SecurityCenter 4.8 Upgrade Guide

December 16, 2014

(Revision 5)

Table of Contents

Introduction

This document describes the process of upgrading Tenable Network Security's SecurityCenter product to version 4.8. 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 upgrade to SecurityCenter 4.8.

If upgrading to SecurityCenter 4.8.1, please refer to its upgrade guide.

Since many of Tenable's customers have requirements to maintain separation of duties, the SecurityCenter 4.8 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 4.8 Installation Guide** – This document provides instructions for the installation of SecurityCenter 4. 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 4.8 Upgrade Guide** – This document describes the process of upgrading to version 4.8 of SecurityCenter.
- **SecurityCenter 4.8.x Upgrade Guide** – This document describes the process of upgrading to version 4.8.x of SecurityCenter.
- **SecurityCenter 4.8 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 4.8 User Guide** – This document provides instructions for using SecurityCenter by 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 upgrading and utilize the steps provided to ensure deployment success.

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

Software Requirements

Supported Operating Systems

SecurityCenter 4.8 is available for Red Hat Enterprise Server 5 and 6 (32/64-bit). CentOS 5 and 6 (32/64-bit) are also officially supported.

Dependencies

Third-Party Packages

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** (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-4.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 1.6.0 with “yum” using the command below:

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

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 4.8. 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.

To upgrade to SecurityCenter 4.8, you must be running SecurityCenter 4.7.1 or greater. If you are running an older release of Security Center, upgrade to at least SecurityCenter 4.7.1 before upgrading to SecurityCenter 4.8.

Product	Minimum Version
Nessus	5.x
LCE	4.0 (3.6.1 with limited functionality) 4.2 or higher for LCE Vulnerability features
PVS	4.x
SecurityCenter (remote/offline repository*)	4.x
3D Tool	2.x

* SecurityCenter 4.8 can receive a repository from prior versions of SecurityCenter 4.0.x and above, but cannot share its repositories with previous versions.

Licensing

A license key from SecurityCenter 4.2.x or later will work with SecurityCenter 4.8. This license key can be obtained from the Tenable Support Portal. The Nessus and LCE (if applicable) Activation Code(s) from the upgraded system will be transferred during the upgrade. Please contact Tenable Support (support@tenable.com) or Licensing (licenses@tenable.com) with any issues regarding your key or Activation Code(s).

Disk Size

As a part of the upgrade process, existing **`application.db`**, **`plugins.db`**, **`jobqueue.db`**, **`messages.db`**, **`assets.db`**, and **`organization.db`** databases will be backed up, and the backup given an extension of **`.db.SCVERSION`**. Before performing an upgrade, ensure that there is sufficient space on the disk for copies of all the databases.

Changes in SecurityCenter 4.8

This section provides an overview of some of the new features and changes that are of particular interest to current SecurityCenter 4 customers. For more details on these features and changes, refer to the appropriate SecurityCenter 4.8 document as described in the Introduction.

New Features

- Updated user model to a more common “grouping” method vs the previously used hierarchal model
- Combination asset support adds the ability to create a new dynamic asset list based on exiting asset lists
- Combination asset filtering is supported when creating filters to apply set logic against multiple assets
- Defining User Responsibility by associating an asset list with a user
- Database Credentials are now created in SecurityCenter for ease of reuse and assigned to a scan policy versus the previous method of adding the database credentials to each scan policy individually
- Dynamic asset lists now support Perl Compatible Regular Expressions allowing for negative operators in addition to positive operators
- Communication between SecurityCenter and PVS uses XMLRPC only. All attached PVS scanners must be 4.0 or newer
- Increased the default file upload size to 500MB

Upgrading SecurityCenter

To perform an upgrade, download the new RPM to your current SecurityCenter server from the Tenable Support Portal. Within SecurityCenter, wait for any in-progress scans to finish or manually pause them (scans are held in a state where they can be resumed at any point). Once the upgrade process has begun, normal usage of SecurityCenter will not be available until after the completion of the process.

SecurityCenter 4.8 introduces a new user security model. Access to security data (Repositories and LCEs intersected with defining assets) is now controlled through groups instead of individual users. User access to security data is granted based on the user’s group membership. Users will be able to automatically use Policies, Assets, and other objects created by others in the same group. The new group-based model also allows for more flexibility in user management, object management, and visibility into running scans and reports that is not constrained by the old user hierarchy. Utilizing groups in SecurityCenter makes it quicker and simpler to create, maintain, and assign resources to multiple users.

Due to this new user security model, a part of the upgrade process is to create Groups and assign existing users to Groups in SecurityCenter 4.8. The upgrade process analyzes existing user’s permissions and assigns them to Groups automatically. During the upgrade process you are given the opportunity to make changes as needed. In large installations this can take some significant time and the SecurityCenter is unavailable during the upgrade process.

To facilitate a quicker upgrade, Tenable provides the SecurityCenter 4.8 pre-migration wizard and instructions for its use from its support site at https://support.tenable.com. This wizard installs alongside the existing SecurityCenter 4.7.1 and provides an interface to read the current Organization structure and user configurations and allows changes to be made while SecurityCenter 4.7.1 is running. The wizard saves the changes to a file on the server and when the SecurityCenter 4.8 upgrade is performed it reads the file and applies the changes, saving time during the upgrade process.

Important Prerequisites

It is important to ensure that the following conditions are met prior to beginning the upgrade process.

SecurityCenter Version

SecurityCenter 4.8 upgrades require that the SecurityCenter currently be running version 4.7.1 or greater.

Java Version

If the Oracle Java JRE or OpenJDK is not installed, the following warning is displayed:

```
[WARNING] SecurityCenter has determined that Oracle Java JRE and OpenJDK is not
installed.
One of two must be installed for SecurityCenter reporting to function properly.
```

Remove any existing non-compatible versions and install the latest version of either of these software packages before running any reports.

Perform Backup

Prior to upgrading, it is recommended that the "**/opt/sc4**" directory be backed up to a separate location. After stopping the SecurityCenter services, run the following command from a directory outside of **/opt/sc4** (such as **/** or **/home)** to create the backup:

```
# tar -pzcf sc4_backup.tar.gz /opt/sc4
```

After running this backup command, move the **sc4_backup.tar.gz** file to a different location.

Halt or Complete Running Jobs

The SecurityCenter processes do not need to be stopped manually prior to the upgrade, but is recommended. However, if any jobs are currently running on SecurityCenter (e.g., Nessus scans), the following message is displayed along with the related process names and their PIDs:

```
"SecurityCenter has determined that the following jobs are still running. Please wait a
few minutes before performing the upgrade again. This will allow the running jobs to
complete their tasks"
```

Either stop the processes manually or try the upgrade again after the jobs complete.

Maintain Installation Log

During the upgrade 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 upgrade process is complete, the file will be moved to **/opt/sc4/admin/logs/install.log**.

Attached PVS Versions and Logins

Ensure that all attached PVS scanners have been upgraded to version 4.0 or higher. SecurityCenter 4.8 will not communicate with earlier versions of PVS. Additionally, the logins must be changed from the current user and password to one that exists for the XMLRPC login on the PVS server.

SecurityCenter 4.7.1 or Higher to 4.8 Upgrade

The upgrade process from SecurityCenter 4.7.1 to 4.8 is a two-step process. The first is to install the installation file obtained from Tenable. The second is to complete the upgrade wizard in a web browser.

Command Line Upgrades

To upgrade from Security Center 4.7.1 to SecurityCenter 4.8, use **rpm** with the "**-Uvh**" switches from the command-line of the SecurityCenter server. Use "**sudo -i**" when performing **sudo** upgrades of SecurityCenter to ensure the proper use of environmental variables. Upgrade SecurityCenter using a command similar to the following:

```
# rpm -Uvh SecurityCenter-4.8.0-es6.x86_64.rpm
```

Sample SecurityCenter upgrade output:

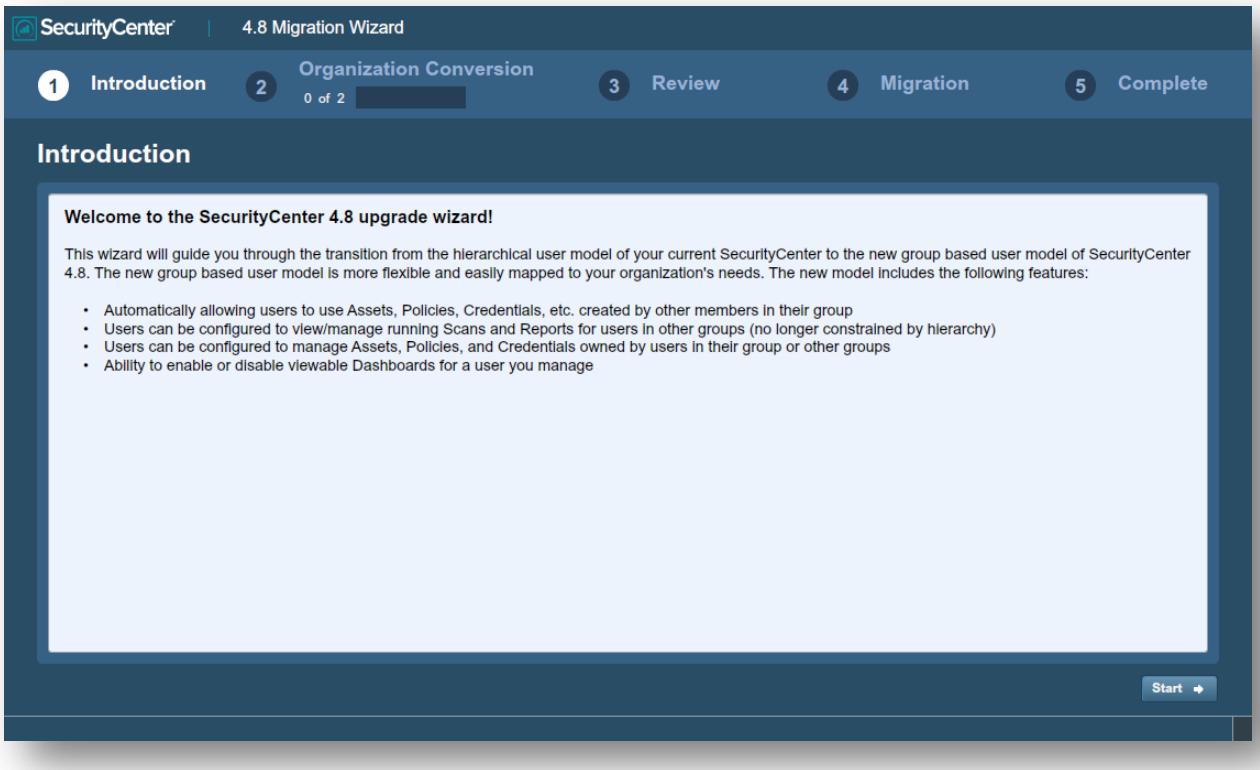
```
# rpm -Uvh SecurityCenter-4.8.0-es6.x86_64.rpm
Preparing...                ########################################### [100%]
Shutting down SecurityCenter services: [  OK  ]
   1:SecurityCenter         warning: /opt/sc4/admin/users/1/messages.db created as
Welcome to the SecurityCenter 4.8.0 migration process. Granted your current
       SecurityCenter installation has been preserved, it's ALWAYS a good idea to have
       a backup available.

SecurityCenter has started the Apache web server successfully.
You may continue the migration process by visiting https://<ipaddress>
The SecurityCenter service will be unavailable until migration has been completed.
```

Web Browser Migration Wizard

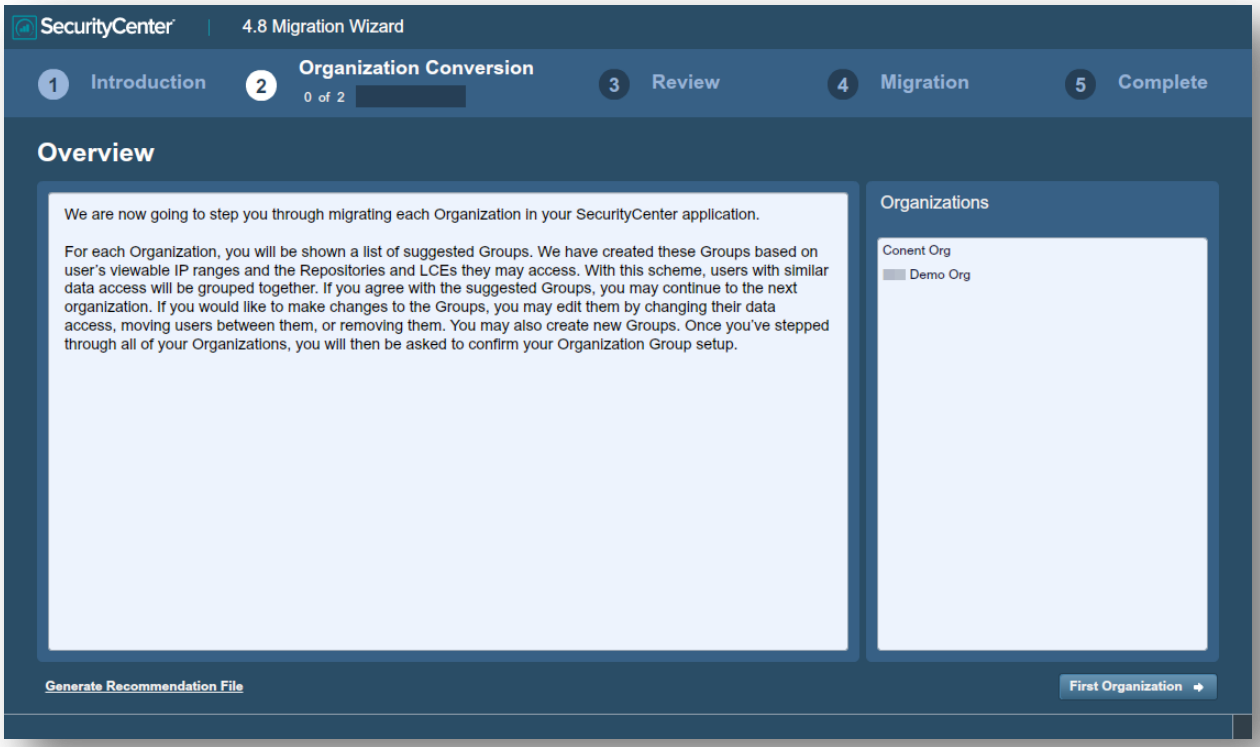
If the Pre-Migration Wizard was run and its configuration file has been saved to a location other than the default, it must be restored at this stage. See the "Restore the Pre-Migration Configuration File" section before proceeding.

Once the rpm installation file has completed the upgrade process, use a web browser to connect to the SecurityCenter server at https://<IP address or hostname>. At this screen, log in using an administrator level account. Once logged in, the Migration Wizard will begin.

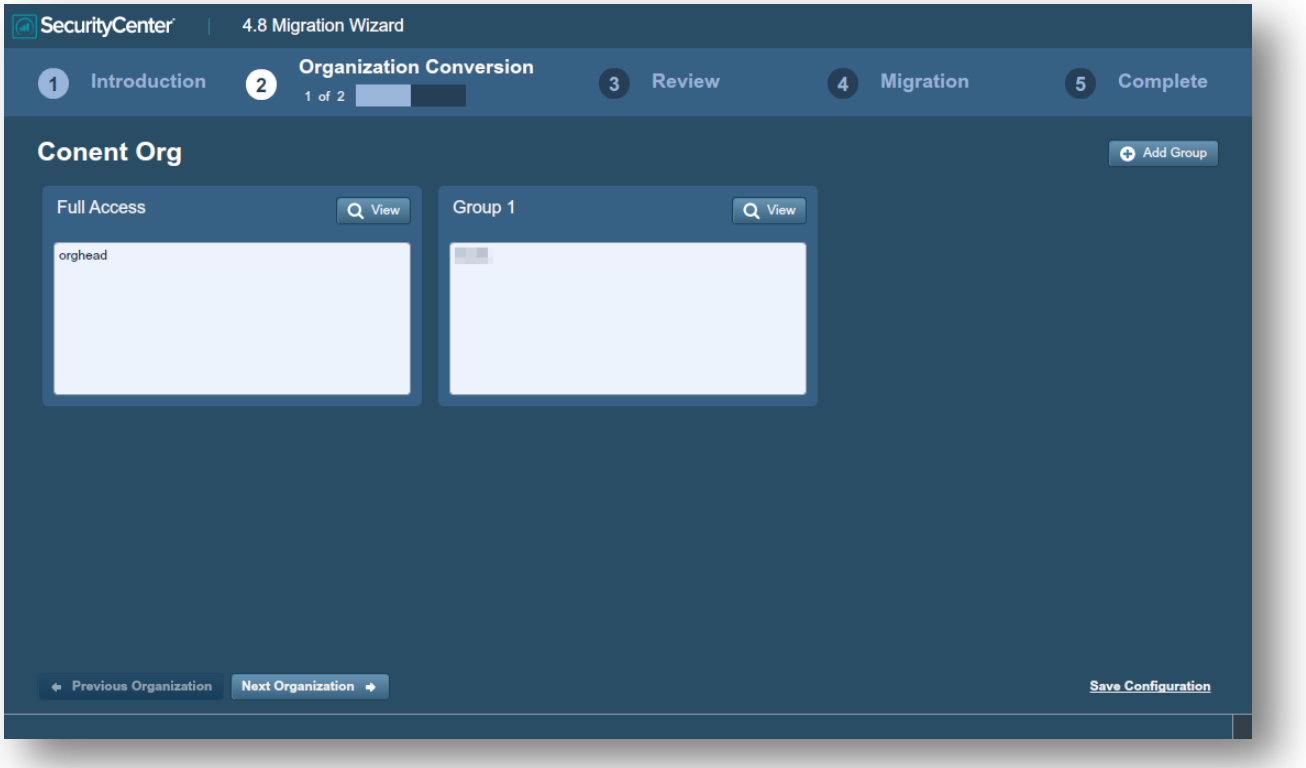
1. Once logged in, the SecurityCenter Migration Wizard is displayed and begins with Step 1, explaining that this wizard guides you through the process of transitioning from the hierarchical user model to the new group user model. When you are ready to continue with the wizard, click the "**Start**" button in the bottom right corner.



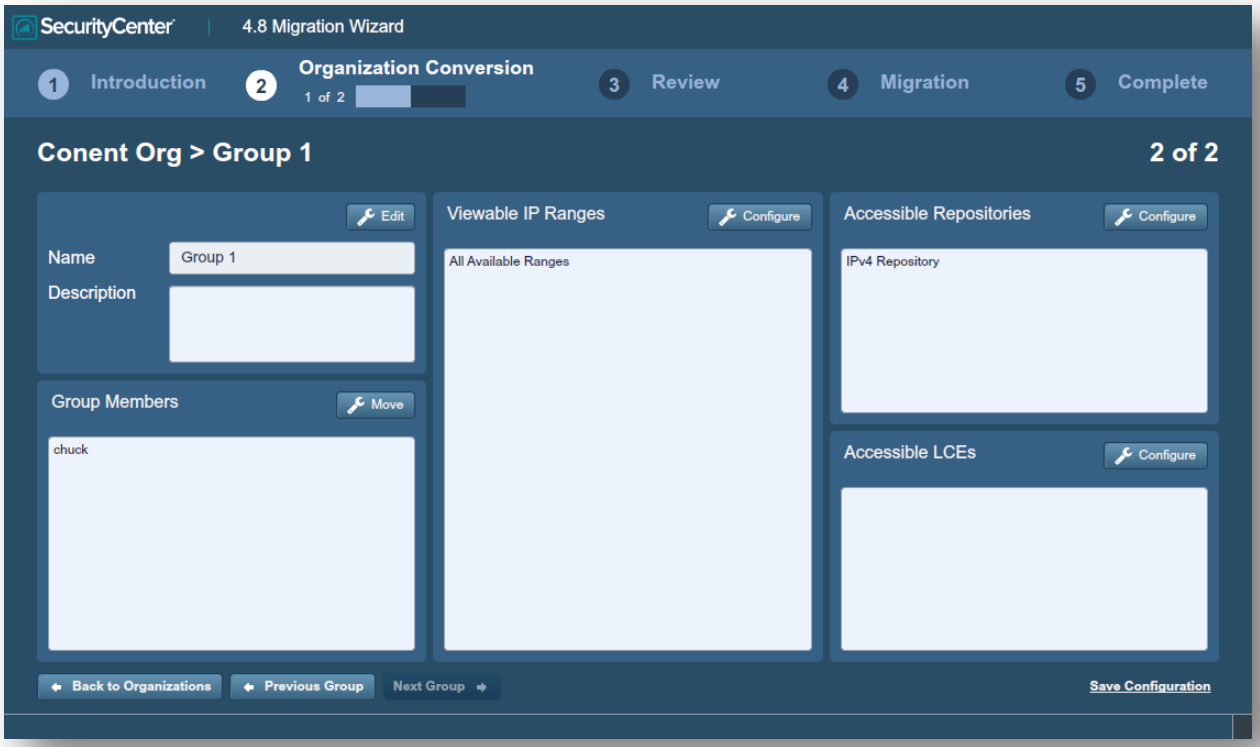
2. The second step is the Organization Conversion process. If the SecurityCenter 4.8 Pre-Migration Wizard has already been run on this system, the response file it created will be used for the defaults. If the Pre-Migration Wizard was not used, a list of suggested Groups is created. Click the "**First Organization**" button on the bottom left to start converting the first Organization.



3. The screen displayed will show various Groups created for the Organization. It will show a “Full Access” group for the existing users who have complete access to the Organization. Typically this will be the Organization Head user and equivalents. Other Groups will be created based on detected permissions and list the exiting users automatically assigned to each Group. The default names will be “Group 1”, “Group 2”, and so on. Other than the “Full Access” Group, Group names may be changed.

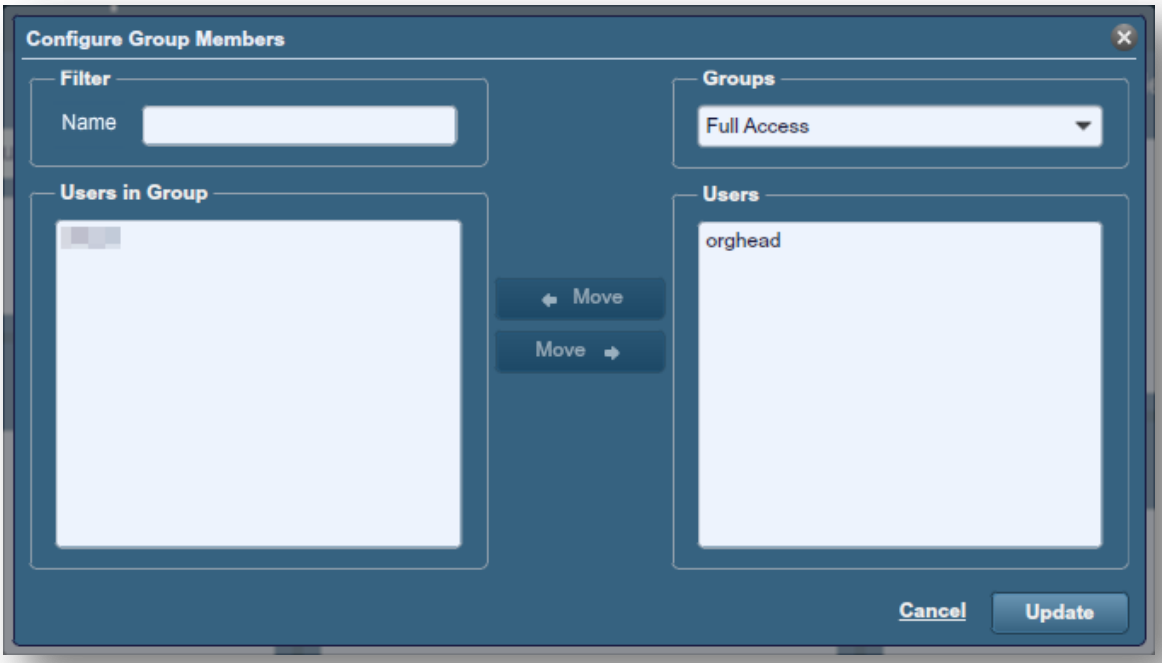


4. There is a “View” button for each Group listed. Clicking this will display the properties of the Group selected. On this screen, the Group properties of Name and Description, Group Members, Viewable IP Ranges, Accessible Repositories, and Accessible LCEs are displayed. Each property may be edited using the configuration button in the top right of its box.

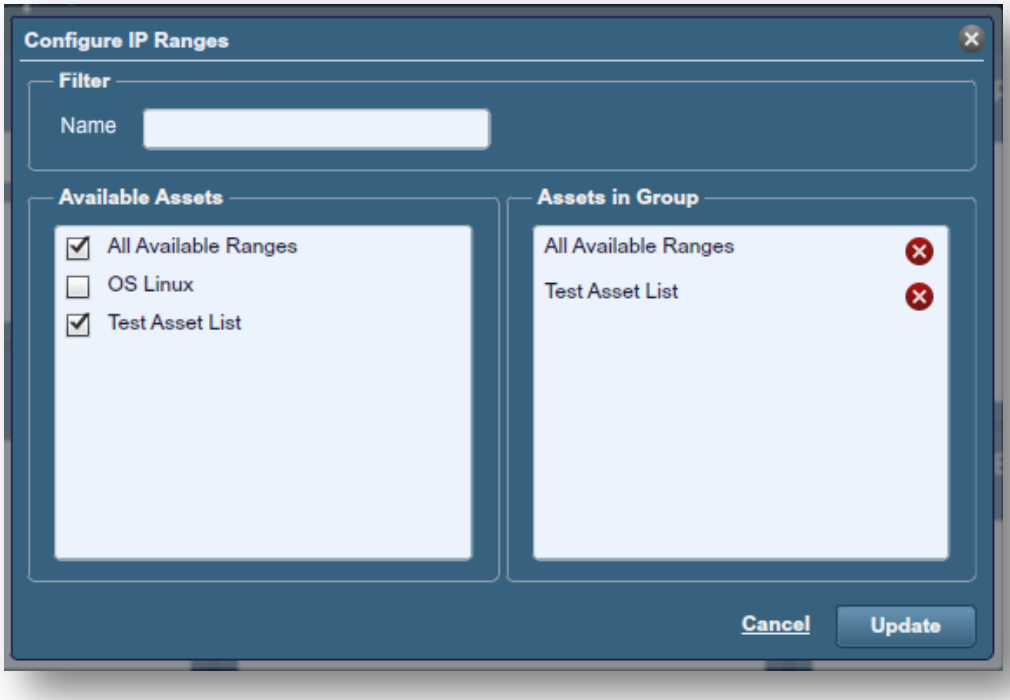


Editing the Name and Description field allows you to customize the fields for the Group when viewing it in SecurityCenter.

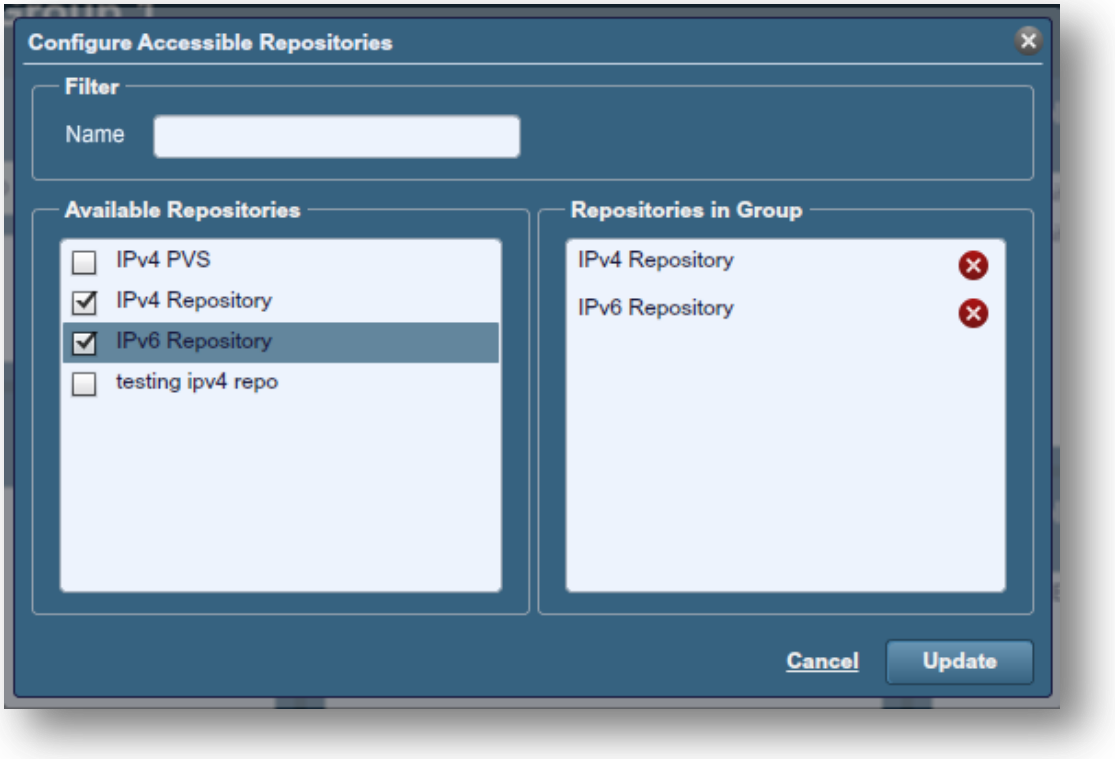
The **Configure Group Members** window allows you to move users among Groups. From the left column, the user(s) to move from the exiting Group to a new Group may be selected and filtered by Name to narrow the list. On the right, a destination Group is selected for the user. Users may also be selected from the right column from another Group to be moved into the Group being edited. When the user(s) is selected, click the “Move” button in the middle with the arrow pointing in the direction to move the user(s).



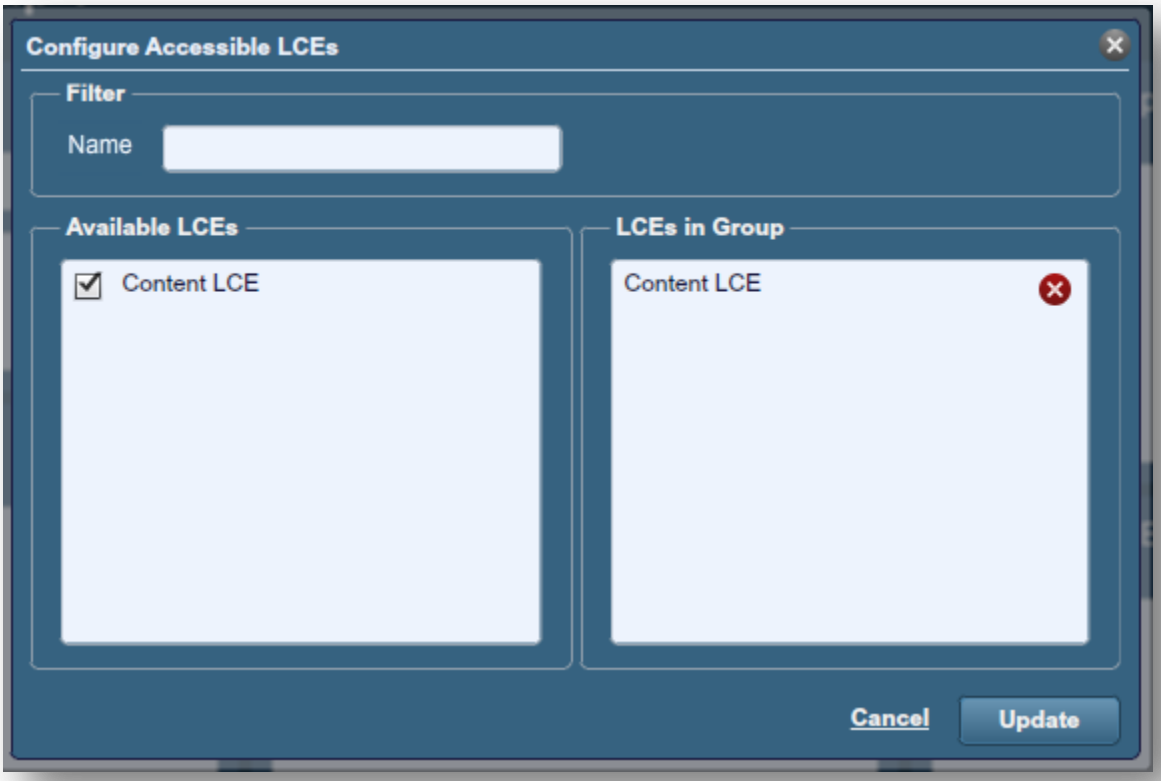
Configuring the IP Ranges defines the IP addresses that can be viewed by the Group, depending on the asset list they belong to. Selecting "**All Available Assets**" grants the right to view all the IP addresses viewable by the Organization. Selecting one or more other asset lists only grants rights to view the IP addresses that are a part of those asset lists. The asset list with the broadest range of IP addresses determines the viewable range. Clicking the red X or unchecking the box next to an asset removes access to that asset from the Group.



Configuring the Accessible Repositories defines the repositories that are available to the Group. Selecting the repository from the list on the left will allow the Group access to the repository. Clicking the red X or unchecking the box next to the repository will remove the repository access from the Group.

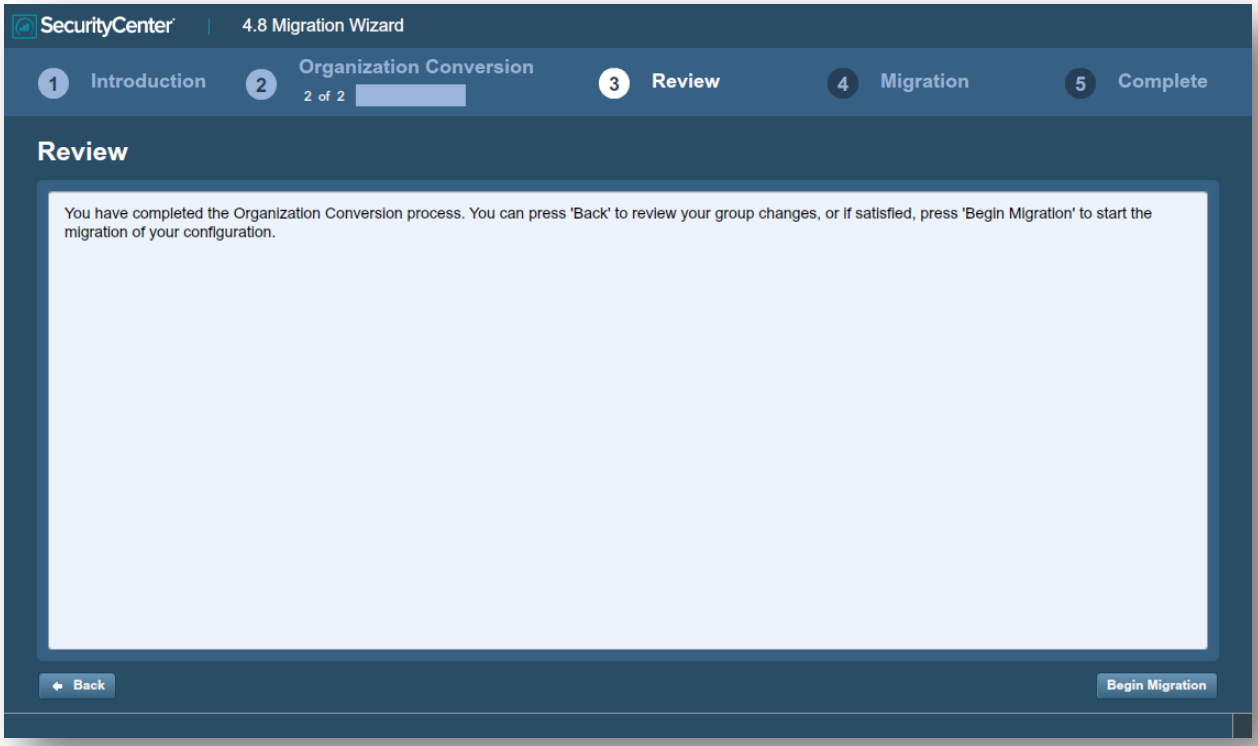


Configuring the Accessible LCEs defines the LCEs that are available to the Group. Selecting the LCE from the list on the left will allow the Group access to the LCE. Clicking the red X or unchecking the box next to the LCE will remove the LCE access from the Group.

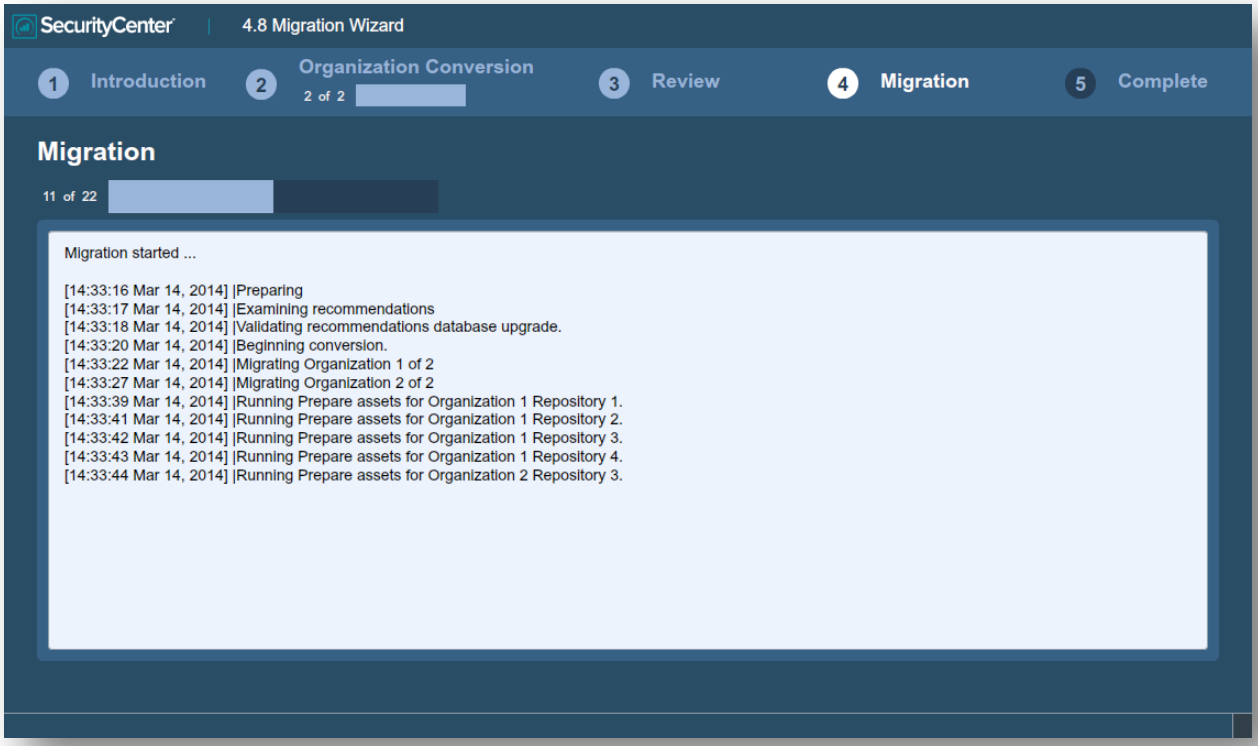


5. Repeat the steps for each Group in the Organization as appropriate by clicking the "**Next Group**" or "**Previous Group**" button to navigate between Groups in an Organization. Once the changes for the Organization is complete, click the "**Back to Organizations**" button to return to the Organization Conversion page. Click "**Next Organization**" or "**Previous Organization**" to make changes to each one as appropriate. After they are all complete, click the "**Review**" button to continue.

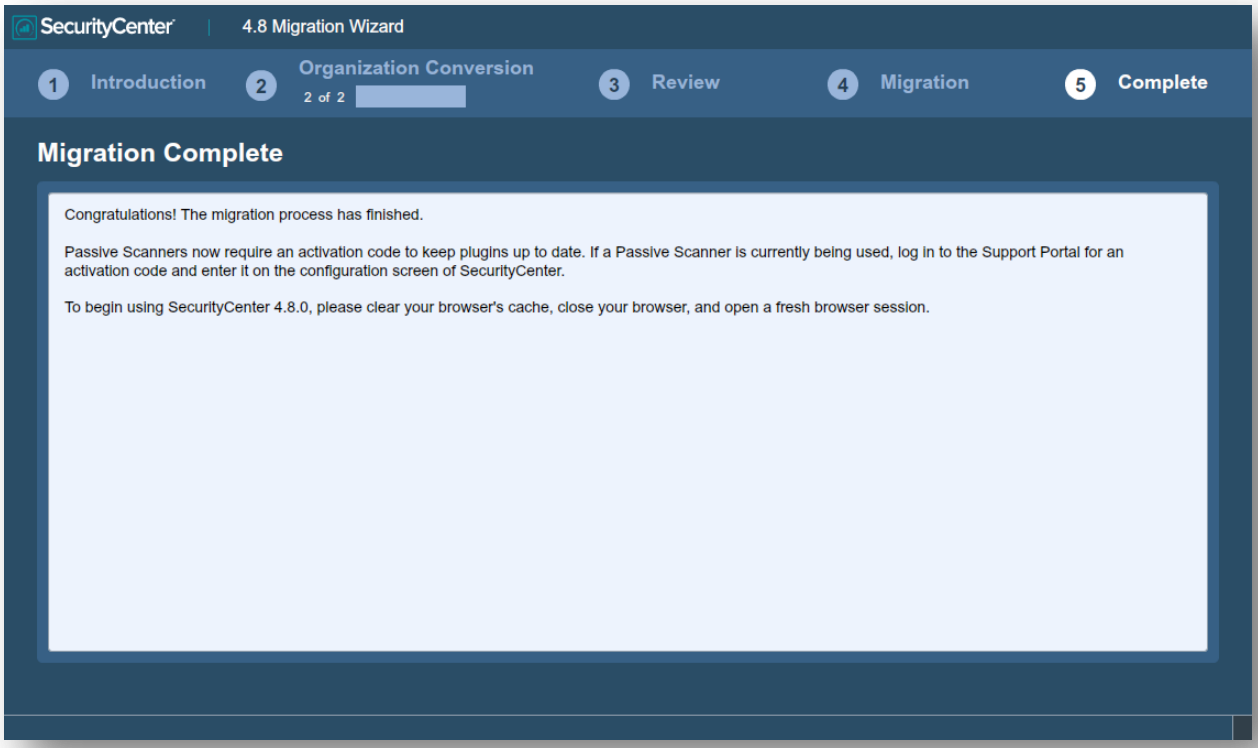
6. Arriving at the Review screen indicates that the Organization migration is ready to begin. Once the migration starts, changes cannot be made until after the upgrade process is complete. Clicking "**Begin Migration**" will begin the migration process to the new Groups hierarchy.



7. During the Migration Process, a window will be displayed with various messages about the progress of the migration. The time it takes the migration to complete will vary depending upon the speed of the server and the amount of objects to be converted to the new Groups hierarchy.



8. After the migration is complete, the "**Migration Complete**" window will be displayed. This contains some important information about using the new SecurityCenter 4.8 server.



Once the upgrade is complete, the SecurityCenter services are restarted. Clear your web browser's cache, close your web browser, and reconnect to your SecurityCenter server to start using SecurityCenter 4.8.

A "Critical" level is available from Nessus 5 scan results that will be used alongside previous vulnerabilities that were recast to "Critical".

Upgrading Custom SSL Certificates

After an upgrade of a SecurityCenter where custom Apache SSL certificates were in use prior to the upgrade they are backed up as part of the upgrade process. The existing custom SSL certificates are copied to the Apache configuration backup directory that is created during the upgrade in the **`/tmp/[version].apache.conf-########`** directory. The exact name of the directory will vary, but is displayed during the upgrade process and is reported in the **`/opt/sc4/admin/log/install.log`** file.

The commands to restore the custom SSL certificates are as follows:

`#` **`cp /tmp/[version].apache.conf-########/SecurityCenter.cert /opt/sc4/support/conf/SecurityCenter.crt`** (Select yes to overwrite the existing file)

`#` **`cp /tmp/[version].apache.conf-########/SecurityCenter.pem /opt/sc4/support/conf/SecurityCenter.key`** (Select yes to overwrite the existing file)

Ensure that the newly copied files have permissions of 0640 and ownership of tns:tns.

Modify the Servername parameter in **/opt/sc4/support/conf/servername** to match the Common Name (CN) of the SSL certificate. To obtain the CN run the following command and note the CN= portion of the result.

```
# /opt/sc4/support/bin/openssl verify /opt/sc4/support/conf/SecurityCenter.crt
```

Then edit the **/opt/sc4/support/conf/servername.conf** file at the ServerName parameter to match your certificate's CN value.

Once complete, restart the Apache server with one of the following commands:

```
# /opt/sc4/support/bin/apachectl restart
```

Or:

```
# service SecurityCenter restart
```

Restore the Pre-Migration Configuration File

If the Pre-Migration Wizard was run and the configuration file has been saved to another location, it must be restored for use prior to performing the migration. The following steps assume the information was saved to the directory **/root** by the "root" user. The user for these instructions is "root", and the file is saved to the home directory of the root user. Any user with sufficient permissions to read and write from the locations and change file permissions may perform these steps.

These steps are performed after the SecurityCenter 4.8 rpm file has been installed.

1. Copy the file from its saved location using the command "**cp /root/groupConfguration.json /opt/sc4/admin/tmp/**".
2. Ensure the ownership and permissions are set for the "tns" user and group by running the command "**chown tns:tns /opt/sc4/admin/tmp/groupConfiguration.json**".
3. Resume the Migration Wizard process following the steps in the "Web Browser Migration Wizard" section of this document.

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 more than 24,000 organizations, including the entire U.S. Department of Defense and many of the world's largest companies and governments. We offer customers peace of mind thanks to the largest install base, the best expertise, and the ability to identify their biggest threats and enable them to respond quickly.

For more information, please visit tenable.com.