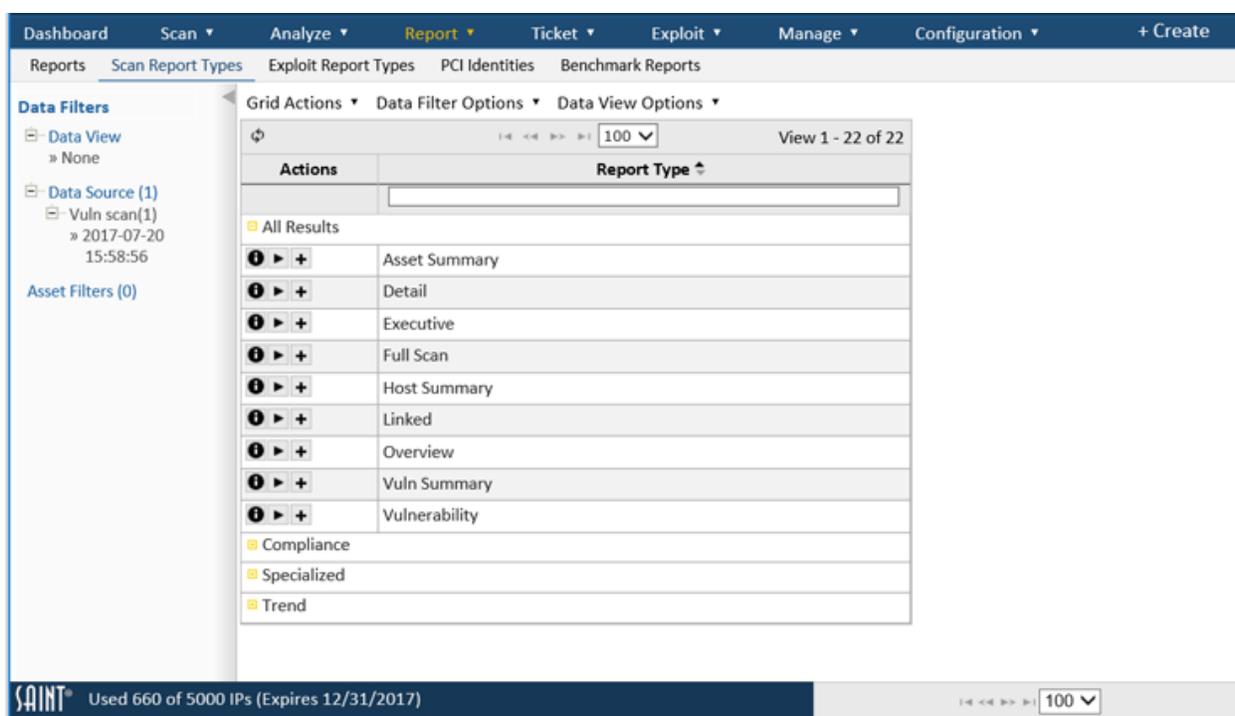
Reports Page

The *Reports* page displays all reports stored in the system, including some basic information about the reports: created by (user), creation date, title, report type and stored format (e.g., PDF, HTML). Reports can be launched, edited, or deleted from this view.

Select the *New Report* option from the Grid Actions dropdown to launch the report creation wizard. The [Create Scan Reports](#) section provides the full details about the report creation wizard. Records can be deleted by highlighting the record and selecting either the *Delete* option or the *Delete* (trash can) icon.

Scan Report Types page

This Scan Report Types page displays a list of available report types (templates) specific to vulnerability and configuration scanning – to include custom report templates. As shown in the example below, you can view all available report types by expanding the *All Reports* category or expand a selected category to see the available report types for that category.



Search for a Report Type

The report type grid provides a search field below the reports header to quickly locate a report type based on an entered value. For example, locate a report type that supports web crawling (keyword: “web”).

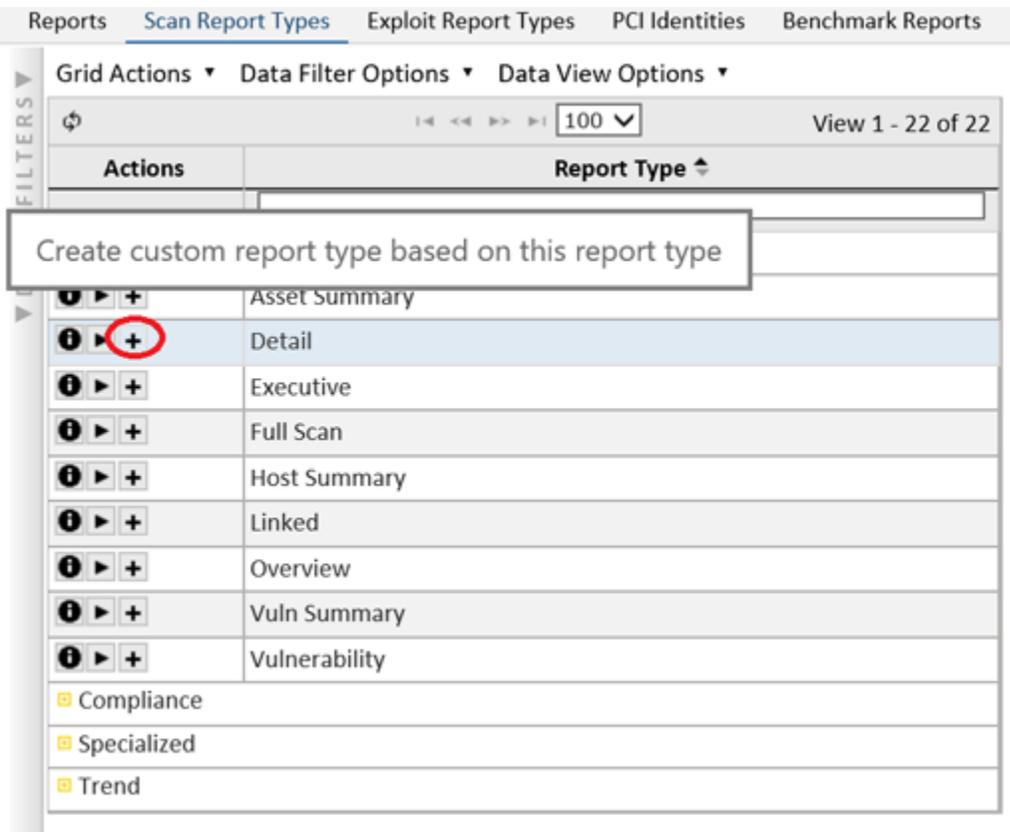
Run a Report based on a selected Report Type

There are multiple ways to launch the *New Reports* creation wizard. One way is by selecting the applicable *Report Type* and then selecting the *Run Report* icon (arrow). This selection will launch the wizard based on the selected report type. A new report can also be executed when reviewing the description of the report type (i) and selecting RUN REPORT from that dialog.

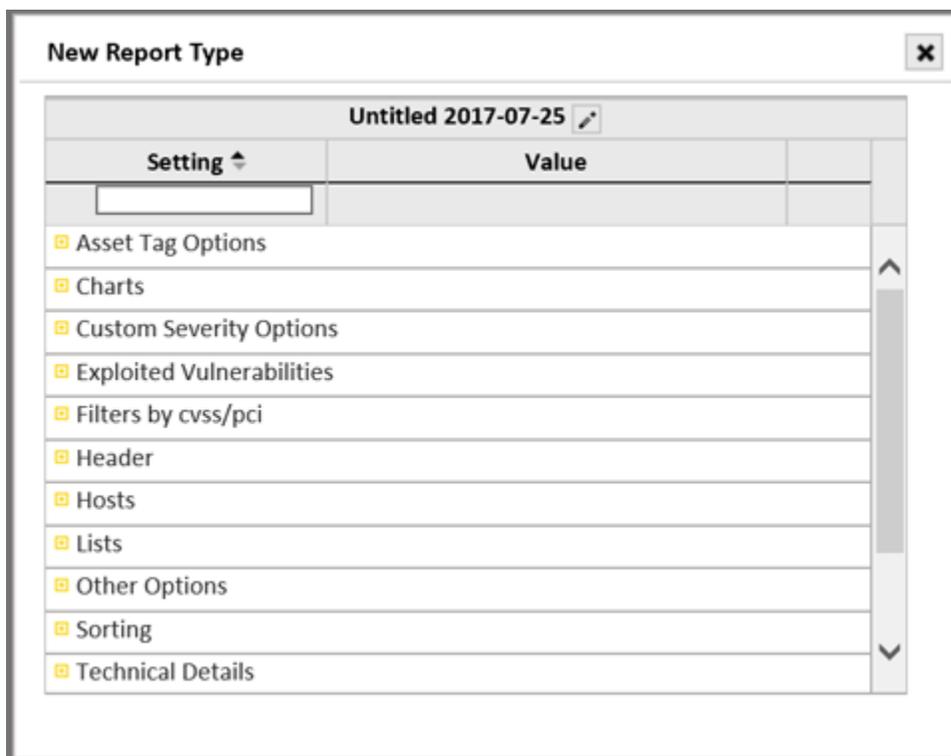
Create a new Report Type using an existing Report Type as a Template

There are two methods for creating custom report templates. First, you can save changes made during report creation within the Job creation wizard. That option can be preferred when creating a report. The second method is to create a custom template by clicking on the “Create custom report type...” action (+) beside the report type in the Scan Report Types data grid. This option can be preferred when building custom report templates for later use, without

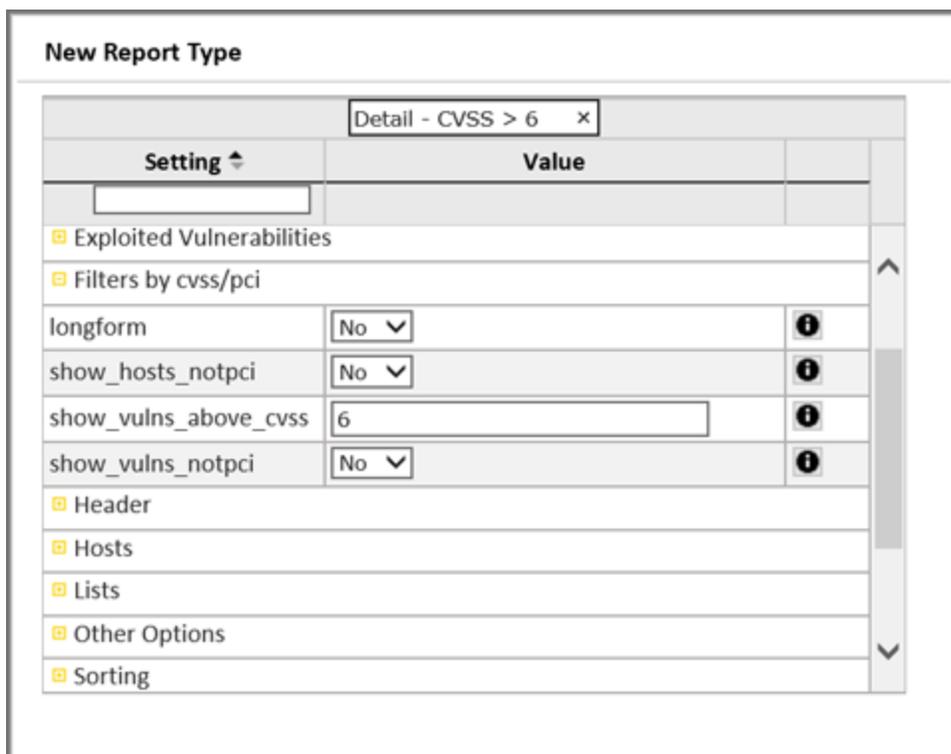
generating reports. Such as creating report templates with your company logo and required formatting, then using the saved templates for future reports.



Choosing this action will launch the *New Report Type* wizard. The wizard contains default settings for the 150+ configuration options available in the report engine. To build the custom template, click on a report section (e.g., Filter by CVSS/PCI) and configure the section as needed.



Once these settings are configured, give the new type a name and save your selections.



The new report type will be available immediately for use under the applicable Report Types “Custom” category.

Custom report templates can be run, edited, deleted or exported as well as configured for user access (security) by clicking on the applicable action under the Actions column, as shown below.

The screenshot shows the SAINT Security Suite interface. At the top, there is a navigation bar with tabs for Scan, Analyze, Report, Ticket, Exploit, and Manage. Below this, there are sub-tabs for Reports, Scan Report Types, Exploit Report Types, PCI Identities, and Benchmark Reports. The main content area is titled 'Grid Actions', 'Data Filter Options', and 'Data View Options'. A table is displayed with the following structure:

Actions	Report Type
<input type="checkbox"/>	All Results
<input type="checkbox"/>	Compliance
<input type="checkbox"/>	Custom
<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	Detail - CVSS > 6
<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	Untitled 2022-03-29
<input type="checkbox"/>	Legacy
<input type="checkbox"/>	Specialized
<input type="checkbox"/>	Trend

Exported report types can be saved to a file and then imported into another SAINT installation using the Import option under the *Grid Actions* menu.

Exploit Report Types

This report page displays a list of available report types (templates) specific to exploit execution. As shown in the example below, you can view all available exploit report types by clicking on the applicable report category's expand (+) button beside the category title, as shown in the following example:

Dashboard		Scan ▾		Analyze ▾		Report ▾		Ticket ▾		Exploit ▾	
Reports		Scan Report Types		Exploit Report Types		PCI Identities		Benchmark Reports			
Grid Actions ▾		Data Filter Options ▾		Data View Options ▾							
						100 ▾		View 1 - 14 of 14			
Actions		Report Type ↕									
		<input type="text"/>									
DATA FILTERS ▾											
All Results											
Compliance											
Specialized											
i ▶ +		Content Search									
i ▶ +		Phishing Info									
i ▶ +		Web Crawl									
Trend											

Search for a Report Type

As with the Scan Report Types, the Exploit Report Type data grid header also provides a Search field below the reports header to quickly locate a report type based on an entered value.

Run a Report based on a selected Report Type

There are multiple ways to launch the *New Reports Creation* wizard to use a custom report template:

1. Click on the global Create option in the upper right corner of the screen. Then select the custom report template in Step one of the wizard.
2. Click *Run Report* (arrow) in the Report Type's Action column for the applicable report type.
3. Click on the Create Reports option in the Report page's Grid Action dropdown and select the custom report template in Step one of the wizard.

Create a new Report Type using an existing Report Type as a template

To create a *New Exploit Report Type* based on an existing type, select the *Plus (+)* symbol beside the report type. This selection will launch the *New Report type* wizard. This wizard contains default settings for the 150+ configuration options available in SAINT's reporting engine. Note, as shown in the example below, there are a number of report configuration options that are unique to exploit output.

Untitled 2017-07-25	
Setting	Value
Asset Tag Options	
Charts	
Custom Severity Options	
Exploited Vulnerabilities	
allblues	No
allsus	No
alluns	No
showphishing	Yes
show_unvulns	No
Filters by cvss/pci	
Header	

As with creating scan report templates, once these settings are configured, give the new type a name and save your selections.

Your new report type will be available immediately for use under the applicable Exploit Report Types *Custom* category. You can also run, edit, configure user access and delete a custom exploit report type from this display.

PCI Identities

This feature is specific to organizations that provide assessment services or must report under the Payment Card Industry (PCI) Approved Scanning Vendor (ASV) requirements. Users assigned to a role that has the applicable permissions to the PCI Identities feature (view, create, modify, delete) can use this feature to pre-define organizational information required for PCI's ASV scanning report submissions. Two types of identity information are required when submitting ASV reports: 1) ASV identity, and 2) customer identity. The PCI Identities feature provides the ability to create **new** organization information based on attributes required by the PCI ASV Program Guide, and maintain these records over time for use in the PCI Attestation Report template (default title - *ASV Scan Report Attestation of Scan Compliance*).

Actions	Company	Contact	Title ↕	Email	Phone	Address	City	State	Country	Zip	URL
 	The Coffee Shop	Ibe Owner	CEO	ibe@mycompany.com	800-555-0011	897 E. 7th ST	Dallas	TX	USA	34534	http://www.thecoffeeshop.com
 	SAINT Corporation	John Doe	PCI ASV Assessor	jdoe@saintemail.com	800-555-1010	1234 Main St	Bethesda	MD	USA	20814	http://www.saintcorporation.com

To create a PCI identity for use in the PCI ASV reports:

1. Select *Create PCI Identity* from the Grid Actions dropdown list
2. Complete the PCI Identity form
3. Click the *Create* button once all fields have been created

Existing records can be edited by double clicking on the record, highlighting the record, and selecting either the *edit* option or the *edit* (pencil) icon. Records can be deleted by highlighting the record and selecting either the *delete* option or the *delete* (trash can) icon.

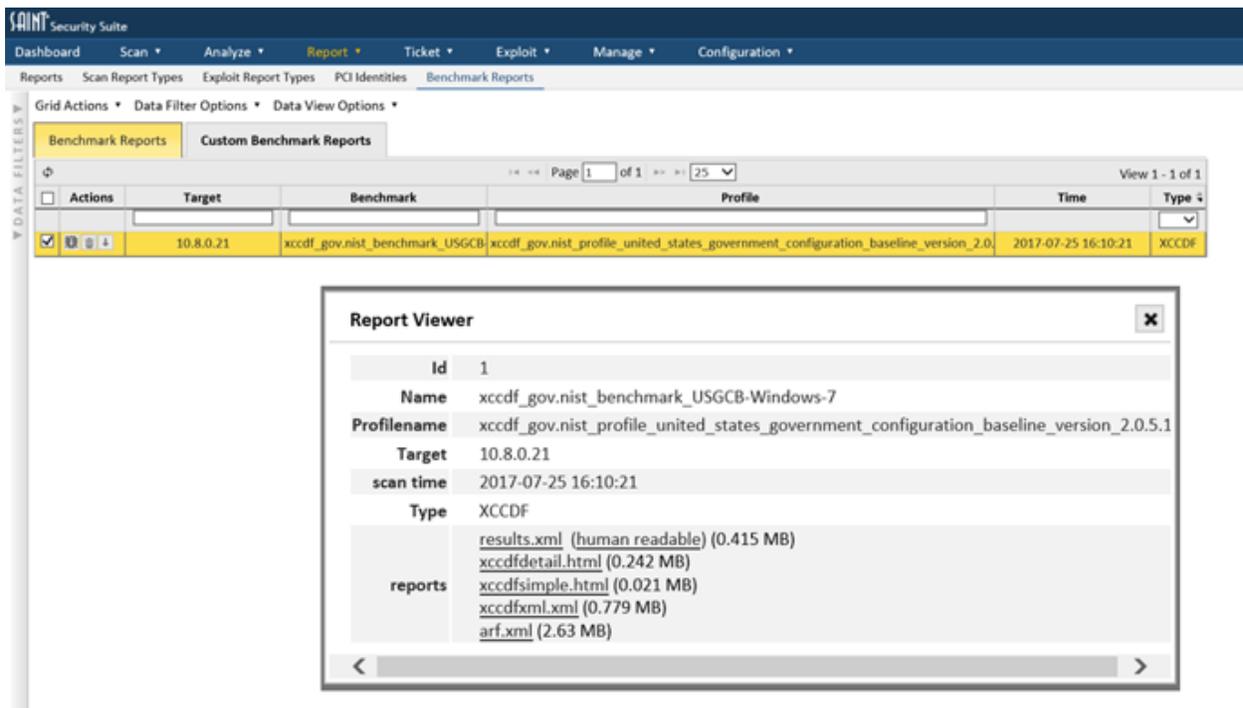
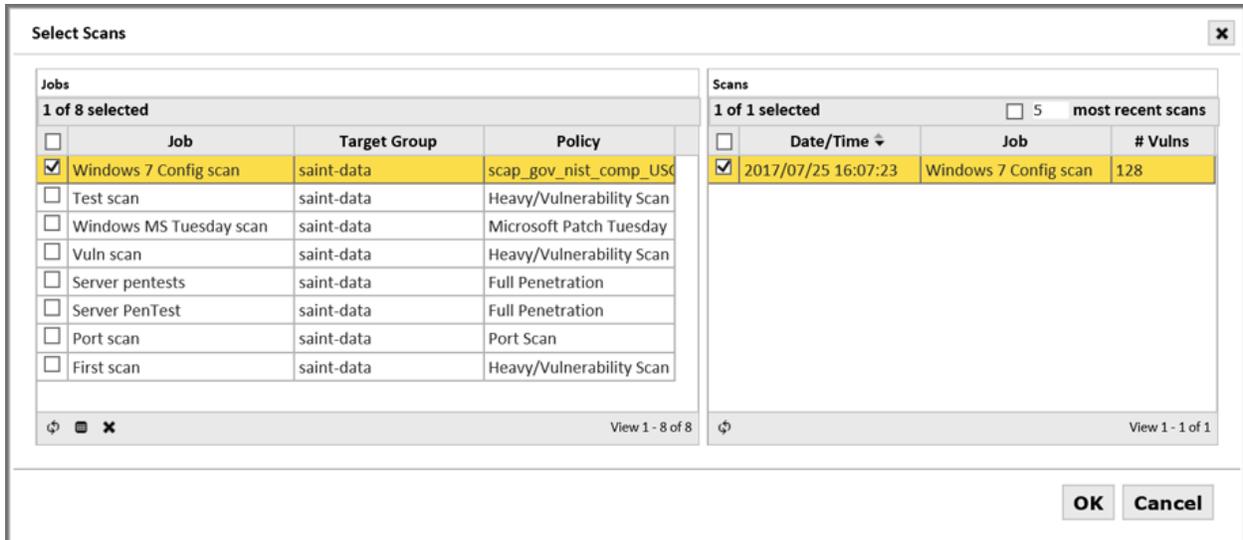
Benchmark Reports

This page provides support for all of the SCAP-compliant output and report types required by the SCAP standard and Cyberscope reporting requirements, as well as additional summary and detailed report templates from benchmark assessments and those created from custom benchmarks.

To create a benchmark report from an SCAP-compliant report format:

- Select a scan based on a benchmark scan and then choose the *View Reports* option for a host that was scanned for the benchmark, as illustrated below:

SAINT Security Suite



Use the Custom Benchmark Reports data grid to create benchmark reports, including Cyberscope compliance output, from SAINT's report templates and the report customization wizard:

1. Navigate to the *Benchmark Reports – Custom Benchmark Reports* tab
2. Select the *Create Reports* option from the *Grid Actions* dropdown list

3. Give the benchmark report a title

The screenshot shows a window titled "New Report" with a close button in the top right corner. On the left side, there is a vertical navigation pane with five steps: "1 Report Info Basic Setup" (highlighted in orange), "2 Headers", "3 Lists Customize the lists.", "4 Other Options", and "5 Summary Review, save, and submit". The main area is titled "Step 1: Report Information" and contains two sections. The first section is "Report Type" with the instruction "Please select the report type." and a dropdown menu currently showing "XCCDF Summary". The second section is "Title" with the instruction "Enter a title for the report." and a text input field containing "Windows 7 Configuraiton Summary Report". At the bottom right of the main area, there are three buttons: "Previous" (disabled), "Next" (active), and "Finish" (disabled).

4. Click *Next* to move to the next section of the report wizard and select option for steps two through four
5. View the summary page of the wizard to validate the customized report configuration
6. Click *Finish* to generate the report

The following shows an example Detailed Configuration Report:

XCCDF Scan Results			
Scan Date	Started 25 Jul 2017 at 16:09:00 and completed 25 Jul 2017 at 16:09:56		
Benchmark	USGCB: Guidance for Securing Microsoft Windows 7 Systems version v2.0.5.1 xccdf_gov.nist_benchmark_USGCB-Windows-7		
Profile	United States Government Configuration Baseline 2.0.5.1 xccdf_gov.nist_profile_united_states_government_configuration_baseline_version_2.0.5.1		
Target	WIN7-64-21		
Identity	SAINTTEST\testadmin authenticated, privileged		
Target Facts	FriendlyName: 10.8.0.21,		
System	cpe:/a:farnamhallventures:joval_sdk:5.11.2-1_SR1		
Scoring			
Method	Score	Max	%
Default Scoring	15.34	100.00	15.34%
Flat Scoring	740.00	2480.00	29.84%
Flat Unweighted Scoring	74.00	248.00	29.84%
Absolute Scoring	0.00	1.00	0.00%
Rule Results			
Rule	References	Result	
USGCB Security Settings → Account Policies Group → Account Lockout Policy Settings			
Account Lockout Threshold	CCE-9136-3	fail	
USGCB Security Settings → Account Policies Group → Password Policy Settings			
Enforce Password History	CCE-8912-8	fail	
Minimum Password Length	CCE-9357-5	fail	
USGCB Security Settings → Local Policies Group → User Rights Assignments			
USGCB Security Settings → Local Policies Group → Security Options Settings			
Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings	CCE-9432-6	fail	
Devices: Restrict CD-ROM access to locally logged-on user only	CCE-9304-7	fail	
Devices: Restrict floppy access to locally logged-on user only	CCE-9440-9	fail	
Interactive logon: Do not display last user name	CCE-9449-0	fail	
Interactive logon: Do not require CTRL+ALT+DEL	CCE-9317-9	fail	

Navigate to the [SCAP section](#) for more details on these SCAP Reports and comprehensive help for generating these reports.

Create Scan Reports

The Report wizard provides a step-based approach to configuring and creating reports based on vulnerability scans, configuration assessments, penetration tests and individual exploits.

Once you've chosen the scan data and data filters from the [Data Filters Options](#), click on the *Report* option from the global + *Create* option or *Create Report* option from the Report page's [Grid Actions](#) dropdown. Either method will launch the New Report creation wizard.

Step 1 – Report Info

Step 1 is to select the report type, report title, and the output format for the report.

The screenshot shows a 'New Report' window with a sidebar on the left and a main content area. The sidebar contains six steps: 1. Report Info (Basic Setup), 2. Charts (Customize the charts), 3. Lists (Customize the lists), 4. Details (Customize the details), 5. Other Options, and 6. Summary (Review, Save, Submit). The main content area is titled 'Step 1: Basic Information' and contains three sections: 'Report Type' with a dropdown menu set to 'Full Scan' and a tooltip that reads 'The Full Scan Report contains all available information, including charts, tables, hosts, vulnerabilities, services, users, shares, and technical details.'; 'Title' with a text input field containing 'SAINTwriter Assessment Report'; and 'Format' with a dropdown menu set to 'PDF'. A yellow tooltip at the bottom of the main area says 'Press Finish to generate the report now, or Next to customize the report.' At the bottom right of the window are three buttons: 'Previous', 'Next', and 'Finish'.

Report Types

Report types are specific to the type of results (i.e., scan and exploit), and are categorized by the type or industry segment the format or content is applicable to. Read the descriptions of the pre-configured report types and select the one that best suits your needs. The report types and detailed descriptions are shown below:

All Results

- **Full Scan** – The full scan report contains all available information including charts, tables, hosts, vulnerabilities, services, users, shares, and technical details.
- **Vulnerability** – The vulnerability report contains all available vulnerability information including charts, tables, hosts, vulnerabilities, and technical details.

- **Executive** – The executive report includes pie charts and bar graphs that summarize the vulnerabilities found on the network. (Available in HTML or PDF format. Note that with HTML format, the pie charts are only visible in Internet Explorer browsers).
- **Overview** – The overview report lists hosts, vulnerabilities, services, and associated information. This report is best for planning a remediation strategy, or for importing into spreadsheet or database applications.
- **Linked** – The linked report lists vulnerabilities and associated information, linked to an appendix containing technical details on each vulnerability.
- **Detail** – The detail report contains technical details on each vulnerability. This report is the most helpful to the administrator responsible for implementing the fixes.
- **Host Summary** – provides a list of all hosts sorted by severity.
- **Vuln Summary** – provides a list of all vulnerabilities and how many hosts are affected by each one.

Trend

- **Trend** – The trend analysis report tracks hosts and vulnerabilities chronologically across multiple data sets. Choose two or more data sets you wish to be included in the trend analysis. Hosts and vulnerabilities will be tracked chronologically across the data sets you choose, producing history charts and status classifications.

Compliance

- **PCI Attestation** – The PCI attestation report contains customer and ASV information; the overall ASV Program Guide compliance status along with the number of targets scanned and the number of failing vulnerabilities; and both the customer and ASV attestations.
- **PCI Executive** – The PCI executive report indicates whether your network is compliant with the latest PCI ASV Program Guide and shows which hosts fail to comply.
- **PCI Detail** – The PCI detail report indicates whether your network is compliant with the latest PCI ASV Program Guide and shows which vulnerabilities fail to comply.
- **PCI Internal** – The PCI Internal report provides a background on the internal vulnerability scan requirement outlined in PCI DSS section 11.2.1 and contains all available information including charts, tables, hosts, vulnerabilities, services, users, shares, and technical details.
- **IAVA** - The IAVA report shows vulnerabilities detected in the selected dataset, and includes the IAVA number associated with each vulnerability.
- **FISMA** – The FISMA report provides a background on FISMA and the security controls that mandate vulnerability and risk management, and reports all available information

including charts, tables, hosts, vulnerabilities, services, users, shares, and technical details.

- **HIPAA** – The HIPAA report provides a background on HIPAA and the security controls that mandate vulnerability and risk management, and reports all available information including charts, tables, hosts, vulnerabilities, services, users, shares, and technical details.
- **NERC CIP** – The NERC CIP report template provides a background on NERC CIP and the security controls that mandate vulnerability and risk management, and reports the results of a vulnerability scan on selected hosts. These reports provide executive level charts, as well as details related to the hosts, services, shares, vulnerability details and remediation guidance.
- **SOX** – The SOX report template supports financial organizations' internal vulnerability and risk management strategies, as well as facilitating provisions in Section 404 of the Sarbanes-Oxley Act, requiring a management report annually on the effectiveness of internal controls for vulnerability management of financial reporting and that external auditors confirm management's assessment.
- **NESA** – The NESA report template provides a background on the Information Assurance Standards specified by the United Arab Emirates National Electronic Security Authority (NESA) and reports all available information, including charts, tables, hosts, vulnerabilities, services, users, shares, and technical details.

Specialized

- **Content Search** – The content search report lists files that contain sensitive information such as credit card numbers or social security numbers.
- **Web Crawl** – The web crawl report lists all the web directories and CGI pages that were detected on the web server.
- **Auth Test** – The auth test report provides a list of hosts, and indicates whether or not authentication was a success/failure or even attempted at all.
- **Patch** – The patch report contains charts and details about patches that are needed on the network.

Custom

- Customized report types developed internally starting with the default options of one of the pre-configured report types.

Report Title

Enter the name for the new report.

Report Format

Choose from the following report formats:

- **PDF** (default) is a convenient format for anyone with a PDF reader. PDF reports appear similar to HTML reports, but are contained in a single file and are rendered the same on any platform.
- **HTML** launches the report in the current web browser. This report format uses Portable Network Graphic (PNG) images to graphically display pie charts and bar graphs. It also uses HTML frames to provide a linked table of contents for report navigation.
- **HTML without frames** is like the HTML format except that it does not provide a linked table of contents.
- **Simple HTML** displays pie charts and bar graphs in-line, not as PNG images. However, the pie charts are only viewable on Internet Explorer.
- **RTF** is a convenient format for viewing or editing reports on Microsoft Windows systems. RTF reports are similar to HTML and PDF reports in appearance, but are contained in a single file which can be opened in either WordPad or Microsoft Word.
- **XML** is useful if the scan data is to be processed by XML-enabled applications.
- **Text** is a useful alternative if you intend to view the report on a machine without a web browser.
- **Tab-separated** reports are useful for importing into documents, spreadsheets, or databases. These formats are useful with the Technical Overview report.
- **Comma-separated (CSV)** is useful for importing into other documents or databases, and can be launched automatically in Microsoft Excel without the need to import.

For quick reporting, this is all that is required. Click the *Finish* button to generate the report. Typically, browser processes will not automatically launch the saved PDF file within the browser window. You may see a message to verify your actions, as shown below:



For more advanced reporting, continue to Step 2 to view charting options.

Step 2 - Charts

In Step 2, the report wizard provides options to choose from a number of bar charts, pie charts and table formats. The following screen shot shows the list of available charts, with a check in the checkboxes that coincide with the default selections.

New Report

1 Report Info
Basic Setup

2 Charts
Customize the charts.

3 Lists
Customize the lists.

4 Details
Customize the details.

5 Other Options

6 Summary
Review, Save, Submit

Step 2: Charts

Charts | Trend Charts | Custom Severity Charts | Asset Tag Charts

Bar Pie Table

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	All
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The number of vulnerabilities in each class
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Hosts by severity level
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Number of hosts needing patches
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Vulnerabilities in each class by subnet
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Hosts by severity and subnet
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Vulnerabilities by severity and subnet
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	The most vulnerable hosts, and how many vulnerabilities affect each
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	The most commonly needed patches, and how many hosts are missing each
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	The most common services, and how many hosts are running each
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	The most common vulnerabilities, and how many hosts are affected by each
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Vulnerabilities by severity level

Previous | Next | Finish

Click on the applicable chart type's checkbox in the **All** row to include all charts for this selected type. For example, click the checkbox immediately under the **Bar** chart type to include all bar charts.

Chart types:

- The Charts tab provides bar, pie and table options for visual presentation of scan data at it relates to such high level rollups as: vulnerability class, severity level, hosts by patch, subnet, and others. These charts aggregate scan results for one or more selected scan results.
- The Trend Charts option provides pie chart, bar chart and table checkbox selectors for charting vulnerability trends based on two or more selected data sets.
- The Asset Tag Charts option provides pie chart, bar chart and table checkbox selectors for charting host and vulnerability data for the Asset Tags (if applicable) associated with

hosts included in the report. When selected, the report will include all applicable asset tags unless specific tags have been excluded in Step 5 Other Options - Advanced Options – Asset Tag Options.

- The Custom Severity Set option provides the capability to compute vulnerability results based on severity codes created in the Custom Severity page under the *Analyze* tab.

These report chart options provide the capability to add bar charts, pie charts and tables to the defined report, based on any previously assigned custom severities codes.

Click on an unchecked box to add a check for the applicable chart type.

Click on a pre-existing check to uncheck the box and exclude the applicable chart type.

Once you've made all chart selections, choose *Next* to continue to the Lists options. Or, select *Finish* if you are ready to complete the report process; chose to create a custom report type based on your customization; or chose not save your customization for later use but *Finish* this process and generate your report.

Step 3 – Lists

Lists are tables which present more specific information on hosts and vulnerabilities. As shown in the sample screen below, the first step is to check the type of lists to be included in the report. The Vulnerability List Columns selection option is also where you will select the Custom Severity column, if you wish to include those assigned custom severity codes to the vulnerability detail records.

New Report

1 Report Info
Basic Setup

2 Charts
Customize the charts.

3 Lists
Customize the lists.

4 Details
Customize the details.

5 Other Options

6 Summary
Review, Save, Submit

Step 3: Lists

Select Lists

Host List Vulnerability Summary Vulnerability List

Host List Columns

1 Hostname 2 NetBIOS name 3 IP address 4 Operating system

→ Next 4 Columns

Vulnerability List Columns

1 Hostname 2 Port 3 Severity 4 Description

→ Next 4 Columns

Previous Next Finish

The Host List (default list type) includes information about a scanned host target, such as IP address, MAC address, Host Name, Operating System, etc. If checked, you will then use the Host List Columns selector to identify the fields and column order for host information to be included in your report.

Selecting the checkbox for the Vulnerability Summary includes a section with the total number of hosts affected by each vulnerability.

The Vulnerability List information (default list type) includes information about the vulnerabilities, such as CVE, CVSS, severity, description, etc. If checked, you will then use the Vulnerability List Columns selector to identify the fields and column order for vulnerability information to be included in your report.

Once you've made all List selections, choose *Next* to continue to the Details options. Or, select *Finish* if you are ready to complete the report process; chose to create a custom report type based on your customization; chose not save your customization for later use but *Finish* this process and generate your report.

Step 4 – Details

Details, the most in-depth part of the report, contains text from SAINT's tutorials. This is where you choose exactly what parts will and will not be included in the report, and options which affect the way the information is presented.

The screenshot shows the 'New Report' window with the 'Step 4: Details' tab selected. The sidebar on the left contains six steps: 1 Report Info (Basic Setup), 2 Charts (Customize the charts), 3 Lists (Customize the lists), 4 Details (Customize the details), 5 Other Options, and 6 Summary (Review, Save, Submit). The main content area is titled 'Step 4: Details' and contains the following options:

- Enable or Disable Details:** Includes two dropdown menus: 'Choose whether to include vulnerability details.' (set to 'Full vulnerability details') and 'Choose whether to include patch details.' (set to 'No patch details').
- Choose how to organize vulnerability details:** A dropdown menu set to 'By Host'.
- Select Detail Sections:** A grid of six checkboxes with question marks, each representing a section:
 - All Sections:
 - Impact:
 - Background:
 - Problem:
 - Resolution:
 - References:
 - Vulnerability Details:
 - Limitations:

At the bottom right of the window are three buttons: 'Previous', 'Next', and 'Finish'.

Choose whether to include vulnerability details. This can be full details, links from the vulnerability list, or no vulnerability details in the report.

Organize the details by host or vulnerability.

Select which details sections to include:

- All Sections – one click selection to include all tutorial content
- Impact – what the vulnerability could allow an attacker to do
- Background – information about the affected products, services or configuration modes
- Problem – details about cause, impact, and attack vectors of the vulnerability
- Resolutions – information related to fixing or remediating the vulnerability
- References – links to additional information about the vulnerability

- Vulnerability Details – Data sent and received or other evidence supporting the detection of the vulnerability
- Limitations – (Exploit only) information about the reliability, supported platforms for pre-requisites for the exploit

Once you've made all *Details* selections, choose *Next* to continue to *Other Options*. Or, select *Finish* if you are ready to complete the report process; chose to create a custom report type based on your customization; or chose not save your customization for later use but finish this process and generate your report.

Step 5 – Other Options

This section of the report wizard allows you to create a custom introductory paragraph, add additional details about the services, and other non-vulnerability information such as users, shares, and web directories.

New Report

1 Report Info
Basic Setup

2 Charts
Customize the charts.

3 Lists
Customize the lists.

4 Details
Customize the details.

5 Other Options

6 Summary
Review, Save, Submit

Step 5: Other Settings

Customize the Introduction

Include an Introduction

Introduction
On %date%, at %time%, a %level% %type% was conducted using the %scanner%. The scan discovered a total of %hosts%, and detected %reds%, %yellows%, and %browns%. The hosts and

Additional Data to Include

? Services

? Information

Advanced Options

Previous Next Finish

The *Include an Introduction* option is checked by default, and includes a boilerplate introduction paragraph that describes the type of report, the type of scan, and summary information about the results returned by the scan. Click in the Introductions text area to edit the content. Note

that SAINT provides a number of variables that begin and end with the % sign to retrieve and populate the text with the applicable value from the selected scan job.

- Current date – %date%,
- Current time – %time%,
- Scan Level value – %level%
- Scan Policy – %type%
- SAINT scanner – %scanner%
- Number of hosts found during the scan – %hosts%
- Total number of vulnerabilities classified by SAINT as “critical” – %reds%
- Total number of vulnerabilities classified by SAINT as “areas of concern” – %yellows%
- Total number of vulnerabilities classified by SAINT as “potential problem” – %browns%
- Total number of vulnerabilities classified by custom severity level – %customseverity%

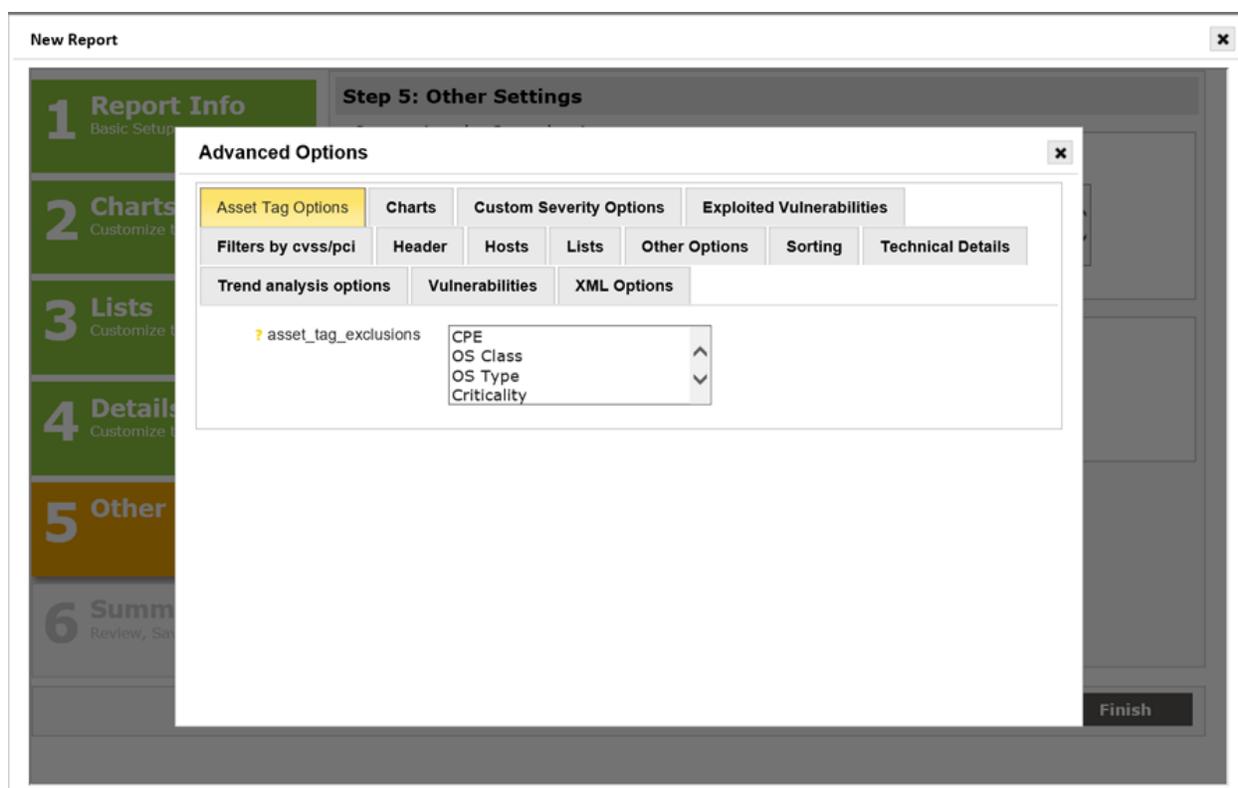
Additional Data to Include

Services – check this box to include the UDP and TCP services running on the host

Information – check this box to include non-vulnerability information found during the scan, such as users, shares, and web directories.

Advanced Options

This section also includes a separate option for configuring advanced report options available in the report engine, including over 300 configuration settings related to chart titles, exploit result filtering, header details, host details, severity code cross-referencing, font sizes and styles, sort options, technical detail and trend settings, vulnerability details, and XML options and tag naming.



The following are some highlights of advanced configuration options you may find useful:

- Adding your own image or logo to custom reports
 1. Scroll down to the "Header" section of Advanced Options.
 2. Select *Yes* in the logo pull down menu.
 3. Enter the path of the image you wish to use in the Logo Path field.
- Include Hosts with no Vulnerabilities
 1. Scroll down to the "Technical Details" section of Advanced Options.
 2. Select *Yes* in the Empty Hosts Detail pull down menu.
- Custom Severity Options
 1. Scroll down to the "Custom Severity Options" section of Advanced Options.
 2. Select the applicable Custom Severity Set to be included in the report.
 3. For "custom_severity_no_saint_severity_output" – choose "Yes" if you only want to use the custom severity; choose "No" if you want to include both types of severity codes.

4. Check or un-check the custom severity codes you want to include or exclude. The default is the include (check) all severity codes for the selected Custom Severity Set.
- Include IAVA code in report
 1. Scroll down to the "Lists" section of Advanced Options.
 2. Select Yes in the IAVA pull down menu.
 - Create custom XML tags of XML output
 1. Scroll down to the "XML Options" section of Advanced Options.
 2. Edit the applicable tag names in the editable form fields.

Once you've made all selections under the Other Options and Advanced Options, choose *Next* or *Finish* to validate your settings and run the report.

Step 6 – Summary

This step provides a summary of the report settings, as well as a field to enter a Custom Report Type name if you wish to save any customization as a new report type for later use.

The screenshot shows a 'New Report' window with a sidebar on the left containing six steps: 1 Report Info (Basic Setup), 2 Charts (Customize the charts), 3 Lists (Customize the lists), 4 Details (Customize the details), 5 Other Options, and 6 Summary (Review, Save, Submit). Step 6 is highlighted in orange. The main content area is titled 'Step 6: Summary' and contains a 'Summary of Report Settings' section with the following details: Title: SAINTwriter Assessment Report3, Type: Full Scan, Format: PDF, Job: Vuln scan, Job: Test scan, Scan Run: 2017-07-20 15:58:56, Scan Run: 2017-07-24 16:00:02, and Scan Run: 2017-07-25 16:00:03. Below this is a 'Save Settings As Custom Report Type' section with a yellow callout box that says 'Optional: Enter a new report type name to save these settings.' and a text input field labeled 'Custom Report Type Name'. At the bottom right, there are three buttons: 'Previous', 'Next', and 'Finish'.

If all settings are OK, select *Finish* to generate your report.

Create PCI Compliance Reports

SAINT provides a pre-configured PCI External Scan policy that adheres to the ASV Program Guide as it relates to assessing Internet-facing hosts based on external, unauthenticated scanning. SAINT also provides pre-configured report types (templates) that support the generation of a complete PCI ASV compliance report package. Each report type is defined below:

1. **Attestation of Scan Compliance** – This is the overall summary that shows whether the scan customer's infrastructure received a passing scan and met the scan validation requirement. (If Attestation of Scan Compliance is enabled in your license, then the Attestation of Scan Compliance can only be generated from the PCI Attestations page, not from the Reports page. See [PCI Attestations](#).)
2. **ASV Scan Report Executive Summary** – This lists vulnerabilities by components (IP address) and shows whether each IP address scanned received a passing score and met the scan validation requirement. This section shows all vulnerabilities noted for a given IP address, with one line per vulnerability noted. For example, an IP address will show one line when only one vulnerability is noted, but will have five lines if five vulnerabilities are noted, etc.
3. **ASV Scan Report Vulnerability Details** – This is the overall summary of vulnerabilities that shows compliance status (pass/fail) and details for all vulnerabilities detected. This section of the report is in vulnerability order, showing each affected IP address as a separate line item for a given vulnerability. Whether or not a vulnerability is PCI ASV Program Guide compliant based on a number of criteria, including CVSS base score, severity level, and the type of vulnerability.

Perform the following steps to generate the applicable PCI ASV reports once a scan result has been selected, based on the PCI scan policy. The basic steps are the same for all reports. However, some report features may be disabled based on PCI ASV Program Guide requirements or additional report options may be displayed to support requirements unique to the applicable report type.

Attestation of Scan Compliance report

Step 1 – Report Information

1. Select *Compliance – PCI ASV Attestation* report type
2. Accept the default report name for modify as text as needed
3. Select your report output format (e.g., PDF)
4. Select *Next*

Step 2 – Charts

All chart options have been pre-configured based on PCI ASV requirements. There are no chart selections for PCI ASV reports. This step can be skipped when creating this type of report.

Step 3 – Lists

The lists step provides the capability to support the special notes requirement in the final reports. This content is specific to the Executive Report. However, the reports wizard provides access to this capability during the creation of any of the PCI report types. Special notes are automatically created based on the scan data as specified in the *PCI ASV Program Guide*. The scan customer is required to provide a declaration for each special note. Select the *Special Notes* button to view any special notes applicable to the scan and add the required declarations for the selected scan results.

Step 4 – Details

All chart options have been pre-configured based on PCI requirements. The detail selections for PCI reports cannot be changed. This step can be skipped when creating this type of report.

Step 5 – Other Options

Attestation Reports require point of contact information for both the customer being assessed and the ASV providing the assessment and attestation process in accordance with the PCI DSS, and the *PCI ASV Program Guide*.

ASV and Customer Identification

If this information has been created previously through the PCI Identity task in the reports screen, the identity name will be available as an option in the applicable drop down menu for selection. If the identity information has not been created prior to building the report, you can select the *New Identity* option for the ASV or customer and create the identification information as you create the new report.

ASV Certification Number

The last step in completing the identification information for the attestation report is to enter the ASV Certification Number issued by the PCI SSC.

Please note that this number is not SAINT Corporation's ASV Certificate Number unless SAINT Corporation is the ASV under contract to provide this service. This attestation for credential is not implied simply as a result of using SAINT's software or PCI-related scanning and reporting tools.

Select *Next* to review and validate the report information.

Step 6 – Summary

Validate the report settings are correct. You can also create a custom scan type (template) from these settings by giving this report a Custom Report Type Name.

Select *Finish* to generate the report and create the custom report type, if applicable.

ASV Scan Report Executive Summary

Step 1 – Report Information

1. Select *Compliance – PCI Executive* report type
2. Accept the default report name for modify as text as needed
3. Select your report output format (e.g., PDF)
4. Select *Next*

Step 2 – Charts

All chart options have been pre-configured based on PCI requirements. There are no chart selections for PCI reports. This step can be skipped when creating this type of report.

Step 3 – Lists

This step provides the capability to support the special notes requirement in the final reports. This content is specific to the Executive Report. However, the reports wizard provides access to this capability during the creation of any of the PCI report types. Special notes are automatically created based on the scan data as specified in the *PCI ASV Program Guide*. The scan customer is required to provide a declaration for each special note. Select the *Special Notes* button to view any special notes applicable to the scan and add the required declarations for the selected scan results.

Step 4 – Details

All chart options have been pre-configured based on PCI requirements. The detail selections for PCI reports cannot be changed. This step can be skipped when creating this type of report.

Step 5 – Other Options

The PCI ASV Executive Reports require point of contact information for both the customer being assessed and the ASV providing the assessment and attestation process in accordance with the PCI DSS, and the *ASV Program Guide*.

ASV and Customer Identification

If this information has been created previously through the PCI Identity task in the Reports screen, the identity name will be available as an option in the applicable drop down menu for selection. If the identity information has not been created prior to building the report, you can select the *New Identity* option for the ASV or customer and create the identification information as you create the new report.

Select *Next* to review and validate the report information.

Step 6 – Summary

Validate the report settings are correct. You can also create a custom scan type (template) from these settings by giving this report a Custom Report Type Name.

Select *Finish* to generate the report and create the custom report type, if applicable.

ASV Scan Report Vulnerability Details

Step 1 – Report Information

1. Select *Compliance – PCI Detail* report type
2. Accept the default report name for modify as text as needed
3. Select your report output format (e.g., PDF)
4. Select *Next*

Step 2 – Charts

All chart options have been pre-configured based on PCI requirements. There are no chart selections for PCI reports. This step can be skipped when creating this type of report.

Step 3 – Lists

This step provides the capability to support the special notes requirement in the final reports. This content is specific to the Executive Report. However, the reports wizard provides access to this capability during the creation of any of the PCI report types. Special notes are automatically created based on the scan data as specified in the PCI ASV Program Guide. The scan customer is required to provide a declaration for each special note. Select the *Special Notes* button to view any special notes applicable to the scan and add the required declarations for the selected scan results.

Step 4 – Details

All chart options have been pre-configured based on PCI requirements. The detail selections for PCI reports cannot be changed. This step can be skipped when creating this type of report.

Step 5 – Other Options

The PCI Executive Reports require point of contact information for both the customer being assessed and the ASV providing the assessment and attestation process in accordance with the PCI DSS, and the *ASV Program Guide*.

ASV and Customer Identification

If this information has been created previously through the PCI Identity task in the Reports screen, the identity name will be available as an option in the applicable drop down menu for selection. If the identity information has not been created prior to building the report, you can select the *New Identity* option for the ASV or Customer and create the identification information as you create the new report.

Select *Next* to review and validate the report information.

Step 6 – Summary

Validate the report settings are correct. You can also create a custom scan type (template) from these settings by giving this report a Custom Report Type Name.

Select *Finish* to generate the report and create the custom report type, if applicable.

PCI Attestations

Note: This page is only available to users with Attestation of Scan Compliance in their license.

After an Attestation of Scan Compliance has been requested (see [Request Attestation of Scan Compliance](#)), it will appear on the PCI Attestations page. This page is accessible either under the Report tab on the main menu bar, or by clicking on the link in the e-mail notification that is generated when the request is submitted. Use the drop-down menu at the top of the Status column to choose either open attestation requests, approved attestations, or denied attestations, as shown below.

⌂ Page 1 of 1 View 1 - 1 of 1					
Actions	Job Name	Status	Created At	Updated At	
ⓘ 📄 🗑️ 📄 🔍 🔄 🛑	first scan	Open	2018-11-02 10:37	2018-11-02 10:37	

Approve or Deny Attestation Request

The user who approves or denies the attestation request must have both *View Results* permission on the scan job, and *Issue AoSC* permission globally. (See [Access Controls](#) and [Assign Permissions to Users](#)). To approve or deny an attestation request, use the following steps:

1. **View the attestation request details** – Click on the Details button (“i” icon). This brings up a dialog with two tabs as shown:

Attestation Request	Scan Information
Job Names	first scan
Status	Open
Response	Not set
Create Time	2018-11-02 10:37:11
Create User	admin
Update Time	2018-11-02 10:37:11
Resolve Time	
Resolve User	
Customer Identity	Joe User
ASV Identity	Not set
ASV Certificate Number	Not set
Customer Attestation	All targets which belong in scope were included in the scan.
Customer Attestation	Attestation #1
Customer Attestation	Attestation #2
Customer Attestation	Attestation #3
Customer Attestation	Attestation #4
Customer Attestation	Attestation #5
Customer Attestation	Attestation #6
Customer Attestation	Attestation #7
Customer Attestation	Attestation #8
Customer Attestation	Attestation #9
Customer Attestation	Attestation #10

The first tab, *Attestation Request*, displays information about the attestation request itself, such as the date and time of the request, the user who requested it, and which attestation boxes were checked when the request was submitted. The second tab, *Scan Information*, shows information about the scan(s) for which the attestation is being requested, such as the scan time and execution history. (If the request includes multiple scans, a pager bar will appear to page through the scan information.) Expand the *Execution History* section to see the log files for the scan.

2. **View the PCI reports** – Click on the *PCI Reports* button (document icon). This opens a pop-up menu allowing you to view either the ASV Executive Summary or ASV Detail report. (The Attestation of Scan Compliance is available here only after the attestation request has been approved.)

3. **Approve or deny the request** – If the scan(s) and corresponding reports meet the requirements outlined in the ASV Program Guide, click on the *Approve* button (checkmark icon) to approve the attestation request. The first time you approve a request, the following dialog appears:

Approve Attestation Request
✕

ASV Identity

-- Select Identity --
▼

or

+ Add New Identity

Save in User Profile

ASV Certificate Number

Save in System Options

✓ Issue Attestation

If the above dialog appears:

- a. Click on *Add New Identity* or choose an existing identity from the drop-down menu. This specifies the information that goes into the *Approved Scanning Vendor* Information section of the Attestation of Scan Compliance.
- b. Enter the ASV certificate number. (This is an eight-digit number issued by the PCI Security Standards Council.)
- c. Optionally, check the *Save* checkboxes. If you check these boxes, the above dialog won't reappear, and future requests will be immediately approved when you click on the Approve button.
- d. Click on the *Issue Attestation* button.

Approving the request will change the request's status, add the Attestation of Scan Compliance to the available reports (as well as a zip file with all three reports, and a feedback form), and send an e-mail notification to the requester with a link to the reports.

OR

If the scan(s) and reports do not meet the requirements outlined in the ASV Program Guide, click on the *Deny* button (X icon) and enter a reason for the denial.

This reason will be included in an e-mail notification to the requester, as well as the request's log.

Delete Attestation Request

To delete an attestation request, go to the *Report -> PCI Attestations* page, and click on the *Delete* button (trash can icon) beside the attestation request. To delete multiple requests at once, check the boxes beside the requests, and choose *Delete Attestations* from the Grid Actions menu.

Attestation Request Log

To view the log for the attestation request, go to the *Report -> PCI Attestations* page, and click on the *Log* button (notebook icon) beside the desired attestation request. The log indicates when the request was created, approved, or denied and the reason for the denial.

Bulk Approvals and Denials

To approve or deny multiple attestations at once, go to the *Report -> PCI Attestations* page, check the boxes beside the desired requests, and choose *Approve Attestations* or *Deny Attestations* from the Grid Actions menu.

Create Other Compliance Reports

SAINT provides a number of additional pre-configured scan policies and report types specific to risk management and vulnerability assessment security controls for such industry compliance standards as HIPAA, FISMA, NERC CIP, SOX, and DoD's IAVA reporting requirements.

Creating compliance reports for non-PCI compliance requirements can be as simple as setting up the scan job, selecting the correct scan "policy" and selecting the applicable report type when the scan is complete. For example, run a vulnerability assessment using the SOX scan policy; then use the pre-configured SOX report template to show the scan results as well as the compliance and security control references that are supported by executing your local risk and vulnerability management scanning program. Reporting logic for these report types has been pre-configured to produce vulnerability scan results based on the associated Scan Policy provided in Step 3 of the Scan Job creation wizard, and provide a boilerplate heading that describes the purpose of the compliance report and shows the mapping to security controls for the applicable industry standards.

Report customization features also allow you to use the default report type as your template and then make modifications, for example:

- Customize the Introduction boilerplate text (Step 5 – Other Options) to support local reporting requirements
- Add your company logo or custom image to the report as part of Step 5's Advanced Options – Header section.
- Save your customizations in Step 6 as a custom report type.

Create the Logo or Header image file for use in Custom Reports

All report templates provide a default logo and report header for all report types, using images bundled with the product. However, you can use your own images to customize the presentation of your reports, following some basic steps. There are two formats to support the two distinct types of output that accept images (HTML and PDF). The following describes the process for creating and using either format as custom images in your reports.

1. First, create an image that is 606 pixels wide by 80 pixels high, in an illustration or image editing program such as Adobe Illustrator, Photoshop or Microsoft Paint.
2. Next, insert/copy your logo or other applicable picture into the 606x80 px image and any other information or background desired for the header.
3. Follow the steps defined below for the format to be supported:

HTML Reports – Save the file as an image file format recognized by a browser. The most often used, and recommended formats are .jpg format (best for photos or gradients); .gif (best for solid colors and lines); bitmap (highest resolution without compression; or .png (a raster image file that uses lossless compression that provides good image quality for web-based output.

PDF Reports – Either flatten all of the image layers and save as a PDF file OR save as an image file (e.g., jpg, gif, bitmap, etc.) and then re-save that image as a PDF in Adobe Acrobat.

4. Place the image file(s) in a directory that can be accessed by your browser or place the image on a shared resource for use by others.

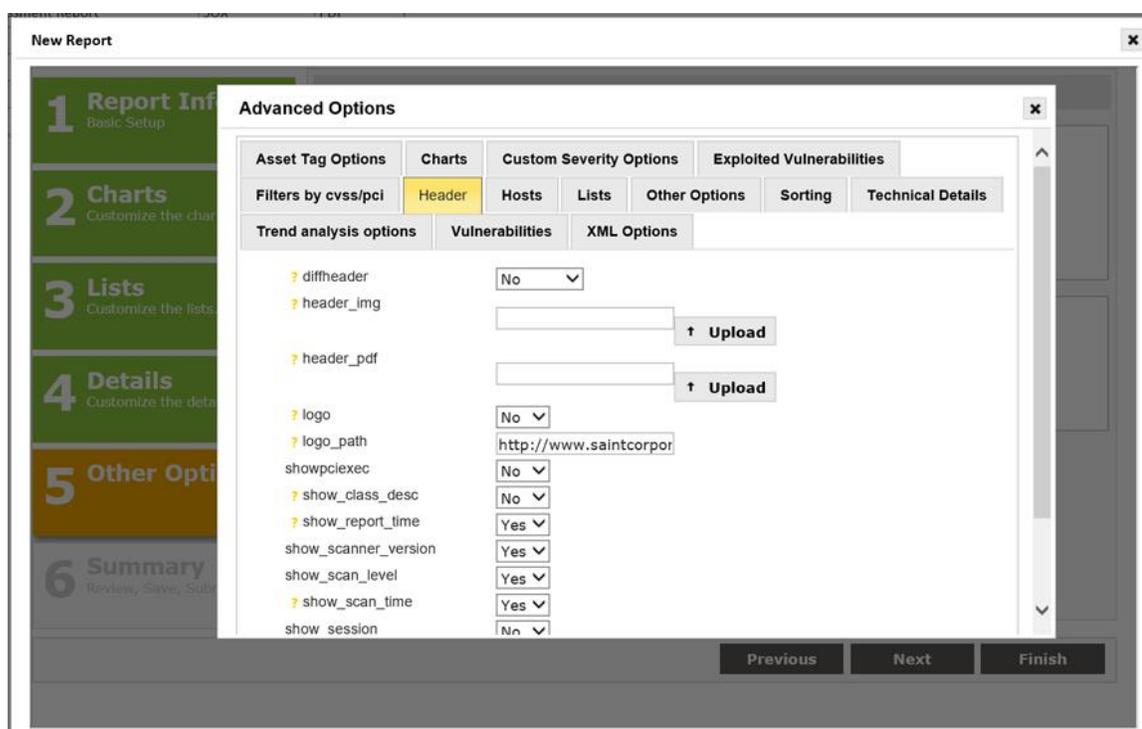
Generate a Report using your Logo/Header

After the logo/header file is created, you are ready to generate your custom report. This is done in one of two ways:

1. In the HEADER section of the report setup process, if you are using the [Scan Report Types](#) or the [Exploit Report Types](#) from the *Report* menu.
2. In the [Advanced Options](#) (Step 5) if you are using the Report wizard.

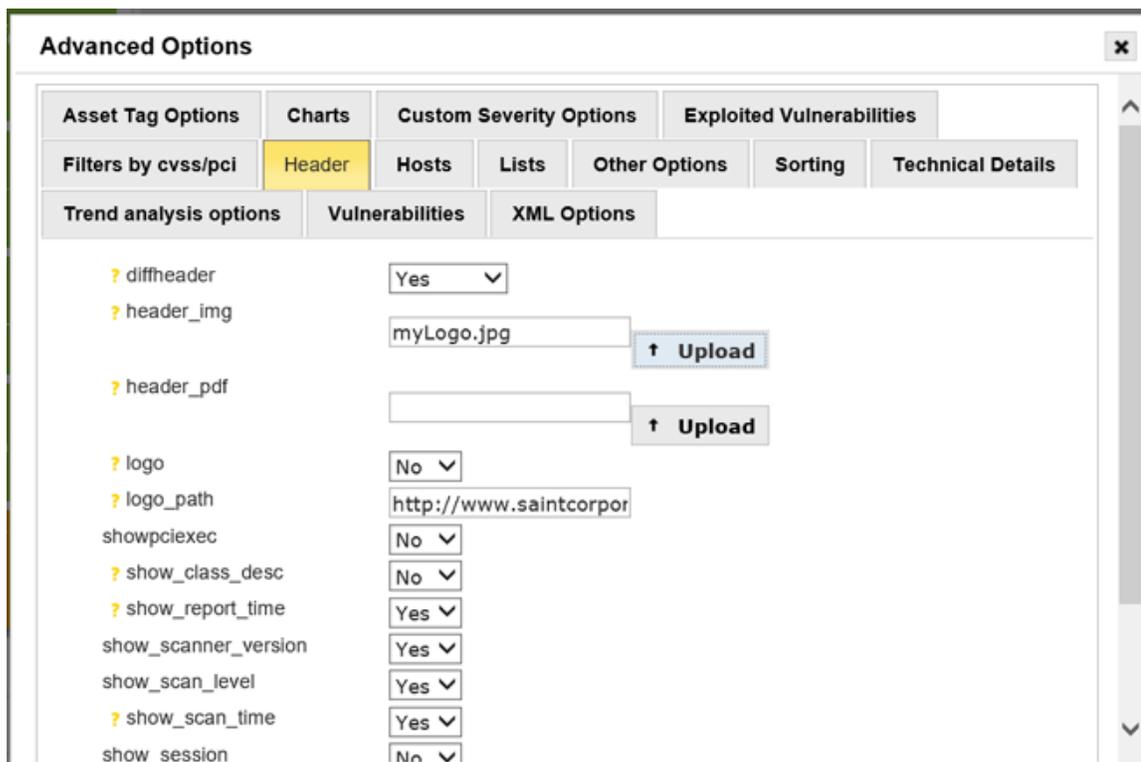
The following shows an example report creation process using the Report wizard to create a report using your own logo:

1. Select the Job/Scan results you wish to use in your report.
2. Create a new Report.
3. Complete Steps 1 through 4 in the wizard to define the report and the structure for the report content.
4. Click on Step 5 - *Other Options*.
5. Click on the *Advanced Options* button.
6. Click on the Header tab.



7. Select **YES** from the *DiffHeader* dropdown menu to replace the default image with your custom image.
8. Click the *Upload image* button for the applicable type of report to be supported:
 - Header image (HTML format)
 - PDF image (PDF format)
9. Use the *Browse...* button to locate the 606px by 80px image you wish to use.

10. Click *Upload*; you will then see a confirmation message that “the selected file has been uploaded.”
11. Close that window to proceed with creating your report. The path and image name should now be visible in the Header section, as shown below:



12. Close the *Advanced Options* window to continue.
13. Click the *Next* button to view the summary of your report selections.
14. Click *FINISH* to generate the report.

Contents

- Introduction
- ▶ Summary
- ▶ Overview
- ▶ Details



Security Services Incorporated

SAINTwriter Assessment Report

Report Generated: July 26, 2017

1 Introduction

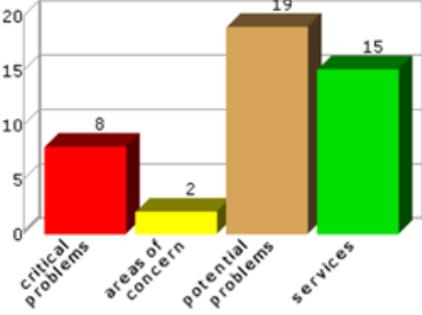
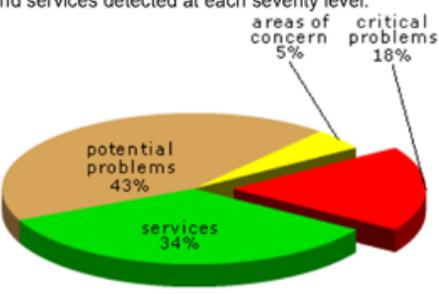
On July 26, 2017, at 10:07 AM, a heavy vulnerability assessment was conducted using the SAINT® 8.15.27 vulnerability scanner. The scan discovered a total of two live hosts, and detected eight critical problems, two areas of concern, and 19 potential problems. The hosts and problems detected are discussed in greater detail in the following sections.

2 Summary

The sections below summarize the results of the scan.

2.1 Vulnerabilities by Severity

This section shows the overall number of vulnerabilities and services detected at each severity level.

Category	Count
Critical Problems	8
Areas of Concern	2
Potential Problems	19
Services	15

2.2 Hosts by Severity

This section shows the overall number of hosts detected at each severity level. The severity level of a host is defined as the highest vulnerability severity level detected on that host.

Ticket

The ticket module provides the capability to create and track work assignment tickets, based on vulnerabilities found during scans, to support remediation activities. Tickets are created automatically by the system, based on configuration options defined in the Configuration tab's *System Options – Ticket Options*. These settings, as well as interacting with the features and functions of the ticketing module are controlled through Group and User permissions for viewing, modifying, assigning, closing and deleting tickets. The following describes the various features and workflow solutions provided in this module.

Ticket Menu

My Open Tickets

This view is the default view when you select the *Ticket* tab. The contents of the ticket grid displays Open (Status = New or Deferred) tickets assigned to the logged on user. This view is a convenient way to limit your focus to just your active tickets, and perform all of the necessary activities for viewing, updating the status, adding comments, viewing tutorial information, etc. as it relates to responding to remediation work assigned to you for the stated vulnerabilities.

As with other grids in the system, actions for viewing and editing content can be accessed from the row-level action buttons, in-line editing for select values, or from grid-level options found at the top and bottom of the grid. As shown below, the Custom Severity Set selector is also provided when viewing All Tickets or All Tickets, to view tickets in relation to locally created severity codes for the applicable vulnerability. Note that the Custom Severity column is not displayed by default, but can be included in the grid by selecting the column from the grid’s column selector.

To assist in managing tickets, there are two additional views, accessible by clicking the tabs at the top of the grid to see Open tickets assigned to the logged-in user which are either past due, or due within seven days (the default). The number of days can be changed by updating the value in the “Days Until Due” field.

The screenshot displays the SAINT Security Suite interface. At the top, there is a navigation bar with the following items: Dashboard, Scan, Analyze, Report, **Ticket**, Exploit, Manage, Configuration, and + Create. Below the navigation bar, there are tabs for 'My Open Tickets', 'All Tickets', and 'Ticket Rules'. The 'My Open Tickets' tab is active. Below the tabs, there is a 'Grid Actions' dropdown and a 'Days Until Due' input field set to 7. The main area contains a grid with the following columns: Actions, Ticket ID, Node Name, Host IP, Service, Description, Status, Due On, and Last Occurred. The grid shows four tickets:

Actions	Ticket ID	Node Name	Host IP	Service	Description	Status	Due On	Last Occurred
[Info] [Edit] [Delete] [Refresh]	2	Local Node	10.8.0.10	ideafarm-door	TLS heartbleed memory disclosure vulnerability	Assigned	2017-07-05	2017-06-30
[Info] [Edit] [Delete] [Refresh]	3	Local Node	10.8.0.10	902:TCP	TLS heartbleed memory disclosure vulnerability	Assigned	2017-07-05	2017-06-30
[Info] [Edit] [Delete] [Refresh]	6	Local Node	10.8.0.14	netbios	Microsoft Data Access Component remote code execution (MS11-002)	Assigned	2017-07-05	2017-06-30
[Info] [Edit] [Delete] [Refresh]	9	Local Node	10.8.0.14	netbios	Windows kernel multiple privilege elevation vulnerabilities (MS10-073)	Assigned	2017-07-05	2017-06-30

At the bottom of the interface, there is a status bar with the following information: SAINT® Used 42 of 500 IPs (Expires 12/31/2018), Page 1 of 1, and System time 11:09 AM.

All Tickets

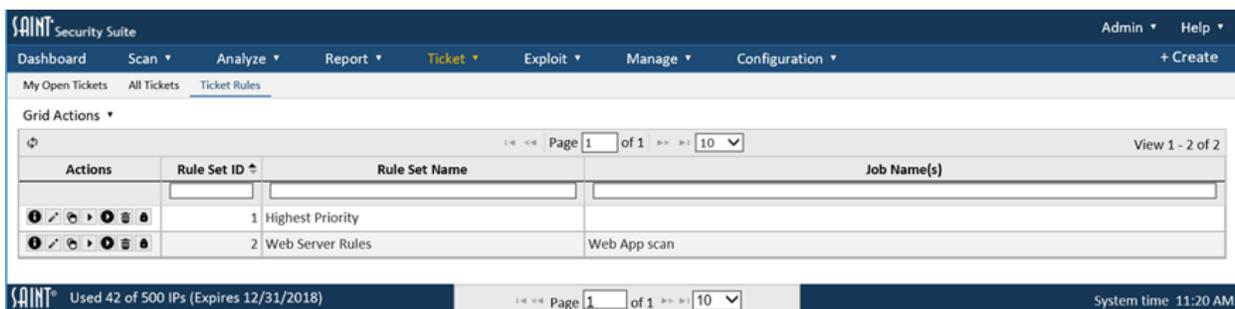
This view shows all tickets which the logged on user has permission to view.

Actions	Ticket ID	Node Name	Host IP	Service	Description	Status	Assignee	Due On	Last Occurred	Severity Level	Severity
<input type="checkbox"/>	1	Local Node	10.8.0.10	https	TLS heartbleed memory disclosure vulnerability	Assigned	bsmith	2017-07-07	2017-06-30	Yellow	information gathering
<input type="checkbox"/>	2	Local Node	10.8.0.10	ideafarm-door	TLS heartbleed memory disclosure vulnerability	Assigned	admin	2017-07-05	2017-06-30	Yellow	information gathering
<input type="checkbox"/>	3	Local Node	10.8.0.10	902:TCP	TLS heartbleed memory disclosure vulnerability	Assigned	admin	2017-07-05	2017-06-30	Yellow	information gathering
<input type="checkbox"/>	4	Local Node	10.8.0.14	netbios	Windows telnet client session variable disclosure	Assigned	bsmith	2017-07-07	2017-06-30	Yellow	information gathering
<input type="checkbox"/>	5	Local Node	10.8.0.14	netbios	active scripting enabled in Internet zone for testadmin.SAINTTEST	Assigned	bsmith	2017-07-07	2017-06-30	Blue	poor security policy
<input type="checkbox"/>	6	Local Node	10.8.0.14	netbios	Microsoft Data Access Component remote code execution (MS11-002)	Assigned	admin	2017-07-05	2017-06-30	Yellow	susceptibility to malicious content
<input type="checkbox"/>	7	Local Node	10.8.0.14	netbios	Windows TCP/IP Stack not hardened	New		2017-07-28	2017-06-30	Blue	check it out for possible vulnerabilities
<input type="checkbox"/>	8	Local Node	10.8.0.14	netbios	Windows DNS Resolution Remote Code Execution	Assigned	bsmith	2017-07-07	2017-06-30	Red	administrator or root shell access
<input type="checkbox"/>	9	Local Node	10.8.0.14	netbios	Windows kernel multiple privilege elevation vulnerabilities (MS10-073)	Assigned	admin	2017-07-05	2017-06-30	Yellow	privilege elevation
<input type="checkbox"/>	10	Local Node	10.8.0.14	netbios	Outlook Express MHTML parsing vulnerability	New		2017-07-28	2017-06-30	Blue	check it out for possible vulnerabilities

Ticket Rule Sets and Rules

Ticket Rules define how tickets are assigned based on target and vulnerability characteristics such as: a target list, host operating system platforms, type of vulnerability, severity of a vulnerability or even ranges of CVSS score. These rules are packaged in a parent Rule Set and then used at job creation time to ensure tickets generated as a result of vulnerabilities detected during a job's scans are assigned to the proper individual for remediation. Without ticket rules, new tickets are not assigned until they are modified individually or in bulk, through the All Tickets page.

Ticket rules are defined and packaged in Rule Sets to support the creation of one or more rules and apply the collection of rules to scan jobs for resulting vulnerabilities. The following shows an example of a list of Rule Sets in the Ticket Rules page.



The example above, shows two rule sets, with one currently being used in a scan job. Click on the *Details* (i) option or the *Edit* (pencil) option to view the Rules defined for a Rule Set. The following shows the rules defined for the *Web Server Rules* rule set. In this example, a rule was defined for assigning remediation tickets to individuals based on the specific IP address of a web server and CVSS score range for high severity vulnerabilities. A Due Date was also defined for two calendar days from the date the ticket is generated and assigned.



Create a Rule Set

1. Click on the *Create Ticket Rule Set* option from the Grid Actions drop down on the *Ticket > Ticket Rules* page to display the rule set creation dialog:



2. Click on the *edit* icon (pencil) to enter a name for the new Rule Set. The default name (as shown above) is the string “Rule Set” plus the rule set’s ID number.
3. At this stage, you can close the edit window and retain the new Rule Set for later use, without ticket rules, or follow steps in the following section to create individual rules.

Edit a Rule Set

1. Navigate to the *Ticket > Ticket Rules* page menu.
2. Navigate to the Rule Set you wish to edit.
3. Click on the *edit* icon (pencil) on the Rule Set’s record.
4. The Edit Ticket Rule Set dialog will display and be available for editing the name or rules within the Rule Set.

Clone a Rule Set

The Ticket Rule Set feature provides a way to use existing rule sets as a starting point to create additional rules. For example, a rule set already existing that has every rule that applies to Subnet 10.1.0.0/24 and assigns tickets to User A. Now you need to create the same rules for Subnet 10.4.0.0/24 and assign those tickets to User B. This can be done by cloning an existing Ticket Rule Set and then editing the Rule Set Name and parameters in the Rules.

1. Navigate to the *Ticket > Ticket Rules page*.
2. Navigate to the Rule Set you wish to clone.
3. Click on the *Clone Ticket Rule Set (multi-doc)* icon for the Rule Set to be used.
4. The *Edit Cloned Ticket Rule Set* dialog will display and be available for editing the name or rules within the Rule Set.
5. Change the name of the new Rule Set to ensure it can be uniquely identified in the Rule Set grid.
6. Add, modify or delete rules as needed to create the new Rule Set.

Delete a Rule Set

1. Navigate to the *Ticket > Ticket Rules page*.
2. Navigate to the Rule Set you wish to delete.
3. Click on the *Delete* icon (trash can) on the Rule Set’s record.

Deleting a Rule Set will cause jobs currently associated with the Rule Set to no longer be associated with any Rule Set.

Create a Rule

1. Click the Edit (pencil) option on the Ticket Rule set you wish to add the rule to. The Create Ticket Rule dialog will be displayed.
2. Click on the *New Ticket Rule* option from the Ticket Rule's Grid Action drop-down to display the *New Ticket Rule* form:

New Ticket Rule
✕

Choose at least one criterion for match and at least one ticket setting. Leave criteria blank if not filtering on them.

Criteria for Match

Node Data

Host Data

Host OS

Severity Level

Vuln Category

Range of CVSS Scores

Low CVSS Operator <input style="width: 100%;" type="text" value="▼"/>	Low CVSS Score <input style="width: 100%;" type="text" value="▼"/>
High CVSS Operator <input style="width: 100%;" type="text" value="▼"/>	High CVSS Score <input style="width: 100%;" type="text" value="▼"/>

Asset Tag Filter:

[Open Asset Tag Selector](#)

Ticket Settings

Set Assignee

Set Days Until Due

Ticket Export Settings

Optional. If set, this will override the email subject setting from the global configuration options. The following macros can be used:

- %job_name%
- %scan_date%
- %description%
- %host_ip%
- %host_name%
- %sys_class%
- %sys_type%
- %service%
- %cve_list%
- %max_cvss_score%
- %tech_details%
- %assigned_to%
- %due_on%
- %created_on%
- %check_id%
- %severity_color%
- %severity_category%
- %severity_description%
- !AssetTagName!

Email Subject

Create

3. Enter values in each applicable form field, based on your rule criteria. Each of the available options are described as follows:
 - Ticket Criteria – These are the options which control whether the ticket rule will match and apply the rule’s ticket settings (user assignment or days until due). The ticket criteria options are:
 - Node Data – The Node Data field contains the literal value of the Scanner Node, or a comma-separated list of values, applicable to a rule. The values may be IPv4/IPv6 addresses, ranges (e.g., 10.0.0.5-10.0.0.9) or CIDR-annotations (e.g., 10.0.00/24). Wildcards (“*” for multiple characters, “?” for a single character) may be used in node names. The Local Node must be identified by its name “Local Node”, not by IP. Leaving this value blank will result in node information being ignored when deciding whether the rule should be applied.
 - Host Data – The Host Data field contains information identifying the target hosts that will be affected by the rule. The data can be a comma-separated list or individual IPv4/IPv6 addresses, DNS names, IP address ranges (e.g., 10.0.0.5-10.0.0.9), or CIDR-notated (e.g., 10.0.0.0/24) hosts. A host DNS name may contain wildcard characters: * matches zero or more characters, ? matches one character.
 - Host OS – The Host OS field allows a user to specify a type of Operating System to be associated with the rule, such as Windows hosts or Linux hosts. This value issued by the rules engine to decide whether the rule applies to this host by comparing the value to the system class identified by SAINT for this host. Wildcards (“*” for multiple characters, “?” for a single character) may be used when choosing “Name” as the Host OS.
 - Severity Level – Choosing a Severity Level will control the types of vulnerabilities that will be assigned to a specified user, using SAINT’s Severity levels: Critical Problems; Areas of Concern; Potential Problems. Each rule can contain only one severity level. Create additional rules in the rule set if a rule set should assign tickets based on multiple severity levels.
 - Range of CVSS Scores – CVSS scores reported by SAINT can be “none”, or in the range of 0 to 10, where “none” is considered lower than 0. Note

that CVSS scores are decimal numbers, not integers. The available Rules settings are:

- Lo CVSS Operator and Low CVSS Score – These settings control the lowest CVSS score in a range if you wish to control assigning the tickets, by rule, based on one or more CVSS scores. For example, setting the “Lo” range to Greater Than 4, specifies CVSS Score of 4.1 as the lowest CVSS score to impact this ticket assignment.
- Hi CVSS Operator and Hi CVSS Score - These values control the highest CVSS score in a range if you wish to control assigning the tickets, by rule, based on one or more CVSS scores. For example, setting the “Hi” range to Less Than or Equal to 10, specifies CVSS Score of 10 as the highest CVSS score to impact this ticket assignment.
- Vuln Category – Choosing a Vulnerability Category will control the types of vulnerabilities that will be assigned to a specified user, using SAINT’s internal categorization of vulnerabilities. For example, assigning tickets to a specified user for all vulnerabilities categorized as Mail vulnerabilities. Each rule can contain only one category. Create additional rules in the rule set if a rule set should assign tickets based on multiple categories.
- Asset Tag Filter – To assign tickets based on an assets tags, click the *Open Asset Tag Selector* link. This will bring up the asset tag selection wizard which allows you to choose the tags attached to hosts which this rule will be applied. Asset tag filters will only apply to newly created tickets, it is not retroactive.
- Ticket Settings:
 - Set Assignee – Select a SAINT User to be assigned the tickets applicable to the rule. An email notification will be sent to the SAINT user’s email address, if defined in the User’s record shown in Manage – Users, and the global Ticket Notifications configuration setting for Email Server is set and Enable Ticket Assignment Notification is checked.
 - Set Days Until Due – The Days Until Due field will define the “due date” for ticket remediation, from the date a vulnerability ticket is generated.

- Ticket Export Settings (only available if [Enable Ticketing](#) is set to *yes but export to another system*):
 - Email subject – Overrides the e-mail subject formatting specified on the [Ticket Export Email](#) configuration tab. The same macros are available here. (See [Macros](#).)

Ticket Export Settings

Optional. If set, this will override the email subject setting from the global configuration options. The following macros can be used:

- %job_name%
- %scan_date%
- %description%
- %host_ip%
- %host_name%
- %sys_class%
- %sys_type%
- %service%
- %cve_list%
- %max_cvss_score%
- %tech_details%
- %assigned_to%
- %due_on%
- %created_on%
- %check_id%
- %severity_color%
- %severity_category%
- %severity_description%
- !AssetTagName!

Email Subject

Optional. If set, this will override the email subject setting from the global configuration options.

The following shows an example Rule defined to assign new Tickets to a user, when the “Local Node” scanner finds vulnerabilities classified as “Areas of Concern” and categorized as “Cisco” vulnerabilities for hosts in the IP range of “10.8.0.11-10.8.0.150”. New tickets will also have a defined due date of 5 days from the date the ticket is generated.

New Ticket Rule
✕

*Choose at least one criterion for match and at least one ticket setting.
Leave criteria blank if not filtering on them.*

Criteria for Match

Node Data
Local Node

Host Data
10.8.0.11-10.8.0.150

Host OS

Severity Level
Areas of Concern ▼

Vuln Category
--- Cisco ▼

Range of CVSS Scores

Low CVSS Operator ▼	Low CVSS Score ▼
High CVSS Operator ▼	High CVSS Score ▼

Ticket Settings

Set Assignee
rderek ▼

Set Days Until Due
5

4. Click the *Create* button once you've verified the rule's setting.

A confirmation message will be displayed to confirm the Ticket Rule with priority 1 was successfully created. Subsequent tickets created in this rule set will have progressively higher numbers.

- Click *OK* to close the confirmation message and view the new rule in the Rule Set:

Edit Ticket Rule Set 1									
Drag and drop rows to change rule priority/order (only when results are unfiltered).									
Grid Actions ▼									
Highest Priority ↗									
View 1 - 3 of 3									
Actions	Rule Priority	Criteria for Match						Ticket Settings	
		Node Data	Host Data	Host OS	Severity Level	CVSS Range	Vuln Category	Assignee	Days Until Due
	1			Cisco				bsmith	1
	2			Windows		>=7 to <=10		wbrown	2
	3			Red Hat		>8 to <=10		yougo	1

- Follow steps 1-4 to add additional Rules to your Rule Set. Or, close the *Edit New Ticket Rule* dialog to Save the Rule Set for use in future scan jobs.
- Ticket rules in a rule set may be reordered by drag and drop. The ability to reorder ticket rules is disabled which the displayed rules are filtered via the grid's toolbar.

Edit a Rule

- Navigate to the *Ticket > Ticket Rules* page.
- Navigate to the Rule Set you wish to edit.
- Click on the *edit* icon (pencil) on the Rule Set's record.
- The *Edit Ticket Rule Set* dialog will display and be available for editing rules contained in the Rule Set.
- Navigate to the rule to be edited. Click on the *edit* (pencil) icon on the rule to display the rule's settings.
- Make the applicable modifications to the ticket rule.
- Click the *Save* button to save your changes. Then select *OK* for the confirmation message.

Delete a Rule

- Navigate to the *Ticket > Ticket Rules* page.
- Navigate to the Rule Set that contains the rule(s) to be deleted.
- Click on the *edit* icon (pencil) on the Rule Set's record.
- The *Edit Ticket Rule Set* dialog will display and be available for editing rules contained in the Rule Set.
- Navigate to the rule to be deleted. Click on the *Delete* (trash can) icon on the rule to be deleted.
- Click *OK* in the Confirmation Message to delete the rule or click *Cancel* to exit without deleting the rule.

Deleting a rule will impact jobs currently associated with the Rule Set by causing the job to no longer have an associated rule set.

Apply a Ticket Rule Set to Existing Tickets

The ticket rules applied during a scan job only affect newly created tickets. They DO NOT apply to existing tickets. However, existing tickets can still be assigned by applying a ticket Rule Set, using the following steps:

1. Navigate to the *Ticket > Ticket Rules* page.
2. Navigate to the Rule Set that contains the rule(s) to be applied to existing, unassigned tickets.
3. Click on the *Run Ticket Rule Set* against New (unassigned) Tickets icon. (This is the run arrow with the light gray background).
4. A Confirmation Message will be displayed to confirm you wish to "... apply ticket rule set x to all New tickets."
5. Click *OK* to confirm and update existing unassigned tickets based on the rule set's rules, or click *Cancel* to exit without performing the ticket updates.

To verify the existing tickets have been updated:

1. Navigate to the *All Tickets* page.
2. Search for tickets that were previously unassigned that should have been updated by the rules in the manually applied Rule Set.
3. Verify the assignee field has been updated according to the rules. Note that the ticket due date is not affected by ticket rule sets applied to existing tickets.

Similarly, a ticket rules set can also be applied to all open existing tickets (this includes tickets with any status other than closed, versus unassigned tickets) by selecting the *Run Ticket Rule Set against all open Tickets* icon (the run arrow with the black background) in step 4 above.

Using the Ticket Grid

View Ticket Details

Select the Information icon (i) on the left of the grid to reveal detailed information about the corresponding ticket. A dialog window (as shown below) will display details about the ticket, including column information not currently visible in the grid, the change history of how the ticket has been modified over time, and comments that have been entered regarding the ticket.

The screenshot shows the 'View Ticket #6' window with the following data:

Detail	
Ticket ID	6
Nodename	Local Node
Host IP	10.8.0.14
Host Name	10.8.0.14
Service	netbios
Severity Level	Area of Concern
Severity	susceptibility to malicious content
Confirmed	No
Tutorial	Windows updates needed
Description	Microsoft Data Access Component remote code execution (MS11-002)
Details	msadco.dll dated 2006-3-1, older than 2010-11-3
Ticket Status	Assigned
Assignee	admin
Due On	2017-07-05
Resolved On	Not set
Resolved By	Not set
Created On	2017-06-28
Last Occurred	2017-07-03
Updated On	2017-07-03
Updated By	admin
Recurred After Close	No
Auto Status	None
Last Reminder	Not set
Assignment Sent	Not set

History		
Date/Time	Modification	Author
2017-07-03 11:05:48	(bulk) Ticket Status: Assigned, Assignee: admin, Due On: 2017-07-05	admin

Comments		
Date/Time	Comment	Author
2017-07-03 11:59:17	Issues currently being investigated by Sys Admin of the impacted systems.	admin

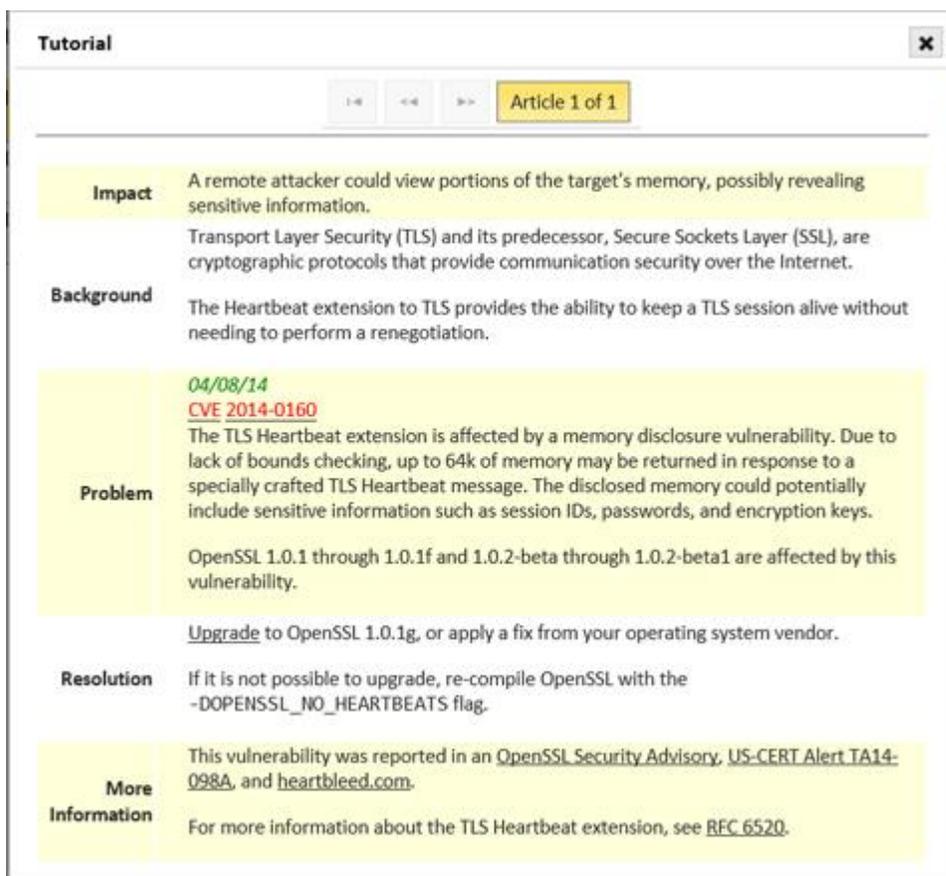
Update a Ticket

Click on the *Edit* (pencil) icon to display the *Update Ticket* window. This window displays all ticket fields that can be modified, based on a user's ticket permission. This window also provides a field for entering comments such as the ongoing progress of the remediation activities, justification for actions or decisions made to support the ticket, or other information you deem valuable in tracking the actions or history about the vulnerability and remediation work.

View Ticket-related Vulnerability Tutorials

Click on the *Tutorial* (page) icon to gain access to SAINT’s custom-developed tutorial articles applicable to the vulnerability associated with the Ticket. These tutorial articles are the same ones visible through the *Analyze* tab and Report details that provide information about the vulnerabilities (background, impact, etc.) and information to facilitate remediation activities to reduce your overall risk posture.

An example tutorial related to the "Heartbleed" vulnerability is shown below:



The screenshot shows a window titled "Tutorial" with a close button (X) in the top right corner. Below the title bar, there are navigation controls: a left arrow, a double left arrow, a double right arrow, and a right arrow, followed by a yellow box containing the text "Article 1 of 1". The main content area is divided into several sections, each with a bolded label on the left and text on the right:

- Impact**: A remote attacker could view portions of the target's memory, possibly revealing sensitive information.
- Background**: Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that provide communication security over the Internet. The Heartbeat extension to TLS provides the ability to keep a TLS session alive without needing to perform a renegotiation.
- Problem**: 04/08/14
CVE 2014-0160
The TLS Heartbeat extension is affected by a memory disclosure vulnerability. Due to lack of bounds checking, up to 64k of memory may be returned in response to a specially crafted TLS Heartbeat message. The disclosed memory could potentially include sensitive information such as session IDs, passwords, and encryption keys.
OpenSSL 1.0.1 through 1.0.1f and 1.0.2-beta through 1.0.2-beta1 are affected by this vulnerability.
Upgrade to OpenSSL 1.0.1g, or apply a fix from your operating system vendor.
- Resolution**: If it is not possible to upgrade, re-compile OpenSSL with the `-DOPENSSL_NO_HEARTBEATS` flag.
- More Information**: This vulnerability was reported in an OpenSSL Security Advisory, US-CERT Alert TA14-098A, and heartbleed.com.
For more information about the TLS Heartbeat extension, see REC 6520.

Bulk Update

One of the most often used features is the ability to update the status, assignment, due date or comments of multiple tickets, at one time. You can update many tickets "in bulk" by selecting (checking) one or more tickets (even across multiple grid pages) and then click the *Bulk Update* option from the *Grid Actions* drop-down. As with other grids, those options are provided to

apply the selected action (grid columns; global search; bulk update; CVS/XML exports; etc.) for all selected records.

The example below shows four new tickets being updated to assign them to user bsmith with a comment to expedite:

The screenshot displays a ticketing system interface. At the top, there are navigation tabs: Dashboard, Scan, Analyze, Report, Ticket (highlighted), Exploit, Manage, and Configuration. Below these are sub-tabs: My Open Tickets, All Tickets, and Ticket Rules. A 'Grid Actions' dropdown and a 'Days Until Due: 7' input field are visible. The main area shows a grid of tickets with columns: Actions, Ticket ID, Node Name, Host IP, Service, Description, Status, Due On, and Last Occurred. Two tickets are selected (checked). A 'Bulk Ticket Update' dialog box is open, showing the following fields:

- Selected Tickets: 2,3,6,9
- Ticket Status: Assigned (dropdown)
- Assignee: bsmith (dropdown)
- Due On: (empty text box)
- or postpone (empty text box) days
- Resolved On: (empty text box)
- Resolved By: No Change (dropdown)
- Comment: Need these tickets expedited. (text area)

A 'Save' button is located at the bottom of the dialog box.

Complex Search

In addition to being able to search for column-specific values in the grid's column search boxes, the ticketing grids also provide an additional *complex search* feature (*Grid Actions > Complex Search* option) to construct ad hoc queries, for greater power and granularity of search results.

The complex search dialog window, as shown here, provides the following options:

SAINT Security Suite

The screenshot shows a search interface with the following elements:

- A search bar labeled "Search..." with a dropdown menu set to "all".
- Buttons for "+ {}" and "+" to add search criteria.
- A search rule configuration: "Ticket ID" (field), "equal" (operator), and an empty text input field.
- A "Reset" button with a left-pointing arrow.
- A "Find" button with a magnifying glass icon.

- The first option allows you to select the scope of your search to include *all* or *any* record that contains the prescribed search criteria. The *all* option is equivalent to logical 'and' applied to all conditions in the group. The *any* option is equivalent to the logical 'or' operator.
- The next option +{} is a subgroup option that will allow you to first pull up a set of values (group), and then further refine the results (subgroup) based on that initial set of values.
- The option with the + symbol is the *Add Rule* option to add multiple search criteria (such as TicketID + Status).
- Below those high level search scoping options, you can define the search parameters for each rule. In the example above, the rule for the TicketID field will be defined to "equal" some defined value.
- The *Reset* option is provided to clear all search criteria and begin again.
- Click the *Find* button once all search criteria has been defined, to locate ticket records that meet your criteria.

In the following example, this search returns all tickets related to Critical vulnerabilities; are not Closed; and Reoccurred after they were originally Closed.

The screenshot shows a search interface with the following elements:

- A search bar labeled "Search..." with a dropdown menu set to "all".
- Buttons for "+ {}" and "+" to add search criteria.
- Three search rule configurations:
 - Rule 1: "Severity Level" (field), "equal" (operator), "Critical Problems" (value).
 - Rule 2: "Status" (field), "not equal" (operator), "Closed" (value).
 - Rule 3: "Reccured After Close" (field), "equal" (operator), "Yes" (value).
- A "Reset" button with a left-pointing arrow.
- A "Find" button with a magnifying glass icon.

Note that the search conditions remain in place until the page is refreshed or the options are cleared via the *Reset* button.

Export to CSV or XML

Tickets can be exported from either the *My Tickets* view or *All Tickets* view, using the CSV or XML export options from the *Grid Actions* drop-down list. This functionality is the same as exporting scan results in the *Analyze* tab grids.

To export tickets, click the applicable CSV or XML option from the *Grid Actions* drop-down list. The system will display a dialog for saving the generated file to a target path. The export feature will export all columns for all tickets returned in the current view. This provides the flexibility to export all tickets or only a defined subset of the tickets by filtering (limiting) the results by either the complex search or column search features.

Close a Ticket

Closing tickets in the system is done by using the update features, as described above. As a best practice, it is recommended that ticket “close” actions include, not only, the status change to “Closed” but also include comments that provide information such as the actions taken, the targets affected, whether any remediation or validation actions were taken to note risk mitigation or reduction, and other information that can support future research, risk assessments and audits applicable to the organization, assets or supported business functions.

Delete a Ticket

Tickets can be deleted, based on a user’s ticket(s) permissions. Tickets are deleted by clicking on the *Delete* (trash can) icon for a selected ticket, and choosing *OK* to the delete confirmation message. Multiple tickets can be deleted in “bulk” in the same manner as a bulk update – by selecting (checkbox) multiple tickets (even across multiple grid pages) and then selecting the *Grid Actions > Delete* option. As with the single row deletion, the user must choose *OK* to the delete confirmation message.

Exploit

SAINT's exploit and penetration testing module includes a variety of exploits designed to gain command execution privileges on remote targets. The exploits can be run on demand or as part of an automated penetration test.

Browse Exploits

To view the list of available exploits select the *Exploit* menu, and then select the *Exploits* page. The grid shows all exploits and detailed information about each – including what can be exploited, and how to set up an exploit or tool for execution. See the [Exploit Tools](#) page for details on how to set up and execute a specific exploit tool.

The exploit grid provides the capability to sort the list by selecting a column heading; search for a specific exploit or tool; or constrain the list to specific exploits or exploit types (*client, local, remote, tool*), target platforms, related CVE or exploit date; as well as other characteristics available in the column selector, such as *Class* and *Protocol (IPv4, IPv6)*. To search for an exploit, enter a keyword in the search box, and then choose one of the options to search for the keyword in the exploit name, CVE, BID, or OSVDB.

When an exploit of interest is found, click on Info () link or double click on the exploit to view detailed information about the exploit, including background information, a description of the problem, fix information, links to references, and limitations. The limitations section may include information such as what software versions the exploit is known to be effective against, whether the exploit depends upon system state, and what type of user interaction may be required on the vulnerable host.

Run Exploits On Demand

Once an exploit has been chosen, it can be executed by clicking on the *Run* icon (right arrow) for the exploit record, or by selecting the *Run* button within an exploit's information dialog. This selection will display the setup form containing information specific to the chosen exploit. Among the most common fields are:

- **Target** – the host name or IP address of the host against which to attempt the exploit
- **Target Type** – the target platform, chosen from the list of platforms in the pull-down menu
- **Port** – the TCP or UDP port on which the vulnerable service is listening
- **Shell port** – the TCP port on which a successful exploit opens a command shell on the target

After filling in the requested information, click the *Run* button to launch the exploit. A status update will appear indicating that the exploit is running, or explaining why the exploit could not run in the case of failure. When the exploit finishes, there will be a status update indicating whether or not the exploit succeeded.

Exploit Types

Remote vs. Local Exploits

Remote exploits target vulnerabilities in network services which listen for connections on a TCP or UDP port. Examples include vulnerabilities in web services (HTTP or HTTPS), mail services (SMTP, POP3, or IMAP), or RPC services. Remote exploits do not typically require prior access to the target before the exploit can be attempted.

1. To run a remote exploit, click on the *Run Now* button beside the exploit name or at the bottom of the exploit description page to display a setup dialog to configure the exploit for execution, as in the example below for the MySQL file remote privilege elevation exploit:

The screenshot shows a configuration window titled "MySQL FILE privilege elevation". It contains the following fields and options:

- Scanner Node: Local Node (dropdown)
- Job: --- New Job --- (dropdown)
- New Job Name: MySQL File Remote Exploit (text input)
- Port: 3306 (text input)
- MySQL User: (empty text input)
- MySQL Password: (empty text input)
- OS: Windows (dropdown)
- Shell Type: Reverse Port (dropdown)
- Shell Code Transfer Port: 14234 (text input)
- Shell Port: 14195 (text input)
- Target: (empty text input)

A "Run" button is located at the bottom center of the window.

2. The first step is to select the scanner "node" to run the exploit from. This node must be able to reach the target. For standalone installations, this will be the built-in local node. For multi-node deployments, this must be a scanner node that can access the host being exploited.

3. Select an existing Job to associate the exploit with, or enter the name of a new Job for the exploit.
4. Enter parameters for each option available in the exploit setup, as shown in the selected exploit. Note that each exploit can have unique characteristics. Context-sensitive help is available via each field's help (?) button for guidance.
5. Enter the target to direct the exploit to.
6. Click *Run* to launch the exploit.

Local exploits target vulnerabilities in entities which are not accessible across a network, such as the operating system kernel or services which do not accept remote connections. Local exploits require prior access to the target, so there must be an existing connection to the target before the exploit can be attempted. Whereas remote exploits target remote command execution vulnerabilities, local exploits target privilege elevation vulnerabilities. To accurately assess the success of a local exploit, the existing connection must not already be at the *root* or *administrator* level.

The steps for executing a local exploit are the same as setting up a remote exploit (Job; Settings; Target). Again, context-sensitive help at the field level is provided for specific help.

Client Exploits

Client applications such as web browsers and media players do not listen for connections on a TCP or UDP port like server applications do. Instead, all data transmission is initiated by the client. Therefore, exploits for client vulnerabilities cannot be executed directly. Instead, these exploits must wait for a connection from the vulnerable application.

1. To run a client exploit, click on the *Run Exploit* icon beside the exploit name or the *Run* button at the bottom of the exploit description page to display a setup dialog to configure the exploit for execution, as in the example below for the Adobe Flash Player client exploit:

Adobe Flash Player OpenType Font Integer Overflow

Scanner Node
Local Node

Job
--- New Job ---

New Job Name
Flash OpenType Font Exploit

Port
8724

OS
Windows

Shell Port
14197

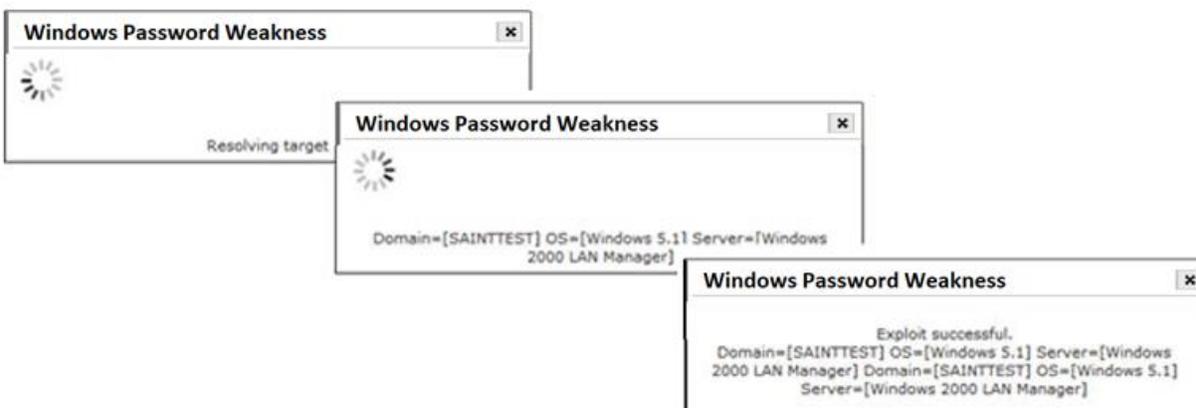
Run

2. The first step is to select the scanner “node” to run the exploit from. This node must be able to reach the target. For standalone installations, this will be the built-in local node. For multi-node deployments, this must be a scanner node that can access the host being exploited.
3. Select an existing Job to associate the exploit with, or enter the name of a new Job for the exploit.
4. Enter the listener port number. This is the TCP port number on which to run the exploit server.
5. Select the operating system of the target computer (if options are available).
6. Enter the Shell Port number. This is the TCP port number to use for controlling the target in the event that the exploit is successful.
7. Click *Run* to launch the exploit.

When a client exploit is run, a server is started that listens for connections from vulnerable clients on a port, and serves the exploit when it receives a request.

Exploit Status

Once an exploit has been executed, a dialog will be displayed to first attempt resolution of the Target and display a message if/when target resolution has occurred; and additional messages to show progress as the exploit executes. The last update will display whether the exploit is successful or unsuccessful. Example status messages are shown below:



Successful exploit results will then be loaded into the repository and available for analysis, via the Analyze pages and Exploit reports.

Exploit Tools

In addition to the remote, local, and client exploits designed to exploit a command-execution vulnerability on a target, SAINT also includes a number of additional tools. Each tool performs a certain information gathering task which might be a useful part of the penetration testing process, but doesn't attempt a penetration in and of itself.

To view the list of Exploit tools like the screen capture below, click on the *Exploit Tools* option under the *Exploits* menu; or use the *Exploits* page and *sort* or *constrain* the list by *tool* in the *Type* column.

⊕ Page 1 of 1 30 ▾ View 1 - 26 of 26					
Action:	Name	Date	CVE	Type	Platform ↕
	<input type="text"/>		<input type="text"/>	toc ▾	<input type="text"/>
 ▶	Linux Dirty COW Local File Overwrite	2016-10-27	CVE-2016-5195	tool	Linux
 ▶	Crack OS X 10.7 Hashes	2011-07-14		tool	Mac OS
 ▶	Mac camera image capture	2011-07-14		tool	Mac OS
 ▶	Get OS X 10.7 Hashes	2011-07-14		tool	Mac OS
 ▶	Screen Capture	2012-04-18		tool	multiple
 ▶	Reverse Shell Applet	2010-10-10		tool	multiple
 ▶	Download connection	2009-03-18		tool	multiple
 ▶	E-mail attachment execution	2009-01-28		tool	multiple
 ▶	WPAD Listener	2013-09-30		tool	platform independent
 ▶	Upgrade Attack	2013-09-30		tool	platform independent
 ▶	Browser Find toolbar phishing attack	2012-02-25		tool	platform independent
 ▶	ARP Spoof	2010-08-23		tool	platform independent
 ▶	Automatic Drive-by Download	2010-07-23		tool	platform independent
 ▶	Click Logger	2009-09-30		tool	platform independent
 ▶	Phishing Tool	2009-09-23		tool	platform independent
 ▶	Find Metadata	2009-06-04		tool	platform independent
 ▶	Find e-mail addresses	2008-09-24		tool	platform independent
 ▶	DNS zone transfer	2008-09-24	CVE-1999-0532	tool	platform independent
 ▶	Chrome Password Grabber	2012-01-10		tool	Windows
 ▶	Password Hash Grabber	2009-05-27		tool	Windows
 ▶	Flash drive/CD autoplay command execution	2009-04-07		tool	Windows
 ▶	Keystroke Logger	2009-03-05		tool	Windows
 ▶	Upload command to Startup folder	2009-01-20		tool	Windows
 ▶	Read passwords stored in web browser	2009-01-09		tool	Windows
 ▶	Disable Firewall	2008-11-25		tool	Windows
 ▶	Read Address Book	2008-10-07		tool	Windows

Viewing the details about a tool and running a tool are both executed through the same point-n-click method used for the exploits. To run an exploit tool, enter the requested information in the tool's setup dialog, and then click the *Run* button. The results will be available in the *Analyze* page after the tool finishes running.

The following describes the exploit tools currently available by SAINT:



ARP Spoof Exploit Tool – This tool sends a forged ARP reply which is stored in a target’s cache, allowing impersonation of that target’s gateway router or another key destination. The tool proceeds to

conduct a man-in-the-middle attack and capture packets being sent between the target and the destination.



Automatic Drive-by Download – This tool waits for client connections, and then gathers information about the operating system and installed software on the client. Next, it chooses the latest and most reliable client exploit for the client's operating system and installed software, and delivers that exploit to the client.



Browser Find Toolbar Phishing Attack – This tool uses the browser's Find toolbar to capture the user's password.



Chrome Password Grabber – This tool uses an existing connection to extract all passwords saved in the Chrome browser for the logged in user.



Click Logger – This tool runs an exploit server which simply returns an error page and logs which users visited it. It can be used to find out which users were susceptible to clicking on the link in an e-mail message.



Crack OS X 10.7 Hashes – This tool will open hashes dumped by the **Get OS X 10.7 Hashes** tool and crack them using a word list. Successfully cracked accounts are saved.



Disable Firewall – Disables the firewall on a target system for further penetration analysis. The connection requires root privileges on Unix and Linux targets.



DNS Zone transfer – This is a process by which a secondary name server copies all DNS records for a domain from a primary name server.



Download Connection – This tool allows you to download a file which, when executed, establishes a command connection. This tool requires a user to execute the downloaded file in order to succeed. The target field must be a licensed target but is unused.



E-mail Attachment Execution – This tool sends an e-mail attachment which, when executed, establishes a command connection. This tool requires a user to execute the e-mail attachment in order to succeed. This tool requires the IP address of a working mail server which allows relaying of mail to the recipients. The target field must be a licensed target but is unused. This tool

accepts either a single recipient or a space-separated list of recipients. If the user's e-mail client blocks .exe attachments, then an attachment filename which doesn't end in .exe must be used, and the file must be renamed to end in .exe before it can be run.



Find E-mail Addresses – E-mail addresses in a given domain can often be found using publicly available information such as Internet search engines, network registrars, and public key servers. This tool attempts to provide a list of e-mail addresses using these resources for automating client type exploits, and is integrated with the SAINT e-mail forgery emulator.



Find Metadata – This tool searches the Internet for PDF and Microsoft Office files in the given domain, and extracts the metadata from those files. This metadata often contains the names or aliases of the document's authors or contributors, which can be used to guess valid e-mail addresses for use in client exploits.



Flash Drive/CD Autoplay Command Execution – A trojan that can be downloaded on a USB drive or CD, and when connected to a computer, will provide a direct connection to the exploit server. This tool allows you to create a USB flash drive which, when inserted into a Windows computer, prompts a user to run a program which creates a command connection. The program is disguised as the *Open Folder* option in the AutoPlay dialog to entice the user to run it.



Get OS X 10.7 Hashes – This tool attempts to retrieve all user names and their associated SHA512 password hashes. If successful the hashes are dumped for offline cracking. This tool works on Mac OS X 10.7 and 10.7.1



Keystroke Logger – This tool records all keystrokes which are typed at a computer's console. The keystrokes can be viewed in the exploit server's log.



Mac Camera Image Capture – This tool attempts to retrieve an image file captured by an iSight camera such as the one built into a MacBook. If it is successful, the picture is displayed.



Password Hash Grabber – This tool grabs the windows SAM file or password hashes of the target. The SAM file/password hashes can

be viewed in the exploit tools previous results section. Results may be used with third party programs to obtain passwords in plain text.



Phishing Tool – This tool serves an HTML form which collects information from users. It allows you to specify a custom header graphic, a custom footer graphic, and an introductory text message. For best results, design the HTML form to look like a legitimate web site so users will be more inclined to enter the requested information.



Read Address Book – This tool attempts to gather e-mail addresses from Outlook and Outlook Express address book files (.WAB, .PAB) on the target. Recent versions of Microsoft Outlook no longer store address books locally by default. Therefore this tool is primarily useful for targets using Outlook Express or old versions of Outlook.



Read passwords Stored in Web Browser – This tool attempts to retrieve web site passwords which have been stored by Internet Explorer. Due to the encryption algorithm used by Internet Explorer, this tool can only retrieve passwords that were entered by the same user that is running the tool. For Internet Explorer 7, due to the encryption algorithm, this tool can only retrieve passwords for web sites that are still present in the browser's history. For Internet Explorer 7, passwords can only be retrieved if AutoComplete is enabled and the user chooses *yes* when prompted to save each one.



Reverse Shell Applet – This tool runs an exploit server which delivers a signed Java applet, embedded in an HTML page, to the target hosts. The user is presented with a signed digital certificate which, when accepted, establishes a reverse shell connection back to the exploit server.



Screen Capture – This tool captures the screen of a remote target, based on an existing connection already established to the target. Note that for Unix and Linux systems, the *xwd* utility must be present on the target in order to exploit the target and perform screen captures.



Upgrade Attack – Like the WPAD Listener, this exploit tool sends fake LLNMR responses to trick browsers into proxying web requests through the exploit tool. It then proceeds to intercept requests for

device driver updates and delivers an executable which establishes a command connection.



Upload Command to Startup Folder – Each user's Startup folder on Windows systems contains programs that run at start-up time. This tool uploads a command connection to a user's startup folder. Then the connection is established the next time the computer starts.



WPAD listener – This tool sends fake LLMNR responses to trick browsers into proxying web requests through the exploit tool. It then proceeds to request NTLM authentication from the browser and collects the resulting password hashes.

Exploit Servers

Once a client exploit has been run, its exploit server will appear in the *Exploit Servers* task area under the *Exploits* menu. In the following example, an Exploit is being run for the Adobe Flash Player OpenType Font Integer Overflow vulnerability.

Actions	Started At	Node	Port	Exploit Name
   	2017-04-06 16:00	Local Node	8122	Adobe Flash Player OpenType Font Integer Overflow

There are several options available at this point. Click on the *Log* icon to see what requests have been received by the exploit server. Click on the *Send E-mail* icon to craft an e-mail message to lead users to the exploit server (see [e-mail forgery](#)). Click on the *Send Text Message* icon to send a text message which leads a cell phone user to the exploit server (see [text messaging](#)). Click on the *Stop* icon to terminate the exploit server.

E-mail Forgery

Once an exploit server has been started, users need to initiate a connection with it in order for exploitation to occur. A good way of telling users to connect to it is through e-mail. Craft an e-mail message to lead potentially vulnerable clients to the exploit. Since it may be more effective if the e-mail appears to come from a colleague or a prospective customer, forge the e-mail message such that it appears to come from any name and e-mail address. A number of graphical templates designed to entice a user into following a link are also included.

The option to craft an e-mail message is available after the exploit server has started by clicking on the Send E-mail icon in the [Exploit Servers](#) section. To enable e-mail, enter one or more recipient addresses, separated by spaces or commas. Click on the light bulb icon followed by the Find E-mail Addresses link, if desired, to search for possible e-mail addresses in the desired domain.

If desired, also change the subject line, the content type, the template, the message body, or the name and address which the message will appear to come from. Use the *preview* links beside the template choices to see how the message will appear to the recipient.

Note that the default message includes the link to the exploit and, for some exploits, special instructions for the recipient to attempt the exploit. The link should remain intact, but the surrounding text can be anything which would be most effective in persuading the recipient to follow the link.

The e-mail will be sent through a mail relay if specified. The relay must accept mail for the recipient's domain, or be configured to allow relaying from the exploit host to the recipient's domain. If a mail relay is not specified, the mail is sent directly to the mail server for each recipient's e-mail domain.

Text Messaging

The section above discusses the use of e-mail to lead users to the exploit server. However, some users may be less inclined to read such e-mail messages, and others may never see the message at all due to spam filters. In these cases, text messaging may be a more effective option for leading users to the exploit server.

To send the exploit server link in a text message, click on the *Send Text Message* icon () for the desired exploit server on the [Exploit Servers](#) page. In the resulting dialog window, enter one or more cell phone numbers in the *To* box, separated by spaces or commas. Each cell phone number should have ten digits, with or without dashes. Next, customize the message content if desired. The URL should be left intact in order to link to the exploit server, but the surrounding text can be anything which would be effective in persuading the recipient to follow the link. Finally, click the *Send* button.

Connections

After a successful exploit, a control channel is created by connecting to a shell port, receiving a shell connection back from the exploit, or recording the parameters which allowed remote access to the target, depending on the payload of the exploit. This control channel is referred to as a *connection*. The connection gives you control over the target after it is exploited, allowing you to view the file structure or take other actions which serve as proof of access.

Connections Manager

To view your current connections, click on the *Exploit* menu followed by the *Tools* task option. If there are any active connections, they are listed on this screen.

 Page 1 of 1 View 1 - 1 of 1					
Actions	Started At ↓	Target	Access Level	Node	Through
   	2017-07-18 16:45:17	10.8.0.14	C share	Local Node	

Connections resulting from exploits, which gained full administrative privileges on the target, are indicated by the word *admin* or *root* in the access level column. Connections which gained access only to a particular resource on the target, such as an SMB share, are indicated by the resource name in the access level column. All other connections are indicated by the word *user* in the access level column.

Clicking on the wrench icon in the right-hand column of any connection displays a menu of actions which may be taken on the connection. These actions are discussed in the sections which follow.

Command Prompt

The command prompt provides the ability to interactively send commands to the remote host and view the resulting output. The command prompt is available in most connections, except those resulting from limited-access exploits such as SMB password guessing.

How to Invoke the Command Prompt

To invoke the command prompt, click on the *Exploit* menu followed by the *Connections* task item to view the connection list. Then click on the wrench icon on the desired connection in the

list, and then *Command Prompt* on the pop-up menu. Enter commands followed by the *Enter* key, and wait for the results to appear.

Note that the commands are sent directly to the command shell on the remote target. Thus, the set of recognized commands depends upon the operating system of the remote target. `dir`, `cd`, and `type` are common commands on Windows targets. `ls`, `pwd`, `cd`, and `cat` are common commands on Unix and Linux targets. Consult an operating system manual for more information on available commands.

Depending upon the type of exploit, the connection may be a virtual connection instead of a real TCP connection to the target. Although the command prompt for a virtual connection appears the same as that for a normal connection, the underlying function invokes a new command shell for each command rather than having a persistent shell. Thus, the shell will have no "memory". The environment of each command will be independent of previous commands. For example, a change to the current working directory using the `cd` command will not be remembered by the next command.

File Manager

The file manager allows you to browse the folders and files on the remote host, to download or upload files on the remote host, or to delete or rename files on the remote host.

How to Invoke the File Manager

To invoke the file manager, click on the *Exploit* menu followed by the *Connections* task item, and then click on the wrench icon for the desired connection, followed by *File Manager*. The files and folders found in the current folder are displayed on the initial grid. Clicking on any of the displayed folders changes it to the current folder. The current folder's full path is shown above the grid, and clicking on any of the folders in the path also changes it to the current folder.

To download a file from the remote host, click on the down-arrow icon beside the desired file in the file manager. To upload a file to the remote host, click on the *Upload* option in the Grid Actions dropdown. On the form, specify the file name on the remote host and the local file to upload.

Security Suite will attempt to upload or download the file using TFTP, active FTP, passive FTP, or SMB—whichever method is available with the current connection type and target operating system. Note that in some connections, the ability to upload and download files may not be available. In these cases, text files can be viewed using the `type` or `cat` command in the [command prompt](#) instead.

Once a file has been downloaded successfully, it will be handled by the browser based upon the file type. HTML, XML, text, and other file types will usually be displayed by the browser itself. You may be prompted to enter a file name to save other types of files.

To delete a file on the remote host, click on the trash can icon beside the desired file, and choose *OK* in the confirmation box.

Screen Capture

The screen capture displays whatever is on the screen of the remote computer at the time the capture is performed. In some cases, this may show useful information, such as an open application or a user's desktop. In other cases, it may just show a login prompt or a screen saver.

How to Perform a Screen Capture

To perform a screen capture on an exploited target, click on the *Exploit* menu followed by the *Connections* task item. Then click on the wrench icon for the desired connection. That will bring up the Exploit Tools grid. Enter *Screen Capture* in the search box below the *Name* column heading, or scroll down and find the Screen Capture exploit tool. Click on the *Run Exploit* icon for that exploit tool to open a dialog box which reports the progress as it captures the screen, downloads the bitmap, converts it to PNG format, and displays it. It can then be copied and pasted using your browser's copy function.

Note that the screen capture function will not be available for remote systems that do not use a graphical user environment. Furthermore, the screen capture function requires the ability to upload and download files on the remote host, which may not be available in some connections.

Exploit Tunneling

Depending on the design of the network, there may be some parts of the network that are restricted or inaccessible from other parts of the network. A thorough penetration test will attempt to use a successfully penetrated target to evaluate other potential targets which may be accessible from the first target. The scan engine achieves this type of penetration test by tunneling exploits through a target which has been successfully penetrated. The tunnel runs on the penetrated target and forwards network data between the scan engine and the new target, essentially allowing most functions, including port scanning, exploit attempts, and shell connections, to run as though the scanner has direct access to the new target.

How to Run Exploits through a Tunnel

To run exploits through a tunnel on a penetrated target, go to the *Exploit* menu followed by the *Connections* task item. Then click on the wrench icon for the desired connection, followed by *Start Tunnel* from the pop-up menu. Wait while the tunnel is established, and verify that it was established successfully. Then, select that connection as your tunnel on the setup page when running exploits either on demand or as part of an automated penetration test.

When the tunnel is no longer needed, follow the same instructions as for starting the tunnel, but click on *Stop Tunnel*. This will also terminate any connections resulting from successful exploits which ran through the tunnel.

Disconnecting

When a connection is no longer needed, it should be disconnected to conserve resources and to avoid misuse by other users.

How to Close the Connection

To disconnect, click on the *Exploit* menu followed by *Connections* and click on the *Disconnect* icon for the desired connection. This will close the persistent TCP connection if there is one, and remove the connection parameters from the disk.

Run an Automated Penetration Test

Pen Test Setup

In an automated penetration test, the exploit process begins by gathering information on operating system types and open services, and then launches a set of exploits specific to those operating systems and services.

To begin a penetration test, set up a scan Job that will execute the penetration test. Use the *PenTest* scan category under the policy step. (See the *Scan* tab [section](#) for setting up a scan job for help on this process).

The scan levels for running a penetration test are as follows:

- **Discovery** will discover live hosts in the selected address range, and then stop. This level does not require a license key. It is useful for figuring out which IP addresses to put in your key. The discovery method depends on the selected [firewall support](#) option.
- **Information Gathering** will discover live hosts, try to determine their operating system types, and scan their ports.
- **Single Penetration** will include all of the above steps and then proceed to run remote exploits for the detected operating system and services, starting with those least likely to cause crashes, until one succeeds in establishing a shell connection.
- **Root Penetration** is similar to Single Penetration but continues until the maximum privilege level is reached on the target. The maximum privilege level is *root* on a Unix or Linux system and *administrator* on a Windows target. The Root Penetration level also runs local exploits if the available remote exploits result in a connection without maximum privileges.
- **Full Penetration** will run all available exploits for the detected operating system and services. This level is the best choice if the objective is to exploit as many vulnerabilities as possible. However, if the objective is to obtain evidence of penetration, such as files or screen captures from the target, then this level is not the best choice because a

successful connection could be severed if a later exploit causes a crash.

- **Web Application** will search the target for Web applications, and run all available exploits against those applications. This level is the fastest way to find exploitable Web application vulnerabilities such as SQL injection.

The exploit functionality also provides support for authentication to the targets. This option is similar to the scanning [Authentication](#) option. For the purpose of penetration testing, authentication is helpful for determining operating system differences, such as service pack levels or Linux varieties, more precisely than would be possible using un-credentialed methods. This information helps the exploit process choose the correct arguments when running exploits, and may improve the success rate. However, the login and password are not typically needed for the exploits themselves.

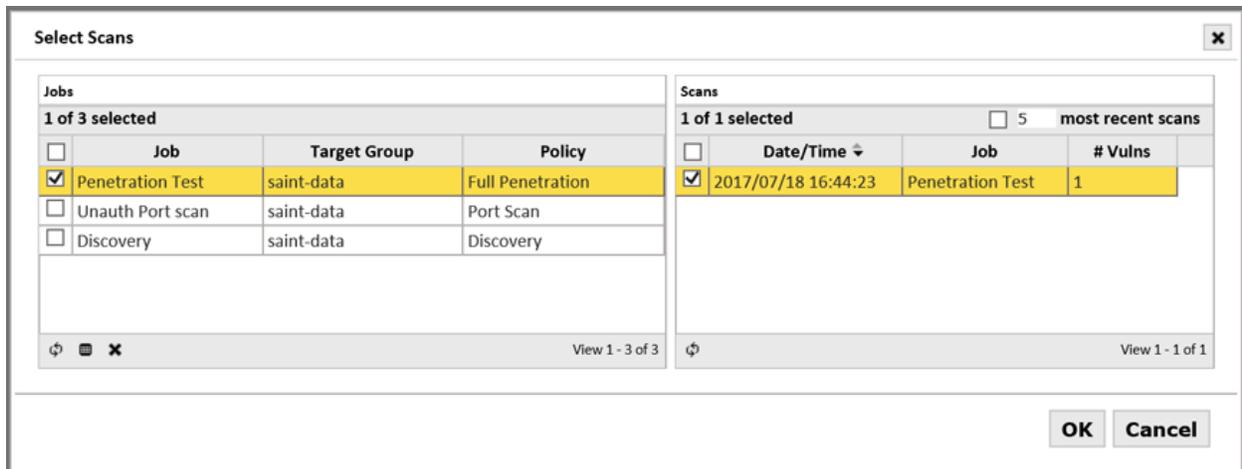
Set up the remainder of the scan Job process as you would other types of scans. Define the schedule for the job and send it to the job queue. Job status for Penetration Testing jobs will be available via the Scan grid.

Analyze Exploit Results

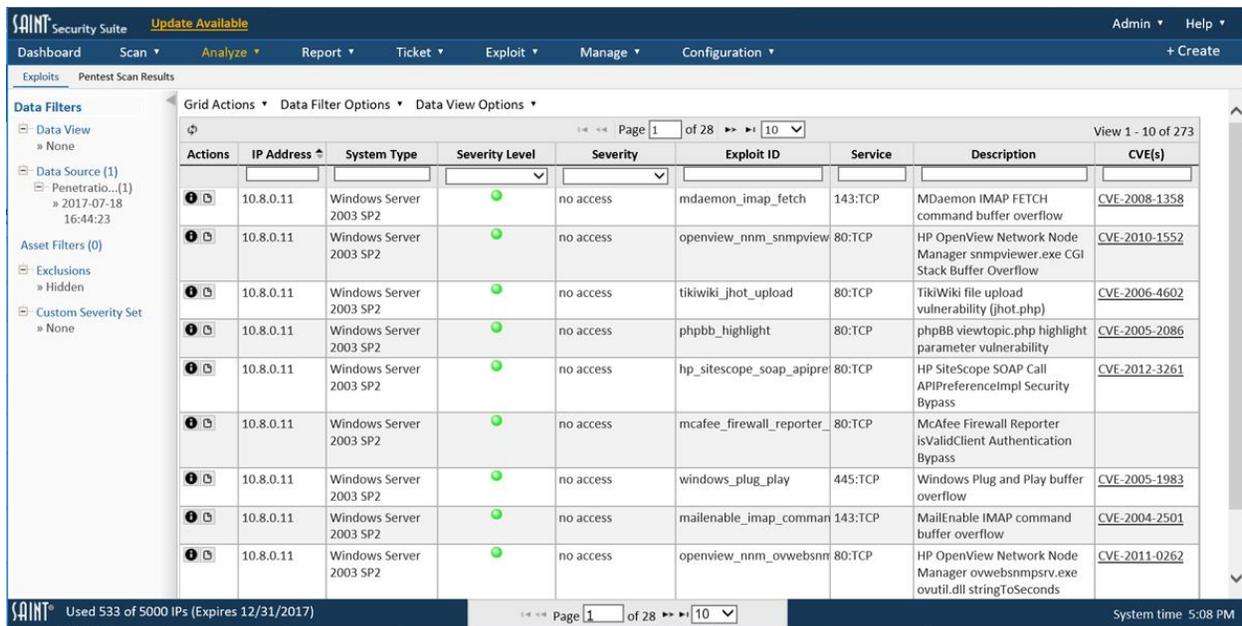
Exploit results are stored and accessible in a manner similar to other types of scans. Therefore, results can be selected and analyzed within the [Analyze](#) page or generated as a report. Refer to those sections for more information for more detailed help. The following shows an example of running a full penetration test and viewing the results of the completed job.

First, select the job and specific scan result. The job can be run multiple times, so it is important to identify the specific scan execution you wish to assess. Note that the scan shows Zero (0) for Number of Vulnerabilities. In this case, the results are not identified specifically as vulnerabilities, as in the case of a vulnerability assessment. However, there may be results retrieved as a result of the exploit that are specific to the type of exploit or test used.

SAINT Security Suite



The *Analyze* pages will display results columns specific to exploits, as there are variances in the types of information collected between vulnerability and exploit assessments. The following shows results from a full penetration test.



This results show the Exploit ID of each exploit, the severity of individual results, the description of the exploit, and references to any related CVEs (with hyperlinks to the CVE authoritative source for additional details on the CVE).

Use the Details () option for a results record to obtain additional information about the result, as well as any other hyperlinks to reference sites for remediation guidance.

MDaemon IMAP FETCH command buffer overflow	
Discovered	2017-07-18 16:57:10
IP Address	10.8.0.11
Host Name	10.8.0.11
System Class	WINDOWS
System Type	Windows Server 2003 SP2
Description	MDaemon IMAP FETCH command buffer overflow
Severity Level	Unsuccessful Exploit
Severity	no access
Service Output	mdaemon_imap_fetch
Service	143:TCP
Class	mail
Exploit ID	mdaemon_imap_fetch
CVE(s)	CVE-2008-1358
CCE(s)	
BID(s)	28245
OSVDB(s)	43111
IAVA(s)	
Vendor ID(s)	
Node	Local Node
Excluded?	No

Exploit Severity Levels

The significance of an exploit result is different from that of a vulnerability check. Therefore, different severity levels are used to classify exploit results. The following severity levels are used by SAINT:

- **Remote Administrative Access (Red):** Exploit resulted in the ability to read files or execute commands with the privileges of the administrator or superuser without any prior access.
- **Remote User Access (Brown):** Exploit resulted in the ability to read files or execute commands with the privileges of an unprivileged user without prior access
- **Client Access (Blue):** Exploit resulted in the ability to read files or execute commands after a local user took some action to cause the exploit to proceed.
- **Privilege Elevation (Yellow):** Exploit resulted in elevated privileges on a target of which some level of access was previously available.
- **No Access (Green):** The exploit was unsuccessful.

There are also two additional colored dots used when displaying host details:

● **Services (Green):** A running service was detected, regardless of whether any exploits were attempted.

● **Other Information (Black):** Other information about the target was detected.

Manage

The *Manage* tab provides a single, common interface for managing various aspects of the software, application environment, and users. These features are only available to users with the proper administrative permissions. The following sections describe each capability in more detail.

Users

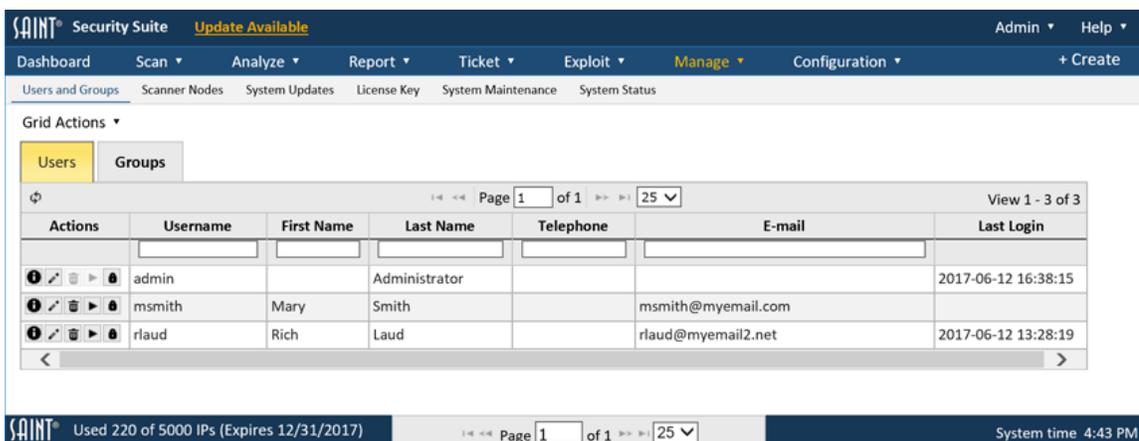
Users are created by the default “admin” user or other users who are in the Administrator's group or have *create user* permission. The following describes the purpose and usage of the admin user, as well as the steps to create and manage locally created users.

Default Admin User

Security Suite provides a default admin user account that has permission to all product features and content. This account is provided to perform system-level activities such as installing and configuring the product; setting up the license key; managing the update process; and performing other high level action such as creating users, groups, and managing permissions. Both Security Suite and SAINTCloud provide support for granular user access control and auditing user activity within the application through assigning individual users to object-based permissions. Therefore, it is recommended that the admin account for your installation (or SAINTCloud account) not be shared by other users and used as a common login, thus eliminating the ability to track and manage individual user activity. If multiple users with full control of the system are desired, those users can be added to the built-in Administrator's group. (See [groups](#) for more information about groups).

Create a User

1. Click the Users and Groups menu option from the *Manage* tab to display the current list of users as shown in the following example:



2. Click *Create User* from the Grid Actions dropdown or select User from the global (+ Create) option at the top right of the page to display the Create User page:

Create User

*Fields with * are required.*

Username *

Authentication Type

Password *

Force Password Change

First Name

Last Name

Address

Telephone

E-mail

Cell Phone

Cell Carrier

Two-Step Verification

Active

3. Enter a unique Username (login ID) for the new user (* required field).
4. Optional – select the Authentication type. The default authentication type, *local*, stores password hashes in the database, and the password is managed through the Manage-Users page. Alternatively, if *Active Directory* is selected, then the user will need to authenticate using his or her Windows domain password. The login name must exactly match the Windows domain login name in order for this option to work. (Note: If the *Active Directory* option does not appear in the drop-down menu, then the system has not yet been configured for Active Directory authentication on the Configuration screen. See [Authentication](#).)
5. If local authentication was selected above, enter a password string for the user account. (* required field).
The user will login with these credentials. If the *Force Password Change* box is checked, then the user will be required to change the password after logging in for the first time.
6. Optional – Enable the desired mode of two-step verification for additional security on the account. See [Two-Step Verification](#) for more information. The user's cell phone number must be specified when using this option.
7. Click *Save*.

The new user account will be created. Use the grid's refresh button to view the new user in the User display grid.

Edit a User

Once a user account has been created, you can now perform routine account updates like changing their passwords or updating their e-mail account, as well as assigning the user to groups or granting them any needed global permissions, and enter individual target hosts (by IP address, subnet, etc.) to further control access to the host environment.

1. Navigate to the Users and Groups page to display the current user list.
2. Navigate to the User or use the search and sort features to locate the user in a large list.
3. Open the Edit User dialog by selecting the user and clicking the *Edit User* (pencil) action on the selected row to display the user management screen, as shown below..

Manage User - user4 ✕

User Info **Group Assignments** Target Assignments Permissions License Key

*Fields with * are required.*

Username *

Authentication Type ▼

First Name

Last Name

Address

Telephone

E-mail

Cell Phone

Cell Carrier ▼

Two-Step Verification ▼

API Token [Create API Token](#)

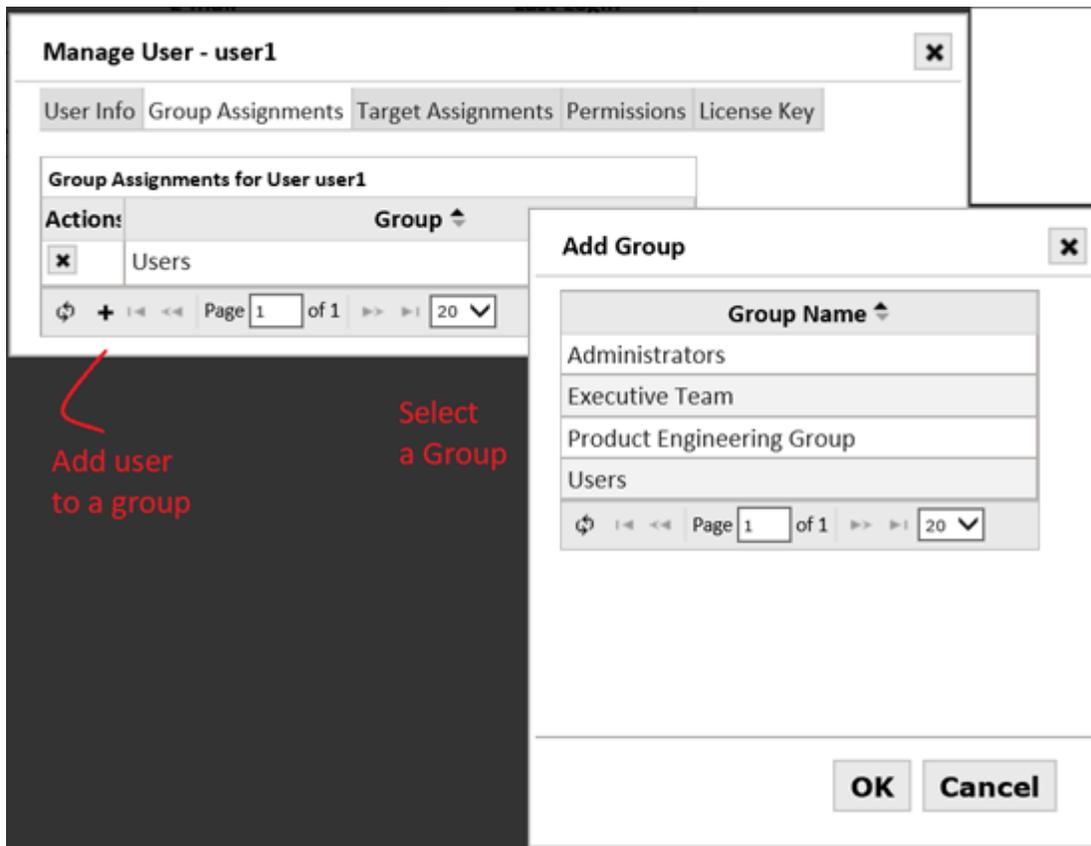
Active

Edit User Information

1. Edit general information about the user from the *User Info* tab.
2. Click the *Change Password* button to expand the form field and expose the Password and Confirm New Password fields.
3. Click *Save* once all changes have been made.

Change Group Assignments

Groups allow you to create a set of users to whom the same permissions can be granted. (See [Groups](#) for more information). Click on the *Group Assignments* tab to find out which groups the user is in or to change the group assignments, as shown below:



To remove the user from a group, from the *Group Assignments* tab, click the *Remove From Group* (X) icon beside the group. To add the user to a group, click the *Add a Group* (+) icon at the bottom of the grid, highlight the desired group, and click *OK*.

Assign Targets to Users

This tab provides the capability to grant user access to specific hosts in the target environment. Leaving this tab blank grants access to any target and leaves target management up to other security mechanisms, like Target Groups. This feature can best be described as a “white list” feature where individual target access is explicitly stated rather than implied. These decisions can be made by individual host IP addresses, space, comma or line-separated lists, target ranges, subnets, CIDR addresses, or even Domain. For example: 192.*, 1.1.1.0-1.1.1.56, 10.0.0.0/24.

1. To create the target assignments, manually enter or copy/paste the target list in the text box provided in the Target Assignments tab.

Manage User - user1 [X]

User Info Group Assignments **Target Assignments** Permissions License Key

Enter space, comma, or line separated lists.
Leave blank to allow any target.

White List:

10.8.0.110-10.8.0.200

Ex: 1.1.1.0-1.1.1.56, 10.0.0.0/24, 10.2.4.8, 10.2.4.9

Assign

2. Click the *Assign* button once the list is complete.
3. The system will refresh to display the “Target Assignments Saved” message.
4. Close the dialog box to return to the User management main page.

The user will now have access to the specified targets to execute actions in the system as specified by the assigned Role(s).

Assign Permissions to Users

To grant the user the ability to perform certain actions on the system, or the ability to modify specified configuration settings, click on the Permissions tab. (Note that object-based permissions, such as allowing the user to modify a target group or to view a report, are applied per object, and therefore don't appear here. See [Object-based Access Controls](#) for more information.)

Global Permissions

Global permissions give users the ability to perform certain actions system-wide. To grant a global permission, check the corresponding box and click on *Save Changes*.

Manage User - user1
✕

User Info

Group Assignments

Target Assignments

Permissions

License Key

▼
Global Permissions

Permissions for user1	
Create user	<input type="checkbox"/>
Exploit	<input type="checkbox"/>
Modify key	<input type="checkbox"/>
Maintenance	<input type="checkbox"/>
Restart	<input type="checkbox"/>
Issue AoSC	<input type="checkbox"/>
Resolve disputes	<input type="checkbox"/>
Quarantine	<input type="checkbox"/>
Create job	<i>This is controlled per node. See scan nodes</i>

Save Changes

▶
Configuration Permissions

Global permissions include:

- **Create User** – Allows the user to create users and groups.
- **Exploit** – Allows the user to run exploits, penetration test jobs, and related actions, if the user also has the required permissions on the appropriate object, e.g., node or job.
- **Modify Key** – Allows the user to configure the license key and SAINTexpress plug-in.
- **Maintenance** – Allows the user to perform the system functions found on the System Maintenance screen, including taking backups and viewing logs.
- **Restart** – Allows the user to restart the system. On appliances, it also allows the user to shut down or restart the appliance.
- **Issue AoSC** – Allows the user to approve or deny requests for Attestations of Scan Compliance. (See [PCI Attestations](#).) Only users who are certified ASV employees should have this permission. (This permission is only used if Attestation of Scan Compliance is enabled in the license.)

- **Resolve disputes** – Allows the user to approve, deny, or request more information for a dispute. (See [Resolve a Dispute](#).) If the dispute feature is being used in conjunction with ASV scanning, only users who are certified ASV employees should have this permission.
- **Quarantine** – Allows a user to view the Quarantine asset action option for vulnerability results in the *Analyze* tab, and choose to send a quarantine message to Cisco Identity Service Engine (ISE). Note that this action option and communication is only supported for Security Suite installations pre-configured (Security Configuration options and Cisco ISE integration configurations) to provide for security communication between the two products.
- **Create Job** – Allows the user to create scan jobs for scanner Nodes the user has permissions to. Selecting this option will transfer you to the Manage Nodes page to setup scan permission for the applicable scanner(s).

Configuration Permissions

Click on the *Configuration Permissions* bar to expand the Configuration Permissions panel. These permissions allow a user to modify the values contained in the corresponding configuration setting categories, either globally or per scan. If the checkbox in the “modify globally” column is checked, then the user is allowed to change the global default values, which will be applied in every scan job for which the corresponding setting hasn’t been overridden. (See [Configuration](#).) If a checkbox exists in the “override per scan” column and it is checked, then the user is allowed to override the default values when creating scan jobs. (See [Advanced – Step 4](#).) The bold categories are top-level categories which include the categories below it. Click on *Save Changes* at the bottom of the panel to save your changes.

Groups

A *group* is a set of users to which permissions can be granted as a single unit. There are several benefits to using groups. Firstly, granting permission to a group only involves a single step, whereas granting the same permission to multiple users individually involves more effort. Secondly, groups allow new users, or users who change job functions, to be granted an existing set of permissions simply by adding the user to an existing group which already has the appropriate permissions for that user’s job function.

Built-in Groups

Even before you create any groups, there are three default groups:

- *Administrators* group – This is a special group which gives all of its members full control of the entire system and all objects. This group allows there to be multiple administrators without requiring all of them to share the one built-in *admin* user.
- *Users* group – All users are automatically assigned to this group when they are created (unless the user was created by a non-administrator who was not a member of this group). This provides a convenient way to share objects (such as reports) with all users if desired.
- *Analysts* group – This group gives its members view access to all scan results in the system, but nothing more. This group is useful for easily allowing a user to perform analytics and reporting, without allowing the user to create jobs or run scans. The *Scan* tab on the top-level menu bar is hidden from users in this group.

Create a Group

1. Click the *Groups* menu option from the *Users and Group* tab to display the current list of groups as shown in the following example:

Actions	Group ID	Group Name	E-mail	Address	Telephone	Last Updated	Last Updated By
	admingroup	Administrators					
	engineering	Product Engineering Group	engineering1@mycompany.com	Build 23	866-000-1111	2017-06-16 11:54:14	admin
	exec	Executive Team	officehq@mycompany.com	Suite 11100, 12342 Tower Dr, NY, NY	800-111-1111	2017-06-16 11:56:15	admin
	usersgroup	Users					

2. Click the New Group (+) option at the bottom of the grid to display the Create Group page:

Create Group

*Fields with * are required.*

Group ID *

Group Name

Address

Telephone

E-mail

3. Enter a unique Group ID and Group Name.
4. Use the remaining fields to enter any other information you wish to store to identify the group.
5. Click *Save*.

Edit a Group

Once a group has been created, you can change the group's information or add members to the group as follows:

1. Click the *Groups* tab in the *Users and Groups* page to display the current group list.
2. Navigate to the desired group, or use the grid's search and sort features to locate the group in a large list.
3. Open the *Edit Group* dialog by selecting the row and clicking on the pencil icon on the row or at the bottom of the grid.

The screenshot shows a web interface titled "Manage Group - engineering" with a close button (X) in the top right corner. Below the title is a tabbed interface with the following tabs: "Group Info", "Members", "Group Assignments", "Target Assignments", "Permissions", and "License Key". The "Group Info" tab is active. Below the tabs, a note states "Fields with * are required." The form contains the following fields:

- Group ID * (required): engineering
- Group Name: Product Engineering Group
- Address: Build 23
- Telephone: 866-000-1111
- E-mail: engineering1@mycompany.com
- API Token: Create API Token

At the bottom of the form is a "Save" button.

The *Group Info* tab can be used to edit the group's name and identifying information. The *Permissions* tab can be used to edit the group's global permissions and configuration setting permissions. (See [Assign Permissions to Users](#) for more information.) The *Target Assignments* tab can be used to assign target ranges which group members are allowed to scan. (See [Assign Targets to Users](#) for more information.)

Note that groups can be members of other groups. In that case, members of that group inherit not only the permissions of that group, but also the permissions of any groups of which that group is a member. This allows creation of groups in a multi-level hierarchy. The *Group Assignments* tab can be used to add the group to other groups. (See [Change Group Assignments](#) for more information.)

User Groups can also have their own License Key. This license key design can be optimal for organizations that have disparate operating budgets, license type requirements (metered versus per IP), or for managed service organizations that license the product for multi-tenant deployments.

Adding Members to a Group

To add members to a group, click on the *Members* tab, and then click on the *Add a Member (+)* icon at the bottom of the grid. Use the paging buttons, sort buttons, and search boxes to locate the desired users and groups if necessary, and check the box beside those users and groups. Then click *OK*.

Note: members can also be added to or removed from groups by editing the member rather than editing the group. See [Change Group Assignments](#) for more information.

Removing Members from a Group

To remove members from a group, click on the *Members* tab; locate the users and groups to be removed, and either click on the *Remove From Group (X)* icon on each row you wish to remove, or select multiple rows and then click the *Remove From Group (X)* icon at the bottom of the grid to remove multiple members at once. Click *OK* at the prompt to confirm.

Assets

The capabilities in the asset management module enable users to view, search, sort, tag, assess and report on hosts scanned by SAINT's scanner(s). As shown below, asset management is segregated into three main collections of data: Assets; Asset Tags; and Target Groups.

The screenshot displays the SAINT Security Suite interface. At the top, there is a navigation bar with tabs: Scan, Analyze, Report, Ticket, Exploit, Manage, and Configuration. Below this, a secondary navigation bar lists various system components: Users and Groups, Assets, Agents, Scanner Nodes, System Updates, License Key, System Maintenance, and System Status. The 'Assets' tab is currently selected. The main area shows a grid of asset records. The grid has columns for Actions, Node Name, Agent Name, IP Address, Hostname, OS Class, OS Type, and Tags. Two records are visible:

Actions	Node Name	Agent Name	IP Address	Hostname	OS Class	OS Type	Tags
[Info] [Edit] [Lock]	Local Node		10.7.0.34	10.7.0.34			[X] [Hostname] 10.7.0.34 [X] [CPE] cpe:/o:microsoft:windows_10
[Info] [Edit] [Lock]	BMNT#1		10.20.0.189	rscnb018.example.com	WINDOWS	Windows 10 Pro	[X] [OS Type] Windows 10 Pro [X] [Hostname] rscnb018.example.com [X] [Netbios Name] RSCNB018 [X] [Production] No [X] [Owner] Steve

With the applicable role-based permissions, you can sort this list, perform column searches, see detailed information about a record in the display, or take other actions such as

adding/removing columns, refreshing the display to dynamically update the content with any new content since you entered the grid, and take other actions related to creating, editing, and deleting content. The following describes these features in more detail.

Assets included in this data grid represent hosts that have been discovered and/or assessed by the scanning engine. By default, post scan processes create system tags for the following system-provided Tag Names:

- Asset ID – unique ID stored in the database for the asset
- Node – this value is the SAINT scanner that identified the asset. For single scanner environments, this is typically the “Local Node”. For Multi-scanner environments, this value will be the Local Node or one of the distributed scanners connected to the central Manager.
- IP Address – IP address (supports both IPv4 and IPv6)
- CPE – Common Platform Enumerator
- Host Name – if collected by any scan associated with this asset
- MAC Address – if collected by any scan associated with this asset
- NetBios Name – if collected by any scan associated with this asset
- OS Type – Operating System and Version (example: Windows 7 SP1)
- OS Class – Operating System vendor classification (examples: Windows; Red Hat)

AWS Asset Tagging – If the SAINT Agent is installed on an AWS asset, then its metadata will be collected and stored as asset tags. This data includes aws-vpc, aws-subnet, aws-size, aws-id, and aws-zone.

Add Asset Tags to Assets

Scanned hosts stored in the database can be ‘tagged’ with descriptive values to enhance the effectiveness of viewing, analyzing, assessing and managing these hosts as business assets. Asset Tags are based on a Key-Value pair concept. For example, each tag will have both a Key (example: Location) and at least one Value (example: Dallas). The following are examples to better illustrate this concept:

- Criticality=High
- Criticality=Medium
- Criticality=Low
- Location=Data Center
- Location=Home Office

- Function=Accounting
- Function=Shopping Cart
- Function=Email Server
- System Owner=John Smith
- Business Cost=\$20,000,000

Tag a Single Asset

The following illustrates how a single asset can be tagged with pre-existing asset tags or creating new one's dynamically as they are being associated with the asset:

1. Navigate to the *Assets* tab under the *Assets* page.
2. Click on the *Edit* (pencil) action button for the asset to be tagged.

An Asset Tag Assignment dialog will be displayed, as shown in this example. This dialog will display existing Tag Names and Values (example: IP Address=10.8.39.188), and the Data Type associated with the tag (default: String) as well as a few blank rows to dynamically apply other existing tags or create and tag the asset with new tags without having to navigate to the Asset Tags data grid and create them first. Note that some asset tags (for example: Node, Hostname, ID Address, OS Class and OS Type) are generated by the scanner when they are scanned and are “read only.”

Asset Tag Assignment ✕			
Tag Name	Data Type	Tag Value(s)	
(Line or pipe separated list)			
Criticality	STRING	High	⬆ ⬇ ⬆
Location	STRING	Bethesda	⬆ ⬇ ⬆
Function	STRING	Accounting	⬆ ⬇ ⬆
Business Cost	NUMBER	2,000,000	⬆ ⬇ ⬆
	STRING		⬆ ⬇ ⬆

Apply an existing Tag:

- I. Select a Tag Name in a blank Tag Name drop-down menu. (Example: Location)
- II. Select a Tag Value in the Tag Value(s) drop down menu for this Tag Name. (Example: Baltimore)

To create a new Tag Name and Value and apply it to the Asset:

- I. Enter the Tag Name directly in a blank row under the Tag Name. (Example: Owner)
- II. Select the Data Type applicable to the tag. (default: String)
- III. Enter a Tag Value to be associated with the Tag. (Example: SOC)

Remove a Tag:

- I. Click on the down arrow for the Tag Name or Tag Value that you wish to remove.
- II. Select the blank row in the drop down menu list.

3. Save the change to tag the asset and new tags into the Asset Tag table.
4. Close the assignment dialog to see:

Actions	IP Address	Asset ID Hash	OS Class	OS Type	Tags
	10.8.0.251	88e8ea908bd918a34965859815626c24	LINUX	Ubuntu 14.04	[Criticality] High [Location] Bethesda
	10.8.0.250	09b45c147f5553c279a8e3b6216f6f65	LINUX	Ubuntu 14.04	[Criticality] Medium [Location] Baltimore [Owner] SOC
	10.8.0.240	a2656ad486f22cb62c51cf5eb646ab50	WINDOWS	Windows	[Criticality] High [Location] Rockville

Tag Multiple Assets from a Single Operation

Adding Tags in Bulk

Multiple assets can be tagged through a single operation by clicking the *Asset grid's Grid Actions > Assign Asset Tags* option. The following describes how to apply tags in bulk through this operation:

1. Navigate to the *Assets* tab on the *Assets* page.
2. Click on the *Grid Actions > Assign Asset Tags* option. The following *Bulk Asset Tag Assignment* dialog will be displayed:

Tag Name	Data Type	Tag Value(s) (Line or pipe separated list)
<input type="text"/>	STRING	<input type="text"/>
<input type="text"/>	STRING	<input type="text"/>
<input type="text"/>	STRING	<input type="text"/>

Apply to Assets: ?
[Open Asset Filter](#)

3. First, select the Tag Name(s) and Tag Value(s) you wish to assign to the collection of assets. This can be done by clicking on each Tag Name and Tag Value drop-down lists to select existing Tags; or by manually entering new Tag Name(s) or Tag Value(s) directly in-line in a blank row, if the required tag has not yet been created.
4. Ensure the “Apply to” action is shown in the cell above the *Save* button.
5. Enter the asset information in the Assets field to identify assets to be tagged.
 - i. Use the Help (?) option to the right of the Assets field for assistance on acceptable identifiers, to include, but not limited to: IP, Hostnames, IP ranges, CIDR blocks, Subnets, etc.
 - ii. Use the “Open Asset Filter” option to select existing assets based on system-defined and custom tags. In the following example, we will use this feature to identify three hosts, by IP address, that we wish to tag as being owned by the Security Operations Center (SOC). Click *OK* to add the assets and close this dialog.

Tag Name	Data Type	Tag Value(s) (Line or pipe separated list)
Owner	STRING	SOC
	STRING	
	STRING	

Add Row

Apply to Assets: 10.8.0.148,10.8.0.150,10.8.0.162 ?
[Open Asset Filter](#)

Save

6. Verify the Asset list and Tag Assignment values and Click *OK* to assign all tags to the collection of assets.

7. Close the dialog and view the resulting tags in the Assets table.

These tags will now be applied to the asset and available for tracking for existing and future scan results.

Removing Tags in Bulk

Just as tags can be assigned in this bulk assignment process, they can also be removed in the same manner. Use the steps defined in the [Adding Tags in Bulk section](#), except you will change “Apply to” to “Remove from” in Step four. This operation will use the Tag and Asset criteria defined in the Bulk Asset Tag Assignment dialog to execute the task in a single operation, as opposed to manually removing tags individually at the Asset row level by clicking on each Asset Tag’s X (delete) option.

Asset Tags

The Asset Tag data grid, as shown below, provides a complete list of all tags in the system, as well as a count of the total number of assets currently tagged with each value.

The screenshot shows the SAINT interface with the 'Asset Tags' tab selected. The table below represents the data shown in the interface:

Actions	Tag Name	Tag Value	Tag Type	# Assets	Created Date
[Edit] [Delete] [Lock]	Owner	SOC	STRING	4	2017-07-03 13:08:54
[Edit] [Delete] [Lock]	Location	Bethesda	STRING	6	2017-06-30 08:12:37
[Edit] [Delete] [Lock]	Location	Reston	STRING	2	2017-06-30 08:12:37
[Edit] [Delete] [Lock]	Location	Baltimore	STRING	4	2017-06-30 08:12:37
[Edit] [Delete] [Lock]	Location	Rockville	STRING	3	2017-06-30 08:12:38
[Edit] [Delete] [Lock]	Criticality	High	STRING	8	2017-06-30 08:12:37
[Edit] [Delete] [Lock]	Criticality	Medium	STRING	4	2017-06-30 08:12:37
[Edit] [Delete] [Lock]	Criticality	Low	STRING	3	2017-06-30 08:12:37

Add Asset Tag

New asset tags can be created by navigating to *Grid Actions > Create Asset Tag* option from the Asset Tags tab to display the Asset Tags creation form:.

The 'Create Asset Tags' dialog box contains the following table structure:

Tag Name	Data Type	Tag Value(s) (Line or pipe separated list)	Tag Value(s) From File
<input type="text"/>	STRING	<input type="text"/>	<input type="button" value="Browse..."/>
<input type="text"/>	STRING	<input type="text"/>	<input type="button" value="Browse..."/>
<input type="text"/>	STRING	<input type="text"/>	<input type="button" value="Browse..."/>

Buttons: Add Row, Save

As shown in the dialog, you can add a completed new Tag Name-Tag Value combination, or you can select an existing Tag Name and add additional values to it. The following example includes adding a New Tag Name: Function, as a Data Type=String, and add 3 values, as well as adding a Tag for Business Availability. Note this can be done direct “in line” in each cell (as shown in these examples) OR you can upload a text file with the values listed in a line separated list. A text file list can save a lot of time, for example, if you have hundreds of values, as in the case of asset owners or locations.

Tag Name	Data Type	Tag Value(s) (Line or pipe separated list)	Tag Value(s) From File
Function	STRING	Accounting Engineering Sales	Browse...
Availability	STRING	High Medium Low	Browse...
	STRING		Browse...

Add Row
Save

1. Click *Add Row* if you wish to add additional tags before saving.
2. Click *Save* to save your tags.
3. Close the dialog window to view the new Asset Tags.

Edit Asset Tag

1. Navigate to the Asset Tags tab under Manage Assets.
2. Click on the *Edit* (pencil) action button on an Asset Tag.
3. You will have the option to edit the Tag Name or Tag Value for the selected tag.
4. Edit the Name(s) and Tag Value(s) as needed.
5. Click *Save*.
6. Close the dialog window to save your changes.

Delete Asset Tag

A user can choose to delete the entire Name=Value collection by choosing to delete a Tag Name or choose to delete just the record associated with a Tag Name's Value.

1. Navigate to the *Asset Tags* tab under Assets.
2. Click on the *Delete* (trash can) action button on an Asset Tag.
3. You will have the option to Delete the Tag Name or Tag Value for the selected tag.
4. The system will display a message to confirm the delete action.
5. Click *OK* to accept and delete the selected tag. Click *Cancel* to exist the process and retain the tag.

Note: Deleting an asset tag does not impact current or future scan results. However, tag values will be removed from reference to any associated scan Jobs or results. For example, if a previous scan contained assets associated with Location=Dallas and the Location tag is removed, then

scan results will no longer be associated with this location. Also, if a Scan Job was configured based on the tag that is being deleted, then that Job will no longer be associated with a Tag or their associated assets. Those jobs will need to be edited, as needed, if the intent is to reuse/re-run them in the future. **A recommended BEST PRACTICE is to retain Asset Tags (not delete them) once they have been associated with scan Jobs and scan Results, unless the tags, jobs and results have no future value. This will ensure existing Jobs work as configured and any scan results continue to be associated with the tag(s), even if they are historic in nature.**

Asset History

SAINT Agents allow us to track what has changed on the asset, such as its IP, hostname, MAC address, etc.

Agent Name	Date Changed	Old IP	New IP	Old Mac	New Mac	Old Netbios	New Netbios	Old OS Type
BMNT#1	2018-11-08 17:41:08	10.20.0.189	10.20.0.189	0A:00:27:00:00:15	00:00:00:00:00:00	RSCNB018	RSCNB018	Windows 10 Pro
BMNT#1	2018-11-08 17:39:47	10.0.0.147	10.20.0.189	0A:00:27:00:00:15	0A:00:27:00:00:15	RSCNB018	RSCNB018	Windows 10 Pro

To view all assets history, navigate to Manage > Assets and click on the *Asset History* tab. When a change occurs, the time is noted in the *Date Changed* column. The old value is highlighted in blue and the new in green. Unchanged fields are left in white. To view the history of a single asset, use the filter tool bar at the top of each column, or go to Manage > Agents and use the history button in the *Actions* column.

Agents

SAINT Agent Overview

Note: The features described in this section require Agents to be enabled in your license key, and the [Agent Server](#) to be enabled in the System Options.

The SAINT Agent is a client-side service which is used to assess a system and report vulnerabilities, configuration issues, and information back to SAINT Security Suite. The collected data can then be analyzed and used within the application the same way it would be when performing remote scans. Some of the benefits of the SAINT Agent are:

1. No credential management or authentication issues

SAINT Security Suite

2. Asset tracking
3. Targets can be scanned the moment they connect within a given assessment duration

The SAINT Agent is currently supported on the following operating systems:

- Windows 7+
- *Mac OS X 10.11+
- *Ubuntu 15.04+
- *Debian 7+
- *Red Hat 7+
- *CentOS 7+
- Amazon 1 and 2

** Indicates that earlier versions can be used if the python version on the target is \geq 2.7.9*

Managing Agents

From the Manage -> Agents tab, SAINT Agents can be monitored, configured, and troubleshooted. This is also where SAINT Agent installers are available for download.

Actions	Name	Hostname	Connection Status	Agent Status	IP Address	External IP Address	Version	System Type
   	rscnb018.example.com	rscnb018.example.com		Active	10.0.0.147		1.0.6	Windows 10 Pro

The agents grid will display all scan agents that have connected to the server at least once. The grid displays information about assets such as their SAINT Agent name, hostname, IP, external IP, system type, as well as each Agent's connection status and registration status.

The following actions are available from the grid's *Actions* column.

- a. View – Lists all the information associated with the Agent.
- b. Edit – Allows you to change the name, registration status, and attach a comment to the Agent.

- c. History – Brings up a list of everything that has changed on the system such as the IP, hostname, MAC address, etc.
- d. Log – If connected, the scanning and update log from the Agent can be downloaded.
- e. Remote Configure – From here, the remote logging level and max processes can be set on the Agent. This can be done in bulk from the Grid Actions menu as well. Agents do not have to be connected when these are set -- they will be set the next time a connection is made.
- f. Permissions – Control who has access to the Agent.

Agent Naming Rules

The screenshot displays the 'Agent Naming Rules' configuration page in the Security Suite. The interface includes a navigation menu at the top with options like 'Users and Groups', 'Assets', 'Agents', 'Scanner Nodes', 'System Updates', 'License Key', 'System Maintenance', and 'System Status'. Below the navigation, there are tabs for 'Agents', 'Agent Naming Rules', and 'Agent Installers'. The main content area shows a table of naming rules. In the first screenshot, the 'Prefix' column contains the value 'BMNT', which is circled in green. The second screenshot shows the 'Name' column containing 'BMNT#1', also circled in green, indicating the result of applying a naming rule to an agent's hostname.

Agents are named using their hostname by default. Rules can be specified to change this behavior. Rules are created by using assignment criteria such as IP, hostname, system type, and asset tags. By clicking on *Apply All Naming Rules* from the *Grid Actions* dropdown, each rule is applied to matching agents based on the application method:

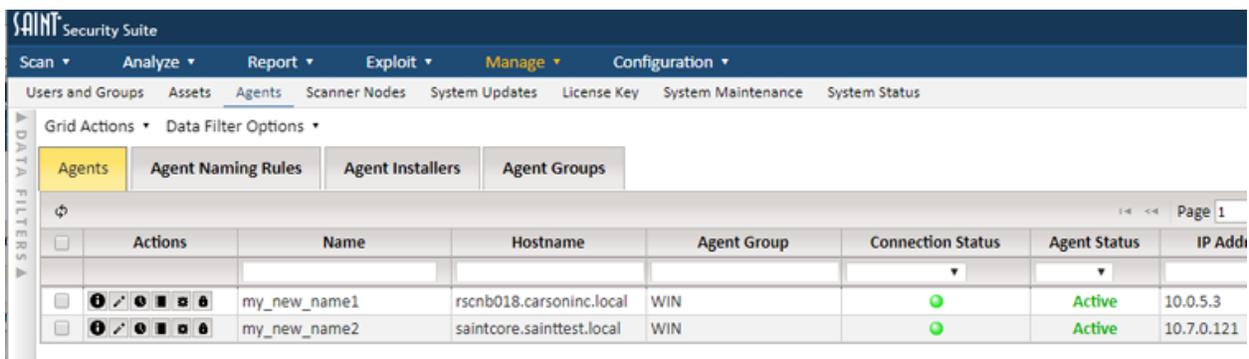
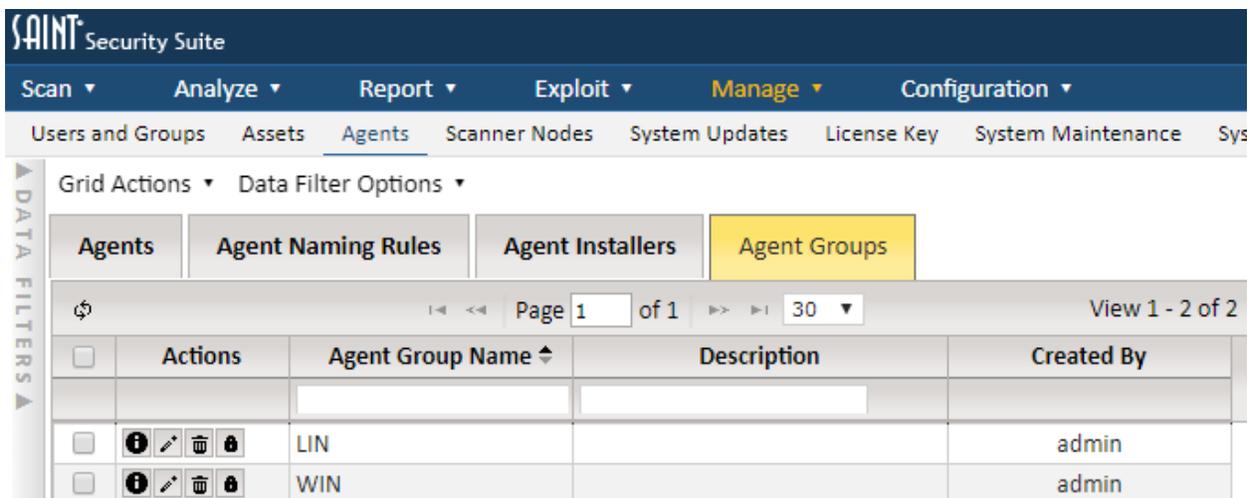
- **Overwrite:** Hostname is overwritten with the given agent name and a unique #N suffix.
- **Prepend:** hostname is prepended with the given agent name.
- **Append:** hostname is appended with the given agent name.

The default names can be restored by clicking on *Reset Agent Names to Hostname* from the *Grid Actions* dropdown.

Agent Installers

The *Agent Installers* tab contains the various installers for different platforms. Note that it is important to download the installer with the correct architecture for Windows, as installing the 32-bit version on a 64-bit machine will cause certain checks to run improperly.

Agent Groups and Permissions



Agent groups can be used to specify the location which an agent resides. This field is configurable at agent installation time and may also be set through the GUI after an agent connects. For example, if you have a set of agents at client A and client B, this field could be used to distinguish them and make searching much easier.

Agent groups also make permission handling much easier. All permissions assigned to a given agent group, also apply to all the agents in that group.

Agent Registration

The number of agents currently registered can be found at the bottom of the UI.



The usage can be decreased by using the edit button and setting the Agent to *Retired*. Agents can be unretired by using the edit button and setting the Agent to *Active*. Only agents that are in the *Active* state can connect and perform scans.

Scanner Nodes

Every installation comes bundled with at least one scanning engine, called a scanner ‘node’. The default scanner node connected to the Manager, and part of the default installation, is called “Local Node”, as shown below. Scanning capability can also be extended for scanning remote locations or large-scale environments by connecting multiple scanner nodes to the manager. For example, deploying scanners inside of multiple subnets, assigning scanning permissions to groups of users to individual scanners, and enterprise-level scalability and performance by directing scan jobs across multiple scanners (e.g., load balanced scans).

Actions	Node Name	IP Address	Node Status	Connection Status	Description	Location	SAINT Version	Last Connection
<input type="checkbox"/>	Data Center South	10.7.0.120	Active	●	Atlanta Data Center	Peach Tree Parkway	9.0.30	2017-11-08 12:26:11
<input type="checkbox"/>	Data Center North	10.7.0.121	Active	●	Boston Data Center	Commonwealth Avenue	9.0.30	2017-11-08 12:26:12
<input type="checkbox"/>	AWS East Region	10.7.0.122	Active	●	Scan AWS EC2 Instance	AWS East Region	9.0.30	2017-11-08 12:26:11
<input type="checkbox"/>	Local Node		Active	●	SAINT Built-In Scanner		9.0.27	2017-11-08 12:26:01

The following describes the various aspects of deploying and connecting scanner nodes, and managing node information via the Node management user interface.

View Nodes

Scanner node information is provided through a grid interface to assist in tracking licensed scanners, as well as providing ease of use in sorting, searching and updating scanners as the size of your organization grows, even scaling to hundreds of distributed scanners. Note that some information can be edited to meet local needs (see [Edit a Node Record](#)), while other information is created and managed internally by the system. The following describes information generated at node connection time and managed by the system:

- **Node Name** – Logical name/title for the scanner node. The default scanner node installed with all deployments is called “local node”.
- **Host Name** – This value is the host name derived from the node when it receives the connection request. In many cases, this is often the IP address of the node’s host.
- **IP Address** – The IP address of a non-local node; this is stored when the node is installed and configured to connect to the manager.
- **MAC Address** – The MAC address of a non-local node; this is stored when the node is installed and configured to connect to the manager.
- **Node Status** – By default, the local node is connected and “active” when the software is started. Additional scanners can be deployed and connected to the installation acting as the “manager,” and dynamically display whether the scanner is active (available), inactive (not available for use), busy (executing scan activity), or retired (decommissioned and no longer needed).
- **Connection Status** – By default, the Local Node is connected when the system is started. Other nodes are connected at the completion of the installation and startup process, but may show a status of “disconnected” if the node is down or, stopped, being restarted, or otherwise loses a physical network connection to the manager.
- **Description** – A text area to support local requirements for stating how the scanner is being used.
- **Location** – A text area to help describe where the scanner is deployed. For example by country, city, state, building, floor, room, etc.
- **Node Version** – The manager maintains an active record of the current version of SAINT software installed and running on each node. This information is a visual reference to ensure all scanners are up-to-date and in sync with the same software version, scanning engine updates and vulnerability check content. Scanner nodes, which have a version lower than the current manager version, have the version highlighted in **red**. Note that the manager version may also be out-of-date. If the manager version is not current, the top menu bar of the UI will display an “Update Available” message, as well as show this status in the Manage System Updates page.
- **Missing Packages** – Each remote scan node checks its own system for package dependencies upon connecting to the manager. This text area provides information about missing packages on the node. See [Package Dependencies](#) for more information about resolving missing packages.
- **Initial Connection** – The initial connection date is the *datetimestamp* when a node is first installed and connected. This information may be of value as node licensing needs change over time, and administrators need to track node resources over time.

- **Administrator** – A SAINT user that is the primary contact that administers or manages the host or node environment.
- **Last Updated By** – This *datetimestamp* is provided to show when node information has been updated, and is updated automatically whenever an administrator edits node information.
- **Retired Date** – This is the *datetimestamp* generated when a scanner node is de-commissioned and no longer needed.

Installing a Distributed Node

Installing a distributed node is done in much the same manner as a typical installation. However, the start-up process provides steps to configure the installation to be run only as a scanning engine, managed by a separate installation, acting as the central manager. See the [Administrator's Guide – Start-Up Options](#) for details on installation and setup of a distributed node.

Edit a Node Record

Editing node information via the node grid is supported by two methods: 1) in-line field editing by clicking in an editable field; and 2) clicking on the *edit* icon (pencil) on a node record to display an edit node dialog window. The following fields are editable through these methods:

- **Node Name** – The default value for the built-in scanner node is “local node.” This value, as well as other connected nodes, can be edited to help uniquely identify the scanner.
- **Administrator** – This is an optional field to assist in tracking the staff member's, team, organization, etc. that is accountable for administration of the node.
- **Description** – This is an optional text field for adding additional information about the node. For example, to describe the purpose or intended target environment a scanner node is connected to.
- **Location** – This optional text field is for describing where a node is installed.

Restarting and Updating

When software updates are available, the remote/distributed (non-local) scanner nodes should be restarted in order to obtain those updates. You can restart an individual node by selecting the *Restart Scannode* icon (🔄), or select multiple nodes via the checkboxes, then choose *Restart Selected Scanner Nodes* from the *Grid Actions* dropdown menu. The *Restart Scannernode* permission is assigned on a per-node basis.

IMPORTANT – Restarting the local node also restarts the manager. As a result, granting a user permission to restart the local node also grants permission for the user to restart the manager as well.

Package Dependencies

When SAINT is first installed, either as a manager or a node, it checks that all of the software packages required for running SAINT are installed on the system. However, new package dependencies may arise over time as new functionality is added to the product. If one or more remote scan nodes are missing packages, an alert is shown in the header bar of the web interface, and the scan nodes with missing packages are indicated with a red background in the *Missing Packages* column of the scan nodes grid.

When a remote scan node has missing packages, there are three ways to resolve them:

- **Single node package resolution:** Click on the *Packages* button (suitcase icon) for the desired scan node on the scan nodes grid. This action button will open a dialog indicating which packages are missing on the node. In that dialog, click on the *Install Packages* button to install the missing packages, and wait for a response.
- **Bulk package resolution:** Check the box for every desired scan node or check the box on the grid's header bar to select all scan nodes at once. Then choose *Install Packages on Scanner Nodes* from the *Grid Actions* menu. The grid will then be updated periodically as the missing packages are resolved. This is the best option if many nodes have missing packages.
- **Command-line package resolution:** Log into a command shell on each remote scan node and run the following command: `cd /usr/share/saint; sudo scripts/check_deps8`. This will give you a more interactive experience, allowing you to see what is being installed and confirm each step of the installation.

Note that the package dependencies on the local node do not need to be managed as described above, since the local node is part of the manager. Package dependencies for the manager can be checked and resolved on the [System Status](#) page.

Configure System Updates

- **System updates process** – (aka SAINTexpress process) provides configuration and control over the process of checking for and obtaining updates from the SAINT update server whenever the product starts. Select the *System Updates* menu option to display

the current configuration, including the required user name, transmission password and transmission key. Refer to the [Administrator's Guide](#) for more information about setting up and managing the update process.

- **Restart and update the system** – The manual restart process can be optimal for obtaining the latest checks, exploits, and tutorial content immediately whenever updates are available, or to ensure all system updates are in place prior to a mission critical scan such as risk or compliance reporting.
- **Manual updates** – This process is vital for organizations that have off-line environments that cannot be configured to obtain updates via an Internet connection. Users can obtain update files from the mySAINT customer portal from an Internet-connected environment. That file can then be used from the off-line installation to execute updates to ensure the scanning solution remains up-to-date with the latest capabilities and content.

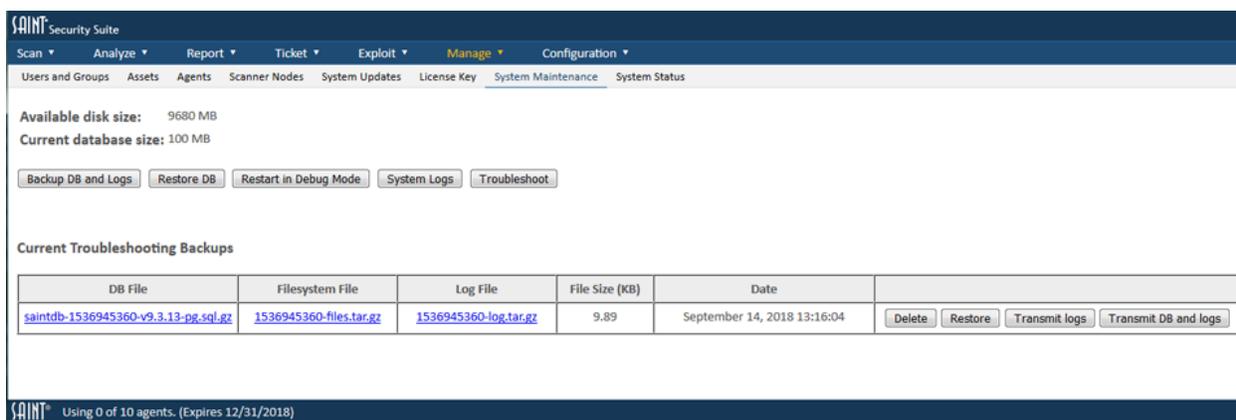
Configure License Key

When installing Security Suite for the first time, one of the first steps is to generate a license key and configure the key in the product. This process also automatically adds the necessary credentials to configure the key credentials, and configures the update process for auto-updates. The License Key page displays the form where you can enter your key into the text box, and displays the current status of your key once it is in place. If you do not already have a key, refer to the Administrator's Guide's section on [How to Obtain a key](#).

Note that this process does require Administrator permissions, as well as the Account credentials provided by SAINT when your account was created.

System Maintenance

System maintenance features are found by selecting the *Manage* tab's *System Maintenance* option. These features enable administrators to perform such actions as data backup/archiving; viewing various system logs; facilitating lower level troubleshooting with SAINT's technical support by enabling debugging to support additional error handling and messaging; transmitting logs and content securely to support, if needed; and viewing system messages directly through the user interface. Each of these features is described in more detail below.



Backup Database and Logs

The backup DB and logs feature provides one-click support for creating a dump file of the current database, any files referenced by the database, and all scan and system transaction log files. A list of prior backups is displayed in the table (as shown above). This capability serves two primary purposes: 1) enables you to store periodic snapshots of your database for archiving in the event of a system failure, or use in an external system; and 2) provides a quick mechanism to create a snapshot of the database in the event you are working with the support team on an issue that requires investigation of the data results. *Note: Only the admin user and members of the Administrators group can download the backup files.*

Restore

The backup files described in the previous section can be used to restore the SAINT database to the state it was in when the backup was taken. This may be useful in the event of data corruption, accidental deletion of data, or migration to a new platform.

There are two ways to restore the SAINT database from backups:

1. Click on the *Restore* button on the desired row of the backups table. This method is useful for restoring the system to a previous backup point on the same system.
2. Click on the *Restore DB* button at the top of the page. This method is useful for restoring the system onto a new platform. Clicking on this button opens a dialog which prompts you to upload two files. The first should be a gzipped SQL command file downloaded from the DB File column of the backup table, with a filename ending in `.sql.gz`. The

second file should be the gzipped TAR file downloaded from the Filesystem File column on the same row of the backup table.

Regardless of which method is chosen, a browser dialog will warn you that restoring the database will entirely delete the current database and confirm that you want to proceed. Then a dialog will inform you that the system needs to be restarted. Click the button to restart the system. It may then take anywhere from a minute to several hours for the system to come back up, since this is when the restoration is taking place. If the restoration fails, the system will usually come up unchanged, depending on where the failure occurred. You can then see the reason for the failure in the manager logs. (See [System Logs](#).) If the restoration succeeds, SAINT will automatically download the database update files needed to make the database schema and static data compatible with the installed software version.

Note: only the admin user and users in the Administrators group may use the restore function.

Delete

Click the *Delete* button in a row of the backups table to delete the files listed in that row.

Restart in Debug Mode

Restarting Security Suite in Debug Mode should only be done upon request from the SAINT support team. This action restarts the manager and turns on debugging/logging actions to capture detailed information about potential system problems that standard logging does not capture. This step is typically requested and monitored when in contact with a support engineer, and is used while reproducing the actions and steps previously taken that resulted in a problem. Once these actions have been completed, the support team will request that you restart the product again, without debugging turned on, by clicking on the *Remote Debug Mode* button displayed while the system is running with debug enabled.

System Logs

This system maintenance feature provides a tool for monitoring the health of the system and troubleshooting issues when they arise. Note that this log information does not automatically constitute system problems or errors in the execution of scans, analysis or reporting. This information may contain a variety of administrative events, regardless of the source. Please provide the messages in this log to SAINT Technical Support, upon request.

System Logs

Grid Actions ▾

Manager ▾ Messages

Page 1 of 894 View 1 - 15 of 13,401

Date/Time	Process ID	Module	Log Level	Message
06/15/17 09:55:17	6791	main	INFO	SAINT Manager (8.14.11) starting up.
06/15/17 09:55:17	6791	main	DEBUG	Registering signal traps and exits.
06/15/17 09:55:17	6791	main	INFO	Registering _modules.
06/15/17 09:55:17	6791	main	INFO	Module 'Datastore' registered.
06/15/17 09:55:17	6791	update	INFO	Checking for software updates...
06/15/17 09:55:27	6791	update	INFO	Checking for data updates...
06/15/17 09:55:27	6791	datastore	WARNING	cannot find common_tcp_ports in tbl_optdefaults
06/15/17 09:55:27	6791	datastore	WARNING	cannot find common_udp_ports in tbl_optdefaults
06/15/17 09:55:27	6791	datastore	INFO	Applying database updates from /usr/share/saint/eSaint/protected/data/000000001.json
06/15/17 09:55:27	6791	datastore	INFO	Applying database updates from /usr/share/saint/eSaint/protected/data/000000002.json
06/15/17 09:56:26	6791	main	INFO	Module 'Update' registered.
06/15/17 09:56:26	6791	main	INFO	Module 'Queue' registered.
06/15/17 09:56:27	6791	crypto	DEBUG	Keys have not been created for this instance.
06/15/17 09:56:27	6791	crypto	DEBUG	Generating RSA Key...
06/15/17 09:56:27	6791	crypto	DEBUG	Generating Certificate...

Used 287 of 5000 IPs (Expires 12/31/2017) Page 1 of 894 System time 12:36 PM

As shown above, the System Logs are broken out into six different types, each available in the dropdown list at the top left of the grid:

- **Manager** – messages produced by the main manager service, including messages related to manager startup and shutdown, connections from nodes, and scan job processing.
- **Scanner** – messages produced by the scanner agent, including messages related to agent startup and shutdown, connection attempts to the manager, and scan activity.
- **Web Server** – log of HTTP requests received by the web server process, and the corresponding responses. (The [verbose](#) option controls how much information is logged.)
- **Application** – messages produced by the web application, such as PHP exceptions and warnings.
- **User** – log of user activity, including logins, password changes, object permission changes, and creation or deletion of users, groups, and scan jobs.
- **SAINTexpress** – log of software update requests and actions.

- **Email** – e-mail messages sent from the software, including scan completion notifications, scan reports, ticket assignment notifications and ticket reminders.

Messages

This capability also provides a quick message search button to display internal system messages, separate from the various logs. As with the log messages, content in this view does not always constitute an error or problem with the operations of the software. However, like the log content, can be a useful tool for the support team to review when investigating an issue.

System Status

The System Status provides an overall summary of the state of the system, from product version number, to the current license information, status of the automated update process (SAINTexpress) and an active status of activity; as well as additional options applicable to system management, such as restarting the system or scan daemon to accept system-level configuration changes.

The screenshot displays the SAINT Security Suite interface. At the top, there is a navigation bar with 'SAINT Security Suite' and 'Update Available' highlighted. Below this is a menu bar with options: Dashboard, Scan, Analyze, Report, Ticket, Exploit, Manage, Configuration, and + Create. The main content area is titled 'System Status' and is divided into two columns: 'System Information' and 'System Actions'. The 'System Information' column lists various system details such as product version, data and content versions, last update time, license key expiration, total and remaining license counts, active users, scan jobs, free disk space, and MySQL data size. The 'System Actions' column provides interactive buttons for 'Check Packages', 'System Updates: Enabled', 'Disable', 'Restart and Update', and 'Manual Update'. A footer bar at the bottom shows the current license usage: 'SAINT Used 287 of 5000 IPs (Expires 12/31/2017)' and the system time: 'System time 12:40 PM'.

The admin user can use this page to quickly see the state of the application, such as the product version number, licensing information and key expiration date.

System Information

This section provides current information about the installation, such as product and content version, license information and status, date of the latest updates, and activity on the system (active users and active jobs). This information can be important for troubleshooting issues as well as determining what will be affected by performing actions such as restarting the system and updating the system as a result of global configuration changes or getting the latest vulnerability checks, exploits and content from SAINT.

System Actions

The System Actions section provides options for checking and validating the status of system dependencies; one-click toggle button to change enable or disable the automated update process; and shortcuts to obtaining system updates or performing manual updates.

Benchmark Scanning

NOTE: This capability is licensed as an additional module to the SAINT Security Suite and SAINTCloud® products.

Contact your Sales representative for information about adding SCAP capabilities to your license.

Summary

The SAINT Security Suite and SAINTCloud provide support to the Security Content Automation Protocol (SCAP) specification as an Authenticated Configuration Scanner (ACS), including the Common Vulnerabilities and Exposures (CVE) option. These SAINT products provide support to SCAP requirements defined for each of these components, as defined in SP 800-126, Revision 2, the SCAP specification, and verified by compliance testing against the Security Content Automation Protocol (SCAP) Version 1.2 Validation Program Test Requirements (NISTIR 7511, Revision 3), dated January 2013 – including updates as of July 2013. These product capabilities are also backwards compatible with SCAP 1.0/1.1 content.

SAINT provides support for open standards languages, enumerations and metrics that currently include XCCDF, OVAL, CCE, CPE, CVE and CVSS, AI, ARF and TMSAD of the specification. SAINT also provides support for DISA STIGs, CIS Benchmarks, and the U.S. Government Configuration Baseline (USGCB) by ingesting valid SCAP-expressed data streams and assessing target configurations against these baselines. This capability also includes support for evaluating SCAP content to scan for compliance, vulnerabilities, and patches using both standalone OVAL definition files and OVAL definitions contained in SCAP-expressed data streams. SAINT solutions

also provide data analysis, links to external authoritative sources of information, policy editing and reporting interfaces to facilitate local policy investigation and analysis. Compliance reporting is provided via pre-defined report templates and custom presentation of output in machine-readable and many human-readable formats, such as HTML, PDF, XML and CSV. Cyberscope report output is also supported using the mandated XML data feed format.

The capabilities provided by this module support scanning for vulnerabilities, patch deficiencies and software inventory, using the vendor-agnostic Open Vulnerability Assessment Language (OVAL), as well as platform security configuration benchmark assessments, using the Extensible Configuration Checklist Description Format (def: <http://scap.nist.gov/specifications/xccdf/>)

The basic components of the SCAP module enable you to choose to scan host targets, using SCAP-compliant policies from the Benchmark Scanning page under the Scan menu; view detailed results from the pages under the Analyze menu; and view SCAP-compliant output from the Report menu, as well as create more general reports using default report templates.

SCAN Menu — Benchmark Scanning

The following shows an example Benchmark scan page. This page displays all supported XCCDF (configuration benchmarks) and OVAL (vulnerability/patch/inventory) platforms available for use.

Actions	Name	Author	SCAP Version	Last Update	Download URL
	USGCB 1.2 Internet Explorer 7	USGCB/TIS	1.2		https://usgcb.nist.gov/usgcb/content/scap/oval510/IE7-2.1.3.1.zip
	USGCB 1.2 Internet Explorer 8	USGCB/TIS	1.2		https://usgcb.nist.gov/usgcb/content/scap/oval510/IE8-1.3.3.1.zip
	USGCB 1.2 Windows 7	USGCB/TIS	1.2	2017-07-25 15:58:48	https://usgcb.nist.gov/usgcb/content/scap/oval510/Win7-2.0.5.1.zip
	USGCB 1.2 Windows 7 Firewall	USGCB/TIS	1.2		https://usgcb.nist.gov/usgcb/content/scap/oval510/Win7-Firewall-1.3.0.1.zip
	USGCB 1.2 Windows Vista	USGCB/TIS	1.2		https://usgcb.nist.gov/usgcb/content/scap/oval510/WinVista-3.0.5.1.zip
	USGCB 1.2 Windows Vista Firewall	USGCB/TIS	1.2		https://usgcb.nist.gov/usgcb/content/scap/oval510/WinVista-Firewall-2.1.0.1.zip
	USGCB 1.2 Windows XP	USGCB/TIS	1.2		https://usgcb.nist.gov/usgcb/content/scap/oval510/WinXP-3.0.3.1.zip
	USGCB 1.2 Windows XP Firewall	USGCB/TIS	1.2		https://usgcb.nist.gov/usgcb/content/scap/oval510/WinXP-Firewall-2.1.0.1.zip
	CyberESI Suspicious Files	CyberESI	1.1		feeds.cyberesi.com/scap/generic/CyberESI-SCAP-SuspiciousFiles.zip
	Microsoft Windows 2008 DC	DISA	1.1		iase.disa.mil/stigs/Documents/u_windows_2008_dc_v6r1.28_stig_benchmark.zip
	USGCB Redhat 5	USGCB/TIS	1.1	2017-07-31 16:59:04	https://usgcb.nist.gov/usgcb/content/scap/USGCB-rhel5desktop-1.2.5.0.zip
	AIX 5.3	DISA	1.1		iase.disa.mil/stigs/Documents/u_aix_5.3-v1r2_stig_benchmark.zip
	AIX 6.1	DISA	1.1		iase.disa.mil/stigs/Documents/u_aix_6.1_v1r3_stig_benchmark.zip

This page provides support for viewing all supported OVAL checks and XCCDF Benchmarks;

features to import the latest content from the authoritative source or from locally developed content; a policy editor to customize and save policies to support local requirements; and output capabilities to support SCAP and Cyberscope reporting requirements.

Keys to Executing SCAP-related Policies

Scanning hosts for compliance with SCAP-related profiles and policies may require modification of configuration settings, firewall rules or starting required services. Refer to the [Target Settings](#) section under *Benchmark Scanning* to learn more and ensure the target network and hosts are properly configured to ensure complete and accurate SCAP assessments.

Running XCCDF Configuration Benchmarks

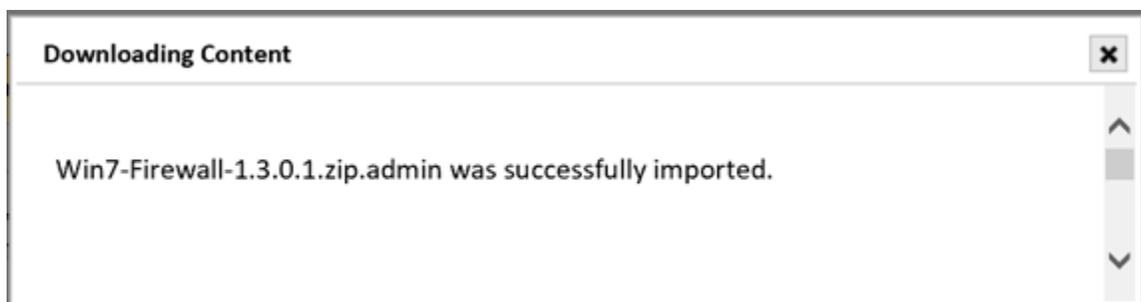


Importing XCCDF Configuration Benchmark Profiles

The Benchmark Scanning page provides two methods to import configuration benchmarks that are in XCCDF format and adhere to the SCAP guidelines for running configuration scans.

Method 1 – Import Latest Content from Authoritative Sources

1. From the Benchmark Scanning page – Configuration grid, click the *Import* (left/right arrow symbol) on the XCCDF Benchmark (i.e., configuration) you wish to import. This process will retrieve the latest content from the authoritative source and make it available for use.
2. The files will be validated, if necessary, and imported into the repository. Info./Warning/Error messages will appear giving details about the progress and status of the file import.



Once the benchmark has been downloaded and passed the validation step, the available profile(s) will be available under the benchmark. All benchmarks that contain downloaded profiles will be identified by a right arrow (>) in the left column of the row,

as shown below:

Actions	Name	Author	SCAP Version	Last Update	Download URL
	USGCB 1.2 Internet Explorer 7	USGCB/TIS	1.2		https://usgcb.nist.gov/usgcb/content/scap/oval510/IE7-2.1.3.1.zip
	USGCB 1.2 Internet Explorer 8	USGCB/TIS	1.2		https://usgcb.nist.gov/usgcb/content/scap/oval510/IE8-1.3.3.1.zip
	USGCB 1.2 Windows 7	USGCB/TIS	1.2	2017-07-31 17:17:04	https://usgcb.nist.gov/usgcb/content/scap/oval510/Win7-2.0.5.1.zip
	USGCB 1.2 Windows 7 Firewall	USGCB/TIS	1.2	2017-07-31 17:12:28	https://usgcb.nist.gov/usgcb/content/scap/oval510/Win7-Firewall-1.3.0.1.zip

- Click the arrow to drill down to view the profiles downloaded from the authoritative source. The following is an example of a profile for the USGCB Windows 7 Firewall benchmark, showing there are 35 different checks for this profile:

Actions	Name	Author	Checks	Pass Threshold	Description
	xccdf_gov.nist_profile_united_states_governme	USGCB/TIS	35	95	

Method 2 – Upload Content from a Local Drive

You may also manually import benchmark content from an external drive by using the *Upload Checklist* option from the Configuration tab's Grid Actions dropdown. Click this option to open up the upload pop-up and locate the applicable file with the *Browse* button.

Upload SCAP content

You can upload any of the following:

- SCAP Data-stream in .zip format
- Data-stream in SCAP 1.2 format (.xml|.zip)

File:

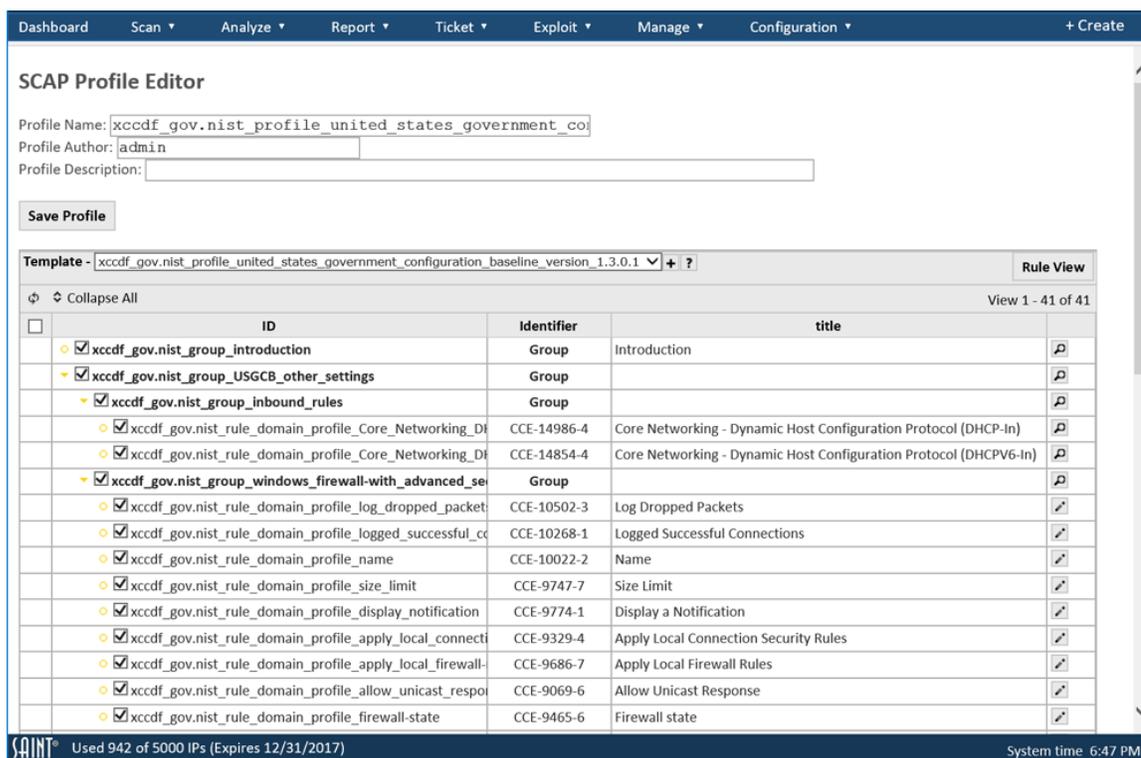
Display Name:

Once you have selected the file, and its path is visible in the *File* field, click the *Upload* button to load the Configuration content into the repository. The files will be validated, as necessary. Info./Warning/Error messages will appear giving details about the progress and status of the file import.

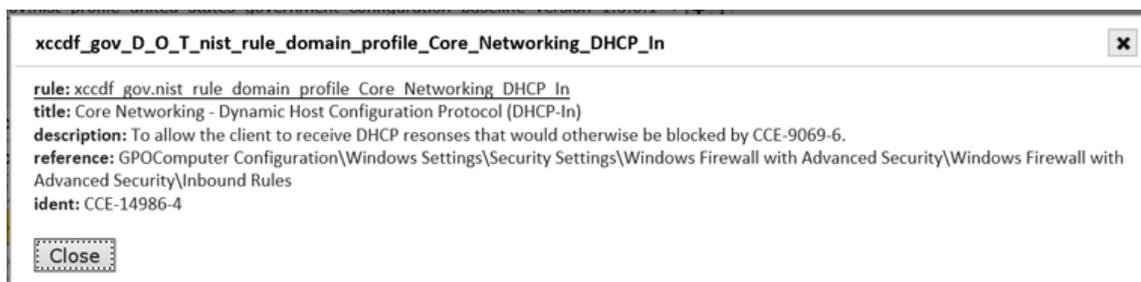
The current configuration profile is now available for analysis, executing an assessment in a scan Job or editing to create a custom profile.

Viewing XCCDF Configuration Benchmark Profiles

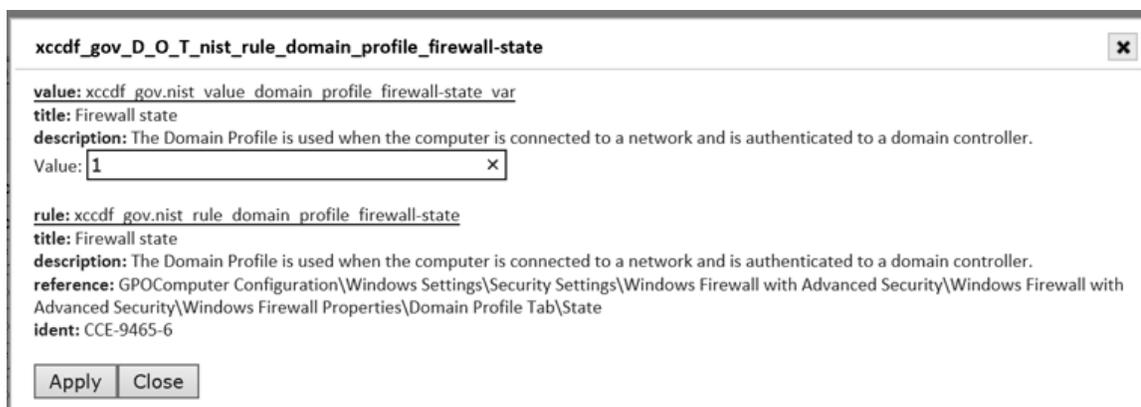
1. Ensure that the applicable benchmark has been imported.
2. Click on the arrow in the left column for the benchmark to show available profiles.
3. Click on the edit option for the profile (pencil icon) or double click on the profile's row. This will bring up a grid containing the selected profile. This view is referred to as the "Full View", and shows specific details about what is being assessed when the profile is run:



This display enables you to view additional information about groups and rules by double clicking a row or selecting the View option (hour glass) for the row.



Rows that contain editable content will provide an Edit option, as well as display an editable "Value" field in the resulting screen, as shown below:



See the section "Configuration Benchmark Policy Editor" for more information on how to edit, save and use customized versions of these profiles.

This content can also be displayed by Rule, by clicking the *Rule View* button in the profile's grid. The following shows the same profile for the USGCB Windows 7 Firewall benchmark as a "Rule View":

SCAP Profile Editor

Profile Name:
 Profile Author:
 Profile Description:

Template:

Page 1 of 1 View 1 - 35 of 35

<input type="checkbox"/>	ID	Identifier	title	
<input checked="" type="checkbox"/>	xccdf_gov.nist_rule_domain_profile_Core_Networking_DHCP_In	CCE-14986-4	Core Networking - Dynamic Host Configuration Protocol (DHCP-In)	<input type="button" value="Run"/>
<input checked="" type="checkbox"/>	xccdf_gov.nist_rule_domain_profile_Core_Networking_DHCPV6_In	CCE-14854-4	Core Networking - Dynamic Host Configuration Protocol (DHCPV6-In)	<input type="button" value="Run"/>
<input checked="" type="checkbox"/>	xccdf_gov.nist_rule_domain_profile_log_dropped_packets	CCE-10502-3	Log Dropped Packets	<input type="button" value="Run"/>
<input checked="" type="checkbox"/>	xccdf_gov.nist_rule_domain_profile_logged_successful_connection	CCE-10268-1	Logged Successful Connections	<input type="button" value="Run"/>
<input checked="" type="checkbox"/>	xccdf_gov.nist_rule_domain_profile_name	CCE-10022-2	Name	<input type="button" value="Run"/>
<input checked="" type="checkbox"/>	xccdf_gov.nist_rule_domain_profile_size_limit	CCE-9747-7	Size Limit	<input type="button" value="Run"/>
<input checked="" type="checkbox"/>	xccdf_gov.nist_rule_domain_profile_display_notification	CCE-9774-1	Display a Notification	<input type="button" value="Run"/>
<input checked="" type="checkbox"/>	xccdf_gov.nist_rule_domain_profile_apply_local_connection_secur	CCE-9329-4	Apply Local Connection Security Rules	<input type="button" value="Run"/>
<input checked="" type="checkbox"/>	xccdf_gov.nist_rule_domain_profile_apply_local_firewall-rules	CCE-9686-7	Apply Local Firewall Rules	<input type="button" value="Run"/>
<input checked="" type="checkbox"/>	xccdf_gov.nist_rule_domain_profile_allow_unicast_response	CCE-9069-6	Allow Unicast Response	<input type="button" value="Run"/>
<input checked="" type="checkbox"/>	xccdf_gov.nist_rule_domain_profile_firewall-state	CCE-9465-6	Firewall state	<input type="button" value="Run"/>
<input checked="" type="checkbox"/>	xccdf_gov.nist_rule_domain_profile_inbound_connections	CCE-9620-6	Inbound Connections	<input type="button" value="Run"/>
<input checked="" type="checkbox"/>	xccdf_gov.nist_rule_domain_profile_outbound_connections	CCE-9509-1	Outbound Connections	<input type="button" value="Run"/>
<input checked="" type="checkbox"/>	xccdf_gov.nist_rule_private_profile_log_dropped_packets	CCE-10215-2	Log Dropped Packets	<input type="button" value="Run"/>
<input checked="" type="checkbox"/>	xccdf_gov.nist_rule_private_profile_logged_successful_connections	CCE-10611-2	Logged Successful Connections	<input type="button" value="Run"/>

Running XCCDF Configuration Benchmark Profiles

SCAP data streams that use a CPE-dictionary will scan only targets that meet the criteria of the dictionary (e.g., Windows 7 targets will not be scanned by a benchmark designed to scan Windows 2012 R2 systems). A range of targets may be used but only the targets meeting the criteria of the CPE-dictionary will be scanned.

There are two methods for running a scan job using an XCCDF benchmark.

Method 1: From the Benchmark Scanning page

1. Once you've imported the benchmark you wish to use, click on the right arrow in the left column to display all profiles.
2. Click the *Run* (right arrow) icon next to the desired profile. This step will launch the Scan Job wizard, pre-defining the policy based on your selection from the Benchmark Scanning page, as shown below:

Create New Job

1 Scan Info
Basic setup and scan policy selection.

2 Targets
Select scan targets.

3 Authentication
Select credentials.

4 Advanced
Additional options.

5 Finish
Create schedules and select ticket rule set.

Step 1: Scan Job Information

Name & Description

Please enter a unique name for this job.
New XCCDF scan job

Please enter a detailed description for this job. (Optional)
scap_gov_nist_comp_USGCB_Windows_7_2_0_5_1_xccdf_xml-xccdf_gov.nist_pro
file_united_states_government_configuration_baseline_version_2.0.5.1

Scan Policy

XCCDF Policy: Scap Gov Nist Comp USGCB Windows 7 2 0 5 1
Xccdf Gov.nist Profile United States Government Configuration Baseline Version 2.0.5.1

Scan Policy Options

Exhaustive Scan ?

Allow Dangerous Tests ?

Previous Next Finish

3. Enter a Name and Description for the Job.
4. Click *Next*.
5. Enter the scan targets in Step 2 of the job wizard.

REMINDER: Target systems must have the following configurations: 1) Remote registry enabled; 2) File and printer sharing enabled; and 3) C\$ share must be read/write/executable

See [Target Settings](#) for additional instructions.

6. Click *Next*.
7. Enter the credentials for the target platforms. For example, Windows Domain Admin credentials for the Windows 7 Firewalls being scanned in our example. This step is mandatory to accurately assess a host with an XCCDF configuration profile.
8. Click *Next*.
9. From the Advanced options, define additional scan configuration settings for this scan. The following are some of the most often used for XCCDF profiles.
 - Authentication sub-tab: ensure NTLMv2 is checked if the targets are using NTLMv2
 - SCAP sub-tab: choose whether to run the “dissolvable” Windows SCAP service; edit the XCCDF Header as preferred.
10. Click *Next*

11. Review and verify the summary of the new job, and define the schedule for the job.
12. Click *Finish* to save the new job and submit it for execution.

The new job will now be present in the Scan status grid under the Scan page:

Actions	Scan #	Job Name	Start Time	End Time	# Targets	# Results	Status	Progress
	21	New XCCDF scan job	2017-07-31 19:12:10		1		Running	30%

You can review the running status and progress of a Job at any time by double clicking on the job and reviewing the Scan status page, or individual running scan activity from the *Scan* grid.

Once the job is complete, this status will be updated and the results available for analysis.

Method 2: From the Job Wizard

1. Click on the global "Create+" option in the upper right corner of the screen.
2. Select the "Job" to launch the Scan Job wizard.
3. Follow the job setup steps for Steps 1 and 2.
4. In Step 1, select the "XCCDF/Configuration" option from the *Select Policy Category* dropdown
5. Select an existing XCCDF profile from the *Select Policy* dropdown
6. Follow the remainder of the job wizard steps in the same manner as defined for [Method 1](#) for initiating scans for a newly imported profile.
7. Review and verify the summary of the new job, and define the schedule for the job.
8. Click *Finish* to save the new job and submit it for execution.

Specifying Two or More Values per Variable

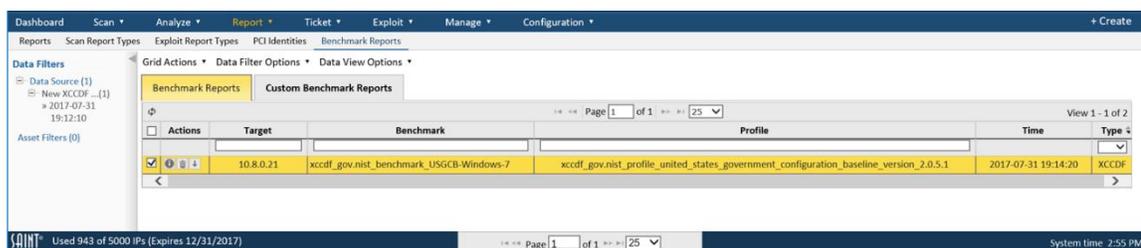
SCAP specifications require configuration benchmarks to provide a mechanism for specifying two or more values for a variable used by one OVAL Definition. XCCDF can be used to run a definition multiple times—each time using a different variable set. For example, two rules are defined in an XCCDF benchmark, along with four values. In the first rule, values one and two are exported. In the second rule, values three and four are exported.

Viewing XCCDF Scan Results

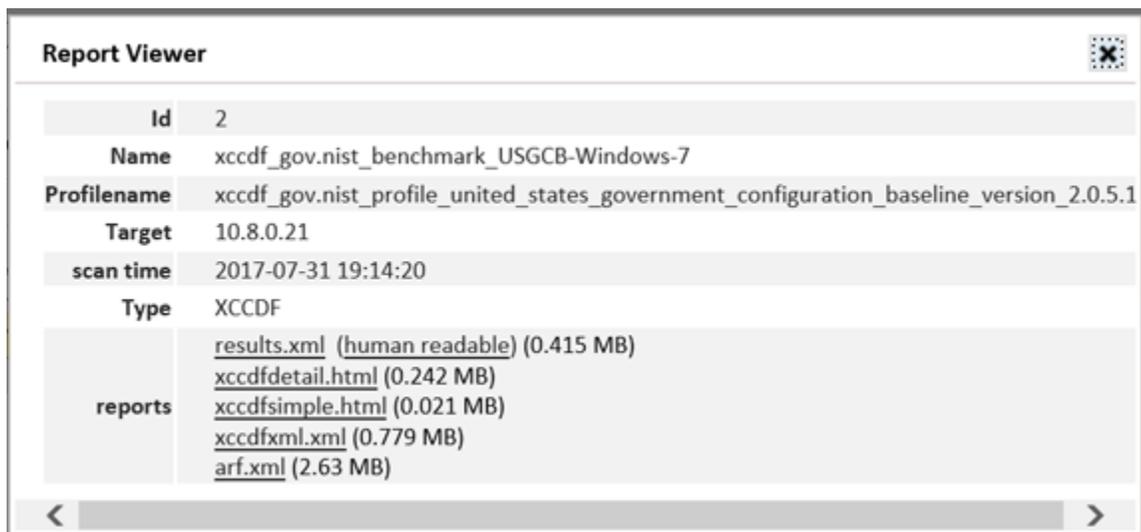
There are two methods for viewing and analyzing scan results based on XCCDF Configuration benchmarks:

Method 1 – View XCCDF Results in SCAP-Compliant Format

1. Navigate to the *Benchmark Reports* page under the Reports Menu.
2. Click on the *Select Data Set* option under the Data Filter Option dropdown to view the current list of scan Jobs and scan results (scans).
3. Select a scan based on an XCCDF profile.
4. Click on the Benchmark Reports tab to view the list of targets assessed for the profile.

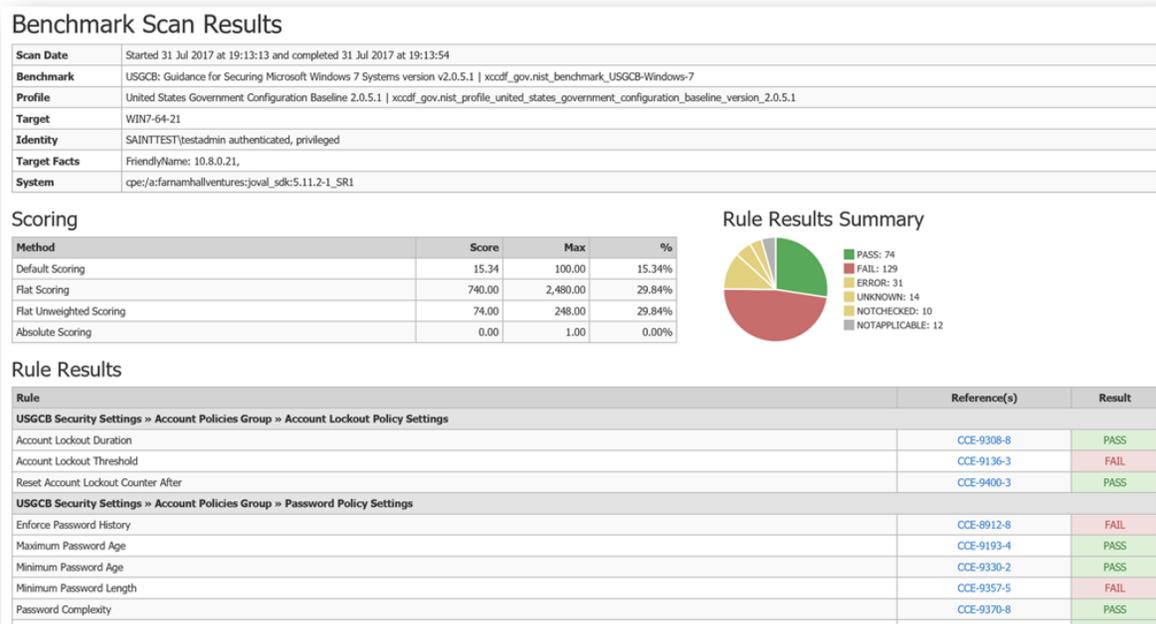


5. Click on the *View Reports* ("i" icon) option to view the current list of SCAP-complaint reports.



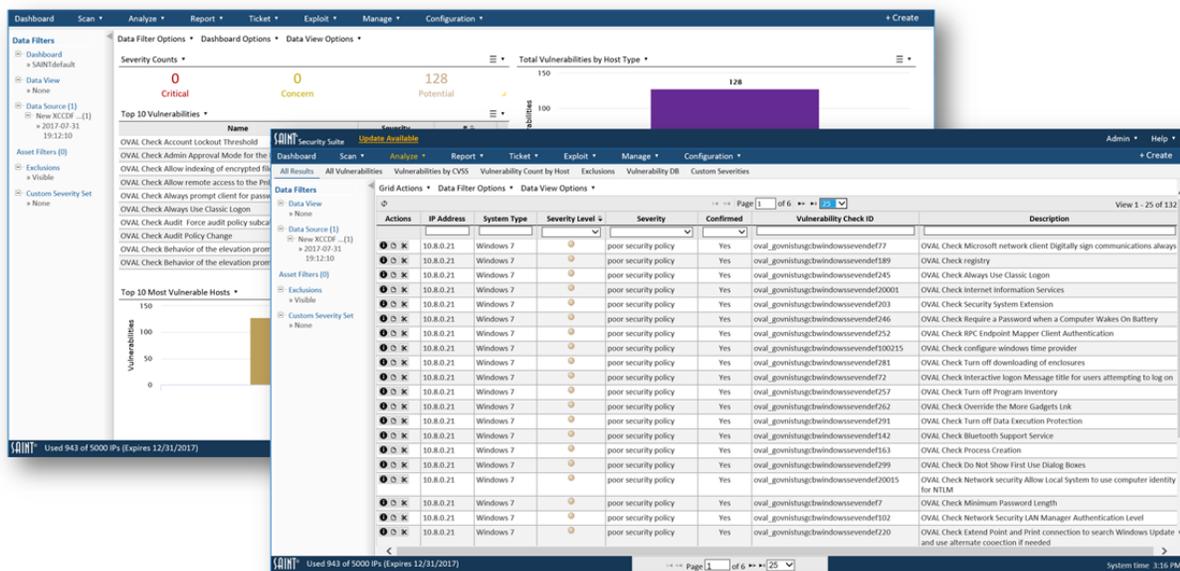
SAINT Security Suite

For example, the following shows a portion of the XCCDF Scan Results report to highlight Pass/Fail results for various policy groups:



Method 2 – Dashboard, Analyze, and Report Tabs

The Dashboard, Analyze, and Report capabilities can be used to investigate and analyze XCCDF content in the same manner as vulnerability scanning, analysis, and reporting capabilities.



Exporting XCCDF Results

Once an XCCDF configuration assessment has been run, results are available for display and export from the Benchmark Reports page. To export XCCDF results:

1. Navigate to the *Benchmark Reports* page.
2. Click on the *Benchmark Reports* tab.
3. If the Target results are not visible in the grid from a prior selection, select a scan based on an XCCDF profile.
4. Once Targets are visible in the data grid, highlight Target(s) to be exported.
5. Click on *Download reports* (down arrow) in the Action column of the target row.

To extract all applicable scan data, produce an export file and launch a dialog window to view/save the content.

6. Click the *Save File* option.
7. Identify the path to save the export file to.
8. Click *OK* to save the file.

NOTE: Human readable oval results.xml file can NOT be viewed in Google Chrome after being downloaded, due to a Chrome security restriction on using local transform files. Firefox, Edge or Safari must be used to view the downloaded file.

Running SCAP Policy Checks

SAINT provides support for a number of today's most often deployed platforms, such as Microsoft Windows, IBM AIX, Red Hat, Cisco and others. The following describes the list of supported test types:



- Unix Schema
 - File Test
 - File Extended Attribute Test
 - Gconf Test
 - Inetd Test
 - Interface Test
 - Password Test
 - Process Test (Legacy and 5.8)
 - Routing Table Test
 - Runlevel Test
 - SCCS Test
 - Shadow Test
 - Sysctl Test
 - Uname Test
 - Xinetd Test
- Independent Schema
 - Environment Variable Test (Legacy and 5.8)
 - Family Test
 - File Hash Test (Legacy and 5.8)
 - LDAP Test (Legacy and 5.7)
 - SQL Test (Legacy and 5.7)
 - Text File Content Test (Legacy and 5.4)
 - Unknown Test
 - Variable Test
 - XML File Content Test
- AIX Schema
 - Fileset Test
 - Fix Test
 - Interim Fix Test
 - No Test
 - Oslevel Test

- HP-UX Schema
 - Getconf Test
 - Ndd Test
 - Patch Test (Legacy and 5.3)
 - Swlist Test
 - Trusted Test
- Linux Schema
 - Dpkginfo Test
 - Iflisteners Test
 - Inet Listening Servers Test
 - Partition Test
 - RPM Info Test
 - RPM Verify Test (Legacy)
 - RPM Verify File Test
 - RPM Verify Package Test
 - SE Linux Boolean Test
 - SE Linux Security Context Test
- Solaris Schema
 - ISA Info Test
 - NDD Test
 - Package Test
 - PackageCheck Test
 - Patch Test (Legacy and 5.4)
 - SMF Test
- Windows Schema
 - Access Token Test
 - Audit Event Policy Test
 - Audit Event Policy Subcategories Test
 - Cmdlet Test
 - DNS Cache Test
 - File Test
 - File Audited Permissions Test (Legacy and 5.3)
 - File Effective Rights Test (Legacy and 5.3)
 - Group Test
 - Group SID Test
 - Interface Test

SAINT Security Suite

- License Test
- Lockout Policy Test
- Metabase Test
- Password Policy Test
- Port Test
- Printer Effective Rights Test
- Process Test (Legacy and 5.8)
- Registry Test
- RegKey Audited Permissions Test (Legacy and 5.3)
- RegKey Effective Rights Test (Legacy and 5.3)
- Service Test
- Service Effective Rights Test
- Shared Resource Test
- SID Test
- SID SID Test
- System Metric Test
- UAC Test
- User Test
- User SID Test (Legacy and 5.5)
- Volume Test
- WMI Test (Legacy and 5.7)
- WUA Update Searcher Test
- Cisco IOS Schema
 - Global Test
 - Interface Test
 - Line Test
 - SNMP Test
 - Tclsh Test
 - Version Test (Legacy and 5.5)
- NETCONF Schema
 - Config Test
- Juniper JunOS Schema
 - Show Test
 - Version Test
 - XML Config Test
 - XML Show Test

- Apple Macintosh Schema
 - Account Info Test
 - Diskutil Test
 - Inet Listening Servers Test (Legacy and 5.10)
 - Nvram Test
 - Plist Test (Legacy and 5.10)
 - Pwpolicy Test (5.9 only)

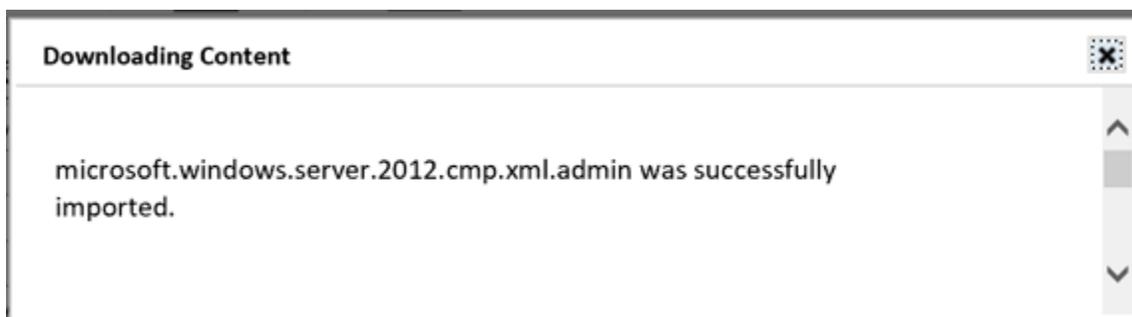
Importing OVAL Checks

To assess host based on OVAL checks, the first step is to import the most current OVAL check content using one of two available methods:

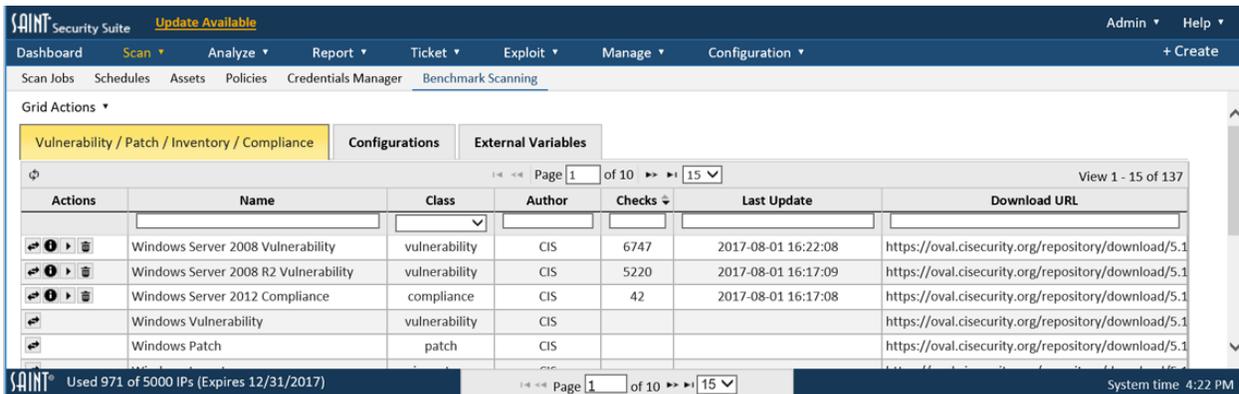
Method 1 – Import Latest Content from Authoritative Sources

From the Benchmark Scanning page – Vulnerability/Patch/Inventory/Compliance tab, click the *Import/Update Checklist* (left/right arrow) symbol on the policy you wish to import. This process will retrieve the latest content from the authoritative source, validate the content, if necessary, and make it available for use.

Info./Warning/Error messages will appear giving details about the progress and status of the file import. The following shows an example of importing the latest OVAL content for the “Windows Server 2012 Compliance” check.

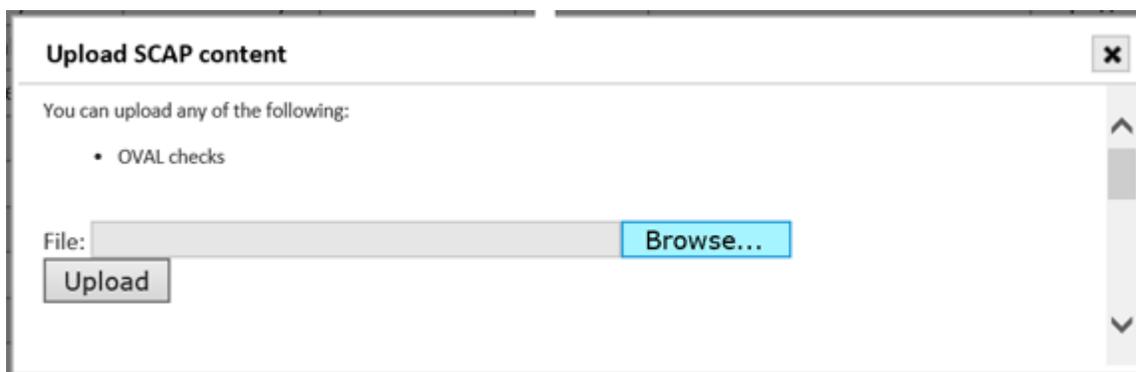


Once the content has been downloaded and has passed the validation step, the available profile(s) will be available for use. Once content has been imported, the data grid will expose the available options at the row level, to include updating the content with the latest checklists; viewing the details about the content; deleting the content; or running a scan policy (right arrow), as shown below:



Method 2 – Upload Content from a Local Drive

You may also manually import OVAL content from an external drive by using the *Upload Checklist* option from the Grid Actions dropdown associated with the Vulnerability/Patch/Inventory grid. Click this option to open up the upload popup and locate the applicable file with the *Browse* button.



Once you have selected the file, and its path is visible in the *File* field, click the *Upload* button to load the OVAL check. The files will be validated, as necessary, and imported for use.

Info./Warning/Error messages will appear giving details about the progress and status of the file import.

Viewing OVAL Checks

1. Click on the *Details* (i) option for the OVAL record you wish to view to open an OVAL Viewer window that provides information about the Checklist, as well as a hyperlink to view the XML-formatted checklists. The following is an example of the OVAL Viewer for

the Windows Server 2008 R2 Vulnerability OVAL check:

OVAL Viewer	
Id	11
Name	Windows Server 2008 R2 Vulnerability
Checkcount	5220
XML File	microsoft.windows.server.2008.r2.xml (34.46 MB)
Updatetime	1501618629
Downloadurl	https://oval.cisecurity.org/repository/download/5.11.2/vulnerability/microsoft_windows_server_2008_r2.xml
Author	CIS

- Click on the XML File hyperlink to view the checklists. The following is a snapshot of the XML content you should see when you view this type of content:

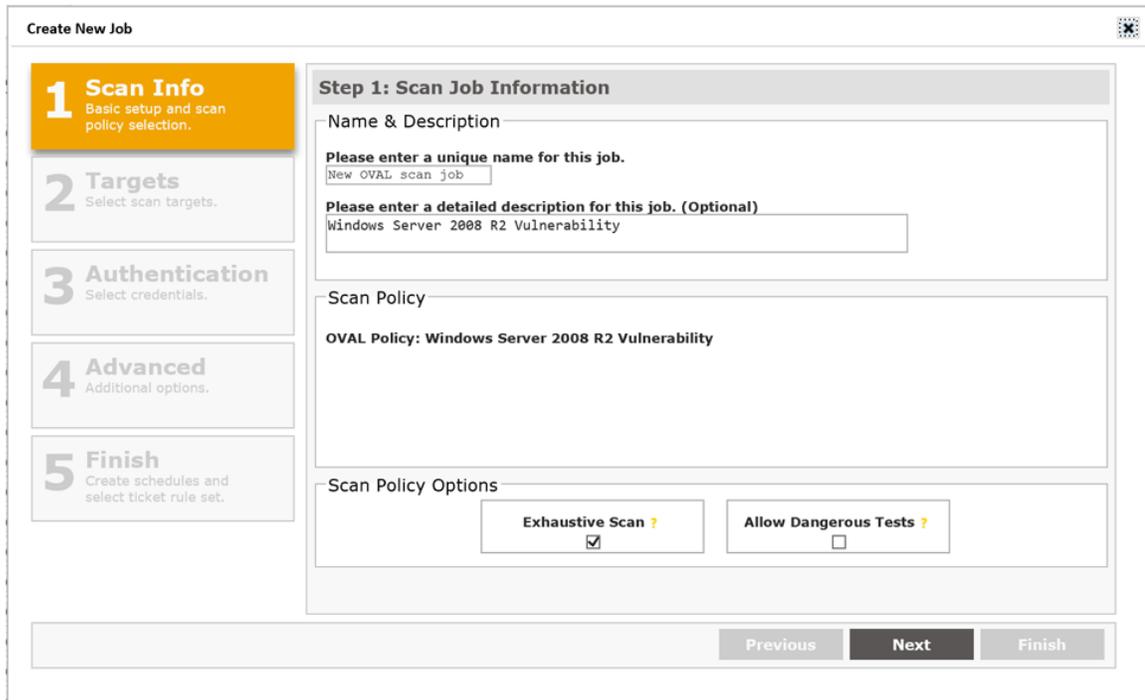
```
<?xml version="1.0" encoding="UTF-8"?>
- <oval_definitions xsi:schemaLocation="http://oval.mitre.org/XMLSchema/oval-common-5 oval-common-schema.xsd
http://oval.mitre.org/XMLSchema/oval-definitions-5 oval-definitions-schema.xsd" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:oval="http://oval.mitre.org/XMLSchema/oval-common-5" xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5">
- <generator>
  <oval:product_name>CIS OVAL Repository</oval:product_name>
  <oval:product_version>0.1</oval:product_version>
  <oval:schema_version>5.11.2</oval:schema_version>
  <oval:timestamp>2017-07-30T08:13:18</oval:timestamp>
</generator>
- <definitions>
- <definition xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5" version="31" id="oval:org.cisecurity:def:1457" class="vulnerability">
  <metadata>
    <title>Windows Common Log File System Driver Elevation of Privilege Vulnerability – CVE-2016-0026 (MS16-134)</title>
    <affected family="windows">
      <platform>Microsoft Windows Vista</platform>
      <platform>Microsoft Windows Server 2003</platform>
      <platform>Microsoft Windows Server 2008</platform>
      <platform>Microsoft Windows Server 2008 R2</platform>
      <platform>Microsoft Windows Server 2012</platform>
      <platform>Microsoft Windows Server 2012 R2</platform>
      <platform>Microsoft Windows Server 2016</platform>
      <platform>Microsoft Windows 7</platform>
      <platform>Microsoft Windows 8.1</platform>
      <platform>Microsoft Windows 10</platform>
    </affected>
    <reference source="CVE" ref_uri="http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0026" ref_id="CVE-2016-0026"/>
    <description>The Common Log File System (CLFS) driver in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1,
    Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows
    Server 2016 allows local users to gain privileges via a crafted application, aka "Windows Common Log File System Driver Elevation of
    Privilege Vulnerability," a different vulnerability than CVE-2016-3332, CVE-2016-3333, CVE-2016-3334, CVE-2016-3335, CVE-2016-
    3338, CVE-2016-3340, CVE-2016-3342, CVE-2016-3343, and CVE-2016-7184.</description>
  </oval_repository>
  <dates>
    <submitted date="2016-11-24T23:00:00+08:00">
      <contributor organization="DTCC">Jeff Albert</contributor>
    </submitted>
    <status_change date="2016-11-25T21:49:32.600-04:00">DRAFT</status_change>
    <status_change date="2016-12-09T14:00:00.000-05:00">INTERIM</status_change>
    <status_change date="2016-12-23T14:00:00.000-05:00">ACCEPTED</status_change>
  </dates>
  <status>ACCEPTED</status>
  <min_schema_version>5.10</min_schema_version>
</oval_repository>
</metadata>
- <criteria operator="OR">
  <criteria operator="AND" comment="Vista/2008 + file version">
    <extend_definition comment="Microsoft Windows Vista (32-bit) Service Pack 2 is installed"
      definition_ref="oval:org.mitre.oval:def:6124"/>
    <extend_definition comment="Microsoft Windows Vista x64 Edition Service Pack 2 is installed"
      definition_ref="oval:org.mitre.oval:def:5594"/>
  </criteria>
</criteria>
</definition>
</definitions>
</oval_definitions>
```

Running OVAL Checks

There are two methods for running a scan Job using an OVAL check.

Method 1: From the Benchmark Scanning page

1. Once you've imported the checklist for the OVAL check you wish to run, click on the Run option (right arrow) for the associated record. This step will launch the Scan Job wizard, pre-defining the policy based on your profile selection, as shown below:



2. Enter a Name and Description for the Job.
3. The scan policy section is pre-populated with the OVAL policy chosen for the job.
4. Click *Next*.
5. Enter the targets to be scanned, based on the platform applicable to the OVAL policy..

REMINDER: Target systems must have the following configurations: 1) Remote registry enabled; 2) File and printer sharing enabled; and 3) C\$ share must be read/write/executable.

See [Target Settings](#) for additional instructions.

6. Click *Next*.
7. Enter the credentials for the target platforms. For example, Windows Domain Admin credentials for the Windows 2008 R2 servers being scanned. As with other types of vulnerability scans, running a credentials scan ensures a more thorough assessment of the targets.
8. Click *Next*.

9. From the Advanced options, define additional scan configuration settings for this scan. The following are some of the most often used for OVAL scans.
 - Authentication sub-tab: ensure NTLMv2 is checked if the target is using NTLMv2
 - SCAP sub-tab: choose whether to run the “dissolvable” Windows SCAP service; choose the type of OVAL characteristics to be collected (System/Thin results)
10. Click *Next*
11. Review and verify the summary of the new job, and define the schedule for the job.
12. Click *Finish* to save the new job and submit it for execution.

The new job will now be present in the Scan grid in the Scan page..

Actions	Scan #	Job Name	Start Time	End Time	# Targets	# Results	Status	Progress
	23	Win 2008 R2 OVAL scan job	2017-08-01 17:30:11		1		Running	9%

Once the job is complete, this status will be updated and the results available for analysis.

Method 2: From the Job Wizard

1. Click on the global Create option in the upper right corner of the screen and select "Job" to launch the Scan Job wizard.
2. Enter a name for the job.
3. Select the “OVAL” option from the Select Policy Category drop down list.
4. Select an existing OVAL check from the Select Policy drop down list.
5. Follow the remainder of the job wizard steps in the same manner as defined for [Method 1](#) for initiating scans for a newly imported profile.
6. Review and verify the summary of the new job, and define the schedule for the job.
7. Click *Finish* to save the new job and submit it for execution.

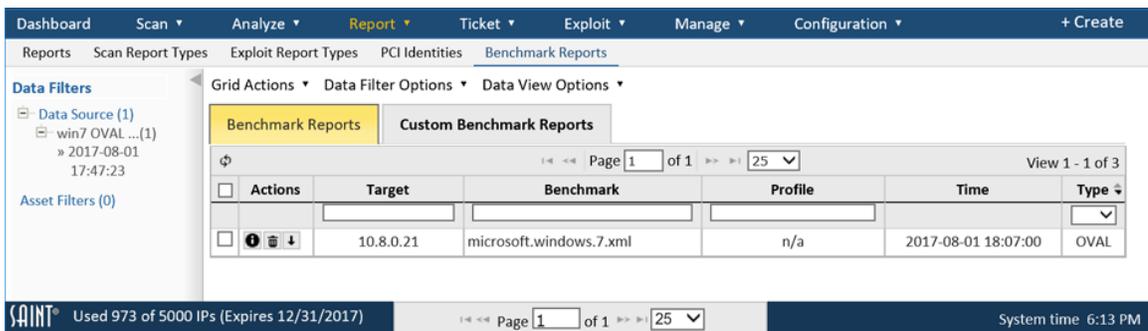
Viewing OVAL Scan Results

There are two methods for viewing and analyzing scan results based on the OVAL schema and platform checklists.

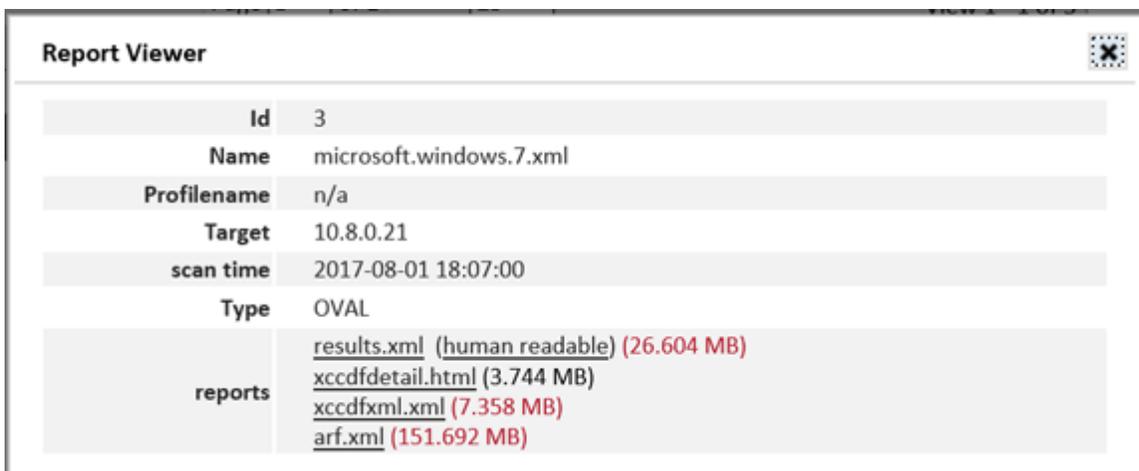
Method 1 – View OVAL results in SCAP-compliant format

1. Click on the *Benchmark Reports* tab in the data grid.
2. Click on the *Select Data Set* option from the Data Filter Options dropdown to view the current list of scan Jobs and scan results (scans).
3. Click on the applicable OVAL Job to view the current list of completed scans for that job.
4. Click on the completed scan in the Scans window. For example, an OVAL Vulnerability scan for a Windows 7 host.

SAINT will display a list of all Targets (in this case, one) that were assessed from the OVAL scan, along with information OVAL checklist that was run, and the datetime stamp of the scan.



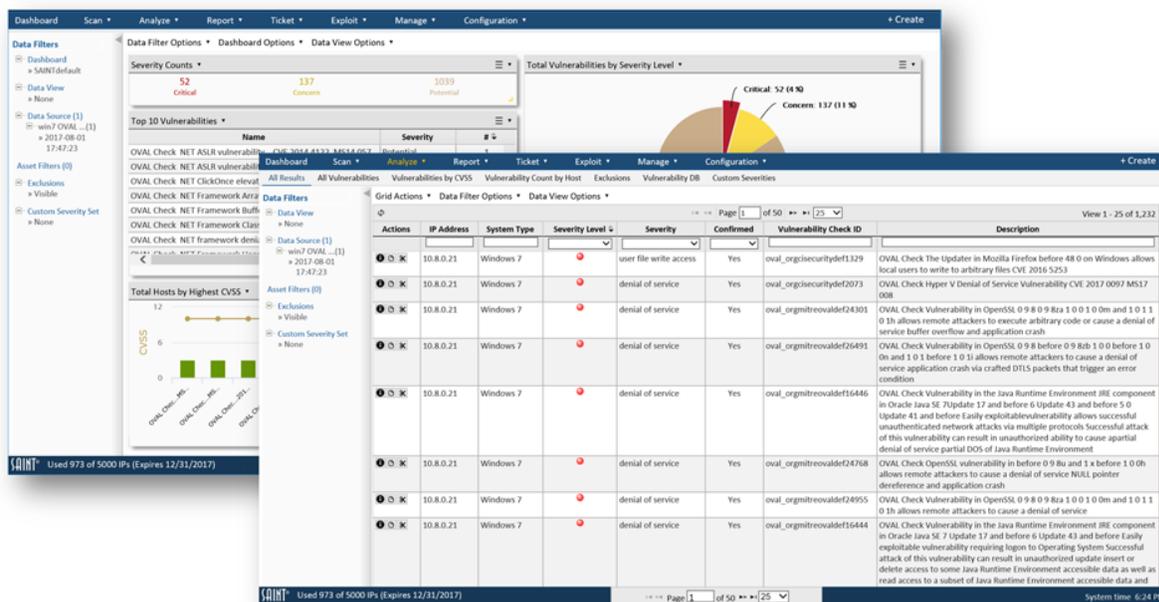
5. Click on the *View Reports* ("i") action for the target record to view the current list of SCAP-complaint output products, a Report Viewer with summary information about the OVAL scan, and hyperlinks to the various types of output products specified for SCAP compliance:



- Click on any of the hyperlinks to view the OVAL scan output in SCAP-compliant format.

Method 2 – Dashboard, Analyze, and Report Tabs

SAINT's main Dashboard, Analyze, and Report capabilities can be used to investigate and analyze OVAL vulnerability scan content in the same manner as vulnerability scanning, analysis and reporting capabilities.



Export OVAL Results

Once an OVAL scan has been run, results are available for display and export from the Benchmark Reports page. To export OVAL results:

- Click on the *Benchmark Reports* tab.
- If the Target results are not visible in the scan results grid from a prior selection, click on the *Select Data Set* option from the Data Filter Options and select scan results based on the applicable OVAL scan.
- Once the Target is visible in the grid, highlight the Target(s) to be exported.
- Click on the *Download Reports* (down arrow) option in the Actions column for the target row to extract all applicable scan data, product an export file and launch a dialog window to view/save the content.

OVAL content can also be exported directly from the *Analyze* tab, as you would other SAINT vulnerability assessment content. See the [Analyze](#) section for more information on how to export content from that feature.

NOTE: Human readable oval results.xml file can NOT be viewed in Google Chrome after being downloaded, due to a Chrome security restriction on using local transform files. Firefox, Edge or Safari must be used to view the downloaded file.

Upload and Use External Variables

OVAL external variables can be imported via the Benchmark Scanning page by clicking on the *External Variables* tab and then clicking on the folder icon. Once external variables are uploaded, they can be used in OVAL scans and will be listed in a drop down box after choosing the OVAL scan policy when creating a scan job.

SCAP Reports – Custom Benchmark Report

The custom Benchmark Reports grid provides the capability to produce various types of output from XCCDF configuration and OVAL (inventory, vulnerability, patch) scans, to Cyberscope reports, multi-target XCCDF summary reports (example shown below) and OVAL summaries.

Non-Compliant Hosts Summary			
# Hosts	# Non-Compliant Hosts	% Non-Compliant	Non-Compliant Hosts
1	1	100.00%	10.7.0.104

Compliant Hosts Summary			
# Hosts	# Compliant Hosts	% Compliant	Compliant Hosts
1	0	0.00%	

Group Summary						
Group	Pass	Fail	NC	NS	Score	Max %
Programs and Features Group	3	0	0	0	3	100.00%
Local Computer - Administrative Templates - System Settings - Error Reporting	0	1	0	0	1	0.00%
Password Policies	2	4	0	0	6	33.33%
Windows Explorer	0	1	0	0	1	0.00%
Windows Update	1	3	0	0	4	25.00%
Terminal Services	0	4	0	0	4	0.00%
Security Patches	0	1	0	0	1	0.00%
User Rights Assignment Settings	20	17	0	0	37	54.05%
Computer_Configuration - Administrative_Templates - System: Remote Procedure Call	0	2	0	0	2	0.00%
Power Management settings	0	0	0	1	0	100.00%
System Services Settings	13	9	0	0	22	59.09%
Security Options Settings	36	37	0	0	73	49.32%
Total	80	147	0	1	227	35.24%

(controls not checked) **NC**

(controls not selected for evaluation) **NS**

(controls configured correctly) **Pass**

(controls not configured correctly) **Fail**

(actual controls configured correctly) **Score**

(possible max controls configured correctly) **Max**

(Score/Max) **%**

Failed CCEs Summary by Host							
10.7.0.104							
Failed CCEs:							
CCE-4791-0	CCE-2807-6	CCE-3116-1	CCE-2981-9	CCE-2918-1	CCE-2829-0	CCE-2661-7	CCE-2930-6
CCE-2896-9	CCE-2994-2	CCE-2847-2	CCE-3053-6	CCE-18099-2	CCE-2933-0	CCE-3026-2	CCE-2299-6
CCE-8400-4	CCE-3025-4	CCE-8406-1	CCE-2824-1	CCE-2198-0	CCE-2145-1	CCE-3236-7	CCE-2843-1
CCE-4513-8							

NOTE: In some cases, hyperlinks to non-SAINT content (such as links to SCAP content on the NIST site) may not work. SAINT maintains hyperlinks to internal content, and links to these other

sites, but in some cases, these links have been found to be broken due to incorrect attributes for the URL at the external source. In those instances, the results page will be blank.

The following describes the process for creating an SCAP formatted custom report, using the CyberScope Report output.

CyberScope Report

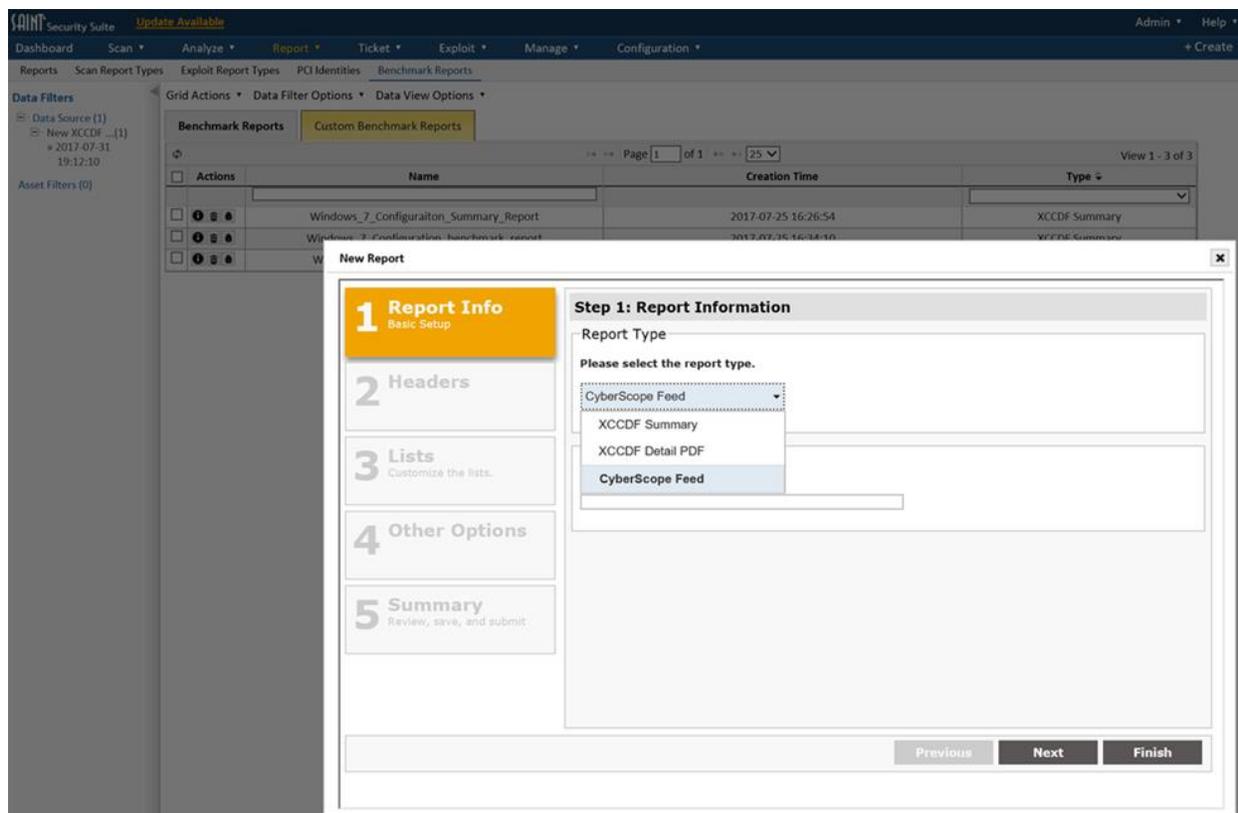
CyberScope is an application co-developed by the Department of Homeland Security and the Department of Justice to automate and standardize manual and automated inputs of agency data for FISMA compliance reporting for configuration benchmark assessments.

Select Scan Data to be Submitted

1. Navigate to the *Benchmark Reports* page under the Reports menu.
2. Click on the *Custom Benchmark Reports* tab to create, view and use reports.
3. Select the XCCDF scans you want to report on to display all Targets scanned and assessed for the selected scans.
4. Click on the Grid Options – *Create Reports* option from the Custom Benchmark Reports tab to begin the process of generating the Report.

Generate the Report

Step 1 – Report Information



Step 2 – Complete Header Information

The Header step is only relevant to the CyberScope report format. Click *Next* after completing this content or to progress to the next step.

The screenshot shows the 'New Report' wizard in the SAINT Security Suite. The window title is 'New Report'. On the left, there is a vertical progress bar with five steps: 1 Report Info (Basic Setup), 2 Headers (highlighted in orange), 3 Lists (Customize the lists), 4 Other Options, and 5 Summary (Review, save, and submit). The main content area is titled 'Step 2: Headers' and contains a form for 'CyberScope Organisation'. The form has three input fields: 'Full Organisation Name' with the value 'Department A', 'Organisation Abbreviation' with the value 'Dept A', and 'Organisation Enclave' with the value 'Vendor'. At the bottom right of the form area are three buttons: 'Previous', 'Next', and 'Finish'.

Step 3 – Configure List Options

Step 3 of the wizard does not apply to this type of report, as there are no editable lists for CyberScope report formats. However, for other types of reports, options can include:

- Compliant Hosts Summary
- Non-Compliant Host Summary
- Group Summary
- CCEs by Host
- Hosts by CCE

Click the checkbox for each type of results list to be included in your report.

Click *Next* to continue.

Step 4 – Apply Exclusions

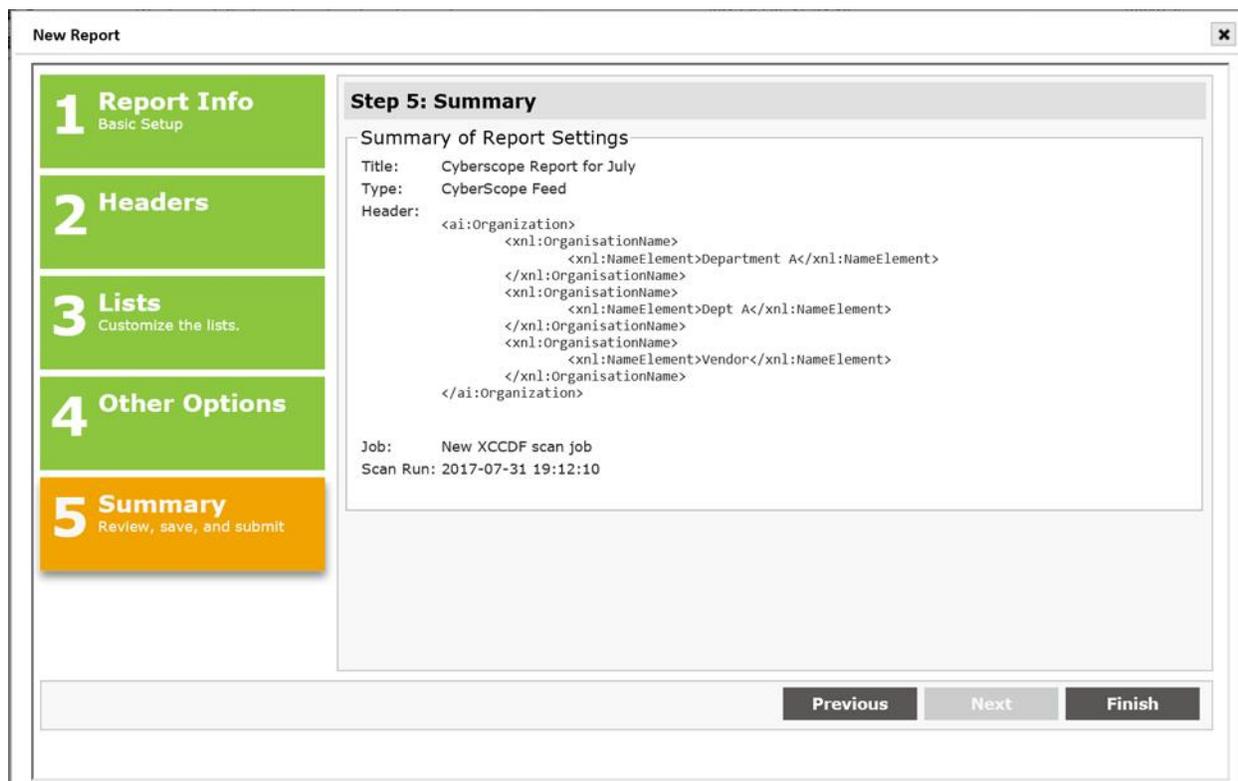
As with other types of vulnerability output, SAINT analytics and report configurations provide the capability to investigate scan results and identify vulnerabilities that are considered of low priority, potentially false positives or otherwise considered not relevant to including in reports.

These types of results are considered “exclusions” and can be identified and flagged in [Analyze](#) pages and managed by the Data Filter Options – View/Hide Exclusions option. Step 4 of the SCAP report wizard enables you to set the “Apply Exclusions” flag to ensure those results are not included in the report.

This option is set by default. Uncheck to box to ensure all vulnerability results are included in the report.

Step 5 – Validate Report Details

The last step is to validate the report details, including the scan content being submitted and the Header information to be included in the report. The example shows the summary for the new Cyberscope report.



Click the *Finish* button to generate the report.

SAINT will generate all required output formats. In the case of Cyberscope, this will also include all XML-formatted products required for the Cyberscope Feed. A snapshot of the example output is shown below:

```

- <AssetReport xsi:schemaLocation="http://scap.nist.gov/schema/asset-identification/1.0 http://scap.nist.gov/schema/asset-ide
reporting-format_1.0.0-eal.xsd http://scap.nist.gov/schema/lightweight-asset-summary-results/1.0 http://scap.nist.gov/schema/
- <Subject>
  - <ai:Organization>
    - <xnl:OrganisationName>
      <xnl:NameElement>SAINT Corporation</xnl:NameElement>
    </xnl:OrganisationName>
  - <xnl:OrganisationName>
    <xnl:NameElement>SAINT</xnl:NameElement>
    </xnl:OrganisationName>
  - <xnl:OrganisationName>
    <xnl:NameElement>Vendor</xnl:NameElement>
    </xnl:OrganisationName>
  </ai:Organization>
</Subject>
- <ReportInformation>
  - <Report>
    - <ReportMetadata>
      <DateTime>2013-04-05T10:48:43.0Z </DateTime>
    - <Tool>
      - <ai:Software>
        <ai:CPE>cpe:/a:saintcorporation:saintscanner:8.0</ai:CPE>
      </ai:Software>
    </Tool>
  </ReportMetadata>
- <ReportPayloads>
  - <ReportPayload>
    - <sr:SummaryReport id="FISMA_auto_feed_fy10" version="1.0beta1">
      - <sr:DataPoint id="configuration_management_agency_deviations">
        - <sr:GroupedData>
          <sr:NamedAttribute name="checklist_name">USGCB-Windows-XP</sr:NamedAttribute>
        - <sr:GroupedData>
          <sr:NamedAttribute name="checklist_version">v2.0.0.0</sr:NamedAttribute>
        - <sr:GroupedData>
          - <sr:NamedAttribute name="checklist_profile">
            united_states_government_configuration_baseline_version_2.0.0.0_high_800_53
          </sr:NamedAttribute>
          <sr:AggregateValue name="number_of_systems" type="COUNT">1</sr:AggregateValue>
        - <sr:GroupedData>
          <sr:NamedAttribute name="http://cce.mitre.org">CCE-4791-0</sr:NamedAttribute>
          <sr:AggregateValue name="non_compliant_systems" type="COUNT">1</sr:AggregateValue>

```

The new report will also be displayed in the Custom Benchmark Reports tab.

Click on the *Report Viewer* (magnifying glass) to view the high level details about the report and click on the XML-based reports hyperlink to view the content or save it externally for submission or off-line storage.

The screenshot shows the 'Benchmark Reports' interface with the 'Custom Benchmark Reports' tab selected. A table lists four reports, with the last one, 'Cyberscope_Report_for_July', highlighted. A 'Report Viewer' dialog box is open, displaying details for the selected report.

Actions	Name	Creation Time	Type
<input type="checkbox"/>	Windows_7_Configuraiton_Summary_Report	2017-07-25 16:26:54	XCCDF Summary
<input type="checkbox"/>	Windows_7_Configuration_benchmark_report	2017-07-25 16:34:10	XCCDF Summary
<input type="checkbox"/>	Windows_7_Detailed_Configuration_Report	2017-07-25 16:36:56	PDF XCCDF Detail
<input type="checkbox"/>	Cyberscope_Report_for_July	2017-08-01 20:03:58	Cyberscope

Report Viewer	
Id	4
Name	Cyberscope_Report_for_July
Type	Cyberscope
reports	Cyberscope_Report_for_July-admin-1501632238.xml (0.002 MB)

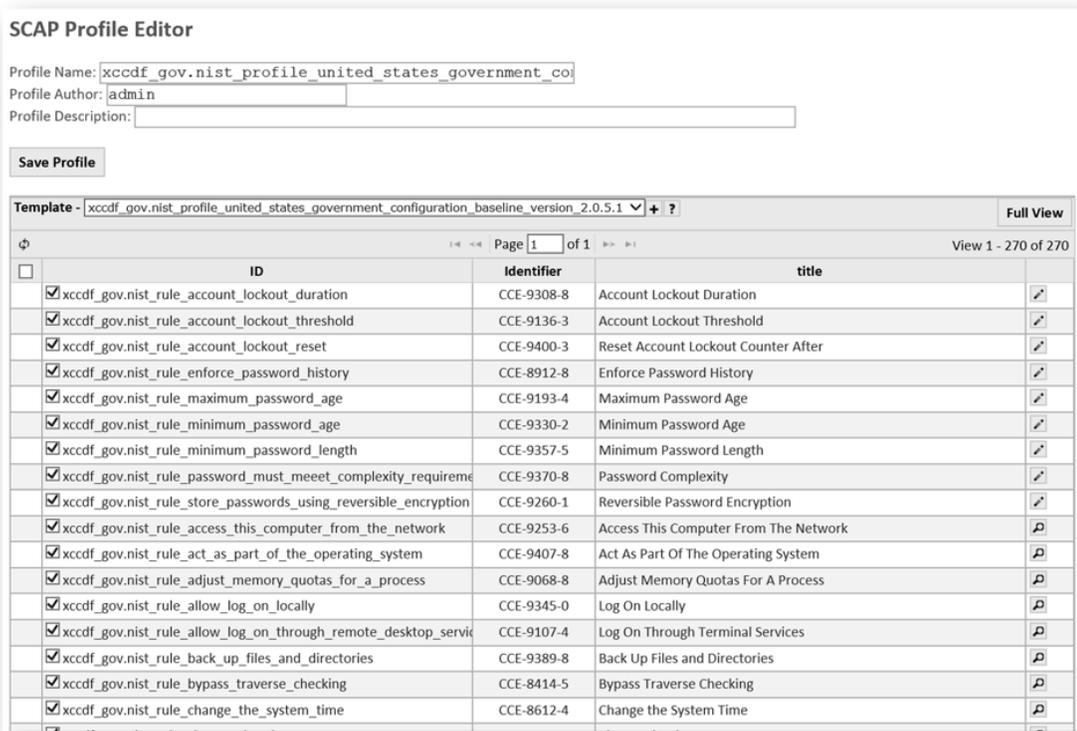
Configuration Benchmark Policy Editor

The Policy Editor provides the capability to edit many of the configuration settings found in Configuration Benchmarks to support creating custom configuration policies. The process for editing, storing and using custom configuration policies is described below.

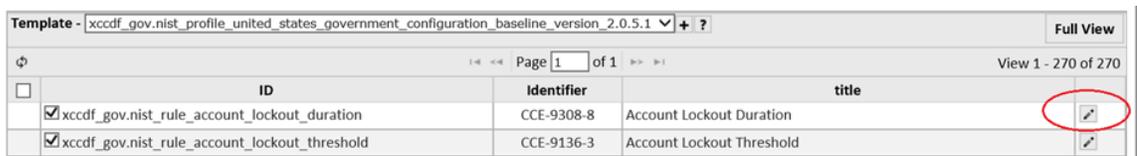
Creating a Custom Configuration Benchmark

1. First, ensure you have downloaded a current version (Import or Update content options) using the steps defined in the [Importing XCCDF Configuration Benchmark Profiles](#) section.
2. Click the down arrow option in the left column of the benchmark platform you wish to edit. The grid will expand to show all of the available configuration Profiles download from the authoritative source.
3. Launch the policy editor by clicking on the Edit (pencil) option next to the profile you want to use as a template. This step will open the editor and display a blank Title and Description field to describe the custom profile.

The following is a snapshot of a portion of a Windows 7 profile displayed in the editor using the grid's Rule View:



The grid will display a list of all content, both editable and read-only. The policy is broken down into a set of groups and rules. The editor allows you to view detailed descriptions of each group and rule contained in the policy, enable and disable checks (rules), and modify values associated with certain rules. Content that cannot be customized will provide the capability read the details about the configuration item, using the View option. Configurations that can be edited will expose the Edit (pencil) option for the row, as shown below in the highlighted row:



4. To launch the edit dialog for a Configuration setting, double click or click on the *Edit* option for the applicable setting.

The following shows the edit dialog for the “minimum_password_length” configuration setting.

xccdf_gov_D_O_T_nist_rule_minimum_password_length ✕

value: `xccdf gov.nist value password minimum length var`

title: Minimum Password Length

description: The minimum number of characters required for a password

Value:

rule: `xccdf gov.nist rule minimum password length`

title: Minimum Password Length

description: This setting specifies the minimum length of a password in characters. The rationale behind this setting is that longer passwords are more difficult to guess and crack than shorter passwords. The downside is that longer passwords are often more difficult for users to remember. Organizations that want to set a relatively large minimum password length should encourage their users to use passphrases, which may be easier to remember than conventional passwords.

reference: GPOComputer Configuration\Windows Settings\Security Settings\Account Policies>Password Policy

ident: CCE-9357-5

5. Click in the value field and change the setting to meet your specific requirements.
6. Click *Apply* to save the setting. A confirmation message will be displayed that the value is applied for this setting. Note, however, that this change will not be final until you save the complete profile.
7. Close the dialog box to return to the Editor page.
8. As a convenience, the policy editor also allows you to edit all values at once or in a particular set of groups or rules by using the checkboxes found on the left side of the page. For example, in the following screen shot, we have disabled both "Reverse Password Encryption" and "Log On Through Terminal Services" Rules. This level of customization can be done at the individual configuration level or as a Group by unchecking the checkbox at the Group level.

<input checked="" type="checkbox"/>	xccdf_gov.nist_rule_password_must_meeet_complexity_requireme	CCE-9370-8	Password Complexity	
<input type="checkbox"/>	xccdf_gov.nist_rule_store_passwords_using_reversible_encryption	CCE-9260-1	Reversible Password Encryption	
<input checked="" type="checkbox"/>	xccdf_gov.nist_rule_access_this_computer_from_the_network	CCE-9253-6	Access This Computer From The Network	
<input checked="" type="checkbox"/>	xccdf_gov.nist_rule_act_as_part_of_the_operating_system	CCE-9407-8	Act As Part Of The Operating System	
<input checked="" type="checkbox"/>	xccdf_gov.nist_rule_adjust_memory_quotas_for_a_process	CCE-9068-8	Adjust Memory Quotas For A Process	
<input checked="" type="checkbox"/>	xccdf_gov.nist_rule_allow_log_on_locally	CCE-9345-0	Log On Locally	
<input type="checkbox"/>	xccdf_gov.nist_rule_allow_log_on_through_remote_desktop_servic	CCE-9107-4	Log On Through Terminal Services	
<input checked="" type="checkbox"/>	xccdf_gov.nist_rule_back_up_files_and_directories	CCE-9389-8	Back Up Files and Directories	

9. Follow steps 4-8 for other configuration settings until you have completed your work for the new profile.
10. Once you are done, scroll to the bottom of the profile's grid and click the Save option and refresh the page to show that the new Profile has been saved.

Viewing a Custom Configuration Benchmark

1. Navigate to the *Configuration* tab in the Benchmark Scanning page
2. Click on a Configuration Benchmark Platform to view the current list of imported profiles and all locally generated custom profiles. The following shows the Windows 7 profiles, including a custom benchmark profile described in the previous section:

Actions	Name	Author	Checks	Pass Threshold	Description
	Custom Win7 Config	admin	268	95	Excludes Reversible Password Encryption and
	xccdf_gov.nist_profile_united_states_governer	USGCB/TIS	270	95	

3. The custom profile can also viewed in detail, as well as edited, by double clicking the profile or clicking the *Edit* (pencil) option.
4. The Name and Description can also be edited, in line, by clicking in the cell and changing the text string without launching the editor.

Running a Custom Configuration Benchmark

Custom Configuration benchmarks can be run in the same manner as imported benchmarks either by clicking on the “Run” (right arrow) option for a profile, or selecting it directly in the Scan Wizard (Step 1 – Scan Category: XCCDF/Configuration; Scan Policy: [your custom profile]). See the [Scan](#) section and [Running XCCDF Configuration Benchmark Profiles](#) section for more details.

Command-Line Mode

The command-line interface is ideal for those without a good HTML browser, for those who wish to schedule scans using *cron*, or for those who would rather not run the HTML browser, as it may consume several megabytes of valuable memory. All of the probing functionality is accessible via the Unix shell prompt. The results will be sent to standard output in a fixed text format. If graphical data analysis is desired, then invoke SAINT in the usual manner after the command-line scan is finished, and go directly to *Data*.

SAINT runs a scan using the command-line interface if one or more targets are specified on the command line, or if the `-F` option is used to specify a target file. Otherwise, SAINT invokes the HTML browser and runs interactively. The syntax for running SAINT is:

```
./saint [options] [target1] [target2]...
```

Type `./saint -H` for a list of command line options. *target1*, *target2*, etc. can be host names, IP addresses, IP subnets, or IP address ranges. As many targets as desired can be specified on the command line, separated by spaces.

Following is a list of the command line options, what they do, and what SAINT variables they correspond to. Further explanations of the variables that are mentioned here can be found in Configuration Management.

<code>-a level</code>	Attack level (Vulnerability Scan Levels: 6=discovery; 7=portscan; 0=light; 1=normal; 2=full; 3=heavyplus; 4=top20; 5=custom; 8=webcrawl; 9=sql/xss; 10=windows patch; 11=content search; 12=PCI; 13=OVAL; 14=anti-virus; 15=FISMA; 16=auth test; 17=XCCDF; 18=pwguess; 19=MS Tuesday; 20=OWASP; 21=IAVA; 22=OS Password Guess; 23=NERC; 24=software inventory; 25=HIPAA; 26=SOX; 27=mobile device; 28=network device; 29=local; 30=local benchmarks; 31=local OVAL; 32=NESA.. Penetration Test Levels: x0=discovery; x1=information gathering; x2=single penetration; x3=root penetration; x4=full penetration; x5=web application). Variable: <code>\$attack_level</code> , <code>\$pentest_level</code>
<code>-A proximity</code>	Proximity Descent. Variable: <code>\$proximity_descent</code> .
<code>-b</code>	Brief port scan (common ports only). Variable: <code>\$allports = 0</code>
<code>-bb</code>	Heavy port scan. Variable: <code>\$allports = 1</code>
<code>-c 'name = value; name = value...'</code>	Change SAINT variables. Use this to overrule configuration variables that do not have their own command-line option.
<code>-C custom level</code>	Custom attack level. Argument specifies which custom attack level definition to use. (Overrides <code>-a</code> option.) Variable: <code>\$custom_level</code> .
<code>-d directory</code>	SAINT database (data directory) to read already collected data from, and to save new data to. Variable: <code>\$saint_data</code> .

SAINT Security Suite

<code>-e email%server</code>	E-mail a report when scan finishes. Variables: <code>\$send_email</code> , <code>\$send_report</code> , <code>\$email_address</code> , <code>\$mail_server</code>
<code>-f</code>	Enable firewall analysis (TCP discovery). Variable: <code>\$firewall_flag</code>
<code>-ff</code>	Extensive firewall analysis (fully scan entire range). Variable: <code>\$firewall_flag</code>
<code>-fff</code>	Enable firewall analysis (ARP ping discovery). Variable: <code>\$firewall_flag</code>
<code>-ffff</code>	Combined firewall analysis (ICMP+TCP+ARP discovery). Variable: <code>\$firewall_flag</code>
<code>-F filename</code>	Read list of primary targets from file. Variable: <code>\$use_target_file</code> , <code>\$target_file</code>
<code>-g guesses</code>	Number of passwords to guess against each account. Variable: <code>\$password_guesses</code>
<code>-h "host1 host2 ..."</code>	IP addresses which are allowed to use SAINT remotely. (Used with <code>-r</code> , <code>-R</code> , or <code>-w</code> option.) Variable: <code>\$allow_hosts</code>
<code>-i</code>	Ignore already collected data
<code>-k</code>	Kill the SAINT process running in remote mode and exit. If more than one server is running, the <code>-p</code> option can be used to kill only the server running on the specified port. If <code>-p</code> is not present, all SAINT processes are killed.
<code>-K filename</code>	Specifies the license key filename. The default is <code>saint.key</code>
<code>-l proximity</code>	Maximal proximity level. Variable: <code>\$max_proximity_level</code>
<code>-L [realm:] [prefix:]login% password</code>	Authentication credentials for targets. Realm is either <code>ssh</code> (for Linux, Unix, or Macintosh), <code>smb</code> (for Windows admin), <code>smb_user</code> (for Windows non-admin), <code>oracle</code> , <code>mssql</code> , <code>mysql</code> , or <code>basic</code> (for HTTP Basic). Default realm is <code>smb</code> . Optional prefix is private key for <code>ssh</code> or SID for <code>oracle</code> . Variables: <code>\$domain_user</code> and <code>\$ssh_user</code>
<code>-m threads</code>	Maximum number of probes which can be run concurrently. 1 disables multitasking. Variable: <code>\$maximum_threads</code>
<code>-n netmask</code>	Netmask(s) of target hosts. Variable: <code>\$target_netmask</code>
<code>-o list</code>	Scan only these hosts, domains or networks. Variable: <code>\$only_attack_these</code> .
<code>-O list</code>	Don't scan these hosts, domains or networks. Variable: <code>\$dont_attack_these</code> .

<code>-p port</code>	TCP port to listen on. Variable: <code>\$server_port</code> .
<code>-P</code>	Preserve existing data in session archive.
<code>-q</code>	Quiet mode. Do not display results of scan.
<code>-Q</code>	Quick start-up. Do not check for updates.
<code>-r</code>	Remote mode. Variable: <code>\$remote_mode</code>
<code>-R</code>	Remote mode without password prompt. Variables: <code>\$remote_mode</code> and <code>\$skip_passwd</code> .
<code>-s</code>	Enable subnet expansions. Variable: <code>\$attack_proximate_subnets</code> .
<code>-S status_file</code>	SAINT status file (default <code>status_file</code>). Variable: <code>\$status_file</code> .
<code>-t level</code>	Timeout length (0 = short, 1 = medium, 2 = long). Variable: <code>\$timeout</code> .
<code>-T</code>	Exhaustive (thorough) scan. Variable: <code>\$exhaustive = 1</code>
<code>-TT</code>	Non-exhaustive scan. Variable: <code>\$exhaustive = 0</code>
<code>-u</code>	Running from an untrusted host. Variable: <code>\$untrusted_host = 1</code>
<code>-U</code>	Running from a trusted host. Variable: <code>\$untrusted_host = 0</code>
<code>-v</code>	Turn on debugging output (to stdout). Variable: <code>\$debug</code> .
<code>-V</code>	Print version number and terminate.
<code>-VV</code>	Get updates, print version number and terminate.
<code>-w</code>	Use an existing web server. This option implies remote mode and assumes that the <code>saint.cgi</code> script is present in the web server's <code>cgi-bin</code> directory. Variable: <code>\$web_server</code>
<code>-x</code>	Extreme mode. Run dangerous tests. (Caution!) Variable: <code>\$extreme = 1</code>
<code>-X</code>	Don't run dangerous tests. Variable: <code>\$extreme = 0</code>
<code>-z</code>	Continue with attack level of zero when the level would become negative. The scan continues until the maximal proximity level is reached. Variable: <code>\$sub_zero_proximity = 1</code>
<code>-Z</code>	Opposite of the <code>-z</code> option. Variable: <code>\$sub_zero_proximity = 0</code>

Architecture

Overview

SAINT's scanning solutions have an extensible architecture, from a proprietary kernel and inference engine, to the middleware to manage activities, and client-side interfaces for interacting with various features, functions and content. At the center of this architecture is a relatively small generic kernel with minimal awareness of system types, network service names, vulnerabilities or other details contained in the architecture. Knowledge about the details of network services, system types, etc. is built into small, dedicated, data collection tools and rule bases. The behavior is controlled from a configuration file and web services. Many of these configurations can be customized via command-line options or browser-based interface.

The kernel consists of the following main parts:

- **[Magic cookie generator](#)** – Each time the management console is started up in interactive standalone mode, the magic cookie generator generates a pseudorandom string that the HTML browser must send to the SAINT proprietary HTTP server as part of all commands.
- **[Policy engine](#)** – Given the constraints specified in the [configuration file](#), this subsystem determines whether a host may be scanned, and what scanning level is appropriate for that host.
- **[Target acquisition](#)** – Given a list of target hosts, this subsystem generates a list of probes to be run on those hosts. The list of probes serves as input to the [data acquisition](#) subsystem. The target acquisition module also keeps track of a host's [proximity level](#), and handles the so-called subnet expansions.
- **[Data acquisition](#)** – Given a list of probes, this subsystem runs the corresponding data collection tools and generates new facts. These facts serve as input to the inference engine.
- **[Inference engine](#)** – Given a list of facts, this subsystem generates new target hosts, new probes, and new facts. New target hosts serve as input to the target acquisition subsystem; new probes are handled by the data acquisition subsystem, and new facts are processed by the [inference engine](#).
- **[Report and analysis](#)** – This subsystem takes the collected data and builds a virtual hyperspace that you can explore with your favorite HTML browser.

Once a SAINT scanning engine is given an initial target host, the target acquisition, data acquisition and inference engine subsystems keep feeding each other new data until nothing new comes up. Technically speaking, the system does a breadth-first search.

Magic Cookie Generator

When you start a SAINT management console in the default interactive standalone mode, i.e., using the browser interface on the local host, the startup process performs the following actions before starting up the browser:

- Start the SAINT daemon. This is a very limited subset of the typical httpd daemon, sufficient to support all activities that the product can perform.
- Generate a 32-byte cryptographic magic cookie for the upcoming startup. Several system utilities are run in parallel and compresses their quasi-random output with the MD5 hashing function. The HTML browser must specify this magic cookie as part of the URLs that it sends to the proprietary SAINT httpd daemon. This key prevents SAINT functions from being called from unauthorized browsers and should never be compromised. This process generates a new magic cookie for each session. The browser always runs on the same host in standalone mode, so there is no need to send the magic cookie over the network.

Policy Engine

The policy engine controls what hosts may be probed. The probing intensity depends on the host's measure for the distance from the initial target host(s).

Target Acquisition

The scan engine can gather data about just the specified host(s), or it can gather data about all hosts within an IP address range or a subnet (a block of 256 adjacent network addresses). The latter processes are called target ranges and subnet scans. Target hosts may be specified by the user, or may be generated by the inference engine when it processes facts that were generated by the data acquisition model (both described later in this section).

Once a list of targets is available, the target acquisition module generates a list of probes according to the scan policy level, derived from the policy engine. The actual data collection is executed under control of the data acquisition module.

Range and Subnet Scans

When requested to scan all hosts in an IP address range or a subnet (a block of 256 internet addresses), the scan engine uses the *fping* utility to find out what hosts in that range or subnet are actually available. This is to avoid wasting time talking to hosts that no longer exist or that happen to be down at the time of the measurement. The *fping* scan also may discover unregistered systems that have been attached to the network without permission from the network administrator.

Data Acquisition

The data acquisition engine takes a list of probes and executes each probe after it has verified that the probe may be run at the target's scan level. What tool may be run at a given scanning level is specified in the scan level definition. The software keeps a record of what probes it has already executed to avoid doing unnecessary work. The result of data acquisition is a list of new facts that is processed by the inference engine.

The scan solution comes with a multitude of tools, each implementing one type of network probe. By convention, the name of a data collection tool ends in `.saint`. All tools produce output according to the same common tool record format. The scan architecture derives a great deal of power from this toolbox approach. When a new network feature becomes of interest, the scan architecture also provides functionality to [add your own probes](#), to further extend the risk management power across your enterprise.

Inference engine

The heart of the scan architecture is a collection of little inference engines. Each engine is controlled by its own rule base. The rules are applied in real time, while data is being collected. The result of these inferences are lists of new facts for the inference engine, new probes for the data acquisition engine, new targets for the target acquisition engine, and service and host type information which is stored in memory structures. Application of these rules in real time to each tool output record, and within the context of all information that has been collected so far, is the core logic that powers data collection.

File Structure

The installation deploys software, configuration and content via the installation directory's file structure; however, typically requiring little or no knowledge or use of the installed content.

The following is provided to describe this structure for advanced users or partners/integrators that may require access to the internal structures of the installation.

The Installation Process

SAINT stores its files under several top-level directories –

bin/	The programs in this directory are used for data acquisition functions.
config/	These files are configuration files that are used to locate needed supplemental programs. These files also contain all default settings.
connections/	Information and communication pipes for active connections are stored in this directory after a successful exploit.
dictionaries/	These files contain word lists which may be used for password guessing attempts.
exploits/	These files are the exploit plug-ins. See Exploit Plugins for more information.
html/	The files found in this directory are either HTML pages or Perl programs. They are used to generate the components of the user interface.
listeners/	Information on active exploit servers is stored in this directory.
perl/	Code modules which power the scan engine and the user interface.
perllib/	This directory contains some modules used by the Perl scripts.
results/	This directory contains all of the scan data. For more information on these files see the Legacy database structure .
rules/	The files in this directory are used to assess the situation and infer facts from the existing information. The underlying rules were built using PERL and may be easily configured. See SAINT rule sets for more information.
scripts/	This directory contains miscellaneous scripts which can be used by the product.
src/	This directory contains the source code to some of the support programs.
var/	These files store miscellaneous runtime data.

Vulnerability Hierarchy

At the root of the scan level configuration model is a vulnerability check hierarchy consisting of categories, sub-categories, and individual vulnerability checks. The vulnerability check hierarchy is defined in the config/vulns.dat file.

Vulnerability Categories

At the top of the vulnerability hierarchy are 12 top-level categories. These correspond to the 12 vulnerability classes defined in reports. Specifically, they are as follows:

1. **web** – Vulnerabilities in web servers, CGI programs, and any other software offering an HTTP interface
2. **mail** – Vulnerabilities in SMTP, IMAP, POP, or web-based mail services
3. **ftp** – Vulnerabilities in FTP and TFTP services
4. **shell** – Vulnerabilities in ssh, telnet, rlogin, rsh, or rexec services
5. **print** – Vulnerabilities in lpd and other print daemons
6. **rpc** – Vulnerabilities in Remote Procedure Call services
7. **dns** – Vulnerabilities in Domain Name Services
8. **database** – Vulnerabilities in database services
9. **net** – Vulnerabilities in routers, switches, firewalls, or any SNMP service
10. **win** – Missing Windows hotfixes or vulnerabilities in the registry or SMB shares
11. **pass** – Missing or easily guessed user passwords
12. **misc** – Any vulnerability which does not fit into one of the above classes

Many of these top-level categories contain sub-categories. For example, mail vulnerabilities are further subdivided into IMAP, POP and SMTP vulnerabilities. Some sub-categories themselves contain sub-categories. The result is a logical hierarchy of vulnerability categories into which individual checks are placed, making it easy to find any desired check by drilling down from the top-level categories to the more specific categories.

Each vulnerability check is assigned a unique identifier. The identifier always starts with the top-level category, followed by the progression of sub-categories if any, followed by a string which identifies the check itself, separated by underscores. For example, the check for vulnerable Apache web server versions is identified by `web_server_apache_version`: `web` is the top-level category; `server` is the sub-category of `web` which contains vulnerabilities in web server software; `apache` is the sub-category of `server` which contains vulnerabilities in the Apache web server; `version` uniquely distinguishes the check from any other checks in the `apache` sub-category.

The vulns.dat file

The `vulns.dat` file, found in the `config` directory, contains the vulnerability hierarchy and all associated information. Similar to [SAINT Legacy Database structure](#), `vulns.dat` consists of

records, one on each line, separated by pipe characters (|). There is also a `vulns_custom.dat` file which contains information on custom checks, if any have been created.

There are two types of records. *Category* records define a category or sub-category and consist of three fields: the category identifier, the category description, and the word *category*, in that order.

The second type of record is for vulnerability checks. Vulnerability check records consist of eight fields:

1. The vulnerability identifier
2. The vulnerability description – This should be the same as or similar to the text (eighth) field of the fact corresponding to the vulnerability.
3. The vulnerability tutorial – This should be the same as the seventh field of the fact.
4. Maximum severity (red, yellow, or brown)
5. CVEs – A space-separated list of CVE numbers. A question mark indicates related entries which may be specific cases of the vulnerability, but which are not generally applicable. "r", "y", and "b" indicate severity levels specific to that CVE entry which differ from that specified in the preceding field. "x" indicates a dangerous check is available.
6. SANS Top 20 – The data in this field is no longer maintained, as SANS has transitioned to more global categorization of security controls. For example, SAINT provides support and is SANS validated for coverage of [SANS Security Control #4](#) (related to vulnerability assessments) and [Security Control #20](#) (penetration testing). However, this field is retained in the repository for legacy support. This field is 1 if the vulnerability falls into the legacy SANS Top 20, and 0 otherwise.
7. Authentication – This field is 0 if no authentication is required; 1 if authentication is required; 2 if an SNMP read community string is required; and 3 if both unauthenticated and authenticated checks exist.
8. Probe dependencies – This field lists all probes which need to run for the vulnerability to be detected, without the *.saint* extensions, and separated by semi-colons. Question marks indicate conditional probes, which are only run if one of the rules in the [todo](#) rule set is matched. *tcpscan* and *udpscan* should be followed by a port number, list, range, or an asterisk which indicates that all ports included at the heavy scan level should be scanned. An asterisk would be used, for example, if the vulnerable application runs on a random port.

Returning to our previous example of the Apache web server version check, the record would appear as follows (with line breaks added for readability):

```
web_server_apache_version|vulnerable Apache version|
Apache vulnerabilities|red|CVE-2002-0392* CVE-2002-0661|
1|0|tcpscan 80;http?
```

This indicates that the maximum possible severity for this vulnerability is red; there are two CVE entries, the first of which is explicitly listed as an example on the legacy SANS Top 20 vulnerability list; the check does not require any special authentication; and the vulnerability is detected by running `tcpscan.saint` against port 80, and if appropriate, `http.saint`.

SAINT Probes

General Information

SAINT's scan probes are the executable programs that contain vulnerability checks. Probes send tests to targets, process the replies and any related tasks. Probe files are stored in the `bin` directory with file names ending in `.saint`. The rules used to infer vulnerabilities are stored in the `rules` directory. (See [Rule Sets](#) for more information on the rule sets.)

The following describes the basic execution of vulnerability check execution:

- Scan probes first conducts the initial data collection. Actions in this phase are carried out by the `.saint` files. Upon completion of the initial data collection, results are written to the repository. Results from this phase include both informational and vulnerability data.
- Next, rulesets are checked to determine whether or not it can infer other vulnerabilities from existing facts. For instance, if an old version of sendmail is running on a system, that can be reasonably inferred that the system will be vulnerable to certain sendmail exploits. If a new vulnerability can be inferred from the output of existing probes, it is not necessary to write a new probe to check for it. See [rules/facts](#) for information on modifying the rule sets.

How to Add a SAINT Probe

SAINT provides the capability to allow users to create custom checks and custom policies through the user interface. (See [Manage Scan Policies](#)). However, there may be instances where this capability is not extensible enough to cover a target environment that is not currently supported by a SAINT probe. In those instances, SAINT provides the capability to allow you to create a probe and use it in the execution of other scan policies. The following describes how to create your own probes and use them within the vulnerability scanning process:

1. Create an executable program that checks for the problem you'd like to scan for. It generally will take one argument—a hostname that is the target of the probe. Place the executable in the *bin* directory. (Example C program structure provided below)
2. Have the probe output a valid output record. See the [Database Format](#) for more information on the output record format. Also, have the probe output the string "BEGIN" on the first line. This is how the scan engine knows that the probe successfully began running if there is no other output.
3. If the probe is a C program or something that must be processed or compiled before being run, either modify the existing makefile or create your own.
4. If the probe is run conditionally, add a rule to `rules/todo.custom` that runs the probe. That is, if the probe should only be run against certain targets, such as targets running a particular service or operating system, add a rule which specifies that the probe should be run under those conditions. Refer to the `rules/todo` file for the structure, content, and examples of what should be added to the `rules/todo.custom` file. IMPORTANT: Do not append rules changes to the `rules/todo` file, as it will be removed during subsequent product updates.
5. Decide what attack level(s) (i.e., scan policy) it will be run from and any relevant custom scan levels. Modify the appropriate `.probe` files(s) in the `config/policy` directory. If the probe is run conditionally as discussed above, then put a question mark after the name of the probe. Note that the *heavy* and *heavyplus* attack levels by default contain the "*" entry, so it is not necessary to list each conditional probe at these levels.
6. Optional: If you want users to be able to select your new probe when creating custom scan levels, you must add it to the vulnerability check hierarchy. Add a vulnerability check identifier to the `config/vulns_custom.dat` file, being sure to specify your probe (with or without a question mark) in the last field, along with any other probes upon which it depends. If desired, you can also make your probe read the configuration file corresponding to the current scan level and check whether the vulnerability check

identifiers added above are enabled before launching specific attacks. The current scan level is always defined in the `SAINT_LEVEL` environment variable. Note that the string "check_" is prepended to each vulnerability identifier in the `.conf` file.

Your probe will now be run against any target that has an attack level that corresponds to your new probe and, if necessary, which meets the conditions in the ruleset.

[IMPORTANT – User-developed probes are the sole responsibility of the user. SAINT does not imply or accept any responsibility for the syntax, logic, accuracy, validity or effects of user-developed probes.]

Example C program with the requisite structure and arguments:

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
main(int argc, char **argv) {
    char *target;
    short vulnerable = 0;
    if (argc < 2) {
        fprintf(stderr, "%s: not enough arguments\n", argv[0]);
        exit(1);
    }
    target = strdup(argv[1]);
    printf("BEGIN\n");

    /* check detection logic goes here */
    if (vulnerable)
        printf("%s|service|a|severity|ANY@ANY|ANY@ANY|Tutorial
Reference|Description|Technical Details\n", target);
    free(target);
}
```

How to Add a Vulnerability Tutorial (Information File)

If you decide to create your own probes, you will also probably want to create an information file to go along with it. We refer to these information files as tutorials. The tutorial should

contain information such as an explanation of the vulnerability, how to fix or devise a workaround for the vulnerability, and pointers to any applicable CERT or vendor advisories. Look in the *html/tutorials/vulnerabilities* subdirectory for sample tutorials.

To ensure that the product will be able to provide a link to the tutorial, look at the seventh field (canonical service output) of the vulnerability record which the tool outputs. (See [Database Format](#) for more details on database records.) The filename of the tutorials should be identical to this field, with underbars ("_") instead of spaces, and an *.html* suffix. For instance, for REXD, the canonical service output is **REXD access**, so the filename is **REXD_access.html**. If you want one tutorial to describe multiple related vulnerabilities, you should end the vulnerability text with "(tag)" and use HTML comment fields "`<!--TAG=tag-->`" and "`<!--/TAG-->`" to surround sections of the tutorial that are relevant to that particular vulnerability. When the tutorial is displayed, anything within tags that do not match the current vulnerability tag will be stripped. See the tutorial *http_cgi_access.html* for an example of how to use the tags. Place the finished tutorial in the *html/tutorials/vulnerabilities* directory.

Finally, if you want the vulnerability to appear within a certain vulnerability class in reports, add the tutorial name to the appropriate section of the *config/saintwriter/classmap.cm* file.

Exploit Plugins

The core of SAINT's exploit capabilities is its many vulnerability exploits. Exploits and related information are stored in separate plug-in files, making it easy to add or remove exploits. The plug-in files have a file name ending in *.sx* and are located in the *exploits* directory.

Each plug-in file contains general information about the exploit, tutorial information about the vulnerability, a definition of the input parameters, conditions under which to run the exploit, the type of shell spawned by the payload, and the exploit code itself. Each exploit component is discussed in more detail below.

General Information

Each exploit plug-in begins by defining some general information about the vulnerability. For example:

```
name = "Microsoft IIS 5.0 printer ISAPI extension buffer overflow";
id = "iis_printer_isapi";
```

SAINT Security Suite

```
date = "20060208";
cve = "CVE-2001-0241";
bid = "2674";
osvdb = "3323";
saint_id = "web_server_iis_iis,web_server_iis_iisx";
```

The *name* is the name of the exploit that is also the text the user sees in exploit results. The *id* corresponds to the file name of the plug-in, minus the .sx extension. The *date* is the date on which the exploit was added, in *YYYYMMDD* format.

cve is the [CVE](#) entry for the vulnerability. *bid* is the SecurityFocus [Bugtraq ID](#) of the vulnerability. *osvdb* is the [Open Source Vulnerability Database](#) entry for the vulnerability.

saint_id is the vulnerability check ID which is used to check for the same vulnerability. All SAINT vulnerability check IDs can be found in the vulns.dat file.

Tutorial Information

The tutorial information contains the information that the user will see when viewing the details of an exploit result.

The tutorial information is divided into five sections: Background, Problem, Resolution, References and Limitations. Each section is enclosed in braces. For instance:

```
problem {
The ISAPI extension which handles requests for file names
ending in <tt><b>.printer</b></tt> is affected by a buffer
overflow which could allow remote attackers to execute
arbitrary commands.
}
```

Notice that the tutorial information is written in HTML format. The only exception is the References section, which is simply a list of URLs. The URLs are shown as hyperlinks when viewed by the user.

Some client exploits have a sixth section, Instructions, which contains the body of the e-mail message that is sent out to prompt users to follow the exploit link. This section is plain text, except for the keyword `%ur1%` which stands for the link to the exploit. If the Instructions section is absent, then the e-mail message is a default string.

Type and Class

The next section of the exploit plug-in specifies the exploit type and class. For instance:

```
type = "remote";
class = "web";
```

- The *type* tells the engine how to run the exploit. The exploit type can be one of four strings:
 1. *remote* indicates that the exploit targets a service running on a remote host.
 2. *local* indicates that the exploit only runs after access to the target has been gained using a remote exploit or some other means. Local exploits usually result in privilege elevation if successful.
 3. *client* indicates that the exploit targets a vulnerability in an application which is initiated by a user. Client exploits use an [exploit server](#) to deliver the exploit to clients.
 4. *tool* indicates that the exploit does not attempt to penetrate the target, but instead performs some information gathering function.
- The *class* groups exploits together based on similar application types or attack vectors. It can have one of eight different values: web, mail, ftp, rpc, passwords, browsers, windows_os, and other.

Parameters

The *parameters* setting is a variable list corresponding to the arguments which are passed to the exploit plug-in when executed. For example:

```
parameters = ($port, $os, $shellport, $thisaddr, $target);
```

In this case, *\$port* is the TCP port number of the remote service, *\$os* is the platform type corresponding to one of the indices in the conditions, *\$shellport* is the port used for remote access (see [Shell Ports](#)), *\$thisaddr* is the address of the machine running the management

console for the purpose of connecting back with a shell, and \$target is the address of the target machine.

The parameter list corresponds to the fields that the user fills in when running the exploit individually. When running an automated penetration test, the values are automatically set by the exploit engine based on available information.

Conditions

Each exploit specifies a set of conditions that determine the circumstances the exploit should be attempted. The exploit engine automatically takes these conditions into account when deciding which exploits to run. For example:

```
platform[0] = "Windows 2012 R";
platform[1] = "Windows 7";
default_port = "80/tcp";
condition = "Microsoft-IIS/7\\.0";
```

In the above example, the exploit runs against Windows 2012 R and Windows 7. The number in the brackets is the index which corresponds to the \$os input parameter. (See [parameters](#).) 80/TCP is the default port when running the exploit individually and the port which triggers the exploit during automatic penetration tests. The string `Microsoft-IIS/7.0`, if found in the received data during a port scan, also causes the exploit to run, enabling exploitation on non-standard HTTP ports. Note that the dot is escaped by a backslash because the string is a Perl-compatible regular expression, in which the dot character alone would have special meaning.

In some cases, it is useful for the condition to have an index as well. For example:

```
platform[0] = "Windows 2012 R";
platform[1] = "Windows 7";
default_port = "80/tcp";
condition[0] = "Microsoft-IIS/7\\.0";
condition[1] = "Microsoft-IIS/7\\.1";
```

In this case, rather than just triggering the exploit, the conditions also specify the `$os` setting when running the exploit. This exploit would be run with `$os` equal to 0 against Windows 2012 R2 servers running IIS 7.0, and `$os` equal to 1 against Windows 7 running IIS 7.1.

It is also possible to specify the exploit's order within the execution sequence of an automated penetration test. For example:

```
order = 4;
```

This line tells the exploit to run after any exploits with an order of 1, 2, or 3, but before any exploits with an order of 5. Controlling the order of execution is useful for ensuring that exploits with a higher potential to cause crashes run after those with a lower potential to cause crashes, to avoid false negatives. Exploits which are not known to cause crashes typically have an order of 1. Exploits which may cause a service to crash typically have an order of 3 or 4. Exploits which could cause the whole system to crash typically have an order of 5. The default order is 3.

Shell Type

The payloads of the exploits vary in the way they allow remote access after successful exploitation. The shell setting tells the engine which method the exploit uses, so that it can properly set up the connection. For example:

```
shell = "reverse port";
```

There are several possible values for this setting:

- **direct:** a command is sent as an argument to the exploit
- **interactive:** an interactive command shell runs in the same socket as the exploit
- **port:** the exploit runs a command shell on the TCP port specified by the `$shellport` parameter
- **port *n*:** the exploit runs a command shell on TCP port *n*
- **reverse port:** a command shell connects back to the manager on the TCP port specified by the `$shellport` parameter
- **reverse port *n*:** a command shell connects back to the manager on TCP port *n*
- **select port:** same as `reverse port` if `$shelltype` parameter is 0 or `port` if `$shelltype` parameter is 1
- **none:** the exploit does not open a command shell

Regardless of the type of shell, the architecture supports the necessary steps to create the connection and transmit commands on behalf of the user. All of the above shell types appear the same under the Connections menu option and behave similarly from the user's point of view.

Exploit Code

The last section of the exploit plug-in is the exploit code. This is the exploit program itself. The start of the exploit code is marked by the word *exploit* followed by an open brace. The end is marked by a close brace. The code is written in SAINT's proprietary exploit programming language, which is syntactically similar to Perl but with some additional functions.

To add exploits written in a different programming language, simply have the code within the plug-in call the code in a separate file. For example, if you want to have the process call a Python program, create an exploit plug-in and put the following code into the plug-in:

```
exploit {
    exec("exploits/myexploit.py", @ARGV);
}
```

Where "exploits/myexploit.py" is the location of the external program. Make sure that the external program handles the input parameters specified in the plug-in's parameter list.

Rule Sets

Rules sets are a collection of files that make up the internal rules. For example, all inferences are done here; as well deriving what the target's operating system and hardware type are from other data collected in the system. The rules also inform the engine to run other probes based on past input. For instance, if a host is found to run *rexid*, then the *rexid.saint* probe might be run, based on a rule.

Each rule set is found in a file under the *rules* directory. The rules are written using standard Perl operators and regular expressions. See a Perl manual or the examples below if you are unfamiliar with Perl.

rules/cve

The cve rule set contains rules that map vulnerability records to the corresponding CVE numbers, DOD-CERT Information Assurance Vulnerability Alert (IAVA) numbers, and other standards if necessary. Each rule is applied once for each record that contains a vulnerability. (See the [Database Format](#) section.)

The rule format is:

```
condition TAB [yes|no] TAB CVE number(s) TAB IAVA number(s)
TAB other
```

Each condition is applied to the text field of each vulnerability record. If there is a match, then the corresponding CVE number(s) and/or IAVA number(s), if present and non-zero, are assigned to the vulnerability. If a record does not match any of the conditions in rules/cve, then no CVE/IAVA number is associated with the vulnerability.

The second field indicates whether or not the vulnerability is one of the legacy [SANS Top 20 Internet Security Vulnerabilities](#). The word "yes" in this field indicates that the vulnerability is on the list. Note: This Top 20 list, as specified here, was retired in 2007 as a top vulnerability list. That project has now shifted to a Top 20 Critical Controls approach. However, SAINT's repository retains the prior list for legacy and backwards compatibility purposes.

For instance, suppose CVE 1999-2501 and IAVA 1999-A-0101 correspond to the vulnerability whose output is `myservice is vulnerable`, which was on the Top 20 list. Therefore, the rule is:

```
/myservice is vulnerable/i   yes   CVE-1999-2501   IAVA 1999-
A-0101
```

The fifth field, "other" is an optional value which can be used to map vulnerability checks to a user-defined index. The value in this field, if present, is included in the scan results and can be included in an optional column in reports. By default, this field is empty.

rules/cvss

The cvss rule set assigns CVSS base scores and vectors to facts. This rule set is only used for vulnerabilities which don't have CVSS scores in the National Vulnerability Database. The CVSS scores in the National Vulnerability Database take precedence if they are available.

The rule format is:

```
condition TAB cvssv2_score cvssv2_vector cvssv3_score  
cvssv3_vector
```

Note: TAB represents the tab character.

For example, the following rule assigns a CVSSv2 base score of 10.0 and a CVSSv3 base score of 9.8 and the corresponding vectors to all vulnerabilities which have a severity code of "rs":

```
$severity =~ /^rs/i 10.0  
(AV:N/AC:L/Au:N/C:C/I:C/A:C) 9.8  
AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
```

If there are multiple matches within the rule set, the first match takes precedence.

Note that the `rules/cvss` file may be overwritten by SAINTexpress. Therefore, a separate file which doesn't get updated `rules/cvss.custom`, is provided. User customizations should go in `rules/cvss.custom` to ensure they are preserved during software updates. If both rule sets contain a matching rule, the one with the higher CVSS base score will be used.

rules/drop

This rule set specifies what data-collection tool output should be ignored. This can be used to prevent the process from saving certain facts which are not important. (Note that this is not the same as an exclusion, which allows saved facts to be hidden from view.) Each rule is applied once for each record that has an "a" in the status field, meaning the host is available. (See [Database Format](#).)

For instance, the scanner may detect what it thinks is an RDS vulnerability on myhost.com, even though you know for a fact that the patch has already been applied. In this case, we would tell the engine not to report the RDS vulnerability for myhost.com:

```
$target eq "myhost.com" && $text =~ /RDS/
```

The *\$target* variable holds the name of the target host (or the IP address if the name couldn't be resolved) and the *\$text* variable holds the output of the probe, which in this case was *http.saint*. Any of the global variables can be used. Note that *eq* with quotes around the expression looks for an exact match, while the *=~* operator with slashes around the expression will catch any string containing the expression. Other options are *ne* (not equal to) and *!~* (does not contain).

rules/facts

The facts rule set deduces potential vulnerabilities from existing data. For example, several versions of the FTP daemon are known to have problems on certain operating systems. Daemon versions can be recognized by their greeting banners.

Each rule is executed once for each record that has an "a" in the status field, meaning that the host is available. (See [Database Format](#).)

The rule format is:

```
condition TAB fact
```

(Note: TAB represents the tab character.)

For example, if we want to assume that if a host is running rexd it is insecure without trying to probe it further, we would put:

```
/runs rexd/
  $target|rexd|a|us|ANY@$target|ANY@ANY|REXD access|rexd
vulnerable
```

In order to understand the *rules/facts* file, you have to understand the [Database Format](#).

There are four macros which can appear in the condition part of the facts rule set:

- **HOSTTYPE** – expands to the host type of the target
- **OFFERS "<service>"** – expands to true if and only if the target offers <service>
- **INFO (*id*)** – expands to a stored information value about the target (see [rules/information](#))
- **check_<id>** – expands to true if and only if check_<id> is enabled in the current scan level

rules/hosttype

The hosttype rule set deduces the operating system version from various sources such as Nmap and Xprobe2 results, HTTP headers, SNMP information, and telnet and ftp banners. These rules are applied to every record that may contain host type information.

The format of this file is:

```
CLASS class_name
condition TAB hosttype TAB certainty
```

(Note: *TAB* represents the tab character.)

The class_name is used for the first rough breakdown by host type in reports. It should be a major software category, such as Ubuntu or Windows. For example, here is the code for recognizing Ubuntu and its major OS revision:

```
CLASS Ubuntu
UNKNOWN && /Ubuntu/                "Ubuntu 14.04"
```

While the code above may look fairly complex, it isn't really. Simply study the examples, and then modify the code in the examples to create your own rules.

The certainty field is a number from 1 to 10 which conveys the level of certainty that the inferred host type is actually correct. If multiple facts match different hosttype rules resulting in conflicting host types for the same target, the rule with the higher certainty is used. If this field is omitted, a value of 5 is assumed.

rules/information

The information rule set instructs the engine to remember a particular piece of information about a target. The information can be recalled later in [a facts rule](#). This allows the engine to infer new facts based upon known information about a target in conjunction with other facts.

The format of this file is:

```
condition TAB identifier TAB value
```

(Note: *TAB* represents the tab character.)

When there is a fact which matches the condition, then the value is stored in memory, and can be recalled later using the identifier. If the value is omitted, then *\$1* (the first group marked by parentheses in the condition) is implied.

An example information rule is:

```
/Internet Explorer version: ([\d\.]+) / ie_version
```

This rule tells the engine that when it finds, for example, a fact containing `Internet Explorer version: 11.0`, then it should remember the number 11.0. Later in the scan, the expression `INFO(ie_version)` can be used in a fact rule to infer a new fact based on the Internet Explorer version number.

rules/pci

The pci rule set assigns PCI automatic pass or failure codes to facts. Each code corresponds to an automatic pass or failure condition described in the ASV Program Guide. These codes are used to populate the exceptions column in ASV reports and are factored into the overall compliance status of the scan. Uppercase codes correspond to automatic failures, and lowercase codes correspond to automatic passes. See `tbl_pci_code_defs` in the database for the definition of all recognized codes.

The format of each rule is:

```
condition TAB code
```

Note: TAB represents the tab character.

For example, the rule:

```
$text =~ /SQL injection/i TAB SQL
```

will set all vulnerabilities whose descriptions contain the string “SQL injection” as an automatic failure for SQL injection. If there are multiple matches within the rule set, the first match will be used. This rule set doesn’t include per-CVE exceptions. Those are defined in `config/cve_cvss`.

Note that the `rules/pci` file may be overwritten by SAINTexpress. Therefore, a separate file which doesn’t get updated, `rules/pci.custom`, is provided. User customizations should go in `rules/pci.custom` to ensure they are preserved during software updates. If both rule sets contain a matching rule, the one with an uppercase code will be used.

In general, custom pci rules should only be created for automatic failures (i.e., uppercase codes). A rule with a lowercase code could cause an errant PCI pass status and will therefore generate a warning at the beginning of the scan.

rules/services

The services rule set translates cryptic daemon banners and/or network port numbers to more user-friendly names such as *WWW* or *diskless NFS client*. Each rule is executed once for each record that has an "a" in the status field.

The format of this file is:

```
class_name  
condition TAB service_name TAB host
```

(Note: *TAB* represents the tab character.)

If *host* is omitted, the host in the target field of the fact is implied.

The `class_name` is one of the following:

- **SERVERS:** The host offers a service, such as telnet, FTP, or NFS.
- **OTHER_SERVERS:** The same as above, except that OTHER_SERVERS are not listed individually in reports if there are more than five of them running on the host (unless, of course, *show all services* is selected). Services which are unknown or unimportant from a security perspective would fall into this class.
- **CLIENTS:** The host is a client of a service. For example, a host which mounts filesystems from an NFS server would fall into this class.

For instance, to classify a host as an NNTP server, you'd simply do this in the SERVERS section:

```
$service eq "nntp"                NNTP (Usenet news)
```

rules/software

This rule set classifies services according to the software providing the service. For example, *WWW* service might be provided by Apache or IIS software. These rules are applied to records for the identified service.

The format of this file is:

```
SERVICE service_name
condition TAB software_name TAB host
```

(Note: *TAB* represents the tab character.)

The *service name* should match the beginning of one of the service names in the [rules/services file](#). The *condition* is a Perl expression, with full access to the standard global variables (e.g., `$target..$text`). The *software name* specifies a name to identify the software, such as "Apache" or "IIS". If this field is not specified, the default is the first string captured by the pattern match with the *condition* (i.e., `$1`). The *host* field specifies the host that takes or provides the service. When no host is specified, the host in the target field of the fact (`$target`) is assumed.

For example, to classify Qualcomm as software type for the POP service, you might have a section:

```
SERVICE POP
/QPOP/i                Qualcomm
```

rules/todo

The todo rule set decides what probe to perform next. For example, when the target host offers the FTP service, and when the target is being scanned at a sufficient level, the engine will attempt to determine if the host runs anonymous FTP, and if the FTP home directory is writable for anonymous users.

Each rule is executed once for each record that has an "a" in the status field. (See [Database Format](#))

The format of this file is:

```
condition TAB target tool tool-arguments
```

(Note: *TAB* represents the tab character.)

The condition is a logical expression, with the usual internal variables, that has to be satisfied in order to run the probe specified. When the condition is satisfied, and the tool is allowed to be run conditionally at the current attack level (see [SAINT Configuration](#)), the tool is executed as:

```
tool tool-arguments target
```

The engine keeps track of which tools have already been executed against which targets.

For instance, if a host is running *ypserv*, we would typically run the *ypbind.saint* probe against it. This would be done as follows:

```
$service eq "ypserv"           $target "ypbind.saint"
```

It's easy to put in a probe that depends on the type of system that you're looking at. For instance, SGI/IRIX hosts have *guest*, *lp*, and other accounts with no password when taken out-of-the-box from SGI. Here's how you could check to see if this is a problem:

```
    /IRIX/                                $target "rsh.saint" "-u
guest"
```

This rule would tell the engine to run *rsh.saint* against every IRIX target. The "-u guest" argument tells *rsh.saint* to do an *rsh* as user *guest* to see if commands can be executed remotely, then record this fact in the results.

The todo rule set recognizes two macros. **HOSTTYPE** is expanded to the host type of the target. **SHORT_HOSTTYPE** is expanded to a shortened version of the host type, stripped of OS revision and release numbers.

rules/trust

This rule set helps the engine classify the data that was collected by the tools on NFS service, DNS, NIS and other cases of trust. Each rule is executed once for each record that has an "a" in the status field. (See [Database Format.](#))

The format of this file is:

```
condition TAB name of relationship
```

(Note: *TAB* represents the tab character.)

The current *rules/trust* file handles the most easily detected forms of trust:

```
$severity eq "1"                remote login
$text =~ /exports \S+ to/      file sharing
$text =~ / mounts \S+ /        file sharing
```

Database Format

Data gathered and inferred during scans is stored in a back end relational database as well as on the scanners' file system for backwards compatibility of legacy systems and partner integration. The following describes the database architecture, as well as the "legacy" database structure for files stored on the file system.

Database Structure

The SAINT VM deployment option is bundled with MySQL to simplify setup and configuration, as well as pre-loading and maintaining "static" system content, such as SAINT's vulnerability checks, exploits and tutorial library; and 3rd party content such as CVE, CVSS, CCE, and CPE content from authoritative sources and vendor reference information such as Microsoft Bulletins, Red Hat advisories, and IAVA codes. The database design is not published in this help product; however, is augmented by interaction via a RESTful API (application programming interface), used internally within the architecture and available upon request, to facilitate scan and content management external from the provided user interface.

Legacy Database Structure

File content stored on the file system are stored in the *results* directory. Each database contains four tables: [facts](#), [all-hosts](#), [todo](#) and [CVE](#). The tables are each plain text files where each line corresponds to one record. Fields are separated by the pipe character ("|"). Data directories may also contain a fifth file called *exclusions* which is a table of facts to exclude, but this file could be saved elsewhere and does not necessarily need to be in the data directory.

Data Files are stored in sub-directories named after the scan names. Archived files are stored under the current databases in a directory called *archive*. Each archived file is stored in a separate directory named by the Unix time (that is, the number of seconds since the start of the year 1970) that the scan completed.

facts

The **facts** file keeps track of all vulnerabilities detected, services offered, and any other information SAINT is able to collect throughout the scan. All information found in the **facts** database is in the form of text records. In each record are eight or nine fields, each separated by a pipe ("|") character. The inferences and conclusions found in this database are always in the same format.

The fields in the **facts** database are as follows:

- [Target](#)
- [Service](#)
- [Status](#)
- [Severity](#)
- [Trusted](#)
- [Trustee](#)
- [Canonical Service Output](#)
- [Text](#)
- [Technical Details \(optional\)](#)

Target

The Target field contains the name of the host that the record refers to. In order of preference, it uses FQDN, IP, estimated, or partial. Partial can result from service output getting truncated. For example, finger can return "*foo.bar.co*"; is that "*foo.bar.com*", or something longer? The scanning engine is designed to attempt to interpret the correct result. However, accuracy in these instances is not guaranteed.

Service

The Service field contains, in most cases, the basename of the probe which produced the record. This usually corresponds to the network service. The term *basename* refers to fact that most of the files corresponding to the individual probes have a ".saint" extension. When the probe name is written to the Service field, this extension is stripped off, and only the basename is written.

In the case of probes that check multiple services, such as *rpcinfo* or *tcpscan*, the name of the service being probed is used instead of the basename of the probe.

Status

Examining the Status field will, much as the name suggests, let you know the status of a certain probe. For instance, was a host reachable, did a probe timeout, etc. The codes that indicate the current status of the probe follow:

SAINT Security Suite

a	available
u	unavailable (e.g., timeout)
n	network (e.g., network or broadcast address)
b	bad (e.g., unable to resolve)
m	mobile device (discovered but not actually scanned)
x	look into further?

Severity

The Severity field distinguishes informational facts, service facts, and vulnerability facts. If a vulnerability was found during a probe, the Severity field will tell you how serious the vulnerability is. Each severity level is represented by a particular two to four letter code. These codes are listed below:

Critical Problems (red):

<i>rs</i>	administrator or root shell access
<i>us</i>	user shell access
<i>ns</i>	unprivileged (nobody)shell access
<i>ur</i>	user file read access
<i>uw</i>	user file write access
<i>nr</i>	unprivileged file read access
<i>nw</i>	unprivileged file write access
<i>ht</i>	evidence of penetration (hacker track)
<i>bo</i>	root acces via buffer overflow
<i>nfs</i>	access to NFS file systems
<i>dos</i>	denial of service

Areas of Concern (yellow):

<i>yus</i>	unlimited X server access
<i>yi</i>	information gathering
<i>ype</i>	privilege elevation
<i>ycs</i>	use as an intermediary (cross-site)

<i>ymc</i>	susceptibility to malicious content
<i>ysb</i>	security bypass
<i>ydos</i>	authenticated denial of service

Potential Problems (brown):

<i>zcio</i>	check it out for possible vulnerabilities
<i>zwoi</i>	do you want this accessible on the Internet?
<i>zp</i>	poor security policy
<i>zdos</i>	possible denial of service
<i>zur</i>	possibly unreliable scan results

Others (not vulnerabilities):

<i>g</i>	services (green)
<i>i</i>	information

If the severity code for a red, yellow, or brown vulnerability is capitalized, then the vulnerability is confirmed. If the severity code is lowercase, then the vulnerability is inferred.

Trustee and Trusted

These two fields will list the trustee and the trusted entities, respectively. The trustee is an entity which trusts the trusted entity. The trusted entity is the entity that is trusted by the trustee. The entries in these fields are comprised of two tokens, separated by the "at" sign ("@"). To the left of the "at" sign, you will see an entry which indicates the user or object. To the right of the "at" sign is the host. Either entry can be the word ANY. For example, consider the following Trustee field:

`/home@target.com`

This Trustee field would indicate that the `/home` directory on the host `target.com` trusts the trusted entity. That is, the trusted host(s) are allowed access to `/home`. Now suppose the same record contains the following Trusted field:

`ANY@goodhost.com`

This Trusted field would indicate that any user on *goodhost.com* is trusted. That is, any user on *goodhost.com* is allowed to access the */home* directory on *target.com*. Now suppose that the Trusted field is:

ANY@ANY

Now any user on any host is trusted, meaning that anyone on the Internet is allowed access to */home* on *target.com*. This fact could be very serious indeed.

Canonical Service Output

In the case of non-vulnerability records, this is a reformatted version of the output from the network service. In the case of vulnerability records, this is a description of the problem type. This name is used in reports by vulnerability type, and uses it to locate the corresponding vulnerability tutorial.

Text

This field contains English messages which are displayed in the final report.

Technical Details

This field contains technical details about the vulnerability check, usually including data that was sent or received or a brief description of how the vulnerability was detected.

all-hosts

The *all-hosts* file keeps track of what hosts the scan engine has seen, including hosts that may or may not exist. Non-existent hosts might include, for instance, hosts reported from the output of the *showmount* command. The database is an ASCII file, with fields separated by a pipe ("|") character. The fields follow:

- **Hostname:** The hostname of the host
- **IP address:** The IP address of the host
- **Proximity Level:** How many jumps away the host is from the original target(s).
- **Attack Level:** The attack level at which the host was scanned. A negative number indicates that the host was not scanned.

- **Subnet Expansion:** Whether or not subnet expansion was enabled, where 1 denotes yes and 0 denotes no.
- **Time:** The overall completion time of the scan against the host, if any, measured in Unix internal time; that is, the number of seconds since January 1, 1970
- **Version:** The SAINT product version number which was in place when the host was last scanned
- **MAC Address:** The Media Access Control (MAC) address of the host, if known (The MAC address can only be determined for hosts which are on the same network segment as the host running the SAINT product.)
- **System Class:** The host's general system type, such as Windows or Linux.
- **System Type:** The host's specific operating system - including the version number or service pack level, if known.
- **CPE:** The operating system's name in the [Official Common Platform Enumeration \(CPE\) Dictionary](#), if known.
- **Original Target:** The original target entered by the user, before any range expansion, URL parsing, or hostname resolution.

See [Configuration](#) for more information on these variables and concepts.

todo

The *todo* database keeps track of what probes have already been done. This database contains text records, each containing the following three fields separated by a pipe ("|") character:

- **Hostname:** The hostname of the targeted host
- **Probe name:** The name of the probe which was run against the host
- **Arguments:** The arguments with which the probe was run

The tools perform .saint probes against the *hostname* with the arguments, if any.

cve

The *cve* file keeps track of any vulnerabilities found which have a corresponding [CVE](#) name, DOD-CERT Information Assurance Vulnerability Alert (IAVA) number or any other index number. This database contains text records, each containing the following fields separated by a pipe ("|") character:

- **Top 20 flag:** Whether or not the vulnerability was on the Top 20 list ("yes" or "no") prior to its retirement in 2007.
- **CVE name(s):** The CVE name or names corresponding to the vulnerability, if any
- **Vulnerability Text:** Corresponds to the [text](#) field in the [facts](#) database
- **IAVA number(s):** The DOD-CERT IAVA number(s) corresponding to the vulnerability, if any
- **Other index:** Any other standardized index number, besides CVE and IAVA, that may be associated with the vulnerability (This field is empty unless a user-defined index has been added to [rules/cve](#).)
- **Check ID:** The SAINT check ID which detected the vulnerability
- **BID number(s):** The BID number or numbers corresponding to the vulnerability, if any
- **OSVDB number(s):** The OSVDB number or numbers corresponding to the vulnerability, if any
- **NSID number(s):** The Nessus script ID number or numbers corresponding to the vulnerability, if any
- **CPE(s):** The CPE (Common Platform Enumeration) version 2.3 entries corresponding to the vulnerability, if any. To save memory, the first two fields and the wildcard fields are removed from each entry.
- **CVSS and PCI information:** The CVSSv2 (Common Vulnerability Scoring System version 2) base score, condensed CVSSv2 base vector, PCI status code, CVSSv3 base score, and condensed CVSSv3 base vector for the vulnerability, joined by dashes. The PCI status code indicates whether the vulnerability causes PCI failure and why. Capital codes indicate the vulnerability causes PCI failure, and lowercase codes indicate the vulnerability does not cause PCI failure. The most common codes are "NVD" and "nvd", indicating that the vulnerability fails or passes PCI based on the CVSS score found in the National Vulnerability Database. Other codes indicate automatic failures or other exception types explained in the ASV Program Guide. If multiple words are listed, the first one (before the colon) applies to the vulnerability as a whole, and the remaining ones (after the colon) correspond to the CVEs found in the second field.

pentest

The *pentest* directory stores exploit data, including the results of all exploit attempts and other information gathered during automated penetration tests.

The exploit files have the same names as the vulnerability files (all-hosts, todo, facts and CVE). The formats of exploit files are the same as their vulnerability counterparts, with the following exceptions:

- Instead of the [trustee](#), the fifth field in exploit facts is the exploit class.
- Instead of the [canonical service output](#), the seventh field in exploit facts can be the exploit ID. This corresponds to the file name of the exploit plug-in which produced the fact, but without the .sx extension.
- CVE records can contain three additional fields. The sixth field is the SecurityFocus [Bugtraq ID](#) (BID) number. The seventh field is the [Open Source Vulnerability Database](#) (OSVDB) number. The eighth field is the [Nessus script ID](#) (no longer supported via open source).

The Severity field in exploit facts include the following:

- **ra**: remote administrative access
- **ru**: remote user access
- **c1**: client access
- **pe**: privilege elevation
- **un**: no access (unsuccessful)

For more information on these severity levels, see [exploit severity levels](#).

Glossary and Terms

Asset

Scan targets that have been discovered and collected into the Security Suite or SAINTCloud data repository are considered Assets. Unlike Target Groups, that are logical collections of 'like' scan targets, identified by a network address identifier (IP address; Hostname; URL; etc.), Assets represent actual, physically identified hosts that have been scanned by the scan engine.

Asset Tag

Asset Tags are descriptive names that logically describe a scanned host (aka Asset). They are designed as Key:Value pairs, to support local requirements for tracking, managing and analyzing scan results in a business context. For example, an Asset Tag with key="Criticality" can have one or more values, such as High, Medium and Low. The Assets component of SAINT products provide the capability to create Asset Tags and then associate them to hosts that have been scanned and stored in the asset repository. For example, IP="10.2.0.1" with Hostname='local.Msmith" can be associated with an Asset Tag "Criticality=High". Once tagged, scan jobs can be created by Asset Tags to manage scan activity in a business context, as well as used in analysis and reporting to prioritize remediation efforts with the same business context.

Asset Identification (AI)

Asset Identification (AI), under SCAP, is a format for uniquely identifying assets based on known identifiers and/or known information about the assets. The SCAP specification describes the purpose of asset identification, a data model for identifying assets, methods for identifying assets, and guidance on how to use asset identification. It also identifies a number of known use cases for asset identification.

SAINT Security Suite and SAINTCloud support the AI specification, version 1.1, by generating Asset Identifiers as part of the Asset Report Format (ARF) output. Output generated for scans are executed for any SCAP scan profile or benchmark, for both OVAL and XCCDF content. Asset identifiers are make available as content in the pre-configured ARF output in the SCAP module, by selecting a completed OVAL or XCCDF scan and viewing the ARF Report from the *Manage Results Data* page. Asset Identifiers are then available to users by selecting individual output files for any target assessed during the scan. The AI and ARF report can then be viewed within

the SCAP user interface or exported in XML format to support local requirements and/or compliance reporting.

Asset Reporting Format (ARF)

The Asset Reporting Format (ARF), under SCAP, expresses the transport format of information about assets and the relationships between assets and reports. The SCAP specification prescribes the standardized data model to facilitate the reporting, correlating and fusing of asset information throughout and between organizations.

SAINT Security Suite and SAINTCloud support the ARF specification, version 1.1, by generating ARF-formatted output. Output generated for scans are executed for any SCAP scan profile or benchmark, for both OVAL and XCCDF content. ARF formatted output is made available as pre-configured output in the SCAP module, by selecting a complete scan and viewing the SCAP-compatible results from the *Manage Results Data* page. The final ARF output is then made available as one of the selectable output formats for individual targets assessed during the scan. The ARF report can then be viewed within the SCAP user interface or exported in XML format to support local requirements and/or compliance reporting.

CCE™

Common Configuration Enumeration (CCE) is a dictionary of names for software security configuration issues (e.g., access control settings, password policy settings). As such, CCEs describe system configuration issues to facilitate correlation of configuration data across multiple information sources and tools. SAINT products provide support for CCEs by displaying CCE IDs, in accordance with the specifications and CCE 5.0 schema located at <http://cce.mitre.org> for each configuration item in scanning results produced for XCCDF scanning policies and profiles. Analytics capability also provides data drill-down and report configuration options that include displaying CCE ID and Descriptions. CCE IDs are displayed in several of the different reports offered via the data analysis in the Benchmark Reports page. These include the required output format defined as “CCE ID, pass/fail” and a detail format which organizes results by XCCDF Rules, and displays results for each XCCDF Rule, to include: the CCE IDs; CCE descriptions; whether or not the CCE passed/failed against the target system; and why the CCE passed/failed against the target system. A policy editor is also provided to allow users to disable and enable configuration checks by CCE to meet specific network requirements.

Checks (Vulnerability Check)

A vulnerability check is the programming logic used to interrogate a target host for the evidence of a specific vulnerability. A check contains the check ID, a description, the associated CVE identifier, as well as other information used SAINT's inference engine to determine whether a vulnerability exists.

Confirmed Vulnerability

Vulnerabilities identified using a definitive test, such as an exploit that gains read access to a file on the target or a successfully guessed password.

CPE™

CPE (Common Platform Enumeration) is a structured naming scheme for information technology systems, software and packages. SAINT products provide support for CPE, version 2.3, by using the CPE names which are defined in the official CPE dictionary at <http://nvd.nist.gov/cpe.cfm>, then mapping all known CVE(s) to the corresponding CPE(s) for a given year. SAINT also facilitates CPE content updates directly from the authoritative source, as a product feature, to remove the burden of data maintenance from the user and to ensure accurate and complete source data when CPE data is used. This CVE-CPE mapping is used within the reporting component as an available option in custom reports.

Custom reporting features enable users to select all vulnerabilities in a given severity level, as well as define report parameters and options related to specific vulnerability categories and services, such as CPE, to display the CPE entries corresponding to displayed vulnerability, if any. SAINT's reporting options also enable users to select the output format from a number of available formats, such as HTML, XML and CSV.

CVE®

CVE (Common Vulnerabilities and Exposures) is a dictionary of publicly known information security vulnerabilities and other information security exposures. The CVE repository is maintained by MITRE and is a free-use site. SAINT products provide support for CVE with the capability to execute vulnerability scans for vulnerabilities, by CVE ID—they internally identify vulnerabilities by proprietary vulnerability check IDs and then cross-references with CVE names. The scan engine returns all vulnerability checks that detect the CVE and includes CVE numbers

in its vulnerability data analysis, reports and tutorials for ease of reference to related tools and resources. At the conclusion of vulnerability scan execution, analytics features provide users with the capability to view the list of vulnerabilities and continue the analysis by supporting customized scanning by selected CVE for a given vulnerability or by selecting other categories or values relevant to the analysis.

Analytical and report writing features then provide the capability to produce report output containing CVE IDs in a number of formats, such as HTML, XML and CSV. These features also provide hyperlinks to related resources, such as an online CVE Index that includes the CVE ID, description and custom SAINT tutorials; as well as linking directly to the official CVE descriptions at <http://cve.mitre.org> to facilitate further analysis, assessment and remediation.

CVE data is updated dynamically as part of each release/update cycle – routinely twice each week. The “Generated Date” (by MITRE) and “Updated Date” (by SAINT) are part of this content. Note that there is a subclass of CVEs, called "candidates" that are potential CVEs but have not yet been approved. The candidate CVEs are prefixed by "CAN" in the SAINT/CVE cross-reference list. When candidates become approved in a new CVE version, they are moved from the "CAN" section of the cross-reference list to the "CVE" section, and then made available for report output and vulnerability tutorials. The SAINT/CVE cross-reference list includes CAN and CVE entries on the same page, so the browser's search function can search for both CVE and CAN entries when the YYYY-NNNN portion of the identifiers are specified in the search. The complete list of CVEs supported by SAINT can be found on our customer portal site ([mySAINT](#)).

CVSS

CVSS (Common Vulnerability Scoring System) is “a vulnerability scoring system designed to provide an open and standardized method for rating Information Technology vulnerabilities framework for communicating the characteristics and impacts of IT vulnerabilities.” CVSS helps organizations prioritize and coordinate a joint response to security vulnerabilities by communicating the base, temporal, and environmental properties of a vulnerability. For more information see the [CVSS web site](#).

SAINT products provide support for CVSS through scanning, analysis and reporting capabilities providing users with the capability to create custom scanning policies that include specified CVSS ranges when defining scan levels and setting up custom scans. Reporting options also enable the user to show the CVSS base score and CVSS base vector for each vulnerability

detected, as an optional column, when creating custom reports. Custom reporting features within the *Report* page enable users to select all vulnerabilities in a given severity level, as well as define report parameters and options related to specific vulnerability categories and services, such as CVSS base scores and CVSS base vectors, to display the CPE entries corresponding to displayed vulnerability, if any. SAINT products then enable users to select their output format from a number of available formats, such as HTML, XML and CSV. Additionally, SAINT products provide support for CVSS as part of Payment Card Industry (PCI) Compliance. CVSS base scores are shown as part of PCI compliance reports. CVSS base scores are used as the primary factor in determining whether a given device is compliant during a PCI compliance assessment.

SAINT backend processes import CVSS base scores, CVSS vectors and “date generated” from the National Vulnerability Database ([NVD](#)), and delivers that information, as well as the date updated, to our customers through our SAINTexpress maintenance release process. The raw CVSS content is stored in the product database and is also available in the configuration sub-directory of the SAINT installation directory (e.g., `config/cve-cvss`). Each line in the `cve-cvss` file contains the name of the source file the data following that line was extracted from, along with both the “generated” and “updated” dates for the source file - prefixed with the “#” character.

Distributed Node

Like a Remote Node, a Distributed Node is a term that describes a Scanner Node that is not the default Local Node that is a part of the base installation. A distributed node can be synonymous with a Remote Node, in that the term may also apply to a scanner node that has been installed (e.g. distributed) in a remote location. But, this term is more commonly used to describe any connected scanner other than the default Local Node. For example, for a large network, an installation may include the Manager, Local Node and 25 additional Scanner Nodes to distribute the workload, either through load balancing or directing specific scan jobs across multiple scanners. In this use case, the scanners are not deployed remotely. Simply installed along with the Manager to manage scanning from the central location.

Exploits

An individual exploit is programming logic used to interrogate and penetrate a vulnerable host based on the weakness identified by a vulnerability scan. An individual exploit is specific to a

CVE. However, an individual vulnerability may be associated with multiple CVEs, and as a result, may have multiple exploit paths for a single vulnerability.

FDCC

FDCC is the Federal Desktop Core Configuration. The Federal Government first instituted security guidelines in 2007 with a directive from the Office of Management and Budget (OMB) on the “Implementation of Commonly Accepted Security Configurations for Windows Operating Systems.” This directive – called the “Federal Desktop Core Configuration” or FDCC – required agencies to adopt security configurations defined by the National Institute for Standards and Technology (NIST) for Windows XP and Vista operating systems. This initiative has evolved over time into the USGCB. SAINT products provide support to FDCC by ingesting SCAP-expressed data streams and assessing targets for compliance.

FISMA

The [E-Government Act \(Public Law 107-347\)](#) passed by the 107th Congress and signed into law by the President in December 2002 recognized the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, entitled the [Federal Information Security Management Act \(FISMA\)](#) requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

SAINT products provide support to Security Controls CA-7 – Continuous Monitoring; RA-3 – Risk Assessment; and RA-5 – Vulnerability Scanning as a vulnerability scanner and penetration testing tool. SAINT products provide a FISMA scan policy as one of its default scan levels, as well as providing a pre-configured FISMA Vulnerability Assessment Report through the report engine. These capabilities enable managers to use the results of the vulnerability scans to execute penetration testing of target hosts. The results can then be used as “evidence of the potential harm” from the identified vulnerabilities, thus allowing for a more holistic approach to risk analysis and management.

HIPAA

The Health Insurance Portability and Accountability Act (HIPAA), enacted in 1996, mandates that companies take extraordinary steps to protect the medical information they collect from patients. The law affects insurers, hospitals, laboratories, doctor's offices and the pharmaceutical industry. The law also applies to employers who keep employee health data for insurance purposes.

SAINT products provide support to HIPAA by providing a customized scanning template that supports requirements from recent compliance requirements and security rules. Related to HIPAA, the scan template is based on standards requirements from the Security Rule, focused on Risk Analysis and Risk Management, as well as overall vulnerability scanning and output specifications outlined through NIST. SAINT products also provide support for a customized HIPAA Vulnerabilities Assessment Report that enables managers to assess their security posture and make informed decisions related to compliance, corrective action and on-going risk management. These capabilities also provide managers with penetration testing tools to attempt exploitation of selected vulnerabilities to gather further evidence of the impact of these vulnerabilities and risk to their assets.

Inferred Vulnerability

Vulnerabilities determined from information such as service banners and software version numbers or potentially derived from the existence of other related vulnerabilities.

Job

A scan Job is the heart of the vulnerability or penetration testing setup and execute. A Job contains a unique name, description, target list, possibly target exclusions (e.g., target list is a Subnet but must exclude individual hosts), a scan policy, authentication credentials (or run as uncredentialed), configured as a single "one off" scan or configured as a recurring scan, and contains specific scanning configurations for all scans to be run for the job. Jobs can be associated with a Target Group, and inherit the targets defined in the group, or can be run and managed outside of a Target Group.

Key (SAINT key)

The key contains all information about your product license and is used by the software to validate the status of the license and retain the current status of your usage. For example, total number of licensed targets and the current usage.

Local Node

A Local Node is the default scanning engine (see Scanner Node) that is pre-installed with all installations that are set up and configured as the main management console. For most installations, this configuration (Manager-Local Node) is the most common deployment for Security Suite.

mySAINT

The mySAINT portal (<https://www.saintcorporation.com/cgi-bin/secure/customer/logon.pl>) is the back end customer website that provides content, help, and a lot more to enhance your user experience with SAINT products. This site provides the capability to download licensed products; create and manage license keys; view information about all licensed products; see the details about the latest product updates, vulnerability checks and exploits; download useful tools and help content; view detailed information about product content related to OVAL, XCCDF, exploits and vulnerabilities; and a whole lot more.

Nodes

Each SAINT scan is executed by a SAINT scanner “node”. A scanner Node is an instance of the scanning engine, managed by a Security Suite or SAINTCloud user interface, through the SAINT API or from a command line interface (CLI). The scanner Node receives scan job instructions from the software, communicates between the SAINT inference engine, scanner probes and target hosts; and communicates results back to the software for storage and presentation. Each installation comes pre-packaged with a single scanner node (aka “local node”).

OVAL®

Open Vulnerability and Assessment Language (OVAL) is an international information security standard to promote open and publicly available security content, and to standardize the transfer of this information across the entire spectrum of security tools and services. SAINT

SAINT Security Suite

products support OVAL definitions of the patch, vulnerability, compliance and inventory class for most platforms and adheres to the latest OVAL schema (e.g., v.5.10.1 as of the date of SCAP v.1.2 validation). The scanning engine then consumes and executes selected definitions and assesses hosts, without the need for a local agent or plugin, to determine and report issues found on the hosts.

SAINT products support OVAL compliance checking by allowing users to import OVAL checks (standalone and/or SCAP-expressed data streams) from the OVAL repository, as well as importing user-developed XML files containing OVAL checks. An SCAP-expressed data stream is defined as “a collection of four or more related XML files containing SCAP data using the SCAP components that provide the data necessary to evaluate systems for compliance with a configuration-based security policy.”

SAINT products also provide viewing and downloading OVAL result files via the GUI, as well as viewing human readable (non XML) results.

OWASP

SAINT products provide a pre-defined scan policy that spans the [OWASP](#) Top 10 Web Application Security Risks. The Open Web Application Security Project (OWASP) organization’s primary focus is on improving the security of software.

Pause Window

A Pause Window is a scan status indicating an active recurring scheduled scan is currently paused because a Scan Window was defined for the Job and the active job was still running at the time the defined window was reached. The active scan will resume at the start of the next Start/Resume time of the defined scan window.

PCI

Payment Card Industry (PCI). The PCI Security Standards Council (SSC) is the oversight council that defines the technical requirements and specifications required of merchants, service providers and security assessors as it relates to systems that process credit card transactions or contain credit card information. SAINT Corporation is an Approved Scanning Vendor (ASV) certified by the PCI SSC to perform scanning and attestation services applicable to Requirement 11.2 and the ASV Program Guide. SAINT products provide a pre-defined scanning policy,

analytics, and pre-defined reporting types that are Requirement 11.2 compliant. SAINT scanning and penetration testing products provide support for many other PCI requirements – most notably requirements for internal vulnerability scanning and internal and external penetration testing.

Policy

A scan policy is a logical grouping of vulnerability checks. For example, a PCI policy is a pre-defined scan option that interrogates target hosts for vulnerabilities and configurations required Requirement 11.2 of the *PCI ASV Program Guide*.

Probes

A scan “probe” is a collection of vulnerability checks related to a technology or platform (e.g., Microsoft Windows probe). SAINT products provide a mechanism for users to create custom vulnerability checks that will be accessed by probes based on locating the applicable technology or platform signature found during the discovery phase of a scan.

Remote Node

A Remote Node is a term to denote a Scanner Node that is deployed into a remote network or remote location for the purposes of accessing target hosts that may not be accessible from the Manager’s location. For example, the manager’s location is in a central data center, and a scanner node is deployed into a network in a different state, and makes a secure connection to the central manager used to direct scans to one or more remote mode.

SAINT® ASV

This SAINT product is a SaaS-based (Software-as-a-Solution) ASV scanning and attestation service. This product provides customers with direct access to a scan solution and SAINT's ASV service offering, for those that must comply with Requirement 11.2 of the *PCI DSS and ASV Program Guide*.

SAINTCloud™

This SAINT product is a SaaS-based (Software-as-a-Solution) solution that provides the full functionality and power of SAINT software and appliance-based software (scanner,

configurations, exploit, reporting) but is tailored for those customers that want the convenience of a cloud-based solution with no software installation required and data stored in the cloud. SAINT Cloud is accessed through a secure web portal.

SAINTexpress®

This plug-in is deployed with every installation of the software and is used to communicate back to SAINT's update server and pull the latest vulnerability checks, exploits, bug fixes and product updates.

Scans

Scans are the results of running individual scan job instances against targets. Jobs can include individual "one off" scans or they can include multiple scans as a result of scheduled, recurring scan jobs.

Scan Window

A Scan Window is a feature to enable a user to define when recurring scheduled Job scans can be active. For example, schedule a job to run each night, starting at Midnight, but create a Scan Window of Midnight to 5am, nightly. If a scheduled scan is still running as of 5am, the scan will Pause, with a Status of "Pause Window" and resume at the start of the next scan window (midnight).

Scanner Node

Every installation comes bundled with at least one scanning engine. In SAINT terminology, each scanning engine is called a scanner 'node'. The default scanner node connected to the management console (aka "Manager"), and part of the default installation, is named "Local Node". The SAINT architecture does support connecting more than one scanner node to the manager, to manage scalability, capacity and complex network architectures. For example, scanning remote locations or large-scale environments by connecting multiple scanner nodes to the manager, such as deploying scanners inside of multiple subnets (see Remote Node), assigning scanning permissions to groups of users to individual scanners, and enterprise-level scalability and performance by directing scan jobs across multiple scanners to distribute the workload (see Distributed Node).

SCAP

SAINT Security Suite and SAINTCloud provide support to The Security Content Automation Protocol (SCAP) specification, as an Authenticated Configuration Scanner (ACS), including the Common Vulnerabilities and Exposures (CVE) option. SAINT provides support to SCAP requirements defined for each of these components, as defined in SP 800-126, Revision 2, the SCAP specification, and verified by compliance testing against the Security Content Automation Protocol (SCAP) Version 1.2 Validation Program Test Requirements (NISTIR 7511, Revision 3), dated January 2013 – including updates as of July 2013.

SAINT's release strategy includes a numbering convention that supports periodic feature releases (8.x) and security content (8.x.x) that offer added capabilities and functionality since the 8.0 launch. The version 8.4 major product release was designed and submitted as the first major release to support SCAP Version 1.2 standards. SAINT's release schedule will continue to support this release strategy, however, these releases will not alter the SCAP component of the product in a manner that impacts compliance with the SCAP v.1.2 specification. Thus, SAINT products will remain compliant with SCAP v.1.2 for 8.4 and above, until the specification requires new validation.

SAINT products provide support for open standards languages, enumerations and metrics that currently include XCCDF, OVAL, CCE, CPE, CVE and CVSS, AI, ARF and TMSAD of the specification. SAINT products also provide support for the U.S. Government Configuration Baseline (USGCB) by ingesting valid SCAP-expressed data streams and assessing target configurations against these baselines. These capabilities also provide support for evaluating SCAP content to scan for compliance, vulnerabilities, and patches using both standalone OVAL definition files and OVAL definitions contained in SCAP-expressed data streams.

SAINT products complete this capability by providing data analysis, links to external authoritative sources of information, policy editing and reporting interfaces, to facilitate local policy investigation and analysis, as well as compliance reporting in canned and custom presentation of output in machine-readable and many human-readable formats, such as HTML, PDF, XML and CSV.

STIG

Security Technical Implementation Guides (STIGs) and NSA Guides are the configuration standards for DOD IA and IA-enabled devices/systems. A STIG Security Checklist, typically a companion of a STIG, is essentially a document that contains instructions or procedures to manually verify compliance to a STIG. Since 1998, DISA Field Security Operations (FSO) has continued to enhance the security posture of DoD's security systems by providing these STIGs, that contain technical guidance to "lock down" information systems/software that might otherwise be vulnerable to a malicious computer attack. DISA FSO is in the process of moving the STIGs towards the use of the NIST Security Content Automation Protocol (SCAP) in order to be able to "automate" compliance reporting of the STIGs. SAINT products provide support to STIGs through a combination of SCAP functionality via the XCCDF configuration benchmarks, and through mapping of IAVA codes to vulnerabilities. A Benchmark, in this definition, is an "automated" STIG which may be used in conjunction with an SCAP compliant tool like SAINT Security Suite to provide automated compliance reporting for the applicable STIG. A master list of the current STIGs published by DISA can be found at <http://iase.disa.mil/stigs/a-z.html>

Target

Targets are the hosts to be scanned. SAINT scanning solutions currently scan virtually any physical and virtual host with an IP address, both for IPv4 and IPv6 addresses.

Target Group

This feature allows you to create a logical container or grouping of scan targets in a way that fits business needs, and then associate scans to this logical container. For example, create a Target Group for a subnet at a physical location to reduce the setup time to create jobs for that location's network range (Target Group="Dallas"; Targets: 10.2.0.2/24). Create scan Jobs and associate them to the Target Group, to organize scan jobs in a more logical, hierarchical manner. Once hosts have been discovered and collected in the asset repository, they can then be tracked and managed as Assets by logical Asset Tags.

Trust Model for Security Automation Data (TMSAD)

The SCAP Trust Model for Security Automation Data (TMSAD) is a specification for using digital signatures in a common trust model applied to other security automation specifications. The

SCAP specification prescribes the standardized data model for establishing trust for security automation data.

SAINT products support the TMSAD specification, version 1.0, by verifying the XML signature to ensure the content has not been modified. If a signature is not valid, the scanning engine aborts the scan and generates an error to notify the user of the failed scan.

USGCB

SAINT Corporation asserts that the SAINT Security Suite and cloud-hosted SAINTCloud products are fully functional and operate correctly as intended on systems using the U.S. Government Configuration Benchmark (USGCB). Target settings applicable to performing USGCB assessments are defined in the [SCAP section](#). To run a scan, the targets must meet only the requirements for running a normal authenticated scan. Targets can be scanned for USGCB compliance by importing the desired USGCB SCAP Data Stream, containing XCCDF and OVAL document formats, and selecting it when choosing a scan policy to run. USGCB scans make use of CCE to simply tracking of configuration issues found during a scan. SAINT products produce multiple reports in both the required formats for SCAP and some non-required formats for data analysis. The reports are viewable in the *SCAP Data* section of the GUI and can also be bundled and downloaded to support external requirements such as content backups, compliance reporting or importing into other applications.

XCCDF

XCCDF (Extensible Common Configuration Data Format) is a specification language for writing security checklists, benchmarks and related types of documents defined by NIST. SAINT products provide the capability to import, validate, view, execute policy scans, and report on benchmarks in XCCDF format, version 1.2. SAINT products provide two methods of collection: 1) Select a supported policy to validate and Import or Update content; and 2) Use the *SCAP Upload Benchmark* option in the Benchmark Scanning data grid to manually import definitions for validation and execution by SAINT's scanning engine. This capability includes support for importing SCAP Expressed Data-Streams in .zip and .xml formats.

SAINT products also provide a Policy Editor for those users that wish to use an existing XCCDF-based policy as a template to edit and save a custom policy to support local requirements. This editor allows users to view such information as the detailed descriptions of each group and rule

SAINT Security Suite

contained in a policy; and to enable and disable checks (rules), and modify values associated with certain rules.

XCCDF-based scan results can be viewed or downloaded in a number of compliance formats: XCCDF Results document; XCCDF Human readable results document; OVAL system characteristics for each target; and OVAL Results documents that resulted from the XCCDF scan.