Tenable Network Security
Support Portal

March 11, 2010
(Revision 7)

Table of Contents

Introduction

This document describes the many different functions of Tenable's Support Portal. Customers who have purchased a Nessus ProfessionalFeed or use the Security Center have access to the Tenable Support Portal located at:

https://support.tenablesecurity.com/support-center/

The Tenable Support Portal allows Tenable's customers to:

- Manage and maintain product Activation Codes
- Download Tenable software, such as new Security Center 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.tenablesecurity.com/support-center/. A link to the Tenable Support Portal is also available from http://www.tenablesecurity.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 Security Center, 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:

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 Security Center do not need individual Activation Codes as the Maintenance Activation Code of the Security Center 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 Security Centers, 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:

This screen capture displays an example Tenable customer who has three Nessus ProfessionalFeed subscriptions as well as other Tenable products hidden from view.

The only time a customer must purchase one or more separate Nessus feeds for Security Center is when their scanners are not managed by a Security Center. For example, if the scanners are in physically separate locations, they can be used independently of Security Center 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.
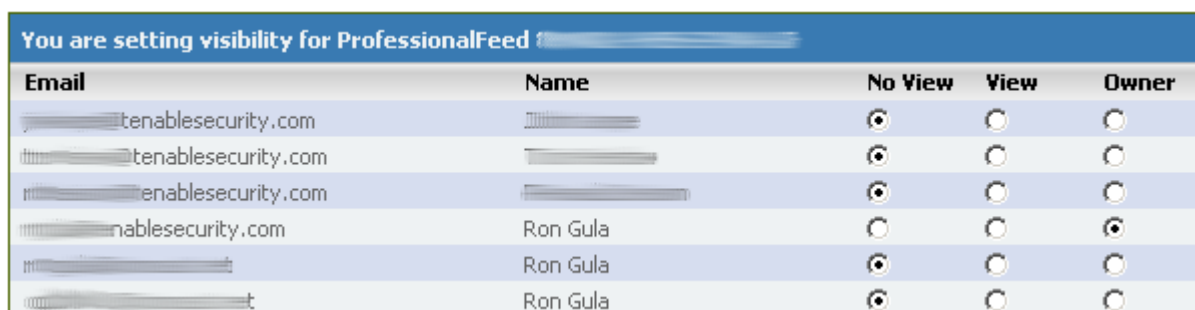
ProfessionalFeeds are associated with permanent servers. If your server has a hardware issue, needs to be upgraded or has some other issue requiring replacement, the Tenable Support Portal allows authorized users to manually reset the Activation Code to re-register with the updated hardware. There are 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@tenablesecurity.com or licenses@tenablesecurity.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.

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:

Ticket Details   Back to Open Tickets

Require assistance running FDCC Scan

ID: CJO-62696-282
Status: open
Priority: unassigned
Opened: Mon Jul 14 2008 01:28PM
Last Msg: Mon Jul 14 2008 01:33PM
Due: Tue Jul 15 2008 01:28PM

Mon Jul 14 2008 01:28PM by nessus-support@tenablesecurity.com

IP: 69.250▓▓▓▓

I'm logging in with the correct credentials to some target Windows Vista desktops, but the FDCC reports are not running.

Mon Jul 14 2008 01:33PM by nessus-support@tenablesecurity.com

Do you have any firewalls on the target system that might be blocking Nessus from logging into the computer? The following blog entry has a good list of procedures for configuring Vista for FDCC audits:

http://blog.tenablesecurity.com/2008/02/testing-windows.html

Tenable Support
http://www.tenablesecurity.com

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@tenablesecurity.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:
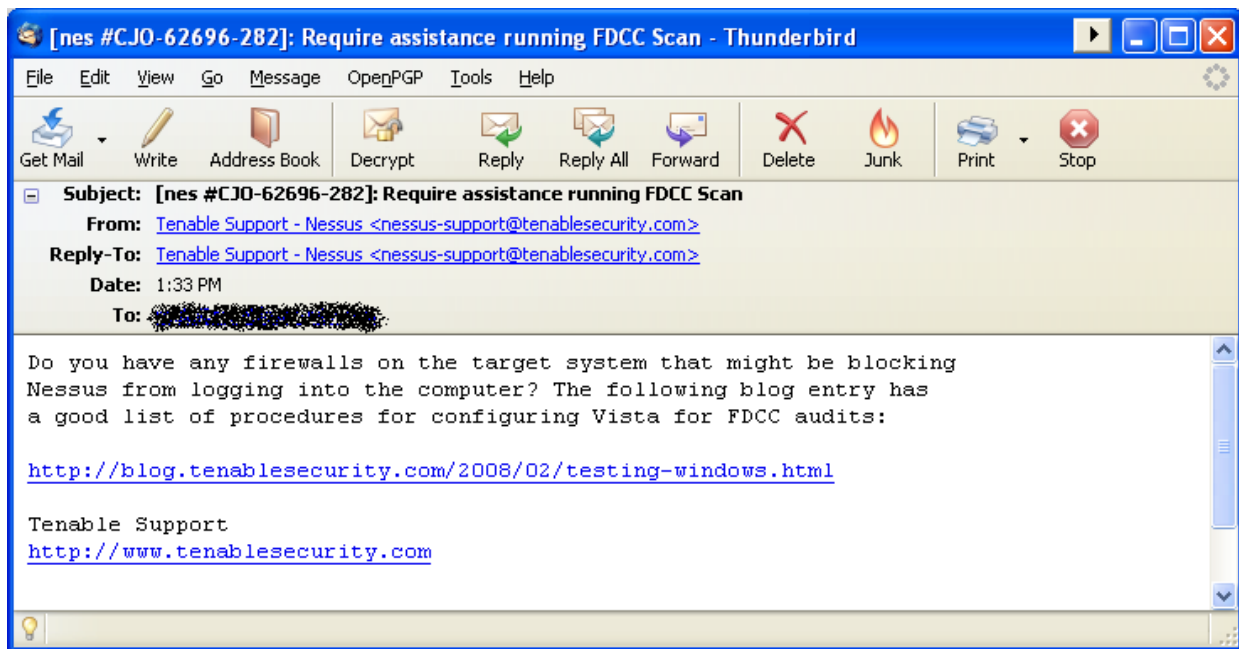
Please note that, for security reasons, we require that all persons emailing support requests for your organization be registered as authorized users. If Tenable receives a request for support from an email address that is not registered, it will not be addressed until that email address is verified. 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 Security Center 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. DISA CERT GLBA HIPAA
Windows Audit Policies Audit policies based upon standard Microsoft security templates. Microsoft	**Antivirus Audit Policies** Audit policies designed to allow users to determine if an antivirus package is installed and set to a working state.
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. TENABLE
Database Audit Policies Audit policies designed to allow users to audit their database configuration using the Nessus Database Compliance Check plugin. SQL	**Nessus NIST and FDCC 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. SCAP-FDCC Settings
Security Center NIST and FDCC Compliance Audit Policies Audit policies that perform FDCC and NIST SCAP configuration audits. These audit files were generated directly from the XCCDF SCAP content and are suitable for reporting to OMB. SCAP-FDCC XCCDF	

The bottom seven 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 Compliant 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** – These policies in this directory that Tenable authored and developed 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 upon standard Microsoft security templates.
- **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.
- **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.
- **Nessus NIST and FDCC Compliance Audit Policies** – These Nessus audit policies aid organizations in achieving compliance with a variety of NIST guidelines including FDCC. Security Center customers can use the "Security Center NIST and FDCC Compliance Audit Policies" that are generated directly from the XCCDF SCAP content and are suitable for reporting to OMB.
- **Security Center NIST and FDCC Compliance Audit Policies** – These Nessus audit policies aid organizations in achieving compliance with a variety of NIST guidelines including FDCC. These audit files are generated directly from the XCCDF SCAP 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. Below is a screen capture of the default Knowledgebase categories:

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.tenablesecurity.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://www.nessus.org/rss/ – Tenable offers six different RSS feeds; one for each product, as well as content updates such as new log correlation rules and audit policies.
- **Discussion Forums** – https://discussions.nessus.org/ – Tenable operates discussion forums that are used by ProfessionalFeed and HomeFeed Nessus users as well as Enterprise customers.
- **Twitter** – http://twitter.com/TenableSecurity – Follow TenableSecurity on Twitter for the latest updates.

About Tenable Network Security

Tenable, headquartered in Columbia, Md., USA, is the world leader in Unified Security Monitoring. Tenable provides agent-less solutions for continuous monitoring of vulnerabilities, configurations, data leakage, log analysis and compromise detection. For more information, please visit us at http://www.tenablesecurity.com/.

TENABLE Network Security, Inc.
7063 Columbia Gateway Drive
Suite 100
Columbia, MD 21046
TEL: 1-877-448-0489
http://www.tenablesecurity.com/