tenable network security

SecurityCenter 5.1 Installation Guide

November 12, 2015

(Revision 2)

Table of Contents

Introduction

This document discusses the installation, initial configuration, and a sample scan using Tenable Network Security's SecurityCenter 5.0 (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 5.1 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 5.1 Installation Guide** – This document provides instructions for the installation of SecurityCenter 5.1. 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 5.1 Upgrade Guide** – This document describes the process of upgrading to version 5.1 of SecurityCenter.
- **SecurityCenter 5.1 Administration Guide** – This document provides instructions for the administration of SecurityCenter by the **admin** user. The **admin** user is the first user to log in to 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 5.1 User Guide** – This document provides instructions for using SecurityCenter from a Security Manager 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/sc/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:** 2 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:** 4 dual-core 3 GHz CPU **Memory:** 16 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:** 8 dual-core 3 GHz CPU **Memory:** 32 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:** 8+ quad-core 3 GHz CPU **Memory:** 32+ 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. It is strongly recommended that the scanner is placed on a secondary machine.
- For deployments of SecurityCenter with more than 25 active users, add additional memory or CPUs to improve performance.
- As a general rule, use the aggregate of the individual software product resource requirements for determining total hardware system requirements. Hosting multiple Tenable products on the same server is not recommended due to potential memory and CPU constraints.

Network Interfaces

Gigabit or faster network cards are recommended for use on the SecurityCenter server. This is to 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 can be configured to save a snapshot of vulnerability archives 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/sc`** 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 5 is available for Red Hat Enterprise Server 5 (64-bit) and 6 (64-bit) and CentOS 5 (64-bit) and 6 (64-bit). 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 Virtual Machine image. Multiple VM images may be deployed on the network to support multiple products. Because of the unique performance considerations with virtualized platforms, please consult your VM software vendor for recommendations, as VMs typically see some 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 5 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-1.7.0-openjdk** (or later) (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 -qp SecurityCenter-5.x.x-es6.x86_64.rpm --requires
```

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 1.7.0 with "yum" using the command below:

```
# yum -y install java-1.7.0-openjdk.x86_64
```

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/sc`
User Data	`/opt/sc/orgs/<Organization Serial Number>`
Repositories	`/opt/sc/repositories/<Repository Number>`
Audit Log	`/opt/sc/admin/logs/`
Organization Logs	`/opt/sc/orgs/<Organization Number>/logs/`
Communication Interfaces	User Access: HTTPS Feed 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

The following table lists the minimum software versions of Tenable products that work with SecurityCenter 5.

Table 3 – SecurityCenter 5.1 Product Compatibility

Product	Minimum Version
Nessus	6.3.6 (For Active Scans)
Nessus Manager	6.5.3 (For Agent Scans)
LCE	4.2
PVS	4.x
SecurityCenter (remote/offline repository*)	5.x
3D Tool	2.x

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 an 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 license key is required.

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

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 by default)
- 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/sc/support/logs matching *log**
2. **/opt/sc/admin/logs/sc-error.log**

During an install/upgrade, the installer will drop a file named "SecurityCenter" 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/sc.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/sc/admin/logs/install.log**.

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

```
# rpm -ivh SecurityCenter-5.x.x-es6.x86_64.rpm
```

Output similar to the following is generated:

```
# rpm -ivh SecurityCenter-5.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/sc** 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

Navigation

To navigate within the SecurityCenter user interface, using the menus and navigation tools within the web interface screen is the preferred method, not the browser's back and forward arrow buttons.

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 5 does not listen on port 80.

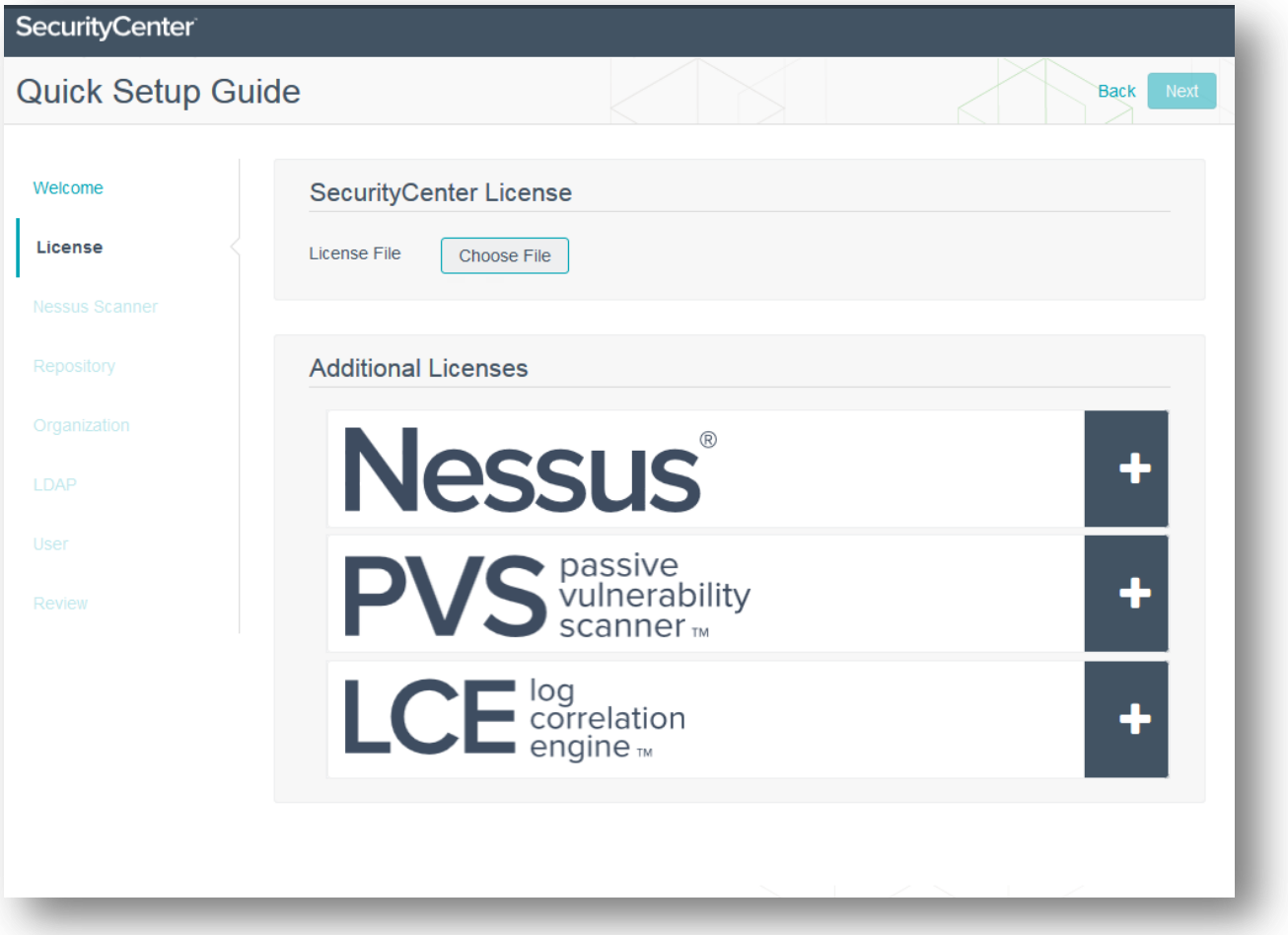
Quick Setup Guide

The user is presented with the Quick Setup Guide welcome screen to begin a multi-step setup process for initial configuration. Each step is displayed on the left side of the screen.

For users that are familiar with SecurityCenter and would prefer to configure the system manually, select the "Exit Quick Setup Guide" to be taken to the Configuration page of SecurityCenter. Details for these options may be found in the SecurityCenter Administration Guide available for download from the Tenable Support Portal.

License

This will present a license upload screen:



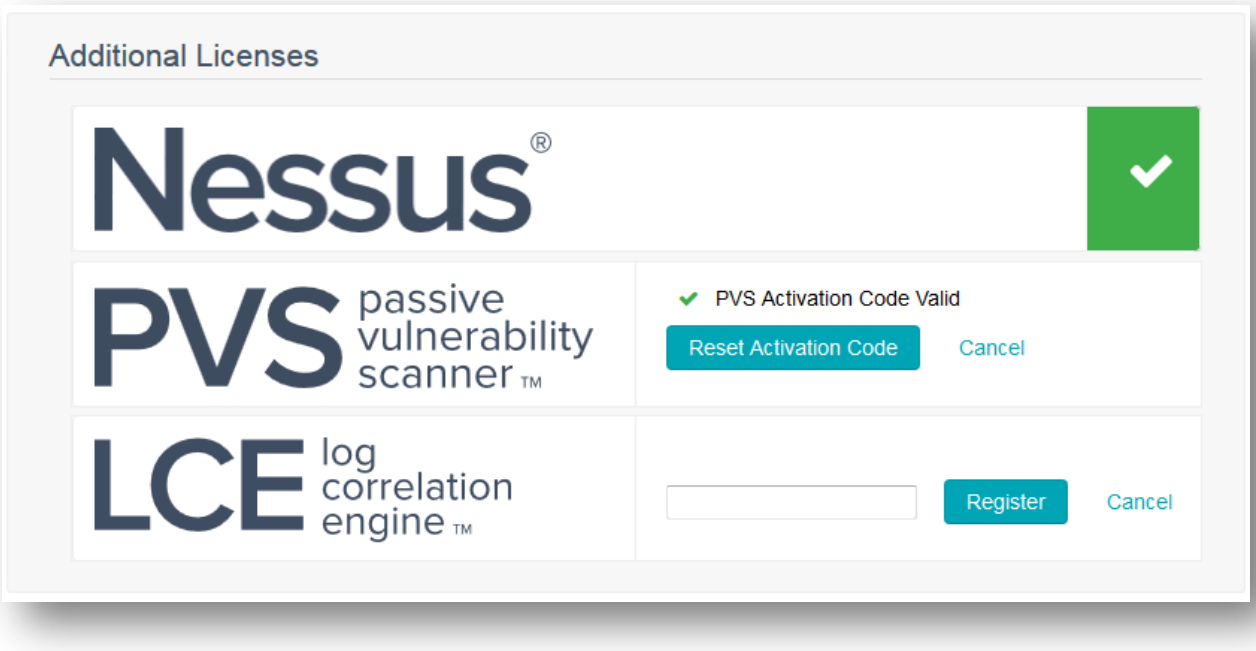
In this step, the user is prompted to upload the license file that was received from Tenable. The format of the key file name is similar to:

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

Click "**Choose File**" and use the browse dialog to upload your license key file. After uploading the license and clicking the "**Activate Button**", 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.

Additional Licenses

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. A valid PVS Activation Code is required to use and manage attached PVS scanners. 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.



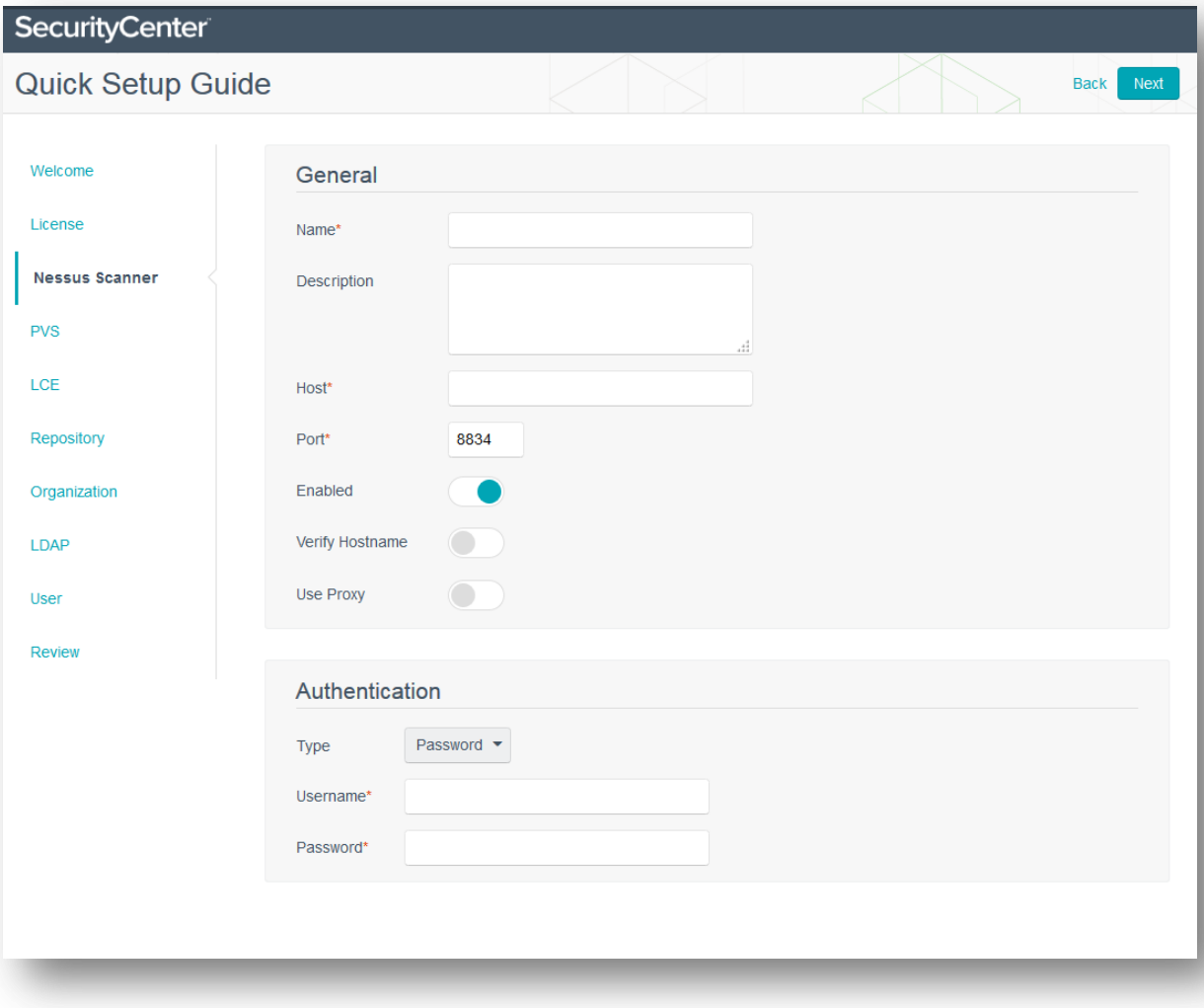
License and Activation Code Input Page

A + sign with a grey background indicates that there has not been a license applied for the product. A green box with a checkmark in it indicates a valid code is entered. A red box with an X indicates an invalid code. Clicking on the symbol will reveal an area to either add or reset the Activation Code. Once a new code has been entered into the text box and registered, it will indicate as valid or invalid.

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.

Nessus Scanner

Once the license and Activation Code(s) have been entered, the next stage of installation is to configure the first Nessus scanner. Nessus Cloud and Nessus Manager scanners that are to be used for Nessus Agent scan imports may enable or add the feature after the initial configuration is complete.



This screen asks for the information to connect to the Nessus scanner and the options are detailed in the following table:

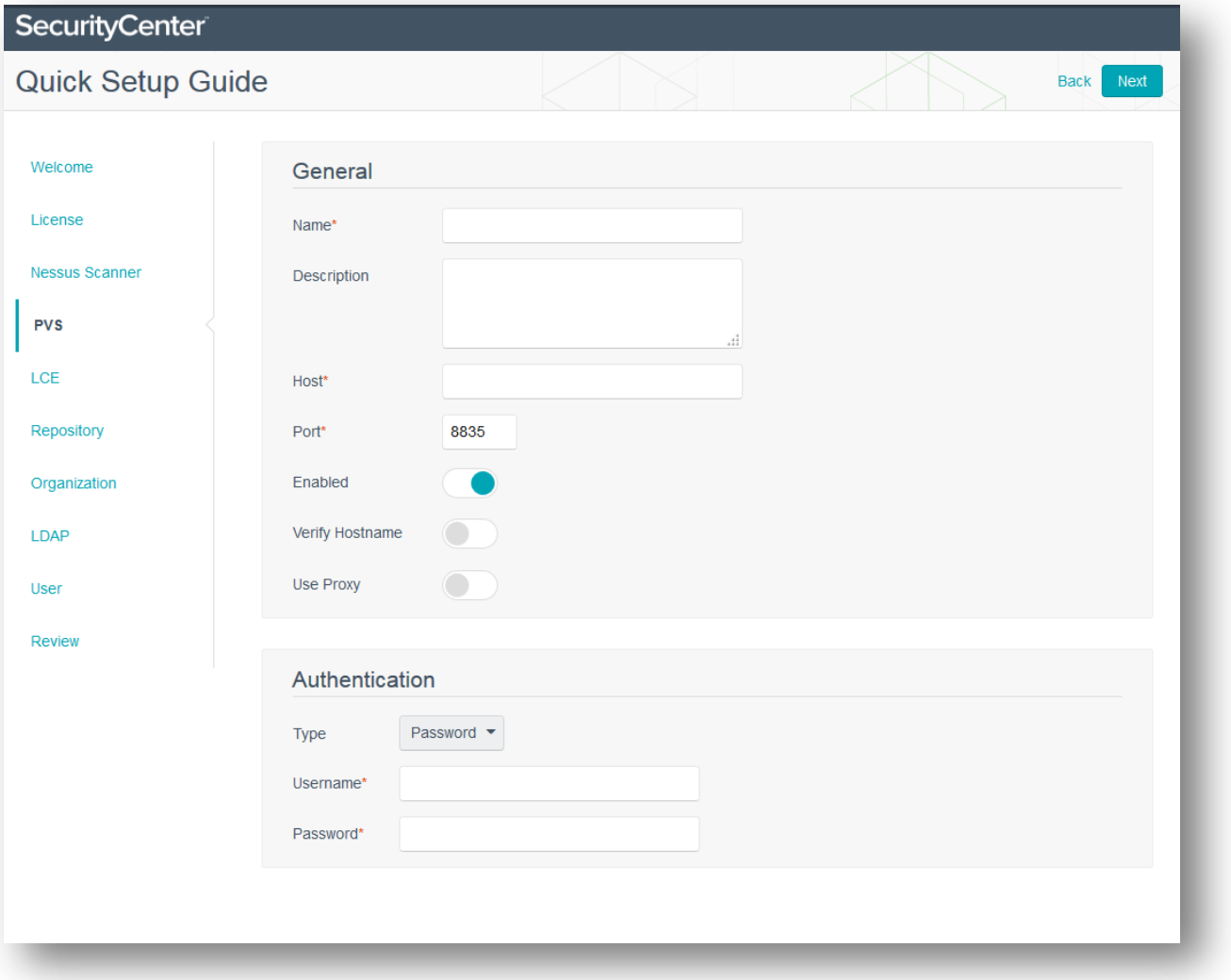
Table 4 – Nessus Scanner Options

Option	Description
Name	Descriptive name for the Nessus scanner.
Description	Scanner description, location, or purpose.
Host	Hostname or IP address of the scanner.

Port	TCP port that the Nessus scanner listens on for communications from SecurityCenter. The default is port 8834.
Enabled	A scanner may be "Enabled" or "Disabled" within SecurityCenter to allow or prevent access to the scanner.
Verify Hostname	Adds a check to verify that the hostname or IP address entered in the "Host" field matches the CommonName (CN) presented in the SSL certificate from the Nessus server.
Use Proxy	Instructs SecurityCenter to use its configured proxy for communication with the scanner.
Authentication Type	Select Password or SSL Certificate for the authentication type to connect to the Nessus scanner.
Username	Username generated during the Nessus install for daemon to client communications. This must be an administrator user in order to send plugin updates to the Nessus scanner. If the scanner will be updated by a different method, such as through another SecurityCenter, a standard Nessus user account may be used to perform scans. This field is only available if the Authentication Type is set to "Password".
Password	The login password must be entered in this field. This field is only available if the Authentication Type is set to "Password".
Certificate	This field is available if the Authentication Type is "SSL Certificate". Select the "Browse" button, choose a SSL Certificate file to upload, and upload to the SecurityCenter.

PVS

When a PVS license is installed, the option to configure the initial PVS scanner is enabled.



This screen asks for the information to connect to the PVS scanner and the options are detailed in the following table:

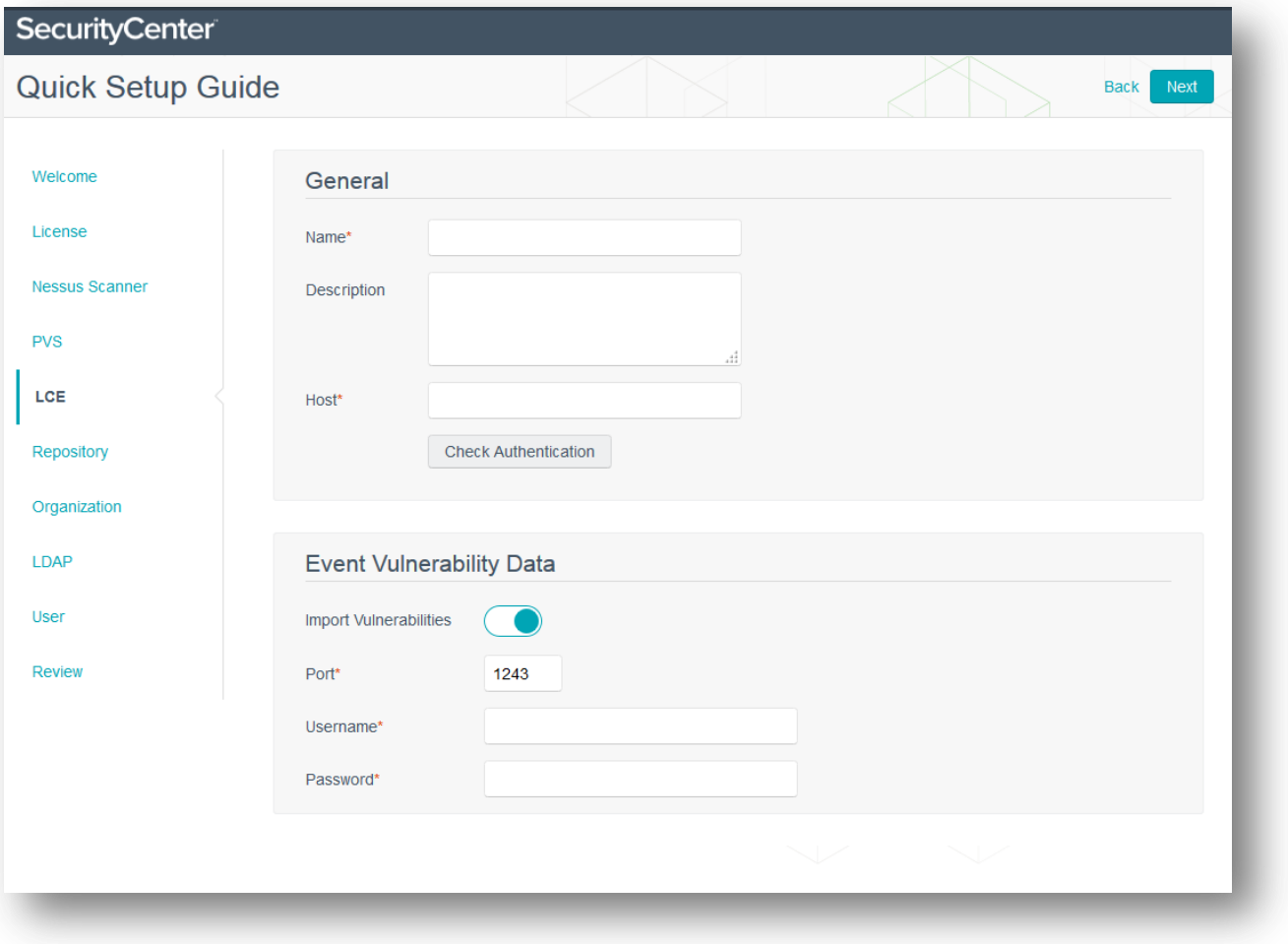
Table 5 – PVS Scanner Options

Option	Description
Name	Descriptive name for the PVS scanner.
Description	Scanner description, location, or purpose.
Host	Hostname or IP address of the scanner.
Port	TCP port that the PVS scanner listens on for communications from SecurityCenter. The default is port 8835.

Enabled	A scanner may be marked as “Enabled” or “Disabled” within SecurityCenter to allow or prevent access to the scanner.
Verify Hostname	Adds a check to verify that the hostname or IP address entered in the “Host” field matches the CommonName (CN) presented in the SSL certificate from the PVS server.
Use Proxy	Instructs SecurityCenter to use its configured proxy for communication with the scanner.
Authentication Type	Select Password or SSL Certificate for the authentication type to connect to the PVS scanner.
Username	Username generated during the PVS install for daemon to client communications. This must be an administrator user in order to send plugin updates to the PVS scanner. This field is only available if the Authentication Type is set to “Password”.
Password	The login password must be entered in this field. This field is only available if the Authentication Type is set to “Password”.
Certificate	This field is available if the Authentication Type is “SSL Certificate”. Select the “Browse” button, choose a SSL Certificate file to upload, and upload to the SecurityCenter.

LCE

When a Log Correlation Engine license is installed, the option to configure the initial LCE server is enabled.



This screen asks for the information to connect to the PVS scanner and the options are detailed in the following table.

Table 6 – LCE Server Options

Option	Description
Name	Name used to describe the Log Correlation Engine.
Description	Descriptive text for the Log Correlation Engine.
Host	IP address of the Log Correlation Engine.
Check Authentication	This button checks the status of the authentication between SecurityCenter and the LCE server.
Import Vulnerabilities	When enabled, allows Event vulnerability data to be retrieved from the configured LCE server.

Port	Enter the port that the LCE reporter is listening on the LCE host.
Username	Enter the reporter username used to authenticate to the LCE to retrieve vulnerability information.
Password	Enter the reporter password used to authenticate to the LCE to retrieve vulnerability information.

Repository

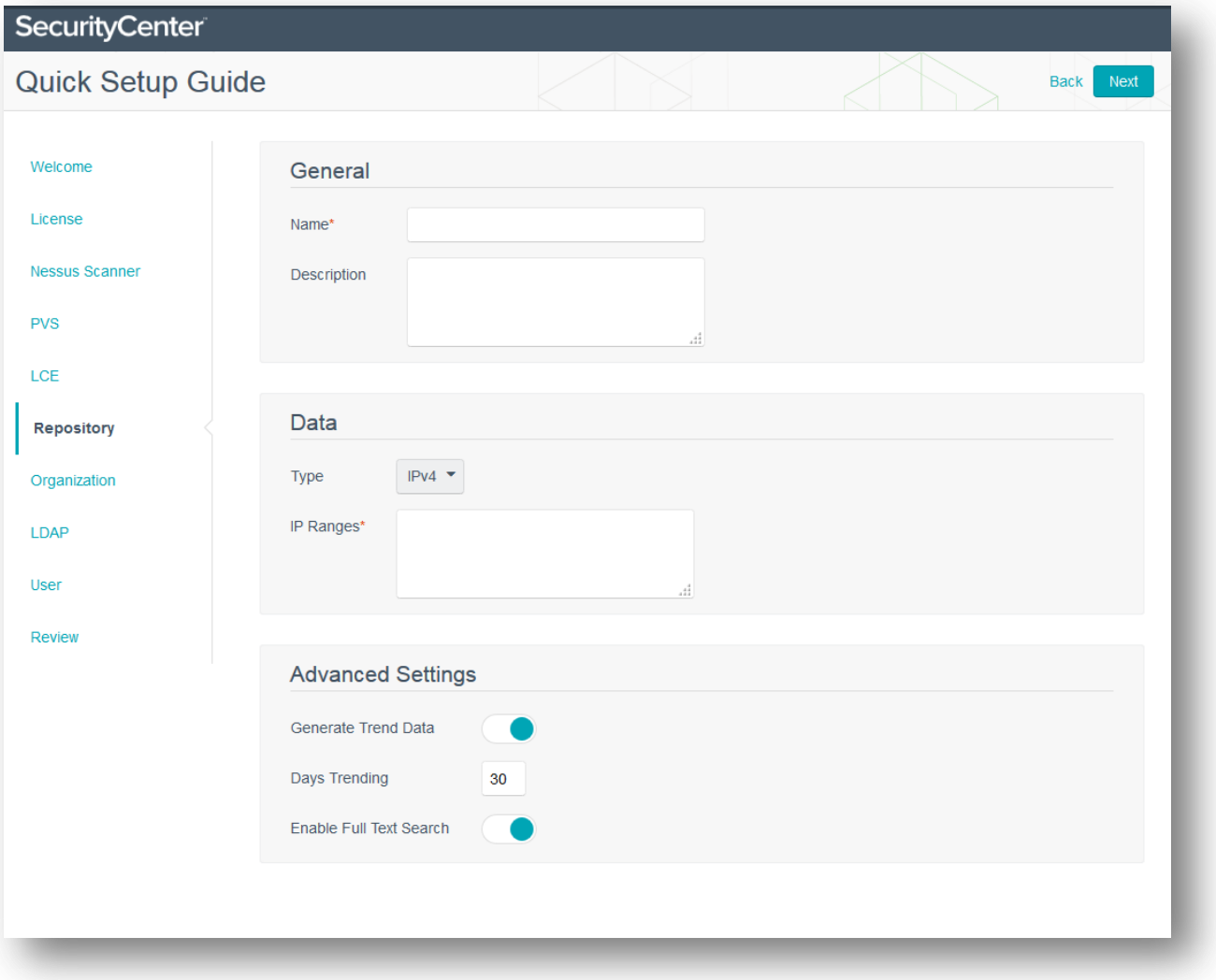
When creating repositories, note that IPv4 and IPv6 addresses must be stored separately. Additional repositories may be created once the initial configuration is complete.

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 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

The following table describes the options available during the repository setup:

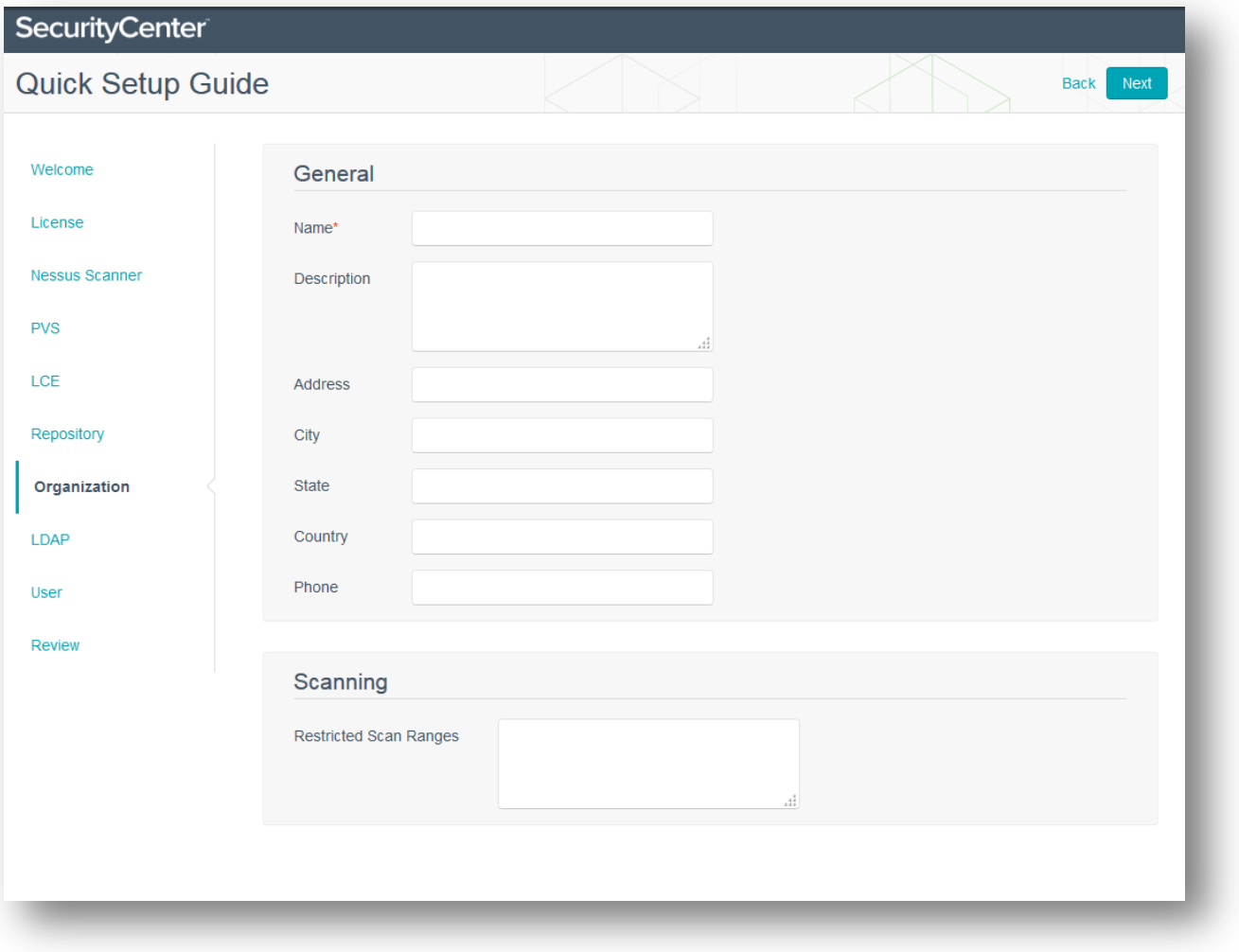
Table 7 – Repository Options

Option	Description
General	
Name	The repository name.
Description	Descriptive text for the repository.

Data	
Type	Determines if the repository being created is for IPv4 or IPv6 addresses.
IP Ranges	Allowed ranges for importing vulnerability data. Addresses may be a single IP address, IP range, CIDR block, or any comma-delimited combination (20 K character limit).
Advanced Settings	
Generate Trend Data	If trending is not selected, any query that uses comparisons between repository snapshots (e.g., trending line charts) will not be available. This option allows for a periodic snapshot of the `.nessus` data for vulnerability trending purposes. This option is useful in cases where tracking data changes is important. In situations where repository datasets do not change frequently – negating the need for trending – disable this option to minimize disk space usage.
Days Trending	Sets the number of days for the trending data to track.
Enable Full Text Search	Determines if the trending data presented is indexed for a full text search.

Organization Setup

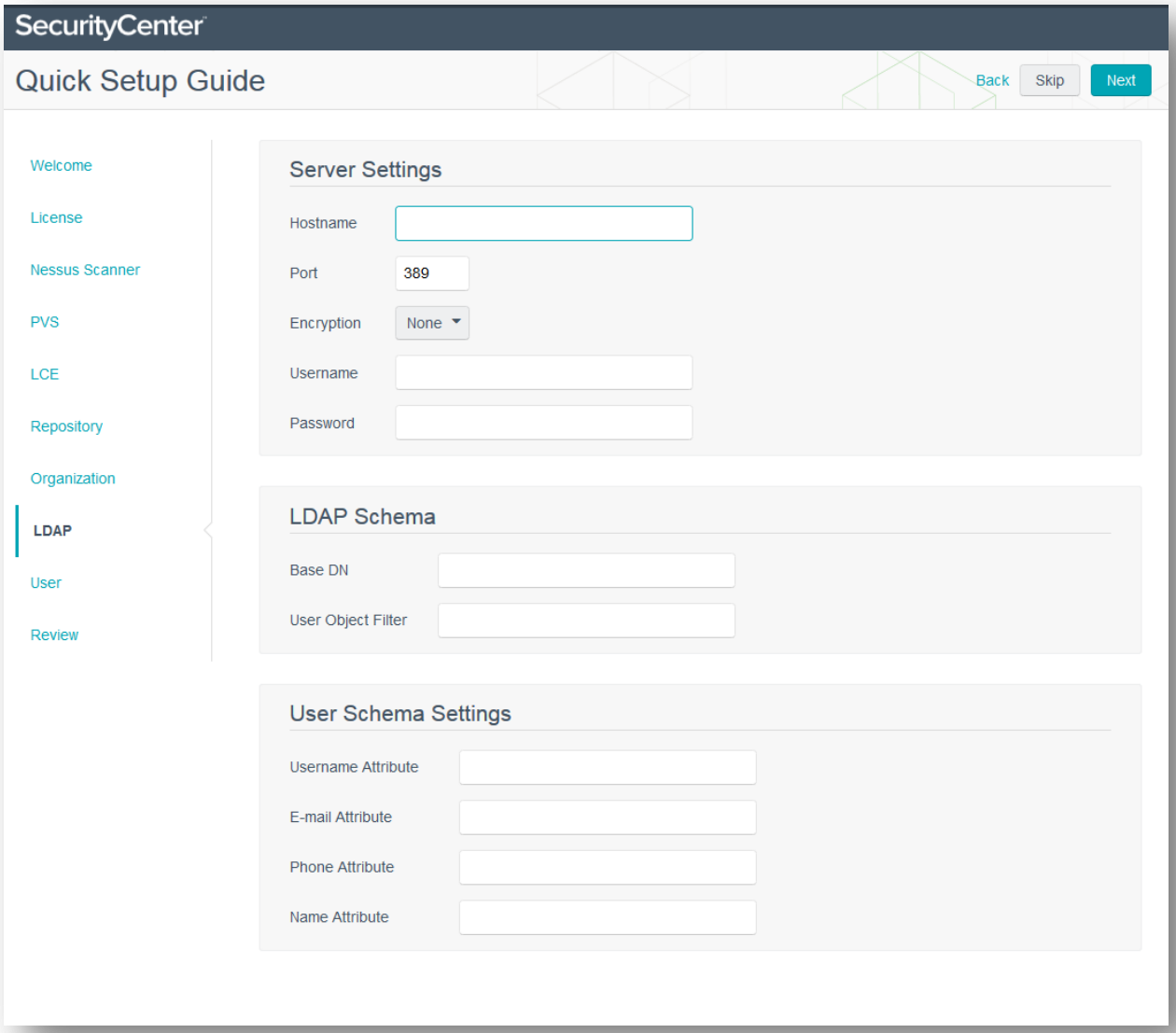
The “Organization” is the primary object within SecurityCenter used to group users and assign resources and permissions.



Organization Setup Page

There are two areas to configure initially for the Organization. In the General area, provide the Organization name, description, and contact/location information as is relevant. The second aspect is to configure the Scanning ranges that the Organization will have access to. The IPs may be entered in CIDR or range notation.

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 "**Skip**" to skip this step if LDAP is not going to be used or configured at this time.

Table 8 – LDAP Options

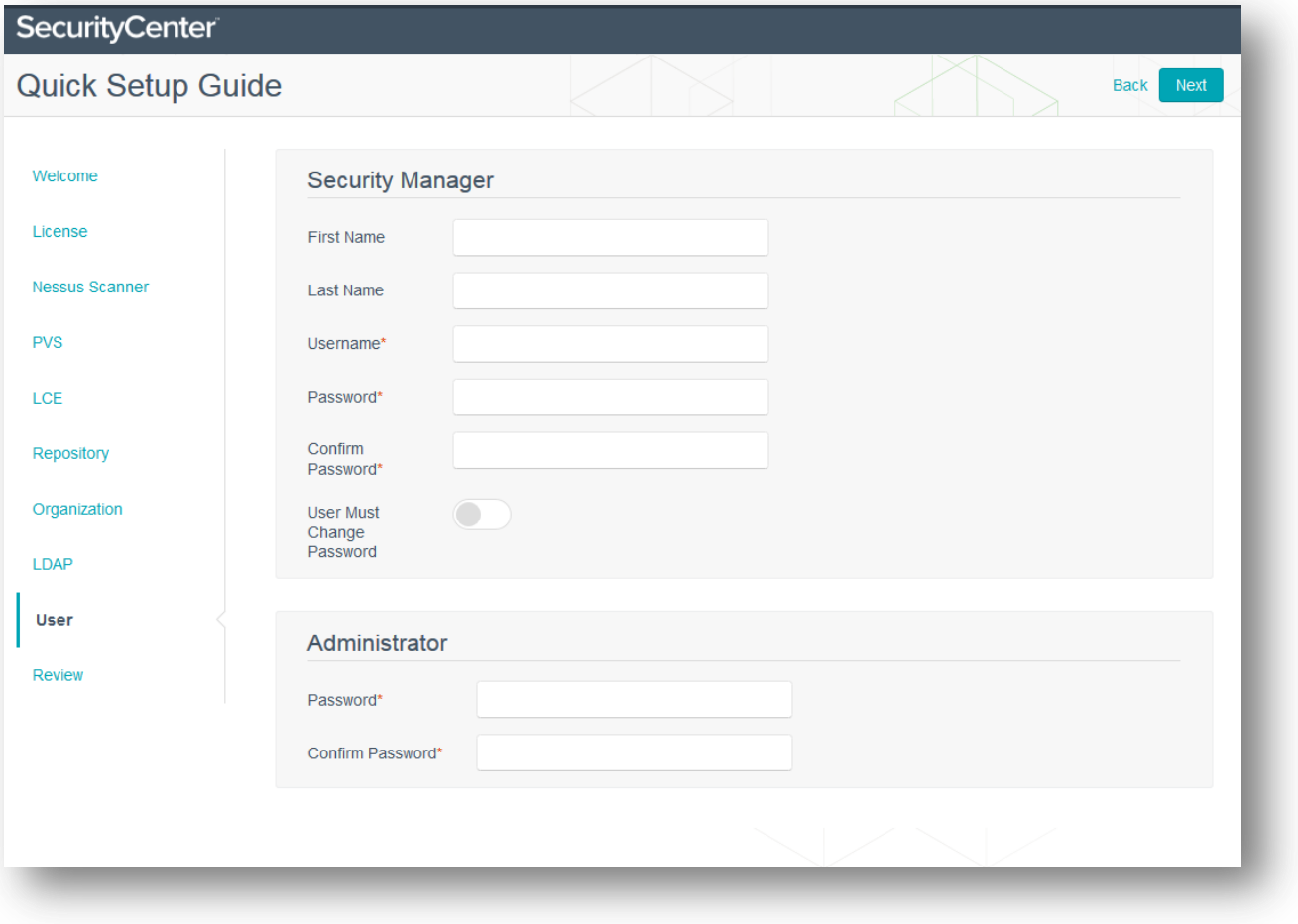
Option	Description
Server Settings	
Hostname	Enter the IP address or DNS name of the LDAP server in this field.

Port	Specify the remote LDAP port here. When Encryption is set to "none", the LDAP port is typically 389, and when TLS or LDAPS is used, port 636 is the typical setting. Confirm the selection with your LDAP server administrators.
Encryption	This selection indicates if Transport Layer Security (STARTTLS) or LDAP over SSL (LDAPS) is used for communication with the LDAP server.
Username	If the LDAP server requires credentials to search for user data, then the "Username" and "Password" fields are required. By default, if an Active Directory server is used for LDAP queries, it requires an authenticated search. Enter the username within this field in the "email" style format (user@domain.com).
Password (optional)	If the LDAP server requires credentials to search for user data, then the "Username" and "Password" fields are required. By default, many LDAP servers require an authenticated search.  It is recommended to use passwords that meet stringent length and complexity requirements.
LDAP Schema Settings	
Base DN	This is the LDAP search base used as the starting point to search for the user information.
User Object Filter	This string may be modified to create a search based on a location or filter other than the default search base or attribute.
User Schema Settings	
Username Attribute	This is the attribute name on the LDAP server that contains the username for the account. This is often specified by the string "sAMAccountName" in Active Directory servers that may be used by LDAP. Contact your local LDAP administrator for the correct username attribute to use.
Email Attribute	This is the attribute name on the LDAP server that contains the email address for the account. This is often specified by the string "mail" in Active Directory servers that may be used by LDAP. Contact your local LDAP administrator for the correct email attribute to use.
Phone Attribute	This is the attribute name on the LDAP server that contains the telephone number for the account. This is often specified by the string "telephoneNumber" in Active Directory servers that may be used by LDAP. Contact your local LDAP administrator for the correct telephone attribute to use.
Name Attribute	This field is the attribute name on the LDAP server that contains the name associated with the account. This is often specified by the string "CN" in Active Directory servers that may be used by LDAP. Contact your local LDAP administrator for the correct name attribute to use.

User

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

The Security Manager user is the primary user created for the Organization and is the highest-level security manager within SecurityCenter. The Security Manager is also the initial Organizational user to log in and is responsible for creating other Organizational users. The Administrator field sets the initial Administrator's (user name admin) password.



Security Manager 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.

Table 9 – User Options

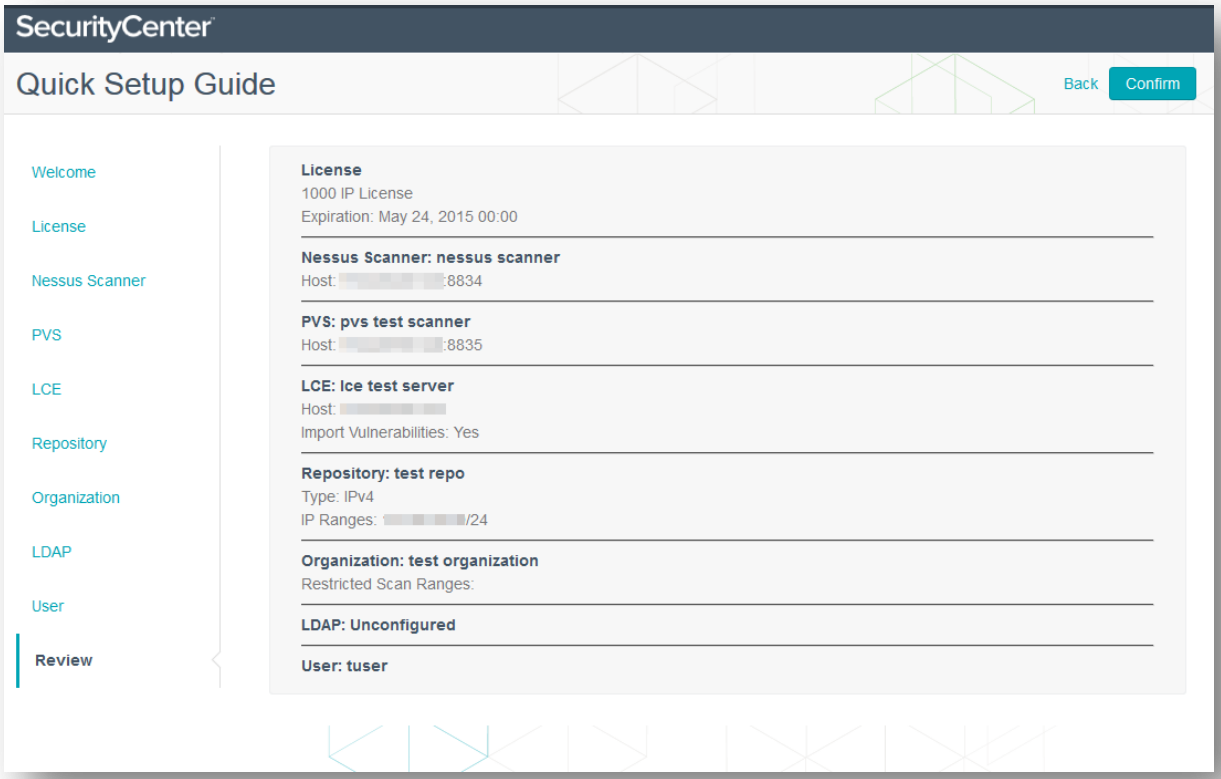
Option	Description
Security Manager	
First Name/Last Name	These fields define the first and last name of the Security Manager user.
Username	This field is to enter the username to be associated with the Security Manager.
Password/Confirm Password	These fields are for entering and confirming the password used for the Security Manager. The password entered should conform to the best practices of the organization where the SecurityCenter installation is being used when possible.

User Must Change Password	When enabled, once the user has successfully logged in for the first time they will be prompted to enter a new password.
Administrator	
Password/Confirm Password	This field sets the first Administrator's password (admin) and both fields must match. The password entered should conform to the best practices of the organization where the SecurityCenter installation is being used when possible.

After creating the Security Manager user and setting the Administrator password, click "**Next**" and setup is complete. You are now taken to the admin dashboard screen where you can review login configuration data.

Review

The review page is the last step of the Quick Setup process. This screen displays the settings entered throughout the process for review. If an area needs to be changed, click on that section's title from the left-hand column. Once the settings are acceptable, click the Confirm button in the top right of the screen.



About Tenable Network Security

Tenable Network Security provides continuous network monitoring to identify vulnerabilities, reduce risk, and ensure compliance. Our family of products includes SecurityCenter Continuous View™, which provides the most comprehensive and integrated view of network health, and Nessus®, the global standard in detecting and assessing network data. Tenable is relied upon by many of the world's largest corporations, not-for-profit organizations and public sector agencies, including the entire U.S. Department of Defense. For more information, visit tenable.com.