tenable network security

SecurityCenter 4.7 Installation Guide

October 17, 2013

(Revision 2)

Table of Contents

Introduction

This document discusses the installation, initial configuration, and a sample scan using Tenable Network Security's SecurityCenter 4.7 (US Patent No. 7,926,113 B1, "System and Method for Managing Network Vulnerability Analysis Systems"). Hardware and software requirements as well as detailed step-by-step instructions are included along with important notes and warnings to help ensure the success of the deployment.

Since many of Tenable's customers have requirements to maintain separation of duties, the SecurityCenter 4.7 documentation has been separated into the following documents to better organize the material based on the organizational role. Note that there may be some overlap in roles as well as content provided with each of the following guides:

- **SecurityCenter 4.7 Installation Guide** – This document provides instructions for the installation of SecurityCenter 4.7. The target audience for this document is system administrators who need to install the SecurityCenter application. Included in this document are quick instructions for the **admin** user to add a Nessus scanner and create a user account to launch a test scan to ensure SecurityCenter is correctly installed.
- **SecurityCenter 4.7 Upgrade Guide** – This document describes the process of upgrading to the latest version of SecurityCenter 4.7.
- **SecurityCenter 4.7 Administration Guide** – This document provides instructions for the administration of SecurityCenter by the **admin** user. The **admin** user is the first user to log into the SecurityCenter after the initial installation and is responsible for configuration tasks such as defining organizations, repositories, Nessus scanners, LCE servers, and PVS sensors. The **admin** user does not have the ability to create and launch Nessus scans.
- **SecurityCenter 4.7 User Guide** – This document provides instructions for using SecurityCenter from an Organization Head user or lesser account.

Please email any comments and suggestions to support@tenable.com.

Users are strongly encouraged to read this entire document before installation and utilize the steps provided to ensure deployment success.

A basic understanding of computer security, Linux/Unix, Windows, computer hardware, and Nessus vulnerability scanning is assumed.

Standards and Conventions

Throughout the documentation, filenames, daemons, and executables are indicated with a **courier bold** font such as **gunzip**, **httpd**, and **/etc/passwd**.

Command line options and keywords are also indicated with the **courier bold** font. Command line examples may or may not include the command line prompt and output text from the results of the command. Command line examples will display the command being run in **courier bold** to indicate what the user typed while the sample output generated by the system will be indicated in courier (not bold). Following is an example running of the Unix **pwd** command:

```
# pwd
/opt/sc4/daemons
#
```

Important notes and considerations are highlighted with this symbol and grey text boxes.

Tips, examples, and best practices are highlighted with this symbol and white on blue text.

Resource Requirements

This section describes SecurityCenter's minimum requirements for hardware, network, and disk storage. Note that the particular needs of your organization must be factored into this guideline.

Recommended Minimum Hardware Requirements

The following chart outlines the minimum hardware requirements for operating the SecurityCenter.

Table 1 – Hardware Requirements

Scenario	Minimum Recommended Hardware
SecurityCenter managing 500 to 2,500 active IPs	**CPU:** 1 dual-core 2 GHz or greater CPU **Memory:** 4 GB RAM **Hard drive:** 120 GB at 7,200 rpm (320 GB at 10,000 rpm recommended)
SecurityCenter managing 2,500 to 10,000 active IPs	**CPU:** 1 dual-core 3 GHz CPU (2 dual-core recommended) **Memory:** 4 GB RAM **Hard drive:** 160 GB at 7,200 rpm (500 GB at 10,000 rpm recommended)
SecurityCenter managing 10,000 to 25,000 active IPs	**CPU:** 2 dual-core 3 GHz CPU (1 quad-core recommended) **Memory:** 8 GB RAM **Hard drive:** 500 GB at 10,000 rpm (1 TB at 15,000 rpm with striped RAID recommended)
SecurityCenter managing more than 25,000 active IPs	**CPU:** 2 quad-core 3 GHz CPU (4 dual-core recommended or 2 quad-core 3 GHz CPU) **Memory:** 16 GB RAM **Hard drive:** 1 TB at 15,000 rpm (3 TB at 15,000 rpm with striped RAID recommended)

In addition to the above guidelines, please consider the following suggestions:

- If the Nessus scanner is deployed on the same system as SecurityCenter, there will be less CPU and memory available during scans, causing slower performance. Use multi-core and/or multiple CPU servers to alleviate this. In addition, placing the scanner on a secondary machine will alleviate performance bottlenecks.
- For deployments of SecurityCenter with more than 25 active users, add additional memory or CPUs to improve performance.
- If one or more Passive Vulnerability Scanners are in use, use multi-core and/or multiple CPU servers to increase performance.
- As a general rule, use the aggregate of the individual software product resource requirements for determining total hardware system requirements.

Network Interfaces

Bandwidth usage during a scan does not sustain higher than a few MB/s. Many of Tenable's customers use 100 MB interface cards for network scanning. There is no compelling requirement to use gigabit network cards at this time. However, such an interface may make sense to generally increase the overall performance of web sessions, emails, LCE queries, and other network activities.

If Nessus is deployed on the same server as SecurityCenter, consider configuring the server with multiple network cards and IP addresses. Nessus uses default routes when scanning target networks and will correctly scan a system from the appropriate interface.

Disk Space

Adequate disk space is critical to a successful SecurityCenter deployment. An important consideration is that SecurityCenter saves a snapshot of the entire vulnerability archive each day. In addition, the size of the vulnerability data stored by SecurityCenter depends on the number and types of vulnerabilities, not just the number of hosts. For example, 100 hosts with 100 vulnerabilities each could consume as much data as 1,000 hosts with 10 vulnerabilities each. In addition, the output for vulnerability check plugins that do directory listings, etc. is much larger than "Open Port" plugins from discovery scans.

For networks of 35,000 to 50,000 hosts, Tenable has encountered data sizes of up to 25 GB. That number is based on storage of 50,000 hosts and approximately 500 KB per host.

Additionally, during active scanning sessions, large scans and multiple smaller scans have been reported to consume as much as 150 GB of disk space as results are acquired. Once a scan has completed and its results are imported, that disk space is freed up.

Disk Partitions

SecurityCenter is installed into **`/opt/sc4`** by default. Tenable highly recommends that the **`/opt`** directory be created on a separate disk partition. For higher performance, using two disks, one for the operating system and one for the system deployed to **`/opt`**, can be more efficient.

If required disk space exists outside of the **`/opt`** file system, mount the desired target directory using "**`mount --bind <olddir> <newdir>`**". Make sure that the file system is automatically mounted on reboot by editing the **`/etc/fstab`** file appropriately.

Deploying SecurityCenter on a server configured with RAID disks can also dramatically boost performance.

SecurityCenter does not require RAID disks for even our largest customers. However, in one instance, response times for queries with a faster RAID disk for a customer with more than 1 million managed vulnerabilities moved from a few seconds to less than a second.

Software Requirements

Supported Operating Systems

SecurityCenter 4 is available for Red Hat Enterprise Server 5 (32/64-bit) and 6 (32/64-bit). CentOS 5 (32/64-bit) and 6 (32/64-bit) is also officially supported. SELinux policy configuration is supported by Tenable in a "Permissive" mode. See the section labeled "Modify Firewall Settings" for more information.

Other SELinux modes are known to work, but the required configuration varies based on policies and custom configurations that may be in place on-site. It is strongly recommended that SELinux implementation configurations are tested prior to deployment on a live network

IT Environment Requirements

Virtualized Environments

SecurityCenter is well suited to virtual platforms and comes prepackaged along with Nessus and PVS on the Tenable Appliance VMware image. Because of the unique performance considerations with virtualized platforms, please consult your VM software vendor for recommendations, as VMs typically see up to 30% loss in efficiency compared with dedicated servers.

Securing the Environment

It is assumed that organizations have the appropriate skill-set required to maintain the operating system environment in a secure manner and that they are configured and maintained with the following conditions:

- The operating system must be configured in a secure manner to ensure that security controls cannot be bypassed.
- The network must be configured to ensure that the SecurityCenter system resides in a secure network segment that is not accessible from the Internet.
- Network time synchronization must be enabled to ensure that accurate time stamps are recorded in reports and log files.

The time zone is set automatically during the installation process with no user interaction. If steps are required for manual time zone configuration, please refer to the following KB article: https://support.tenable.com/support-center/index.php?x=&mod_id=2&root=92&id=444. Important: The time zone configured in **`php.ini`** must be synchronized with the system time zone in **`/etc/sysconfig/clock`**.

- Access control mechanisms must be in place to ensure that only authorized users have access to the OS platform.

Of particular importance is the requirement to monitor system resources to ensure that adequate disk space and memory are available. If system resources are exhausted, there is a risk that audit data could be prevented from being logged due to the system becoming dysfunctional. Refer to the "Troubleshooting" section of the SecurityCenter 4.7 Administration Guide for information on how system administrators can recover the system should SecurityCenter become inoperative due to resource exhaustion. During recovery processes, actions by the system administrator may not be logged by SecurityCenter until sufficient resources have been made available.

The following resource provides details for secure administration of a Red Hat installation:

Even though the security concepts from this guide are written for RHEL 6, most of the concepts and methodologies apply to earlier versions of RHEL that are supported with SecurityCenter.

- Red Hat Enterprise Linux 6. Security Guide. A Guide to Securing Red Hat Enterprise Linux. http://docs.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/6/html/Security_Guide/index.html.

As with any application, the security and reliability of the installation is dependent on the environment that supports it. It is strongly recommended that organizations deploying SecurityCenter have an established and applied IT management policy that covers system administration integrity, resource monitoring, physical security, and disaster recovery.

Dependencies

Either OpenJDK or the Oracle Java JRE along with their accompanying dependencies must be installed on the system along with any additional Java installations removed for reporting to function properly.

Although it is possible to force the installation without all required dependencies, if your version of Red Hat or CentOS is missing certain dependencies, this will cause problems that are not readily apparent with a wide variety of functions. Tenable's Support team has observed different types of failure modes for SecurityCenter when dependencies to the installation RPM are missing. If you require assistance or guidance in obtaining these dependencies, please contact our Support team at support@tenable.com.

The following programs must be installed on the system prior to installing the SecurityCenter package. While they are not all required by the installation RPM file, some functionality of SecurityCenter may not work properly if the packages are not installed. The packages listed below are among those that are most often not installed by default:

- **java-1.6.0-openjdk.i386** (or the latest Oracle Java JRE)
- **openssh**
- **expat**
- **gdbm**
- **libtool**
- **libtool-ltdl**
- **libxml2**
- **ncurses**
- **readline**
- **compat-libstdc++**
- **libxslt**

Using the latest stable production version of each package is recommended.

For a list of required packages, run the following command against the SecurityCenter RPM file:

```
# rpm -qpR SecurityCenter-4.x.x-es6.x86_64.rpm
```

To determine which version of a dependency is installed on your system, run the following command for each of the packages (replace “libtool” with the appropriate package):

```
# rpm -qa | grep libtool
```

If one of the prerequisite packages is missing, it can be installed using the “yum” or “rpm” package managers. For example, install Java 1.6.0 with “yum” using the command below:

```
# yum -y install java-1.6.0-openjdk.i386
```

SecurityCenter Communications and Repositories

The following table summarizes the components’ primary repositories and communication methods.

Table 2 – Repositories and Communication Methods

SecurityCenter	
Installation Directory	`/opt/sc4`
User Data	`/opt/sc4/orgs/<Organization Serial Number>`
Repositories	`/opt/sc4/repositories/<Repository Number>`

Audit Log	`/opt/sc4/admin/logs/`
Organization Logs	`/opt/sc4/orgs/<Organization Number>/logs/`
Communication Interfaces	User Access: HTTPS Plugin Updates: Acquired over SSL from Tenable servers directly to SecurityCenter or for offline installation. Plugin packages are secured via 4096-bit RSA digital signatures.

Tenable Applications

If you are running Tenable's Log Correlation Engine (LCE), please note that LCE 4.2 or higher is required for complete functionality with SecurityCenter 4.6. The **Asset Summary** tool will not work with LCE 3.4 or 3.6. Using a combination of LCE 3.x and 4.x servers will result in most SecurityCenter LCE functionality of all connected servers being limited to what is available using the LCE 3.x server.

Table 3 – SecurityCenter 4.6 Product Compatibility

Product	Minimum Version
Nessus	4.4 (Limited connection options) 5.
LCE	4.0 (3.6.1 with limited functionality) 4.2 or higher for LCE Vulnerability features
PVS	3.4 or higher for IPv4 results 3.8 for IPv4 and IPv6 results
SecurityCenter (remote/offline repository*)	4.x
3D Tool	2.x

* SecurityCenter 4.6 can receive a repository from prior versions of SecurityCenter 4.0.x and above, but cannot share its repositories with previous versions.

Pre-Installation

In order to ensure audit record timestamp consistency between SecurityCenter and its external components, make sure that the underlying OS for SecurityCenter and all components are configured properly and enabled to use Network Time Protocol (NTP) as described in:

http://docs.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/6/html/Deployment_Guide/sect-Date_and_Time_Configuration-Command_Line_Configuration-Network_Time_Protocol.html

SecurityCenter Licenses

SecurityCenter is licensed by the total number of active IP addresses it manages and the hostname of the system on which it is installed. For example, a customer can purchase a 500 IP SecurityCenter license for the hostname of "security". This key allows that particular server to scan several networks, but as soon as 500 IP addresses are discovered, the license limit becomes active.

SecurityCenter generates a warning in the web interface if the license limit has been exceeded or is approaching capacity. Contact Tenable Sales for a temporary or permanent expanded license key.

You will need to provide the hostname of the machine on which SecurityCenter will be installed. This can be obtained by entering the "**hostname**" command at the shell prompt.

SecurityCenter does not support an unlicensed "demo" mode – a temporary or permanent key is required.

Once installation is complete, the initial web interface will generate an upload form to add the license key.

Disable any pop-up blockers for this interface, as they will prevent the license key upload interface from working correctly.

Disable Default Web Servers

SecurityCenter provides its own Apache web server listening on port 443. If the installation target already has another web server or other service listening on port 443, that service needs to be disabled on that port or SecurityCenter must be adjusted to use a different port after installation.

Confirm what, if any, services are listening on port 443 with the following command:

```
# netstat -pan | grep ':443 '
```

Modify Firewall Settings

The default Red Hat firewall settings cause issues with SecurityCenter's web services. To easily alleviate this, SELinux must be either set to "Disabled" or enabled in "Permissive" mode. You can disable SELinux "Enforcing" mode using the following steps:

1. Navigate to: **/etc/selinux**
2. Edit the file named "**config**".
3. Change the SELINUX line from "**SELINUX=enforcing**" to "**SELINUX=disabled**" or "SELINUX=permissive".
4. Save the file.
5. Reboot the system.

Ensure the following incoming services are permitted by the firewall rules:

- SSH (port 22)
- HTTPS (port 443 by default)

Please consult local security and best practices within your environment for the proper usage and configuration of SELinux. SecurityCenter is known to work with SELinux in "Enforcing" mode with some customization of the SELinux rules. However, permitted rules vary from organization to organization.

Log Rotation

The installation does not include a log rotate utility; however, the native Linux "**logrotate**" tool is supported post-installation. In most Red Hat environments, **logrotate** is installed by default. The following logs will be rotated if the **logrotate** utility is installed:

1. All files in **/opt/sc4/support/logs matching *log**
2. **/opt/sc4/admin/logs/sc4-error.log**

During an install/upgrade, the installer will drop a file named “SecurityCenter4” into **/etc/logrotate.d/** that contains log rotate rules for the files mentioned above.

Log files are rotated on a monthly basis. This file will be owned by `root`/`root`.

Obtain the Installation Package

The installer comes in a number of versions based on OS level and architecture. The general format of the installer is shown below:

SecurityCenter-x.x.x-os.arch.rpm

Confirm the integrity of the installation package by comparing the download md5 checksum with the one listed in the product release notes.

Installation

When performing **sudo** installs, use “**sudo -i**” to ensure the proper use of environmental variables.

During the installation process, SecurityCenter will produce the log file **/tmp/sc4.install.log**. This file is important for debugging purposes and should not be removed. Once the installation process is complete, the file will be moved to **/opt/sc4/admin/logs/install.log**.

As the root user, install the RPM by running the following command:

```
# rpm -ivh SecurityCenter-4.x.x-es6.x86_64.rpm
```

Output similar to the following is generated:

```
# rpm -ivh SecurityCenter-4.x.x-es6.x86_64.rpm
Preparing...                ########################################### [100%]
   1:SecurityCenter         ########################################### [100%]

Installing Nessus plugins ... complete

Applying database updates ... complete.

By default, SecurityCenter will listen for HTTPS requests on ALL available
interfaces. To complete your installation, please point your web browser
to one of the following URL(s):

https://x.x.x.x

Starting SecurityCenter services

[  OK  ] SecurityCenter services: [  OK  ]#
```

This will install the package into **/opt/sc4** and attempt to start all required daemons and the web server services.

In some rare cases, a system restart will be required after the installation of SecurityCenter for all services to be properly started.

Initial Configuration

SecurityCenter Web Interface

Adobe Flash Player must be installed to use the SecurityCenter 4 web interface. It can be obtained at http://get.adobe.com/flashplayer/.

Navigation

To navigate within the SecurityCenter user interface, use the menus on the web interface screen, not the browser's back and forward arrow buttons.

Browser Window Size

The minimum recommended browser window size is 1024x580. Resizing the browser window below this size causes some objects to display incorrectly in the SecurityCenter web interface.

Launching the Web Interface

To launch the configuration interface, bring up a web browser on a system that has access to the system's network address space and enter the URL in the following format, using the SecurityCenter's IPv4 or IPv6 address or hostname:

```
https://<SERVER ADDRESS OR NAME>/
```

The SecurityCenter web interface must be accessed using a secure web connection (https). SecurityCenter 4 does not listen on port 80.

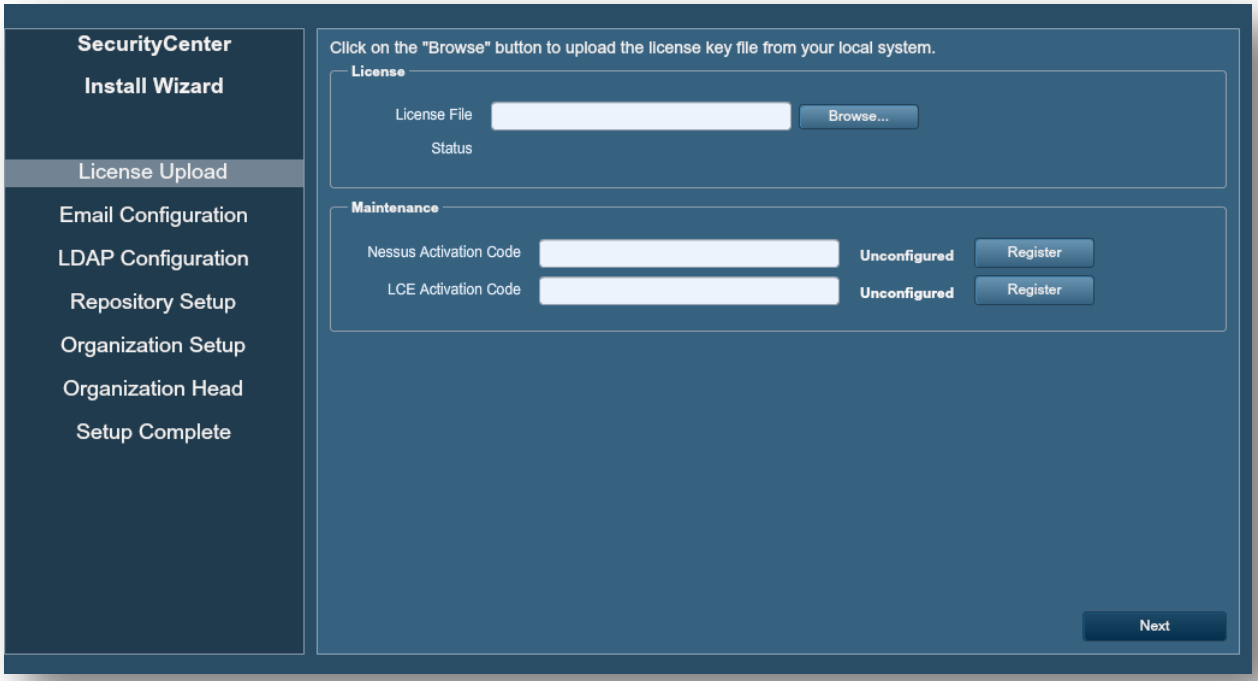
Configuration Menu

If the configuration page times out for any reason, reload the configuration URL specified above and a login page will appear. The default username is "admin" with a password of "password". After configuration is completed, you will be prompted to enter a new admin password.

The user is presented with a multi-step process for initial configuration. Each step is displayed on the left panel and must be completed in order.

License Upload

This will present a license upload screen:



Disable any pop-up blockers for this page, as they will prevent the license key upload interface from working correctly.

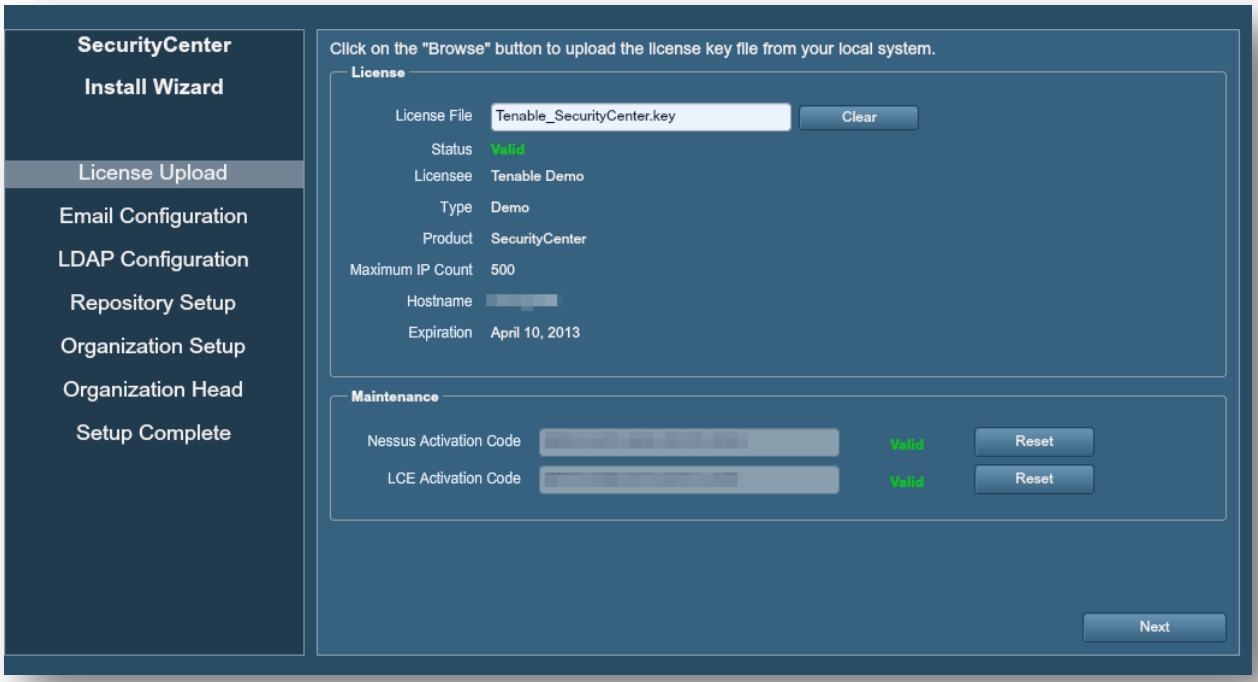
In this step, the user is prompted to upload the license file that was received by email from Tenable. The format of the key file name is:

```
<CompanyName>_SC<IP Count>-<#>-<#>.key
```

Click "**Upload License**" and use the browse dialog to upload your license key file. After uploading the license, the page indicates a valid license has been uploaded. In the event that an invalid license is uploaded, the user is prompted again to upload a valid license key file.

SecurityCenter Configuration

For SecurityCenter installations, a valid Nessus Activation Code must also be entered to register any Nessus scanners used by SecurityCenter. A valid LCE Activation Code must be entered to download the LCE Event vulnerability plugins to SecurityCenter. The Activation Codes are hyphen delimited alpha-numeric strings that enable SecurityCenter to download plugins and update Nessus scanner plugins. The LCE Activation Code allows SecurityCenter to download event plugins, but does not manage plugin updates for LCE servers. After uploading a valid license key and entering a valid Activation Code(s), click "**Next**" to continue.



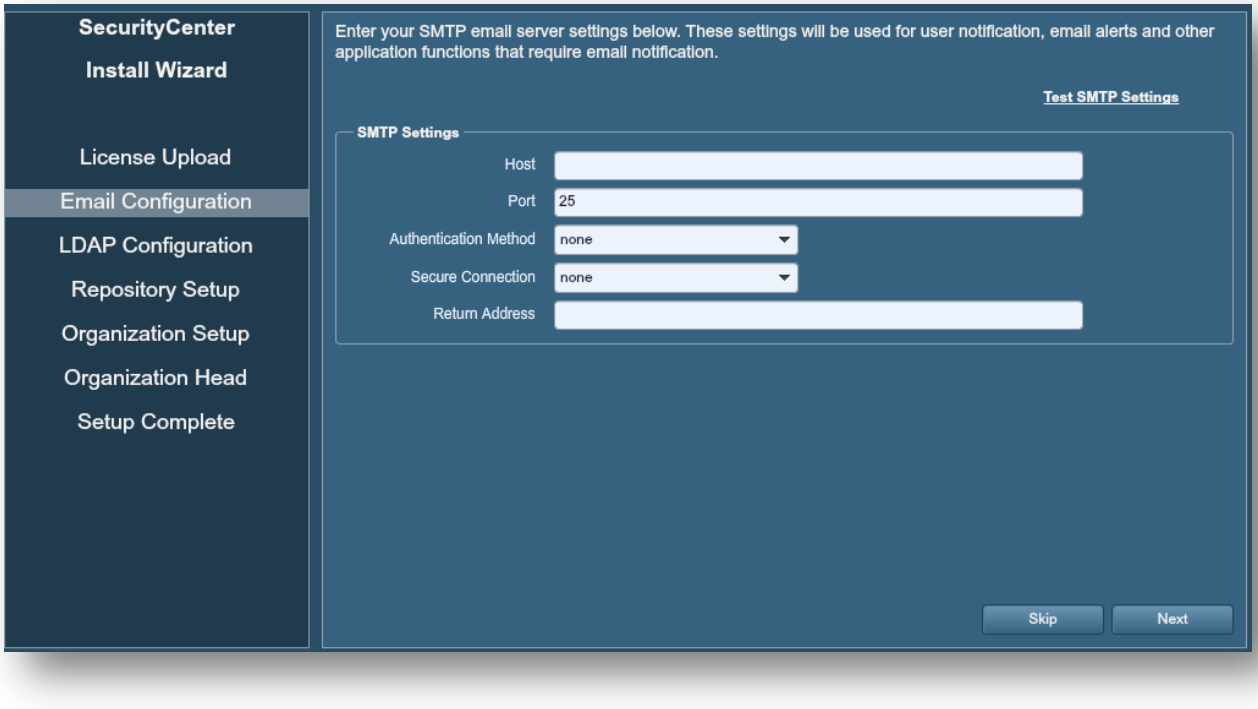
License and Activation Code Input Page

Once a valid license has been uploaded and “Next” has been clicked, a user cannot return to this page. Other configuration steps after this one do contain “Back” buttons.

A plugin download is initiated in the background. This plugin download can take several minutes and must complete before any Nessus scans are initiated. Once the plugin update has occurred, the “Last Updated” date and time are updated on the “**Plugins**” screen.

Email Configuration

Email configuration enables the system to send alerts, reports, and notifications and perform other email-based functions.



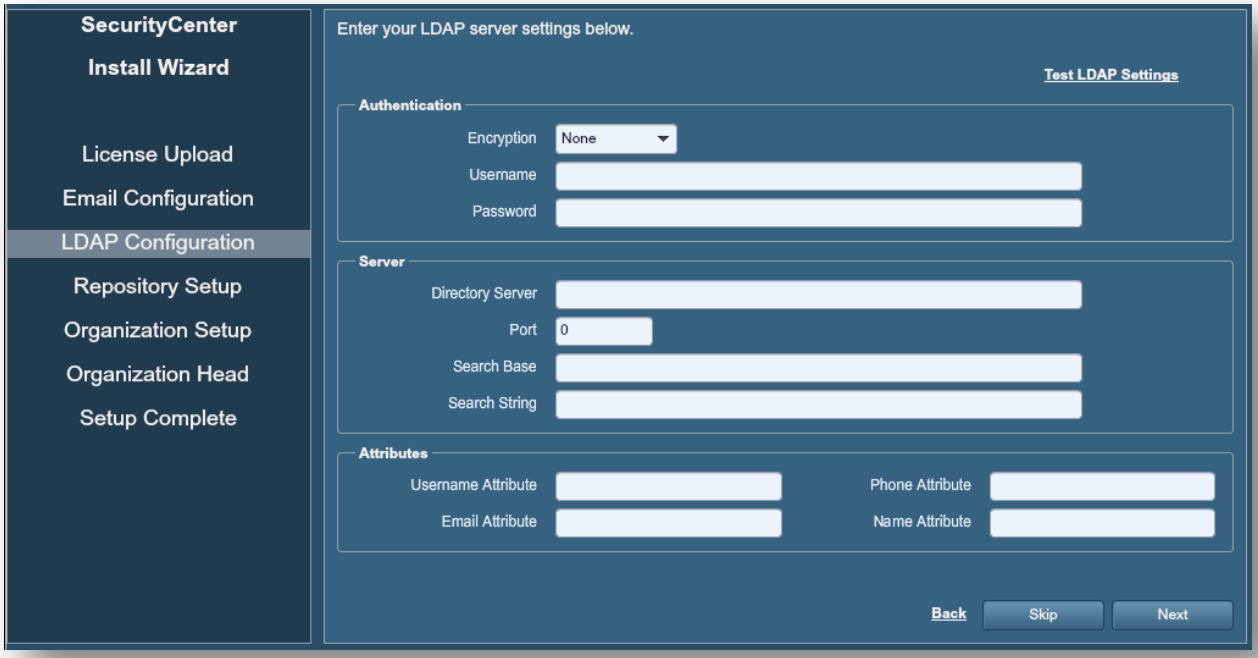
Email Server Configuration Page

After entering the required fields for your SMTP server, click "**Test SMTP Settings**" to confirm that the email settings are correct.

Make sure no white space is included in the hostname field or this will cause the SMTP test to fail.

Click "**Next**" to continue or "**Skip**" to skip this step.

LDAP Configuration



LDAP Configuration Page

LDAP configuration enables users to utilize their external LDAP repository for SecurityCenter logins. Consult with your system administrator for necessary LDAP server settings and once all required fields have been completed, click "**Check LDAP Configuration**" to confirm. Click "**Next**" to continue or "**Skip**" to skip this step.

Repository Setup

When creating repositories, note that IPv4 and IPv6 addresses must be stored separately. Additional repositories may be created once the initial configuration is complete.

Repositories are an excellent way to logically divide vulnerability data up based on organizational needs. For example, three repositories could be created: one for "active" vulnerabilities, one for "passive" vulnerabilities and a third for "compliance" data. Repositories can also be created based on geographical locations, asset importance, user types, etc.

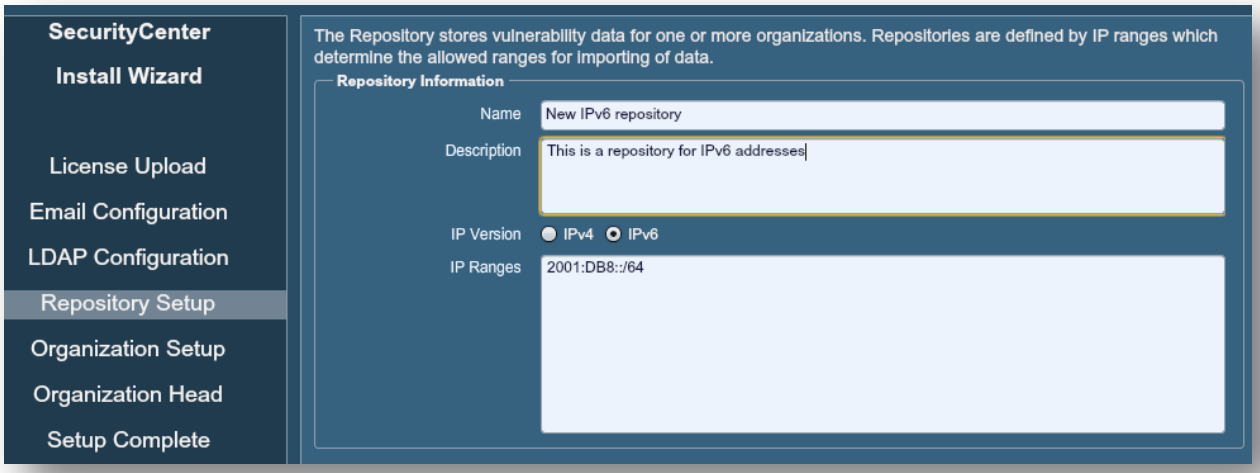
A repository is essentially a database of vulnerability data defined by one or more ranges of IP addresses. When the repository is created, a selection for IPv4 or IPv6 addresses must be made. Only IP addresses of the designated type may be imported to the designated repository. The "Organization" created in steps that follow can take advantage of one or more repositories. During installation, a single local repository is created with the ability to modify its configuration and add others post-install.

When creating SecurityCenter 4 repositories, LCE event source IP ranges must be included along with the vulnerability IP ranges or the event data will not be accessible from the SecurityCenter UI.

Local repositories are based on the IP addresses specified in the "IP Ranges" field on this page during the initial setup. "Remote" repositories use addressing information pulled over the network from a remote SecurityCenter. Remote

repositories are useful in multi-SecurityCenter configurations where security installations are separate but reports are shared. “Offline” repositories also contain addressing information from another SecurityCenter. More information about Remote and Offline repositories may be found in the SecurityCenter Administrator guide. However, the information is imported to the new installation via a configuration file and not via a direct network connection. This facilitates situations where the remote SecurityCenter is isolated from other networks via an “air gap”.

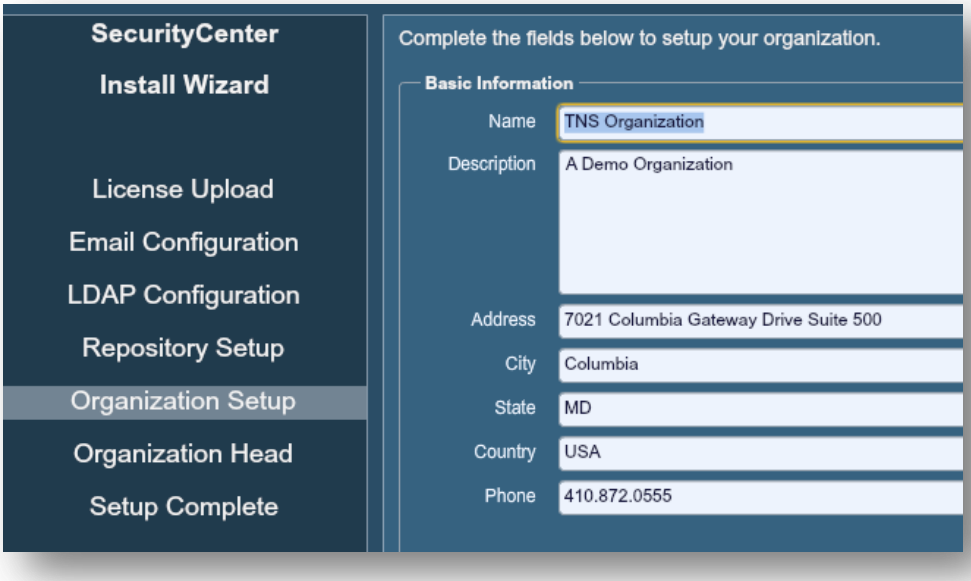
The screen capture below shows a sample repository configuration page using the “Local” repository option (the only type available during installation):



Repository Configuration Page

Organization Setup

The “Organization” is the primary object within SecurityCenter used to group users and assign resources and permissions. Only one Organization Head user is set per Organization.

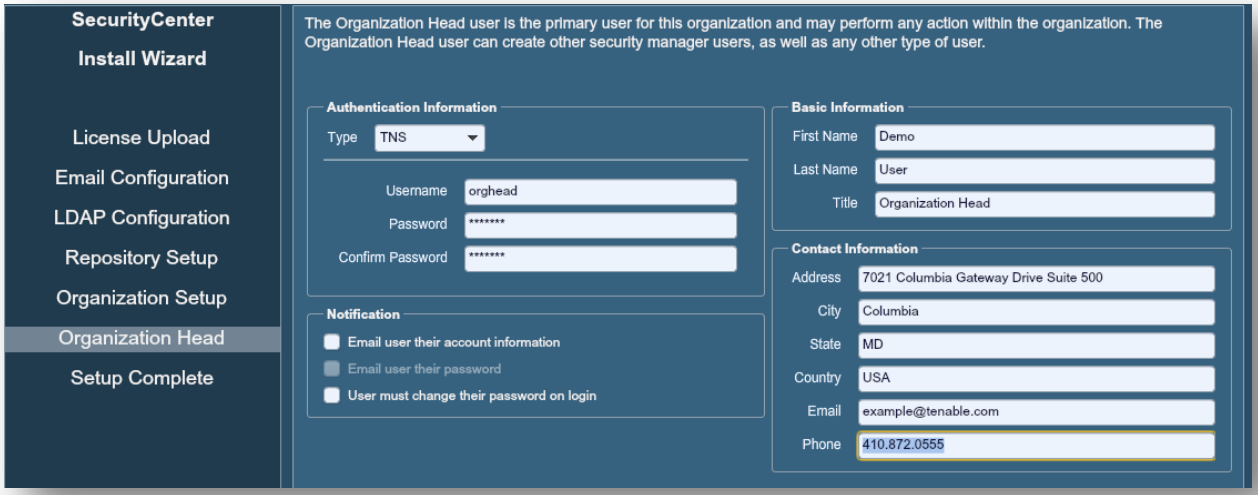


Organization Setup Page

Organization Head Setup

> “Organizational users” refers to users without the admin role who perform day-to-day functions such as scanning and reporting.

The Organization Head user is the primary user created for the Organization and is the highest-level security manager within SecurityCenter. The Organization Head is also the initial Organizational user to log in and is responsible for creating other Organizational users.



Organization Head Setup Page

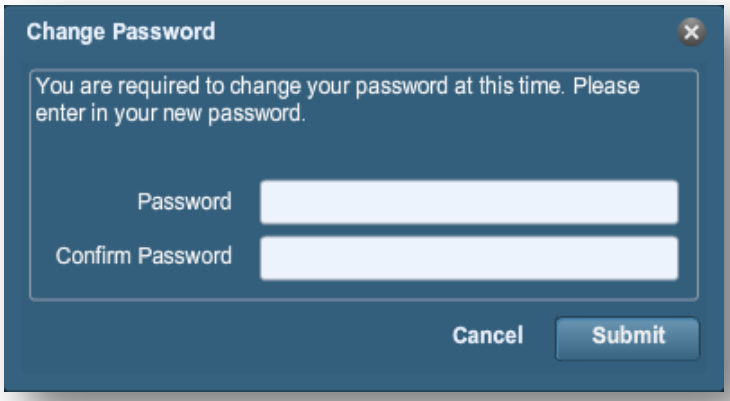
This user can be configured to log in using Tenable’s built-in authentication (TNS) or LDAP authentication with a remote authentication server. Other notification options exist on this screen to allow the user to be emailed their account information/password along with a notification on first login that requires the user to change their password.

After creating the Organization Head user, click “**Next**” and setup is complete. You are now taken to the admin dashboard screen where you can review login configuration data.

Post-Configuration Processes

At setup completion, a screen then reminds of additional configuration steps and prompts for the admin user to change the default admin password as shown in the screen capture below:

> It is recommended to use passwords that conform to the documented organizational policy. If a policy is not in place, a common recommendation is to use passwords that are at least eight characters in length and include a combination of lower and upper-case letters along with non-alphabetic characters.



Password Change Dialog

After changing the password, you are automatically taken to the admin dashboard.

Adding a Nessus Scanner and Test Scan

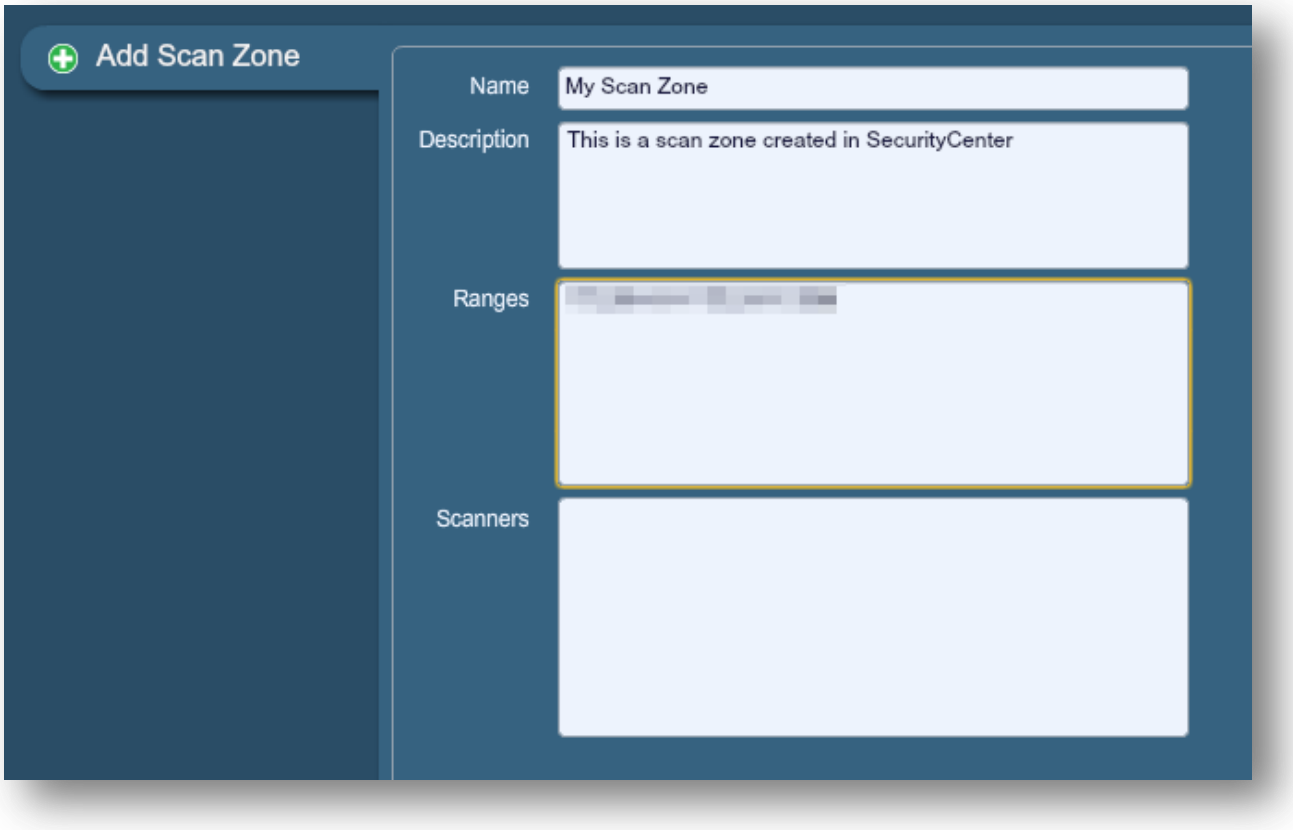
This section will discuss the basic steps for adding a Nessus scanner and then creating and running a test scan. This section assumes that the Nessus software has already been installed and an administrator user has been configured on the Nessus scanner. More detailed guidance including the creation of asset lists, credentials, and schedules is provided in the SecurityCenter User Guide available for download from the Tenable Support Portal located at https://support.tenable.com.

Configure Scan Zones

A Scan Zone is one component of the Nessus scanner configuration and will be demonstrated before the actual scanner addition process.

The order of creation, Scan Zone vs. Scanner, is not important. Either can be created first without the other existing; however, for a scan to complete, both are required.

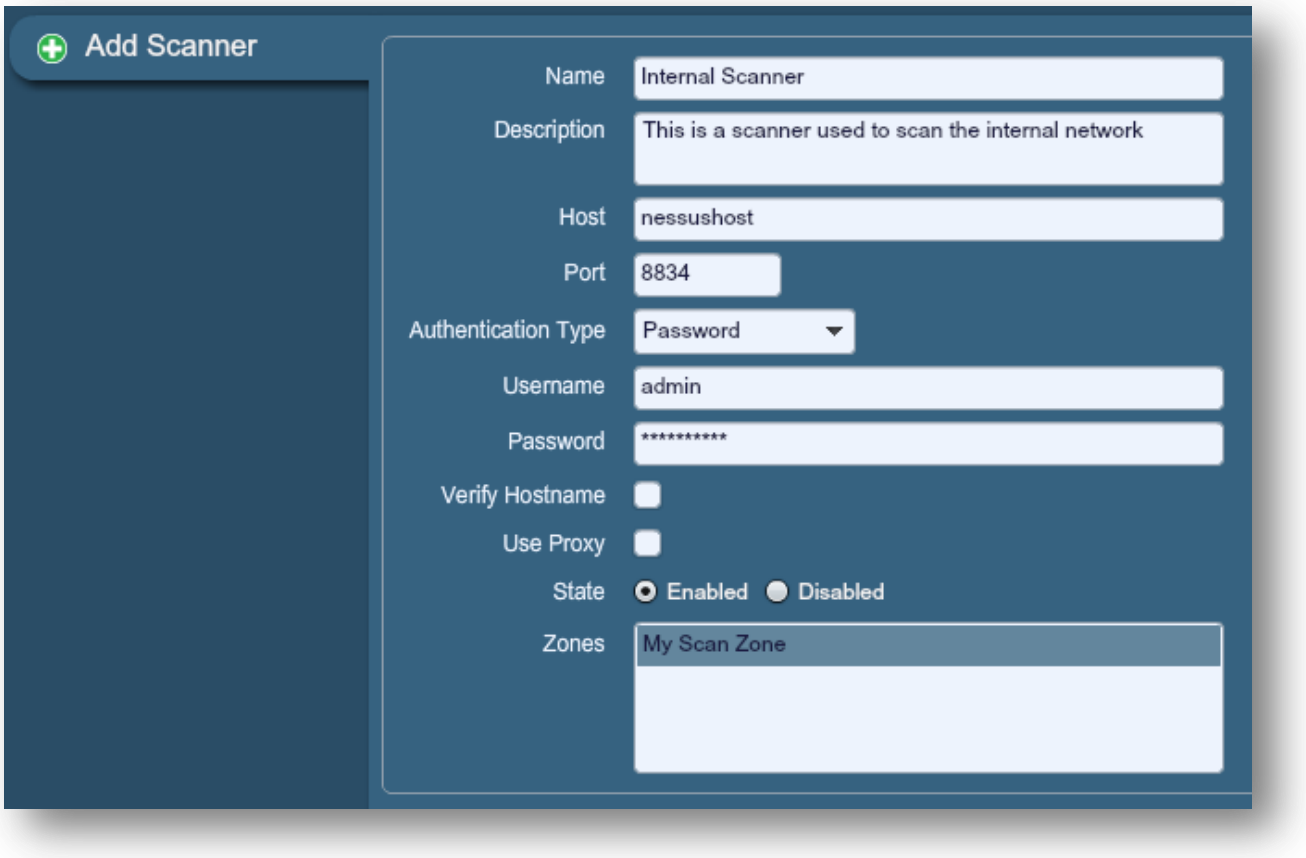
Scan Zones determine the applicable scan ranges of the Nessus scanner being added. Click "**Resources**" and then "**Scan Zones**" to bring up the zone configuration page. Next, click the "**Add**" button. The screen capture below displays the fields required for the new Scan Zone. Since the Nessus scanner has not been created yet, the "Scanner" field is left blank during the Scan Zone creation.



Make sure that the Scan Zone “Name” and “Ranges” have been entered before you click “**Submit**”. The “Description” field is optional, but is a helpful reference to determine the use of the Scan Zone by others in the Organization. The Ranges determine what IP ranges will be allowed to be scanned by the scanner added in the next step.

Add a Nessus Scanner

To add a Nessus scanner, log in as the admin user and click "**Resources**" and then "**Nessus Scanners**". Click "**Add**" and a page similar to the screen capture below is displayed:



Nessus Scanner Add Dialog

Available fields include the scanner Name, Description, Host, Port, Authentication Type, Login, Password, Verify Hostname, Use Proxy, State, and Zones. The "Name" and "Description" fields are descriptive information included to describe the scanner being added.

The Host is the IP address or hostname of the Nessus scanner being added. The Port option refers to the Nessus server's XMLRPC port, which defaults to TCP port 8834. In most cases, this port is kept at the default value. For custom configurations, this can be changed; however, it must be changed on the Nessus scanner first before SecurityCenter attempts to connect to the Nessus server.

The "Login", "Authentication Type", "Username", and "Password" fields are based on settings configured during initial scanner setup.

The "Verify Hostname" checkbox verifies that the hostname or IP address entered in the "Host" field matches the CN (CommonName) presented in the SSL certificate from the server.

The "State" allows the administrator to enable or disable the scanner. When disabled, plugin updates and scans will not attempt to contact the scanner. This can be useful in cases where a WAN link is down, a Nessus host server is down for maintenance, and other similar situations.

Choose a Scan Zone created previously within the "Zone" field. Scanners may belong to multiple Scan Zones.

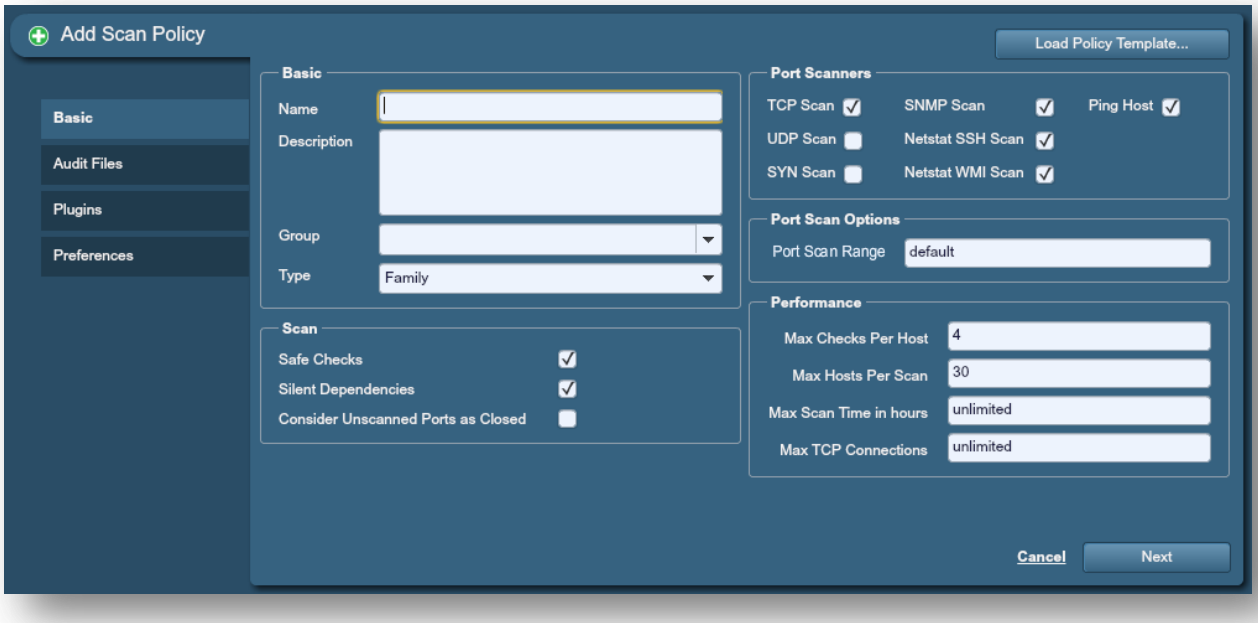
Before a scan is configured, SecurityCenter must push the latest set of plugins to the Nessus scanner. An “Updating Plugins” message is displayed in the Status column of the GUI. To facilitate this, click “**Update Status**” at the top of the “**Plugins**” screen to initiate a manual update of plugins.

Nessus plugins are listed as type “Active”, while Passive Vulnerability Scanner (PVS) plugins are listed as “Passive”. After the Nessus Activation Code is entered, the Nessus plugin update process occurs automatically on the next scheduled interval.

Create a Scan Policy

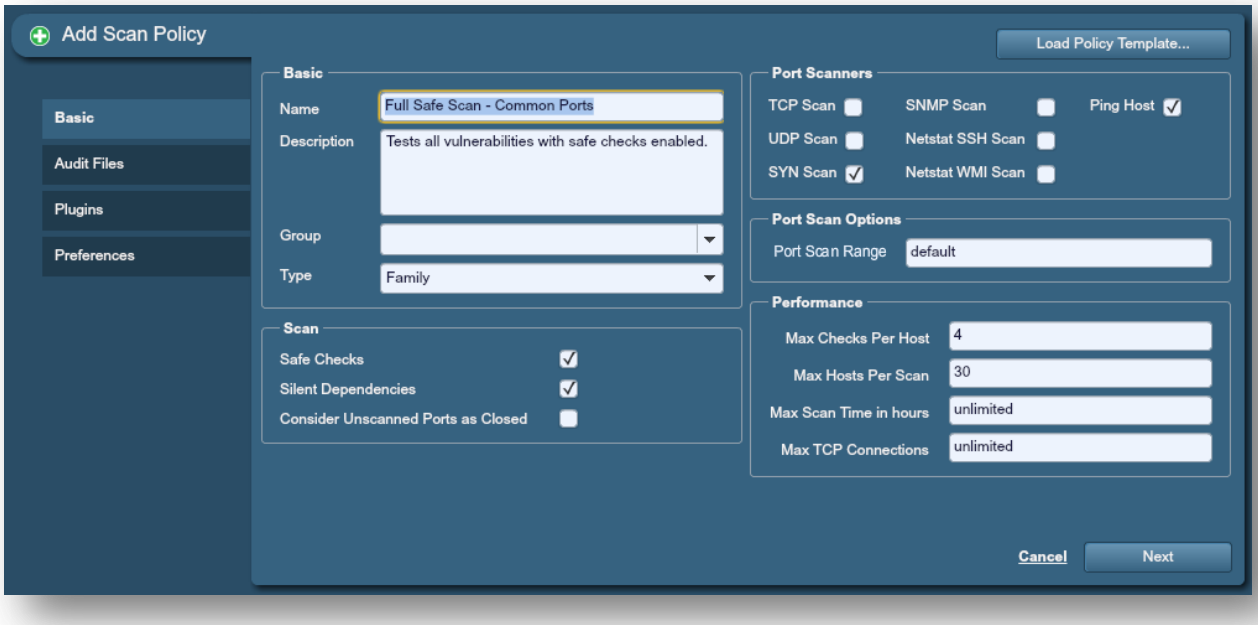
Scan policies created by the admin user are available to every Organization configured on SecurityCenter. Those created by an Organizational user, such as the Organization Head, are only available to members of that Organization.

A Scan Policy contains the desired settings used by the Nessus scanner during its scan routine. For the initial test scan, default settings will be used primarily in the test policy. Later scans can be customized further to refine and improve scan results. To create a scan policy, click the “**Support**” tab and then “**Scan Policies**”. A page similar to the screen capture below is displayed:



Basic Scan Policy Settings

Click “**Load Policy Template**” and select “**Full Safe Scan – Common Ports**”. A page similar to the one below is displayed:



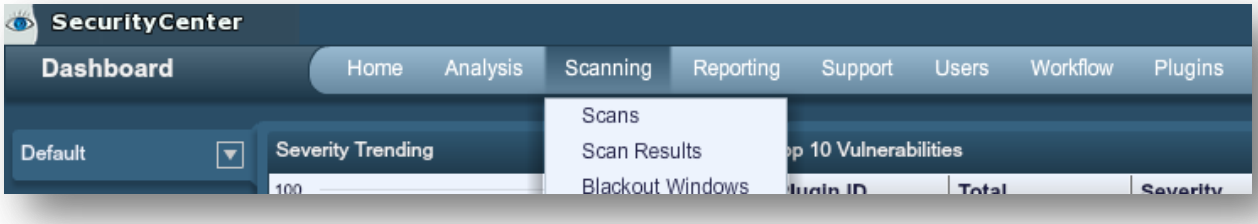
Modify any of the predefined “Basic” settings within this screen based on your scan target environment. For example, if scanning a router that is sensitive to multiple connections, consider lowering the “**Max Checks Per Host**” and “**Max TCP Connections**” to a level less likely to cause issues. Click “**Next**” for each screen, making changes as appropriate, until the “Preferences” screen is displayed and then click “**Submit**” to save your test policy.

Note that Nessus uses smart scanning technology to launch only plugins determined to match the remote host. This occurs even if all plugins are enabled within the policy.

Run a Test Scan

In this section we will create a sample scan of a single host to validate the settings configured in the previous steps. Many other critical configuration items and important processes are covered further in the additional SecurityCenter documentation.

The first step to generating a scan is to log in as the correct user. The “admin” user that we used for the initial configuration of SecurityCenter is used for application management and is not able to perform Nessus scans. Log in as the “Organization Head” user created during the setup process or any other Organizational user with scan privileges. After logging in, click “**Scanning**” and then “**Scans**”.



To create our test scan, click “**Add**” and then fill out the name and description for the scan. Under “**Scan Schedule**”, choose “**Template**” and add a single test IP address or hostname under “Targets”. Select a repository where the scan results will be stored and then click “**Next**”. Under “**Policy**”, choose the policy created earlier, or alternatively, select a plugin from the “**Browse Plugins**” dialog. For “**Scan Zone**” choose “**default**” and then click “**Next**”.

For this test, we will skip credentials; however, credentials can be used in later scans to give more accurate and complete results (such as patch and configuration audits).

Select the options for the “Post Scan” settings and click “**Submit**” to generate the scan template. The “Scans” screen is now displayed with the new template scan shown with a start time of “Never”. Highlight the scan and then click “**Launch**” to generate the new scan.

After the scan is complete, click “**Scanning**” and then “**Scan Results**” to drill down into the scan details and perform target analysis.

At this point, SecurityCenter is installed and ready for more advanced configuration. Please refer to the SecurityCenter User and Admin Guides available for download from the Tenable Support Portal located at https://support.tenable.com for additional configuration guidance.

About Tenable Network Security

Tenable Network Security is relied upon by more than 20,000 organizations, including the entire U.S. Department of Defense and many of the world's largest companies and governments, to stay ahead of emerging vulnerabilities, threats and compliance-related risks. Its Nessus and SecurityCenter solutions continue to set the standard to identify vulnerabilities, prevent attacks and comply with a multitude of regulatory requirements. For more information, please visit www.tenable.com.

GLOBAL HEADQUARTERS

Tenable Network Security
7021 Columbia Gateway Drive
Suite 500
Columbia, MD 21046
410.872.0555
www.tenable.com