



**TENABLE**  
Network Security®

## **Tenable Network Security Support Portal**

May 2, 2011

(Revision 9)

---

Copyright © 2011. Tenable Network Security, Inc. All rights reserved. Tenable Network Security and Nessus are registered trademarks of Tenable Network Security, Inc. The ProfessionalFeed is a trademark of Tenable Network Security, Inc. All other products or services are trademarks of their respective owners.

# Table of Contents

<b>Introduction .....</b>	<b>3</b>
<b>Obtaining Access to the Tenable Support Portal .....</b>	<b>3</b>
<b>Managing Your Nessus Activation Codes.....</b>	<b>4</b>
<b>Adding Multiple Users.....</b>	<b>5</b>
<b>Support Ticketing Systems .....</b>	<b>6</b>
<b>Available Audit Content .....</b>	<b>8</b>
<b>Knowledgebase .....</b>	<b>10</b>
<b>Online Content.....</b>	<b>11</b>
<b>About Tenable Network Security .....</b>	<b>12</b>

## INTRODUCTION

This document describes the many different functions of Tenable's Support Portal.

Customers who have purchased a Nessus ProfessionalFeed or use the SecurityCenter have access to the Tenable Support Portal located at:

<https://support.tenable.com/support-center/>

The Tenable Support Portal allows Tenable's customers to:

- Manage and maintain product Activation Codes
- Download Tenable software, such as new SecurityCenter or Nessus builds
- Open and manage support tickets for assistance with Nessus or Tenable Enterprise product issues
- Download audit content to perform configuration or content audits
- Search the product knowledgebase (KB) for answers and best practices
- Download utilities and tools for use with Nessus and Tenable Enterprise products
- Download product documentation, quick start guides and other useful papers

## OBTAINING ACCESS TO THE TENABLE SUPPORT PORTAL

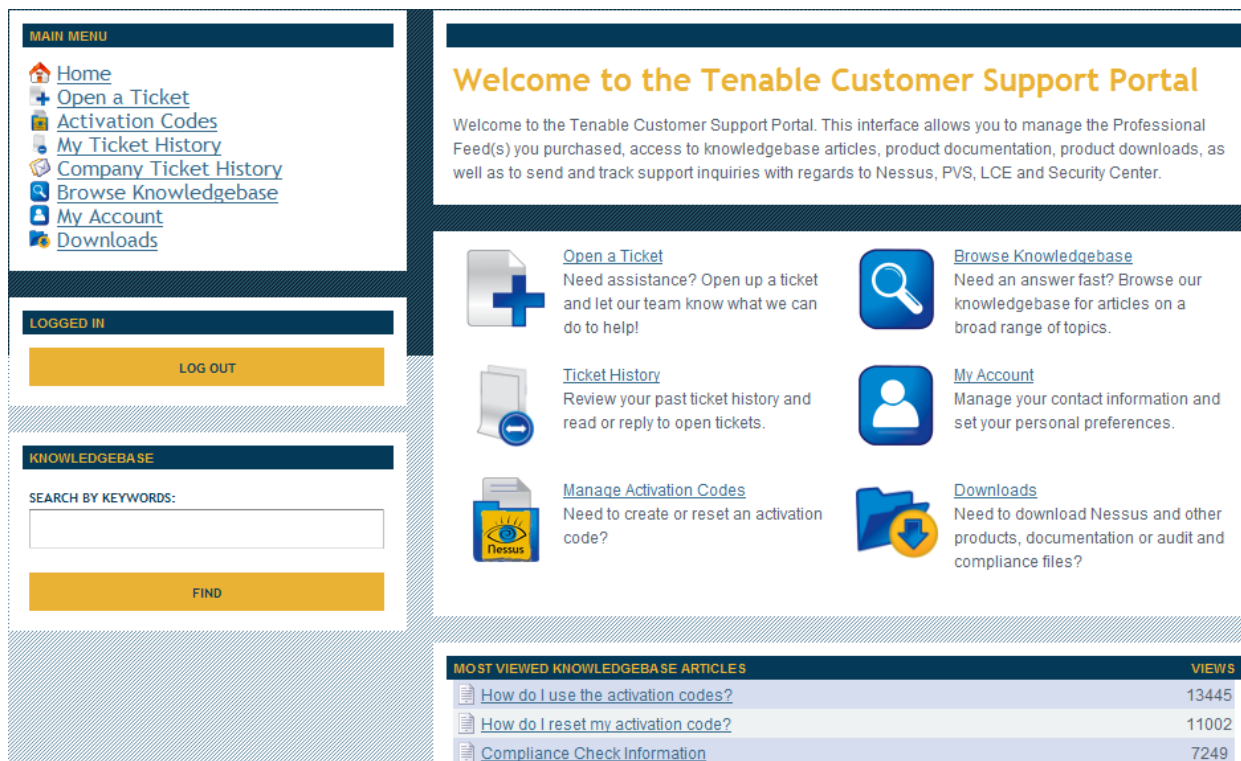
Customers who have purchased a ProfessionalFeed receive an activation email with a unique URL that is specific to the customer to create the customer account in the Tenable Support Portal via <https://support.tenable.com/support-center/>. A link to the Tenable Support Portal is also available from <http://www.tenable.com/> under "Support".

Clicking on this URL brings you to the Tenable Support Portal where you create your account to gain access to your Activation Code(s). Access is granted via a valid email address and the Tenable Support Portal account is tied to individual email addresses. Additionally, shared accounts may be created for your organization by using a common email address and password. Authorized personnel can then access this account using the shared credentials. If you have previously purchased products with the same email address, you will have the option to add these new products to your existing account or create a new account. Please note that if the email address you choose to register with is not already registered with Tenable it cannot be registered under an existing account name. You can register the email address under a new account name and later contact Tenable Licensing Staff to have the accounts combined and the new email address added to the list of authorized contacts for that organization.

When customers purchase a SecurityCenter, a Tenable Licensing Staff representative contacts them to assist in getting established on the Tenable Support Portal.

Once an email address is registered with Tenable, click on "Forgot Password / Activate Account" to log in for the first time.

Once logged in, a main menu is displayed similar to the following:



**MAIN MENU**

- Home
- Open a Ticket
- Activation Codes
- My Ticket History
- Company Ticket History
- Browse Knowledgebase
- My Account
- Downloads

**LOGGED IN**

LOG OUT

**KNOWLEDGEBASE**

SEARCH BY KEYWORDS:

FIND

**Welcome to the Tenable Customer Support Portal**

Welcome to the Tenable Customer Support Portal. This interface allows you to manage the Professional Feed(s) you purchased, access to knowledgebase articles, product documentation, product downloads, as well as to send and track support inquiries with regards to Nessus, PVS, LCE and Security Center.

**Open a Ticket**  
Need assistance? Open up a ticket and let our team know what we can do to help!

**Browse Knowledgebase**  
Need an answer fast? Browse our knowledgebase for articles on a broad range of topics.

**Ticket History**  
Review your past ticket history and read or reply to open tickets.

**My Account**  
Manage your contact information and set your personal preferences.

**Manage Activation Codes**  
Need to create or reset an activation code?

**Downloads**  
Need to download Nessus and other products, documentation or audit and compliance files?

**MOST VIEWED KNOWLEDGEBASE ARTICLES**

	VIEWS
<a href="#">How do I use the activation codes?</a>	13445
<a href="#">How do I reset my activation code?</a>	11002
<a href="#">Compliance Check Information</a>	7249

There are also a variety of links for searching and looking at popular Knowledgebase articles.

## MANAGING YOUR NESSUS ACTIVATION CODES

The “Manage Activation Codes” button provides a list of all of your current products and services including expiration dates.

Nessus scanners managed by the SecurityCenter do not need individual Activation Codes as the Maintenance Activation Code of the SecurityCenter is used to get the updated plugins to the managed scanners. The current Maintenance Activation Code is displayed in the Tenable Support Portal. If your organization operates multiple SecurityCenters, individual Maintenance Activation Codes are displayed.

All enterprise product Maintenance Activation Codes are displayed with the associated IP address of the registered system. This may be useful information for organizations that operate multiple Tenable Enterprise products. Note that Network Address Translation (NAT) devices such as firewalls and some routers may cause the same IP to appear for multiple products.

The Identifier field enables you to track which system the Activation Code is installed on. This optional field can be set to any string that is meaningful to you. This feature is especially helpful for customers that have more than one maintenance code and need to track this information in a central location. The Identifier field can be set at any time. If the Identifier field needs to be reset and changed, the Activation Code will have to be reset and then registered again within the product (please note that the Activation Code must be previously registered in order to reset the Identifier field).

A screen capture (that has obscured the Activation Codes and IPs) listing the product view is shown below:

TENABLE CUSTOMER SUPPORT PORTAL

## Your Registered Products

Product	Activation Code	In Use?	Scanner IP	Identifier	Expires	Manage	Reset	Renew
ProfessionalFeed	[obscured]	yes	[obscured] 72.208	MyServer	2013-12-31	<a href="#">set access</a>	X	
ProfessionalFeed	[obscured]	yes	[obscured] 7.158	godzilla	2013-12-31	<a href="#">set access</a>	X	
ProfessionalFeed	[obscured]	no		megalon	2013-12-31	<a href="#">set access</a>		

This screen capture displays an example Tenable customer who has three Nessus ProfessionalFeed subscriptions.

The only time a customer must purchase one or more separate Nessus feeds for SecurityCenter is when their scanners are not managed by a SecurityCenter. For example, if the scanners are in physically separate locations, they can be used independently of SecurityCenter and have their reports manually uploaded, if needed.

This view also shows the expiration date of each product. Codes set to expire within 60 days are displayed in red. Codes set to expire within 30 days are displayed bold red and underlined. Expired codes are displayed in bold red and have a line through them. To avoid an interruption in plugin updates, renew any subscriptions before their expiration date.

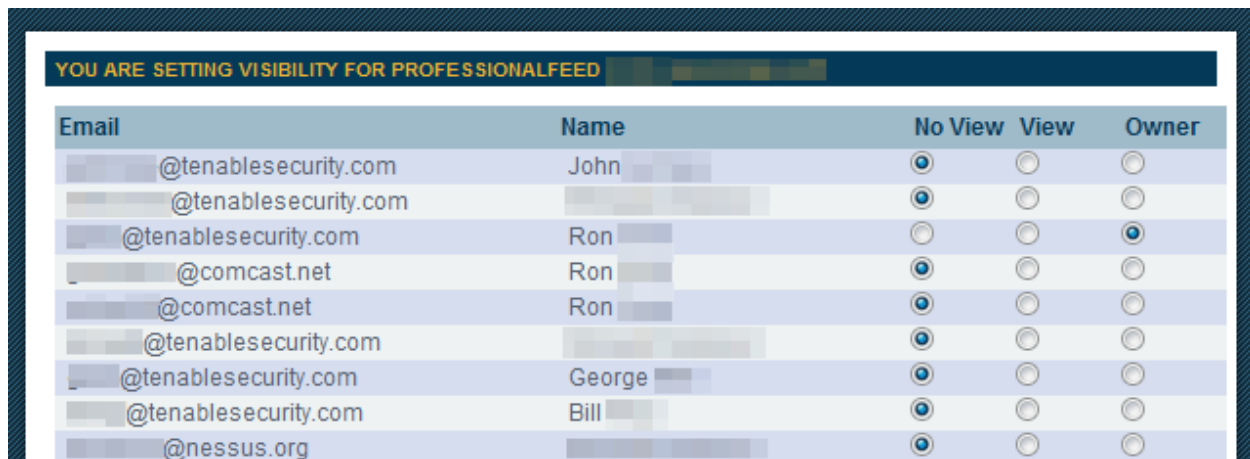
ProfessionalFeeds are associated with permanent servers. If your server has a hardware issue, needs to be upgraded or has some other issue requiring replacement, the Tenable Support Portal allows authorized users to manually reset the Activation Code to re-register with the updated hardware. There are time limits and audits of these transfers. For example, you cannot use the same Activation Code on multiple production Nessus scanners. During an outage, the ability to reset this from the Portal can be invaluable. In addition, users who have the ability to reset Activation Codes are limited to the "owner" of the Code and the Primary Contact (PC). There can only be one Tenable Support Portal account to which the Activation Code is assigned (the "owner") and up to two Primary Contact(s). The Primary Contact also has the ability to assign the Code(s) to other authorized users registered in their organization.

## ADDING MULTIPLE USERS

If your organization requires multiple users to have access to the Tenable Support Portal, the Primary Contact can email [support@tenable.com](mailto:support@tenable.com) or [licenses@tenable.com](mailto:licenses@tenable.com) and request the addition of one or more users. The request to add users' email must include the additional users' full names, email addresses and, when possible, phone numbers. As a Primary Contact, you can then manage which Activation Codes get to be managed by which

authorized users. For example, you may want one user to see all of the support tickets and other users to only have the ability to view their own.

The screen capture below lists an example of users who can and cannot manage and view Activation Codes. "No View" prevents the user from seeing Activation Codes in their Portal. "View" permits the user to see Activation Codes and the information associated with each Activation Code (registration status, registration IP address, etc.), but they do not have the ability to reset Activation Codes. The "Owner" can see all of the information associated with Activation Codes and also has the ability to reset Activation Codes.



YOU ARE SETTING VISIBILITY FOR PROFESSIONALFEED				
Email	Name	No View	View	Owner
...@tenablesecurity.com	John	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
...@tenablesecurity.com		<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
...@tenablesecurity.com	Ron	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
...@comcast.net	Ron	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
...@comcast.net	Ron	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
...@tenablesecurity.com		<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
...@tenablesecurity.com	George	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
...@tenablesecurity.com	Bill	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
...@nessus.org		<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

## SUPPORT TICKETING SYSTEMS

Customers who log into the Tenable Support Portal have access to a web-based ticketing system. The Tenable Support Portal is staffed with experienced personnel who have the ability to escalate tickets to Tenable’s Research, Quality Assurance, Content and Development groups.

Each ticket receives a unique tracking ID. Older tickets that have been closed may be viewed by clicking on "My Ticket History" and then the "View Closed Tickets" link.

The ticketing system also enables secure uploads of Nessus results, logs, packet traces or other information that may assist Tenable with support issue resolution.

Below is a screen capture of the ticketing system at work:

MY TICKET HISTORY

## Ticket Details

[Back to Open Tickets](#)

### New OS fingerprint

ID: QSZ-██████-789  
Status: open  
Priority: unassigned  
Opened: Sun May 01 2011 01:16PM  
Last Msg: Sun May 01 2011 01:23PM  
Due: Tue May 03 2011 12:00AM

SUN MAY 01 2011 01:16PM BY NESSUS-SUPPORT@TENABLE.COM

IP: 173.59.██████

Can I submit new OS fingerprints found by Nessus through this ticketing system? We have a variety of old NAS appliances that I thought were Linux based, but they seem to be based on a variant of VxWorks.

SUN MAY 01 2011 01:23PM BY NESSUS-SUPPORT@TENABLE.COM

Yes, you can submit new OS fingerprints for Nessus here and we will send them to the Tenable Research team for verification and inclusion in the plugin update feeds.

Tenable Support

> IP: 173.59.██████

>

> Can I submit new OS fingerprints found by Nessus through this  
> ticketing system? We have a variety of old NAS appliances that  
> I thought were Linux based, but they seem to be based on a variant  
> of VxWorks.

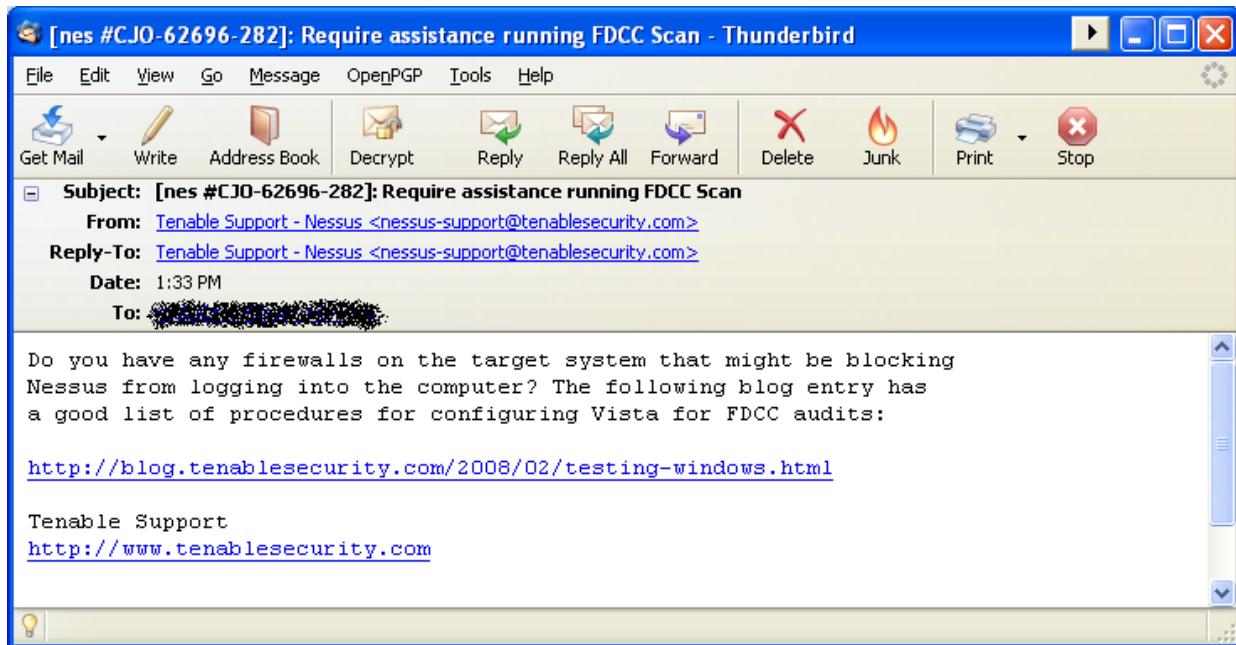
>

>

If you manage accounts for other users in your organization, you can see their tickets if you request that access during account setup; otherwise you can only view tickets designated to

your email. The ability to review ticket history aids with ticket resolution if employees change roles, are unavailable for extended periods of time or are new and need brought up to speed.

Tenable customers can make use of the web-based portal to enter in customer support tickets or they can simply use their email client and send mails directly to [support@tenable.com](mailto:support@tenable.com). The customer will be sent an automatic response that the message has been received and is provided with a ticket number for reference, which can also be tracked within the Tenable Support Portal. All email messages in the thread of support tickets receive a ticket ID pre-pended to their subject line as shown below:



Please note that, for security reasons, we require that all persons emailing support requests for your organization be registered as authorized users. If Tenable receives a request for support from an email address that is not registered, it will not be addressed until that email address is verified. To resolve this situation, Tenable will email the registered authorized contacts to validate the un-registered e-mail address prior to providing support or will ask the unregistered contact to provide the organization's Customer ID and/or Activation Code prior to providing support.

## AVAILABLE AUDIT CONTENT

Nessus and SecurityCenter audit policies can be obtained from several different sections on the Tenable Support Portal. By clicking on the "Downloads" button and then "Compliance and Audit Files", the following buttons become available:



[Compliance Checks Tools](#)  
Download compliance check policy tools and documentation.



[CIS Compliance Audit Policies](#)  
CIS certified configuration audit policies for Windows, Solaris, Red Hat, FreeBSD and many other operating systems.



[Sensitive Content Audit Policies](#)  
Audit policies that look for Credit Cards, Social Security numbers and many other types of sensitive data.



[Configuration Audit Policies](#)  
Audit policies based on CERT, DISA STIG, GLBA and HIPAA standards.



[Windows Audit Policies](#)  
Audit policies based upon standard Microsoft security templates.



[Cisco Audit Policies](#)  
Audit policies that perform configuration audits for IOS-based Cisco devices.



[Antivirus Audit Policies](#)  
Audit policies designed to allow users to determine if an antivirus package is installed and set to a working state.



[Virus Detection Audit Policies](#)  
Audit policies that Tenable's Research group has produced that scan for known trojans and rootkits.



[PCI Audit Policies](#)  
Audit policies developed by Tenable to test AIX, HP-UX, Linux, Solaris and Windows systems for minimum required PCI configuration settings.



[Tenable Application Audit Policies](#)  
Audit policies that examine hosts to determine if Tenable software applications exist and notifies of the presence and state of these packages.



[Database Audit Policies](#)  
Audit policies designed to allow users to audit their database configuration using the Nessus Database Compliance Check plugin.



[Control System Audits](#)  
Nessus audit policies are available for a wide variety of Control Systems and SCADA applications from Digital Bond.



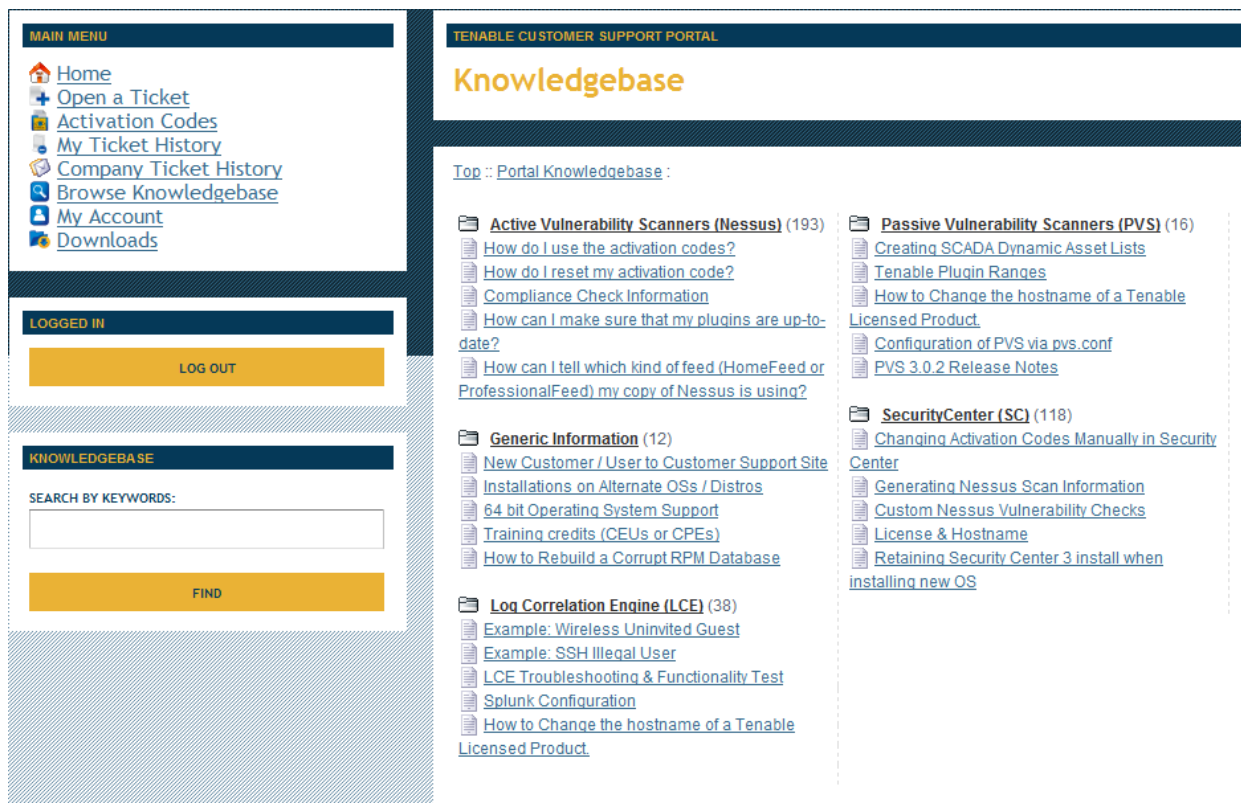
[NIST FDCC and SCAP Compliance Audit Policies](#)  
Audit policies that perform FDCC and NIST SCAP configuration audits. These audit files test for the required settings specified by the NIST SCAP and FDCC programs.

The following buttons provide a variety of content for Tenable's customers:

- **Compliance Check Tools** – This link contains a variety of Unix and Windows tools for generating custom Nessus audit policies. For example, the Windows Nessus Policy Creator can generate an audit policy based solely on the running configuration of a production computer.
- **CIS Compliance Audit Policies** – This link contains Center for Internet Security (CIS) certified audit policies for a wide variety of technologies and platforms.
- **Sensitive Content Audit Policies** – More than a dozen policies are available to help search Windows servers and desktops for sensitive data. This includes searches for credit card, Social Security and other type of numbers as well as federal and commercial sensitive financial, human resources and keyword tags.
- **Configuration Audit Policies** – Tenable authored and developed these policies with customer input concerning best practices from Microsoft, the NSA, GLBA legislation, HIPAA legislation and DISA STIGs. In addition, there is an AIX best practices policy based on CIS checks, but available for the 5.3L platform.
- **Windows Audit Policies** – These audit policies are based on standard Microsoft security templates.
- **Cisco Audit Policies** – These policies are designed to perform configuration audits for IOS-based Cisco devices.
- **Antivirus Audit Policies** – These audit policies are designed to allow users to determine if an antivirus package is installed, enabled and have an up to date signature file. Additionally, there are policies to help determine which systems may have had malware place a specific file or registry entry on them.
- **Virus Detection Audit Policies** – These policies are designed to scan for known Trojans and rootkits.
- **PCI Audit Policies** – The PCI DSS is intended to provide a common baseline to safeguard sensitive cardholder data for all bankcard brands and is in use by many e-commerce vendors who accept and store credit card data. Tenable has a PCI audit policies for a wide variety of OS platforms that can help customers meet compliance.
- **Tenable Application Audit Policies** – These audit policies examine hosts to determine if Tenable software applications exist and notify of the presence and state of these packages.
- **Database Audit Policies** – These audit policies are designed to allow users to audit their database configuration using the Nessus Database Compliance Check plugin.
- **Control System Audits** – These audit policies are available for a wide variety of Control Systems and SCADA application from Digital Bond.
- **NIST FDCC and SCAP Compliance Audit Policies** – These audit policies aid organizations in achieving compliance with a variety of NIST guidelines including FDCC and SCAP. These audit files are generated directly from the SCAP XCCDF content and are suitable for reporting to OMB.

## KNOWLEDGEBASE

Tenable's Support and Content groups maintain a list of commonly asked questions across our entire product line. A screen capture of the default Knowledgebase categories is shown below:



The screenshot shows the Tenable Customer Support Portal Knowledgebase. On the left is a navigation sidebar with a 'MAIN MENU' containing links for Home, Open a Ticket, Activation Codes, My Ticket History, Company Ticket History, Browse Knowledgebase, My Account, and Downloads. Below this is a 'LOGGED IN' section with a 'LOG OUT' button. Further down is a 'KNOWLEDGEBASE' section with a search box labeled 'SEARCH BY KEYWORDS:' and a 'FIND' button. The main content area is titled 'TENABLE CUSTOMER SUPPORT PORTAL Knowledgebase' and shows a 'Portal Knowledgebase' listing. It is organized into three columns of links, each with a folder icon and a count in parentheses: 'Active Vulnerability Scanners (Nessus) (193)', 'Passive Vulnerability Scanners (PVS) (16)', 'Generic Information (12)', 'Log Correlation Engine (LCE) (38)', and 'SecurityCenter (SC) (118)'. Each category lists several specific articles with titles like 'How do I use the activation codes?' and 'Creating SCADA Dynamic Asset Lists'.

All entries are organized into several different areas based on product type. All content may be searched by any Tenable Support Portal user.

## ONLINE CONTENT

In addition to the Tenable Support Portal, Tenable also offers a wide variety of discussion groups and online content:

- > **Tenable Blog** – <http://blog.tenable.com/> – This blog focuses on major new product functionality announcements, in-depth best practices and extensive content on scanning, configuration auditing, log normalization and network anomaly detection.
- > **Tenable Product RSS Feeds** – <http://tenable.com/rss-feeds> – Tenable offers four different RSS feeds: Tenable news, the Tenable blog, Nessus plugins and PVS plugins.
- > **Discussion Forums** – <https://discussions.nessus.org/> – Tenable operates discussion forums that are used by ProfessionalFeed and HomeFeed Nessus users as well as Enterprise customers. Product updates are also announced here.
- > **Twitter** – <http://twitter.com/TenableSecurity> – Follow TenableSecurity on Twitter for the latest updates.

## **ABOUT TENABLE NETWORK SECURITY**

Tenable Network Security, the leader in Unified Security Monitoring, is the source of the Nessus vulnerability scanner and the creator of enterprise-class, agentless solutions for the continuous monitoring of vulnerabilities, configuration weaknesses, data leakage, log management and compromise detection to help ensure network security and FDCC, FISMA, SANS CAG and PCI compliance. Tenable's award-winning products are utilized by many Global 2000 organizations and Government agencies to proactively minimize network risk. For more information, please visit <http://www.tenable.com>.

**Tenable Network Security, Inc.**  
7063 Columbia Gateway Drive  
Suite 100  
Columbia, MD 21046  
410.872.0555  
[www.tenable.com](http://www.tenable.com)