Tenable Core for Tenable.io Web Application Scanning User Guide

Last Updated: March 09, 2018

Table of Contents

Welcome to Tenable Core for Web Application Scanning

The Tenable Virtual Appliance is now known as Tenable Core. The reason for this change is the implementation of a new base operating system. This new model streamlines and simplifies deployment by creating a build for each Tenable on-premises application. Tenable Core is a deployment architecture that shortens time to first scan using a secure and stable platform.

Features

- Built upon CentOS 7 and hardened by targeting the CIS standards for RedHat 7 with SELinux Enabled.
- Provides automatic install and updates via Tenable Public Repositories.
- Consists of Tenable Core and a Tenable Application. These are independent of one other. The following builds are currently available.
    - Consists of Tenable Core and a Tenable Application. These are independent of one other. The following builds are currently available.
        - Tenable Core + Web Application Scanning
        - Tenable Core + Nessus
        - Tenable Core + Nessus Network Monitor
    - Root access is now enabled to Tenable Core builds
- Root access is now enabled to Tenable Core builds

See the following list for additional information about CIS standards adopted:

- **SELinux:** SELinux is enabled by default on this image
- **CIS Benchmarks:** Tenable has implemented the following parts of the CIS Level 1 Benchmark on the Tenable Core:

CIS Level 1 - 1.x

- CIS 1.1.1.* (Disable mounting of miscellaneous filesystems)
- CIS 1.1.21 (Ensure sticky bit is set on all world-writable directories)

- CIS 1.4.* (Bootloader adjustments)
  - CIS 1.4.1 Ensure permissions on bootloader config are configured
  - CIS 1.4.2 Ensure bootloader password is set - set superusers
- CIS 1.7.1.* (Messaging/banners)
  - Ensure message of the day is configured properly
  - Ensure local login warning banner is configured properly
  - Ensure remote login warning banner is configured properly
  - Ensure GDM login banner is configured - banner message enabled
  - Ensure GDM login banner is configured - banner message text

CIS Level 1 - 2.x

- CIS 2.2.* (disabled packages)
  - x11
  - avahi-server
  - CUPS
  - nfs
  - Rpc

CIS level 1 - 3.x

- CIS 3.1.* (packet redirects)
  - 3.1.2 Ensure packet redirect sending is disabled - 'net.ipv4.conf.all.send_redirects = 0'
  - 3.1.2 Ensure packet redirect sending is disabled - 'net.ipv4.conf.default.send_redirects = 0'
- CIS 3.2.* (ipv4, icmp, etc)
  - 3.2.1 Ensure source routed packets are not accepted - 'net.ipv4.conf.all.accept_source_route = 0'
  - 3.2.1 Ensure source routed packets are not accepted - 'net.ipv4.conf.default.accept_source_route = 0'
  - 3.2.2 Ensure ICMP redirects are not accepted - 'net.ipv4.conf.all.accept_redirects = 0'

        - 3.2.2 Ensure ICMP redirects are not accepted - 'net.ipv4.conf.default.accept_redirects = 0'
        - 3.2.3 Ensure secure ICMP redirects are not accepted - 'net.ipv4.conf.all.secure_redirects = 0'
        - 3.2.3 Ensure secure ICMP redirects are not accepted - 'net.ipv4.conf.default.secure_redirects = 0'
        - 3.2.4 Ensure suspicious packets are logged - 'net.ipv4.conf.all.log_martians = 1'
        - 3.2.4 Ensure suspicious packets are logged - 'net.ipv4.conf.default.log_martians = 1'
        - 3.2.5 Ensure broadcast ICMP requests are ignored
        - 3.2.6 Ensure bogus ICMP responses are ignored
        - 3.2.7 Ensure Reverse Path Filtering is enabled - 'net.ipv4.conf.all.rp_filter = 1'
        - 3.2.7 Ensure Reverse Path Filtering is enabled - 'net.ipv4.conf.default.rp_filter = 1'
        - 3.2.8 Ensure TCP SYN Cookies is enabled
    - CIS 3.3.* (IPv6)
        - 3.3.1 Ensure IPv6 router advertisements are not accepted
        - 3.3.2 Ensure IPv6 redirects are not accepted
    - CIS 3.4.* (tcp)
        - 3.4.1 Ensure TCP Wrappers is installed
    - CIS 3.5.* (network protocols)
        - 3.5.1 Ensure DCCP is disabled
        - 3.5.2 Ensure SCTP is disabled
        - 3.5.3 Ensure RDS is disabled
        - 3.5.4 Ensure TIPC is disabled

CIS Level 1 - 4.x

- CIS 4.2.* (rsyslog)
    - 4.2.1.3 Ensure rsyslog default file permissions configured
    - 4.2.1.4 Ensure rsyslog is configured to send logs to a remote log host

> **Note:** 4.2.1.4 requires knowing the address of the central log host, thus not easily done in the kickstart.

- 4.2.4 Ensure permissions on all logfiles are configured

CIS Level 1 - 5.x

- CIS 5.1.* (cron permissions)
  - 5.1.2 Ensure permissions on /etc/crontab are configured
  - 5.1.3 Ensure permissions on /etc/cron.hourly are configured
  - 5.1.4 Ensure permissions on /etc/cron.daily are configured
  - 5.1.5 Ensure permissions on /etc/cron.weekly are configured
  - 5.1.6 Ensure permissions on /etc/cron.monthly are configured
  - 5.1.7 Ensure permissions on /etc/cron.d are configured
  - 5.1.8 Ensure at/cron is restricted to authorized users - at.allow
  - 5.1.8 Ensure at/cron is restricted to authorized users - at.deny
  - 5.1.8 Ensure at/cron is restricted to authorized users - cron.allow
  - 5.1.8 Ensure at/cron is restricted to authorized users - cron.deny
- CIS 5.2.11 (Turn off Weak Ciphers for SSH)
- CIS 5.3.* (password/pam)
  - 5.3.1 Ensure password creation requirements are configured - dcredit
  - 5.3.1 Ensure password creation requirements are configured - lcredit
  - 5.3.1 Ensure password creation requirements are configured - minlen
  - 5.3.1 Ensure password creation requirements are configured - ocredit
  - 5.3.1 Ensure password creation requirements are configured - ucredit
  - 5.3.2 Lockout for failed password attempts - password-auth 'auth [default=die] pam_faillock.so authfail audit deny=5 unlock_time=900'
  - 5.3.2 Lockout for failed password attempts - password-auth 'auth [success=1 default=bad] pam_unix.so'

- 5.3.2 Lockout for failed password attempts - password-auth 'auth required pam_faillock.so preauth audit silent deny=5 unlock_time=900'
- 5.3.2 Lockout for failed password attempts - password-auth 'auth sufficient pam_faillock.so authsucc audit deny=5 unlock_time=900'
- 5.3.2 Lockout for failed password attempts - system-auth 'auth [default=die] pam_faillock.so authfail audit deny=5 unlock_time=900'
- 5.3.2 Lockout for failed password attempts - system-auth 'auth [success=1 default=bad] pam_unix.so'
- 5.3.2 Lockout for failed password attempts - system-auth 'auth required pam_faillock.so preauth audit silent deny=5 unlock_time=900'
- 5.3.2 Lockout for failed password attempts - system-auth 'auth sufficient pam_faillock.so authsucc audit deny=5 unlock_time=900'
- 5.3.3 Ensure password reuse is limited - password-auth
- 5.3.3 Ensure password reuse is limited - system-auth

- CIS 5.4.* (user prefs)
  - 5.4.1.2 Ensure minimum days between password changes is 7 or more
  - 5.4.1.4 Ensure inactive password lock is 30 days or less
  - 5.4.4 Ensure default user umask is 027 or more restrictive - /etc/bashrc
- CIS 5.6.* (wheel group)
  - 5.6 Ensure access to the su command is restricted - pam_wheel.so
  - 5.6 Ensure access to the su command is restricted - wheel group contains root

CIS Level 1 - 6.x

- CIS 6.1.* (misc conf permissions)
  - 6.1.6 Ensure permissions on /etc/passwd- are configured
  - 6.1.8 Ensure permissions on /etc/group- are configured

Web Application Scanning Virtual Image Installation

Reference the following sections to begin the deployment model.

Install the VM Image

Install OVA

Other Configuration Methods

Manual setup

Configuration of static IP addresses

Create a New Account

Create a new account

Connect to the Web Application Scanner

Connect to the Web Application Scanner

Install OVA

The Tenable VM is available for VMware Server, VMware Player, VMware ESX, VMware Workstation, and VMware Fusion (http://vmware.com/) and can be downloaded from the Tenable Downloads Page.

The Tenable Core VMware image for VMware Server, VMware Fusion, VMware Workstation, VMware ESX server, and VMware Player is provided as an **.ova** file with the OS and applications in a 64-bit version.

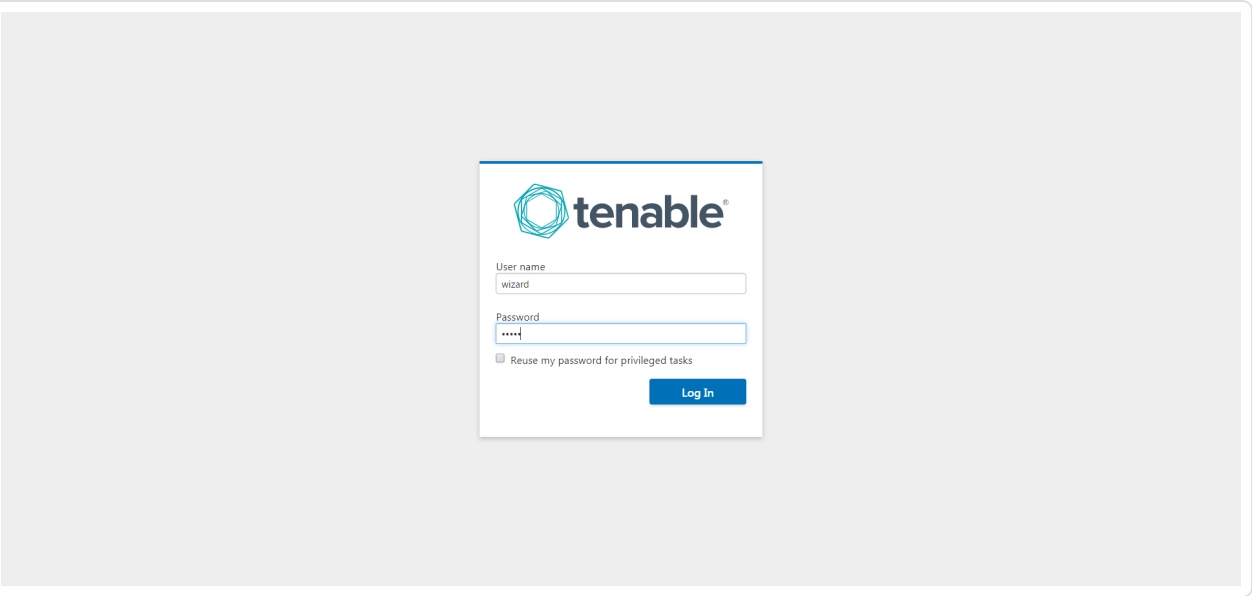
> **Note:** An internet connection is required for updates and upgrades.

Use the following steps to install the VMware.

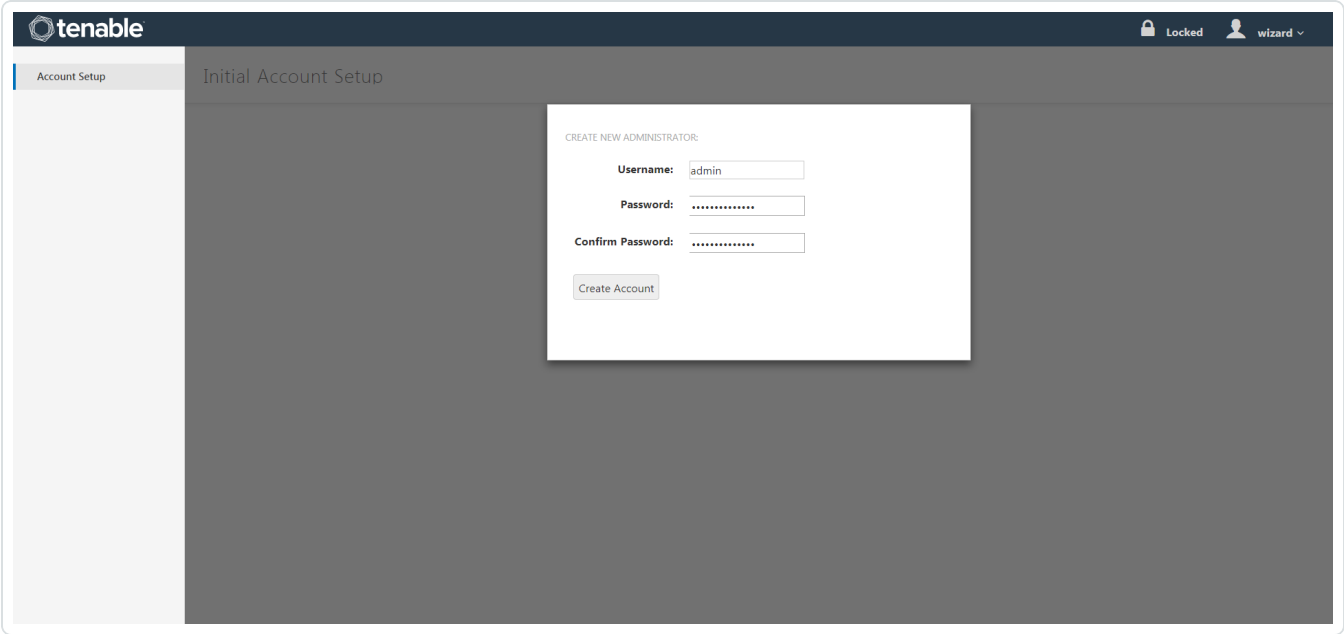
1. Download the OVA from tenable.com/downloads.
2. Launch the VMware program and import the **.ova** file that was downloaded.
3. Adjust the default VM settings as needed for the local environment.
4. The boot process will be displayed in the VM console window when started. (It may take several minutes for the application services to start.)

Create a New Account

1. For the initial log in, administrative users must create an account.
2. The initial screen will request a login. Enter the following:
    - Username: wizard
    - Password: admin

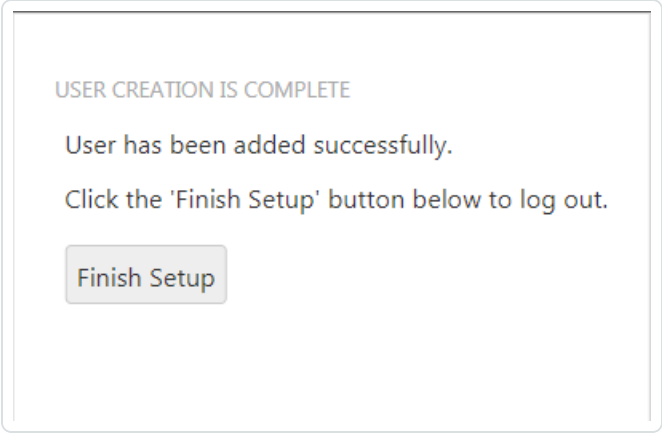


3. The **Initial Account Setup** screen will appear with a new window to create the new administrator. Enter the new user account information.

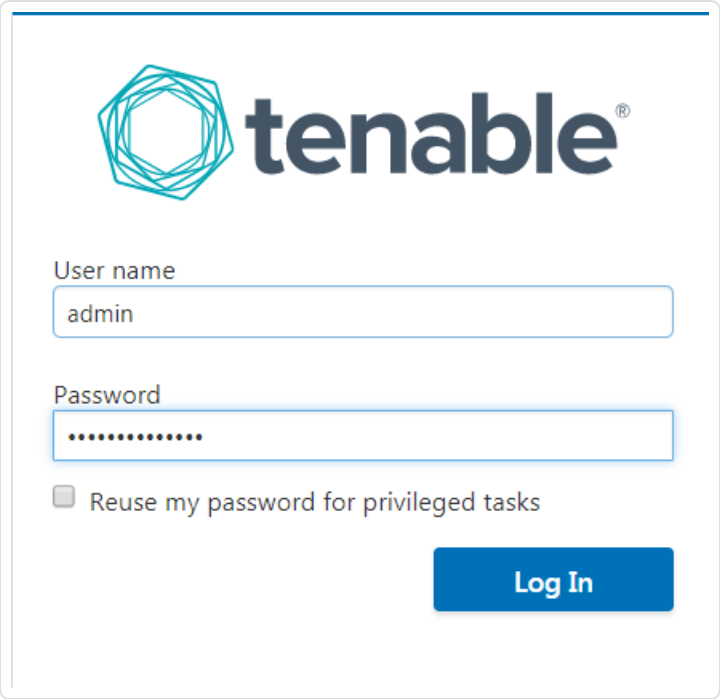


> **Note:** The password must contain at least one capital letter, one numeric character, one non-alphanumeric character, and must be at least 14 characters long.

5. A confirmation message will display. Click **Finish Setup** to complete the new account creation and log out.



6. Click the Create Account button. A new screen with a new log in window will appear.

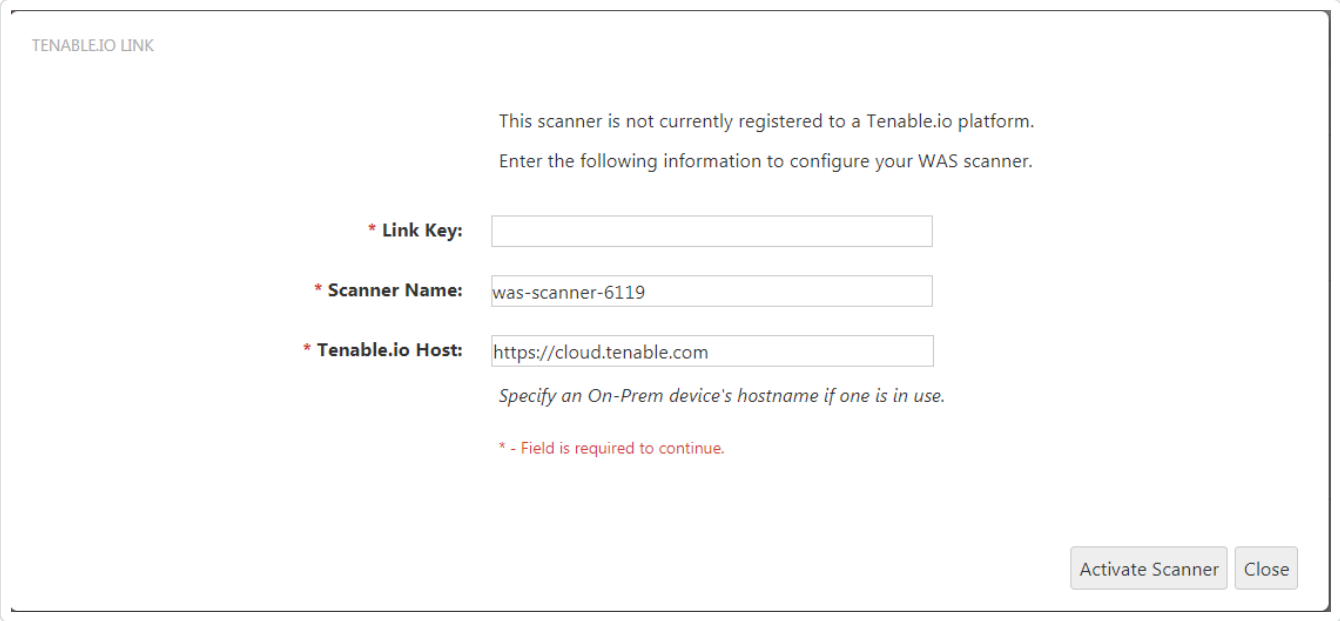


7. Enter the newly created account information to log in to the system.

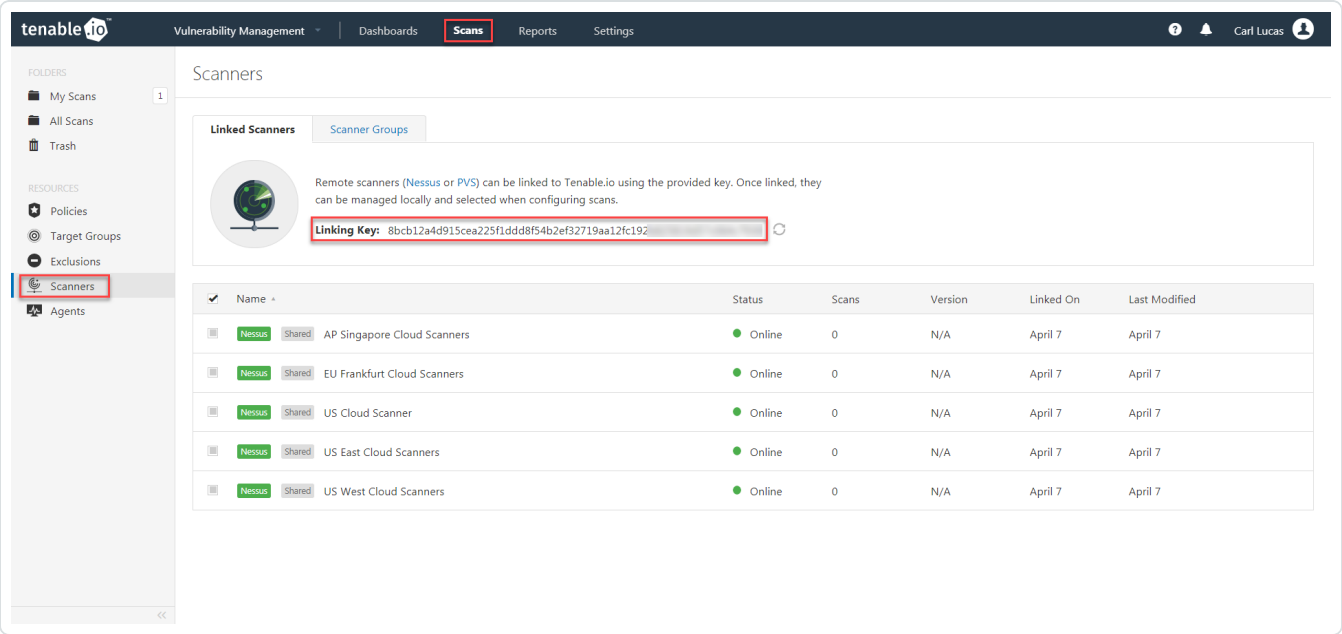
Caution: Select the **Reuse my password for privileged tasks** option at the bottom of the log in screen to ensure access to all of the root administrative tasks. If this is not selected, some root tasks will not work.

Web Application Scanner Configuration

1. After the initial login, the following window will appear.

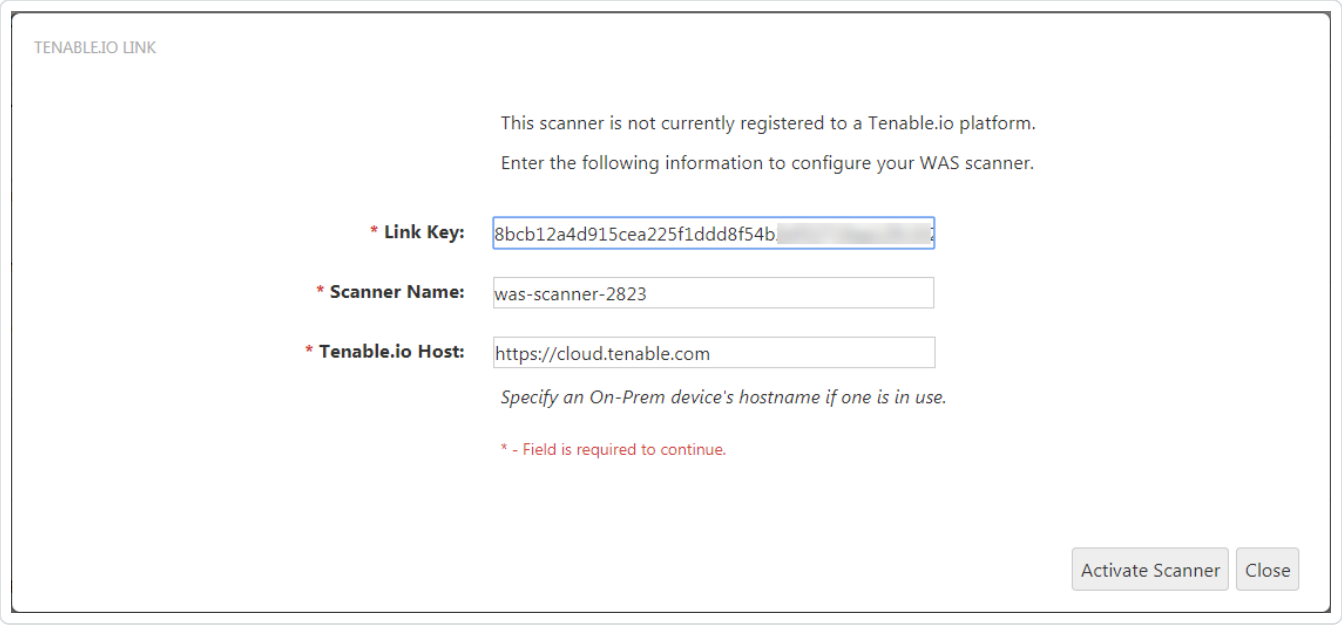


2. The link required for the activation must be retrieved from Tenable.io™.
3. Log in to your Tenable.io™ account.
4. Click the **Scans** option in the top navigation bar.
5. Next, click the **Scanners** option in the left navigation pane.
6. The linking key is displayed in the linked scanners section at the top of the screen.

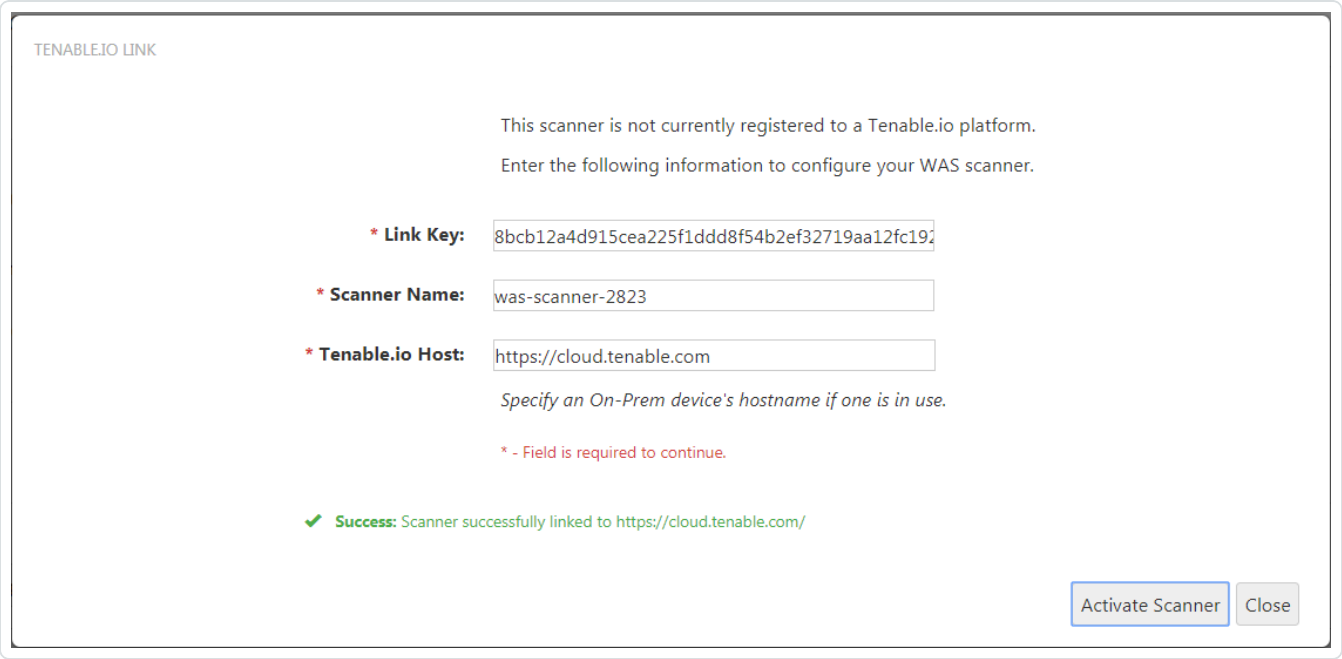


7. Highlight and copy the linking key.

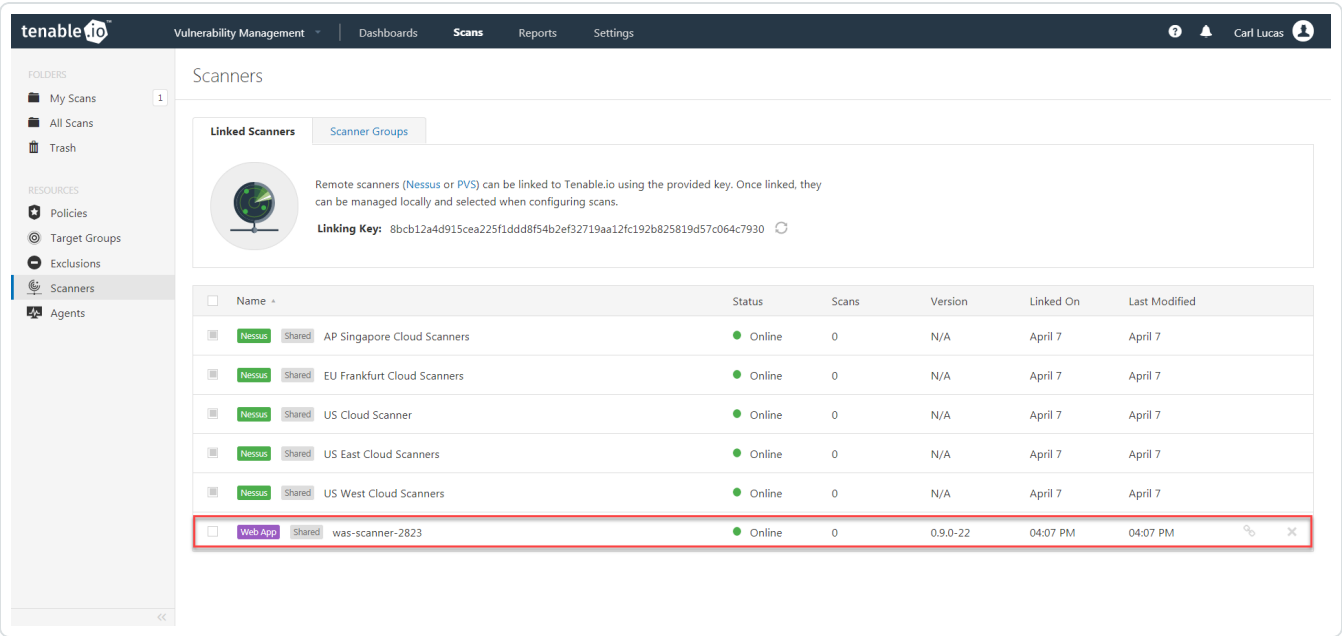
8. Go back to the configuration page and paste the link into the **Link Key** section.



9. Click the **Activate Scanner** button. A success message will appear at the bottom of the screen confirming the systems have been linked.



10. The newly added scanner will be displayed in the Tenable.io™ scanner list.



Manual Setup

For users that want to automate VM deployment using tools like Ansible, Puppet, Chef, etc., use the following scripts to complete the process manually.

1. Run the /usr/libexec/tenablecore/wizard/wizardadduser.sh shell script.
2. Provide two lines of input on standard input.
3. The first line is the username.
4. The second line is the password.

Example

```
$ pkexec /usr/libexec/tenablecore/wizard/wizardadduser.sh <<'EOF'
newadmin
suP3rsaF3p4ssw()rd
EOF
```

or

```
$ pkexec /usr/libexec/tenablecore/wizard/wizardadduser.sh
newadmin
suP3rsaF3p4ssw()rd
```

5. Logout of the wizard account/session.

Configure Static IP Addresses

Static IP addresses can only be configured after creating an admin user and configuring a DHCP connection.

> **Note:** Make sure `Wired connection 1` is selected.

> **Note:** An alternative connection can be made by going to the connection list and modifying it.

Device List

Enter the following to view the current device list.

```
$ nmcli device status
DEVICE TYPE STATE CONNECTION
ens160 ethernet connected Wired connection 1
lo loopback unmanaged --
```

> **Note:** Make sure Wired connection 1 is selected from the list of available connections.

> **Note:** The value in the DEVICE column.

Add Connection

Enter the following to fetch the connection associated with that device.

```
$ conn=$(nmcli -g general.connection device show ens160)
$ echo "$conn"
```

Static Connection

Enter the following to configure a static connection.

```
$ nmcli connection modify "$conn" connection.autoconnect yes ipv4.method
manual ipv4.addr "10.0.0.1/24" ipv4.dns "10.0.1.1, 10.0.1.2" ipv4.gateway
"10.0.0.254"
```

Restart or Reboot the Connection

Enter the following to restart.

```
$ nmcli connection down "$conn" && nmcli connection up "$conn"
```

or

Enter one of the following to reboot.

```
$ systemctl reboot
```

```
$ shutdown -r now
```

```
$ reboot
```

System Layout

The system pages are located in two sections. The Dashboard option is located in the top horizontal menu listing while the other features are listed in the left navigation pane.

- Dashboard
- System
- System Log
- Networking
- Storage
- Accounts
- Services
- Diagnostic Reports
- Terminal
- Update Management
- Software Updates

Dashboard

The **Dashboard** displays a list of systems running on the server. The graph provides information for CPU usage, memory usage, disk I/O, and network traffic. Click on the options above the graph to view the corresponding data.

A list of servers are displayed beneath the graph.

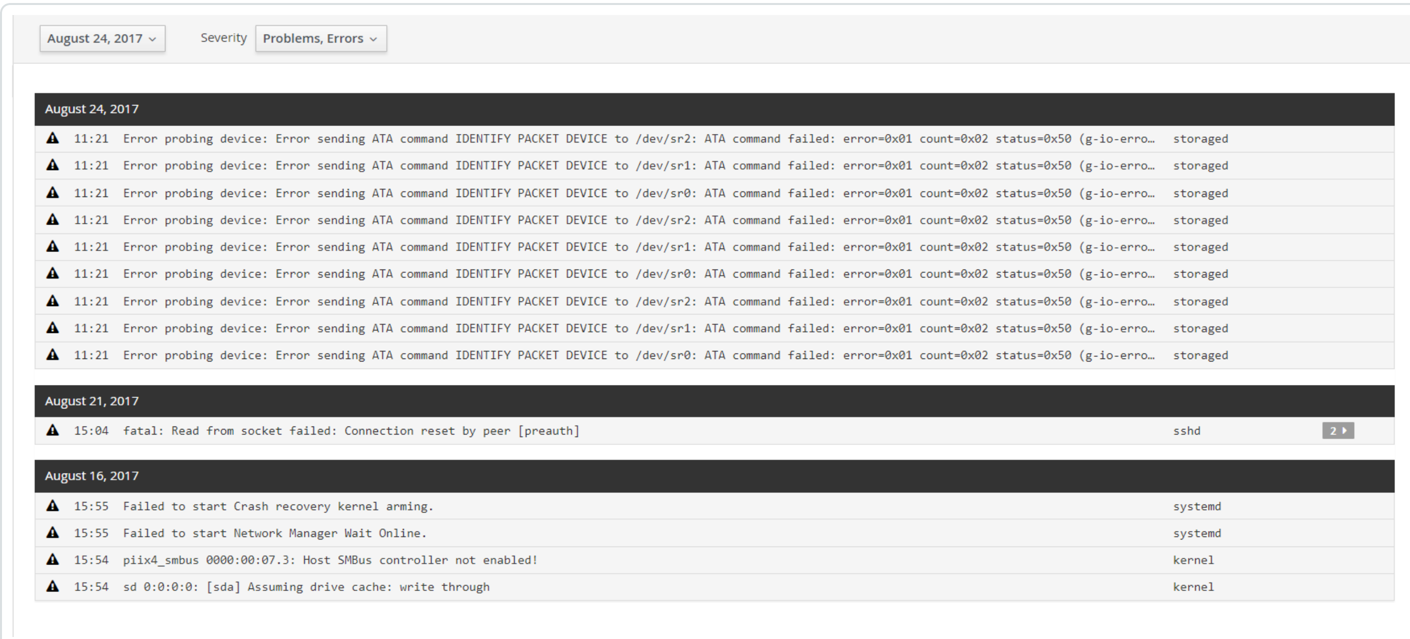
System

The **System** page provides information and graphs about the system on which the machine is running. Graphs provide information for the CPU usage, memory usage, disk I/O, and network traffic. In addition, information for hardware and operating system details are displayed.

Users can view machine SSH fingerprints, view and change the machine host name, time and time zone, restart or shutdown the system, or change the performance profile.

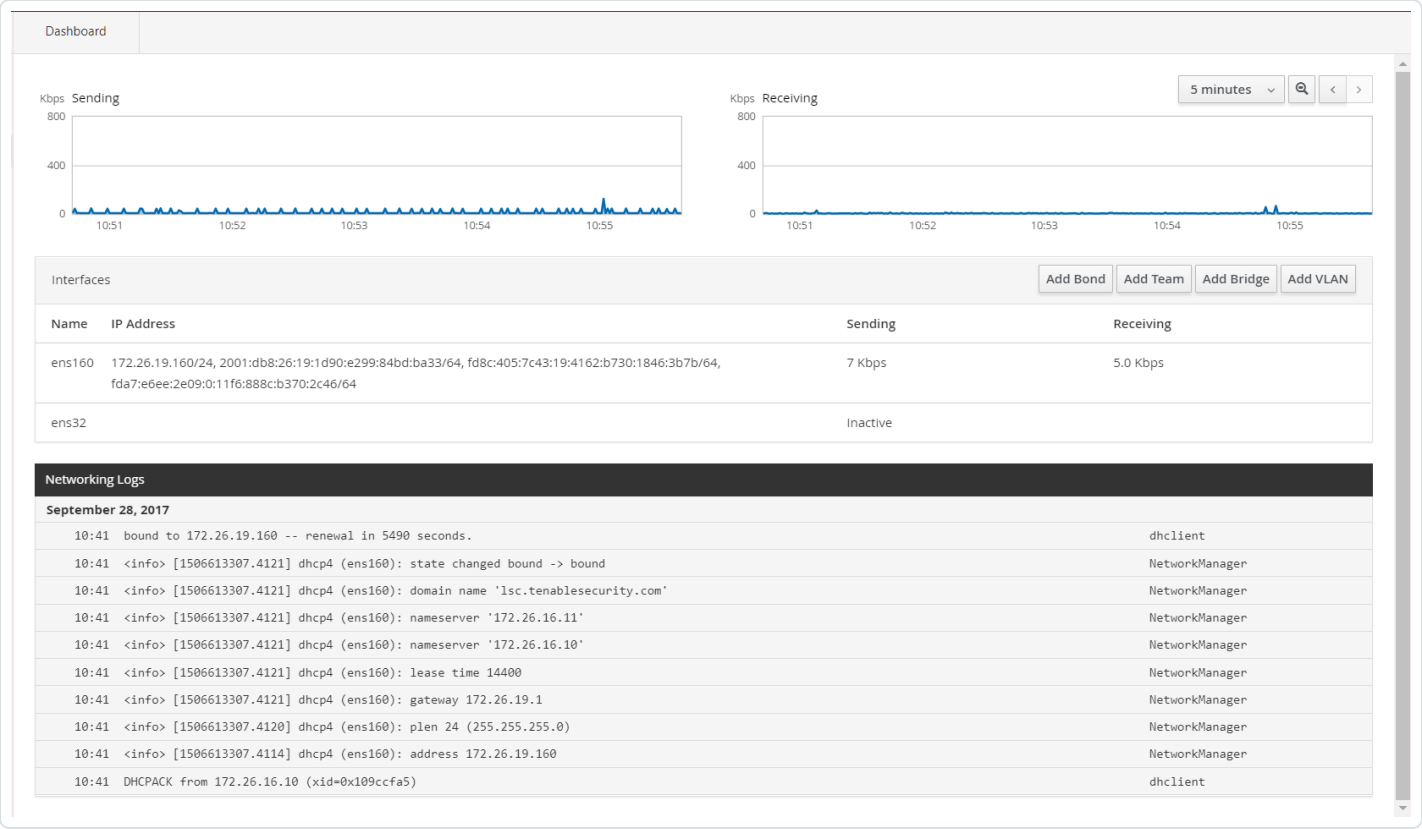
System Log

View the **System Log** when errors are encountered in the system. The **System Log** lists, categorizes, and stores system issues that have occurred within the last seven days. Click on an individual entry (row) to get additional information.



Networking

The **Networking** page provides real-time system sending/receiving information, interface connection options, and logs. The **Interfaces** section provides options for Add Bond, Add Bridge, Add Team, and Add VLAN. The **Add Bond** option provides a method for aggregating multiple network interfaces into a single bonded interface. Configure team settings with the **Add Team** option. Use the **Add Bridge** feature to create a single aggregate network from multiple communication networks. The **Networking Logs** section provides a daily log of activity for the system network.



Storage

The **Storage** section provides real-time reading/writing graphs, **File Systems** information, and **Storage logs**. The **File Systems** section lists each item noting the name, mount point, and size. Additional details can be viewed by clicking on individual file systems (rows). The detailed view provides information for capacity, logical volumes, and correlating file storage logs. The file system name can be updated on the details page. In addition, single file systems can be deleted.

Accounts

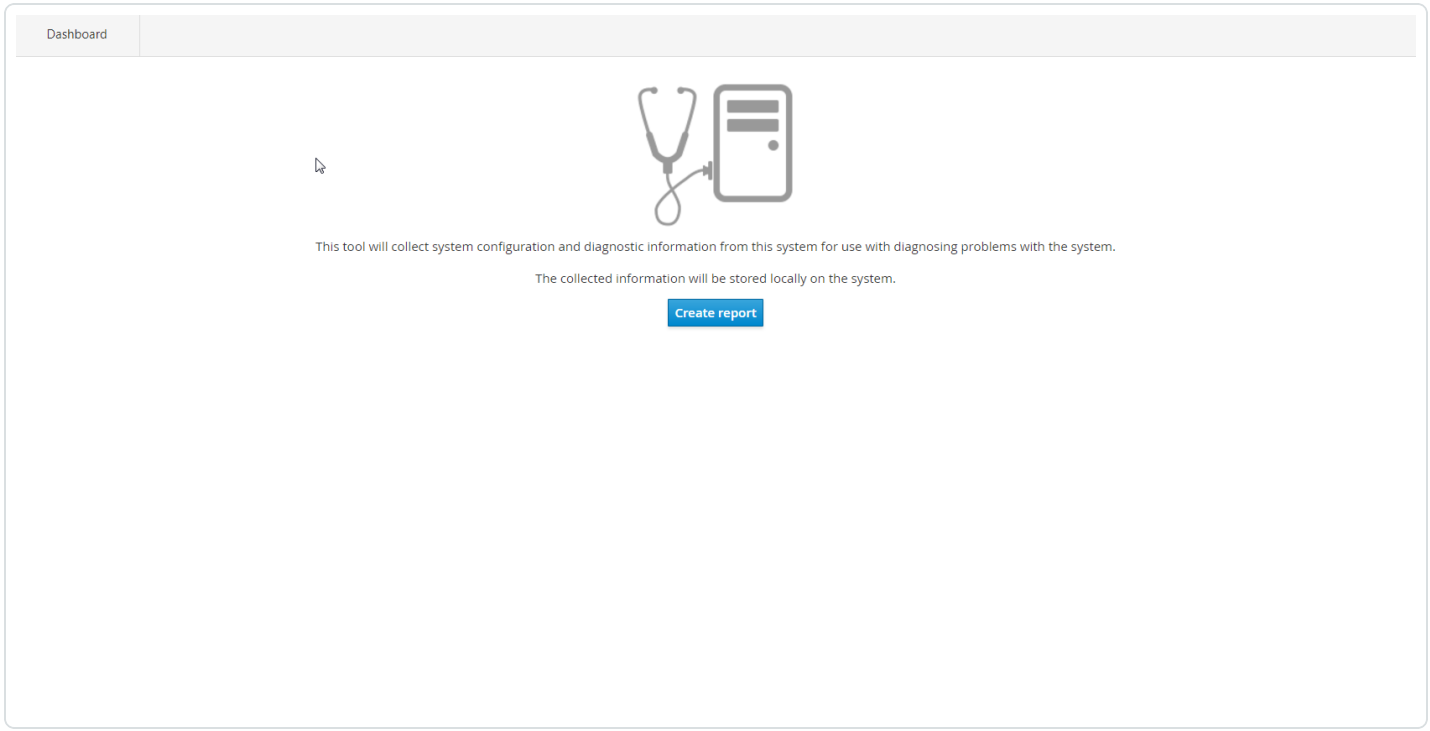
New and existing users are managed through the **Accounts** section. User accounts are displayed in cards on the main screen. Click on the user card to display the user's information. User information can also be edited within the user information box.

Services

The Services page provides detailed information for Targets, System Services, Sockets, Timers, and Paths.

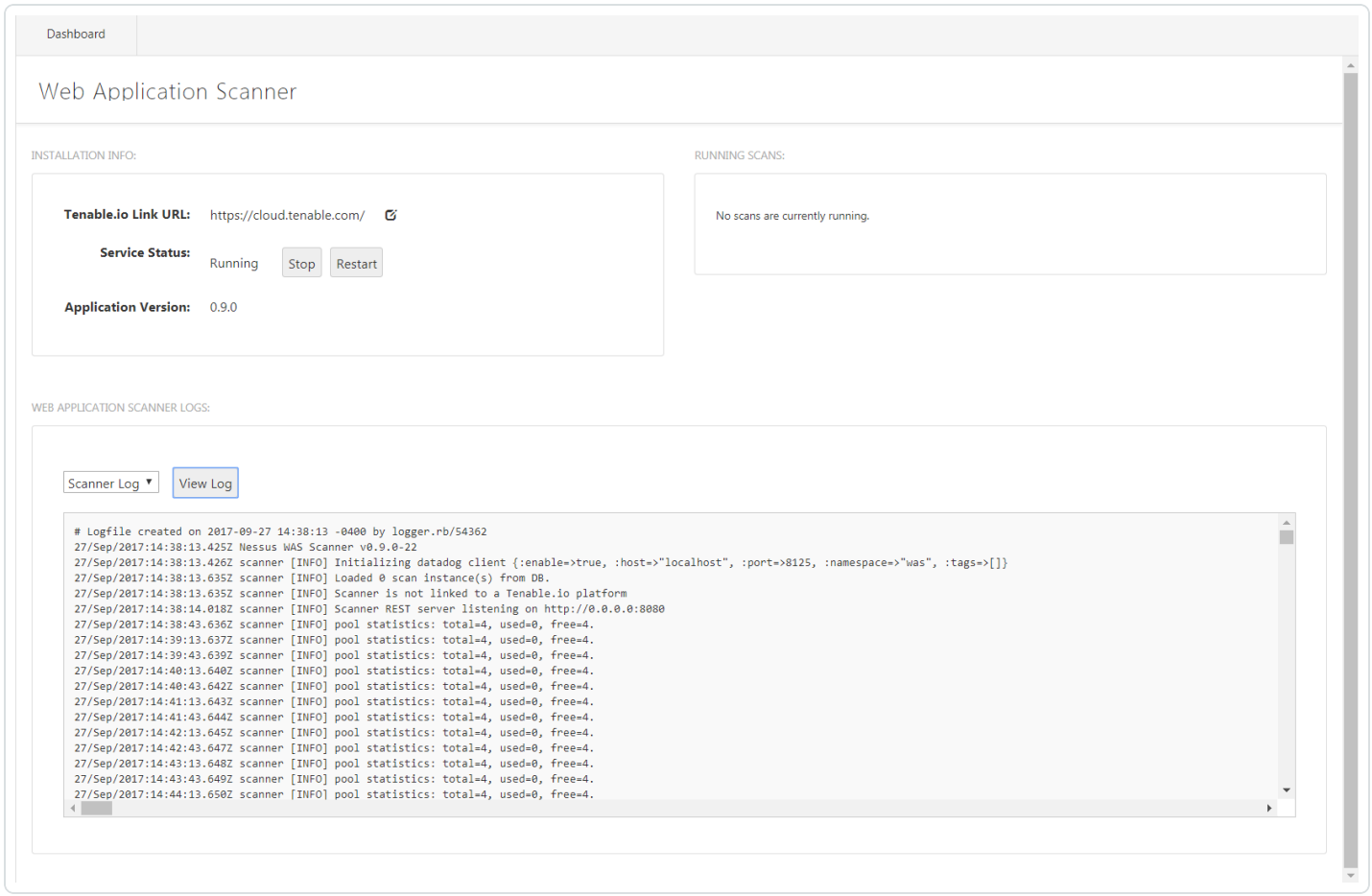
Diagnostic Reports

Diagnostic Reports are helpful when issues are encountered. The **Diagnostic Report** can aid in troubleshooting the problem. If your support team or Tenable support requests a diagnostic report, click on the **Diagnostic Report** option in the left navigation pane. The **Reports** page will appear in the main window.



Web Application Scanner

The Web Application Scanner provides information for different management features. The page is divided into three sections: **Installation Info**, **Running Scans**, and **Web Application Scanner Logs**.



Installation Info

The **Installation Info** section contains information for the **Tenable.io URL**, **Service Status**, and **Version Number**. The system can be stopped, started, and restarted in this section.

Running Scans

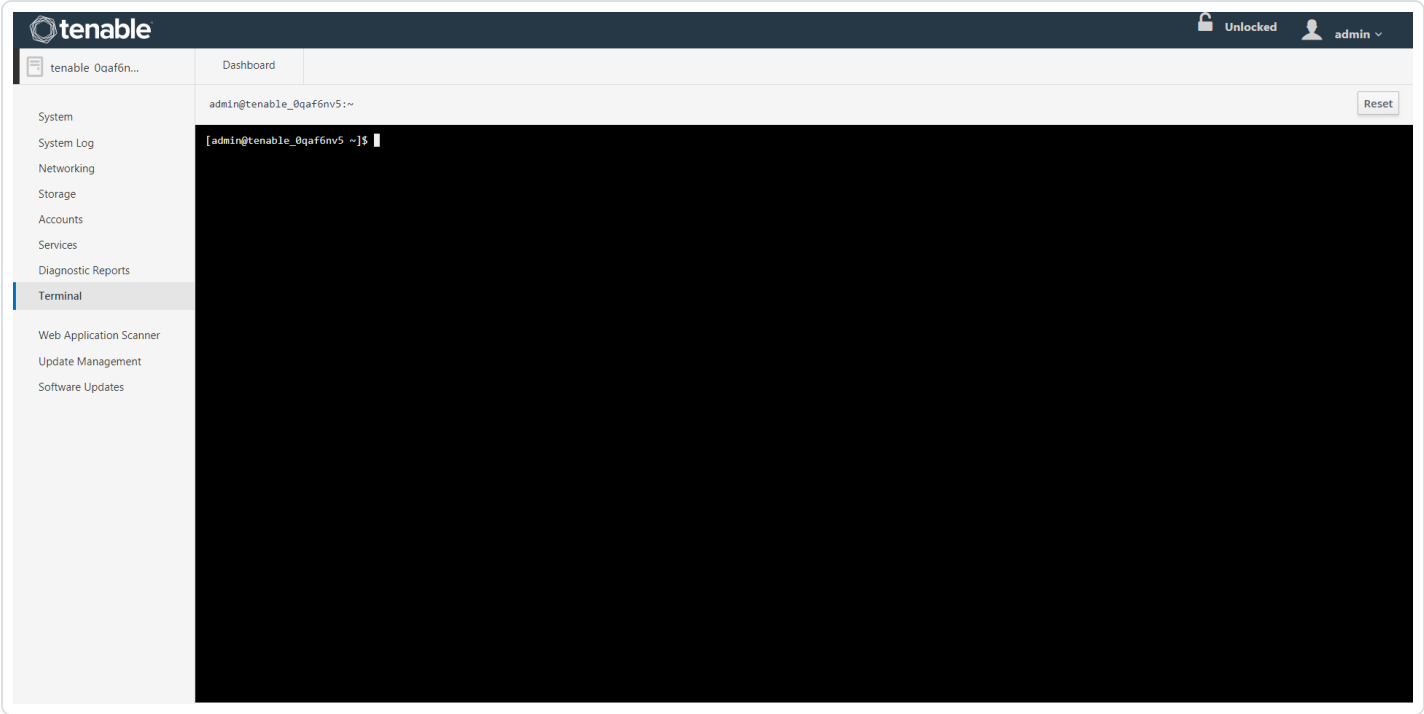
The **Running Scans** section provides information for scans that are currently running in the Web Application Scanner. Currently running scans can be canceled in this section by checking the box adjacent to the scan and clicking the **Cancel Selected Scan(s)** button.

Web Application Scanner Logs

The **Web Application Scanner Logs** section provides a log of the scans that have run on the scanner. Click the **View Log** button to display the **Web Application Scanner Logs**.

Terminal

The Terminal option provides a console for user specific command line interface.



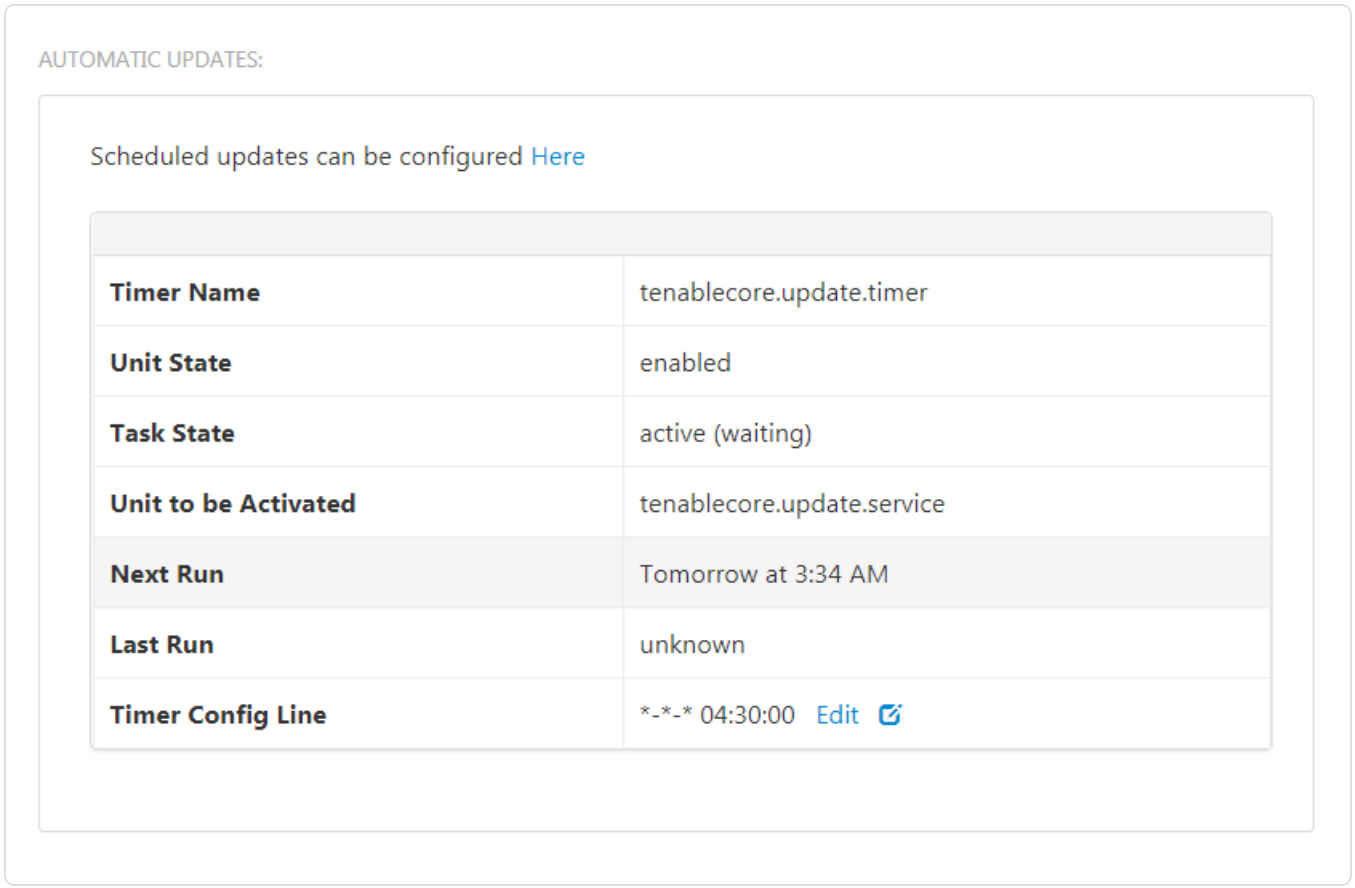
Update Management

The **Update Management** section is divided into two sections: **Automatic Updates** and **Proxy Configuration**. Updates are also supported for air gapped application updates. See the Offline ISO Installation section for air gapped application update information.

Automatic Updates

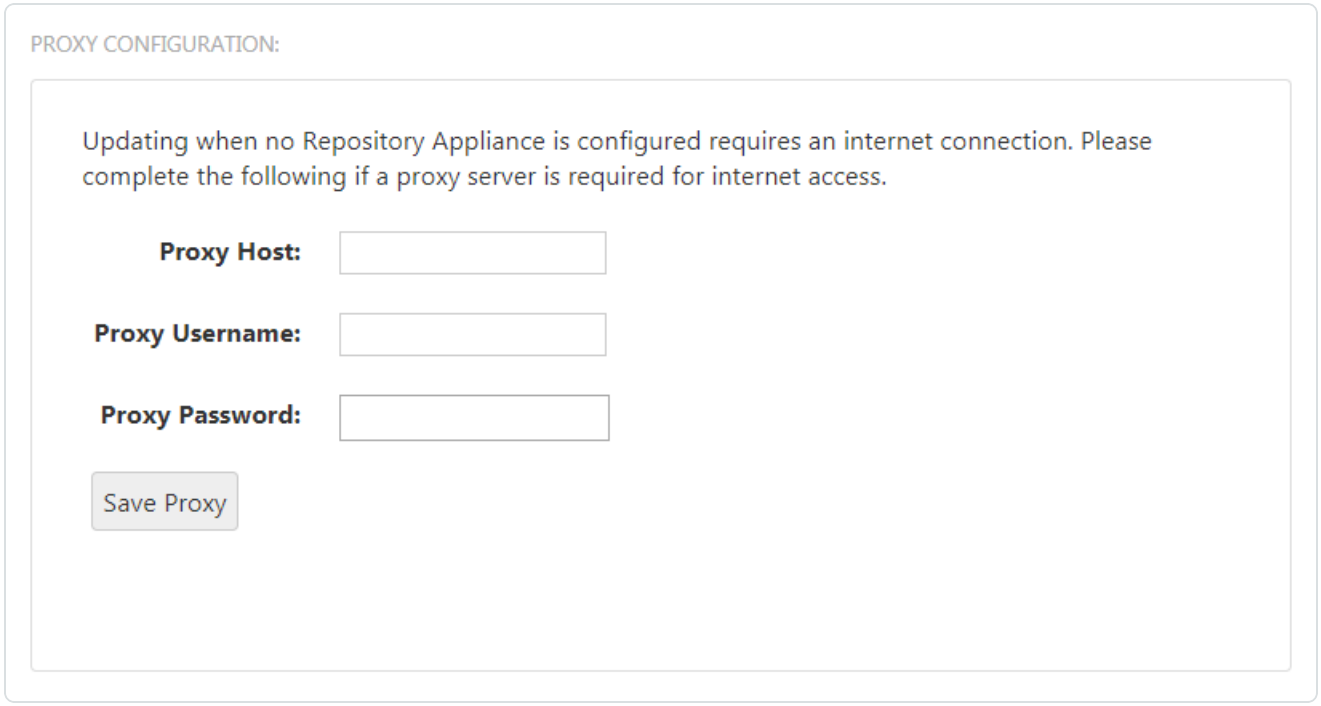
The **Automatic Updates** section provides information for scheduled updates. Updates can be modified by clicking the word **Here** in the statement above the listed information. Clicking the word **Here** will take you to the **Services** page. The **Services** page contains options for configuring automatic updates. The **Automatic Updates** runs a full system update. Reboot the system after the updates are installed.

Note: Additional updates will be needed for systems using On-Prem. Click here to view the required steps.



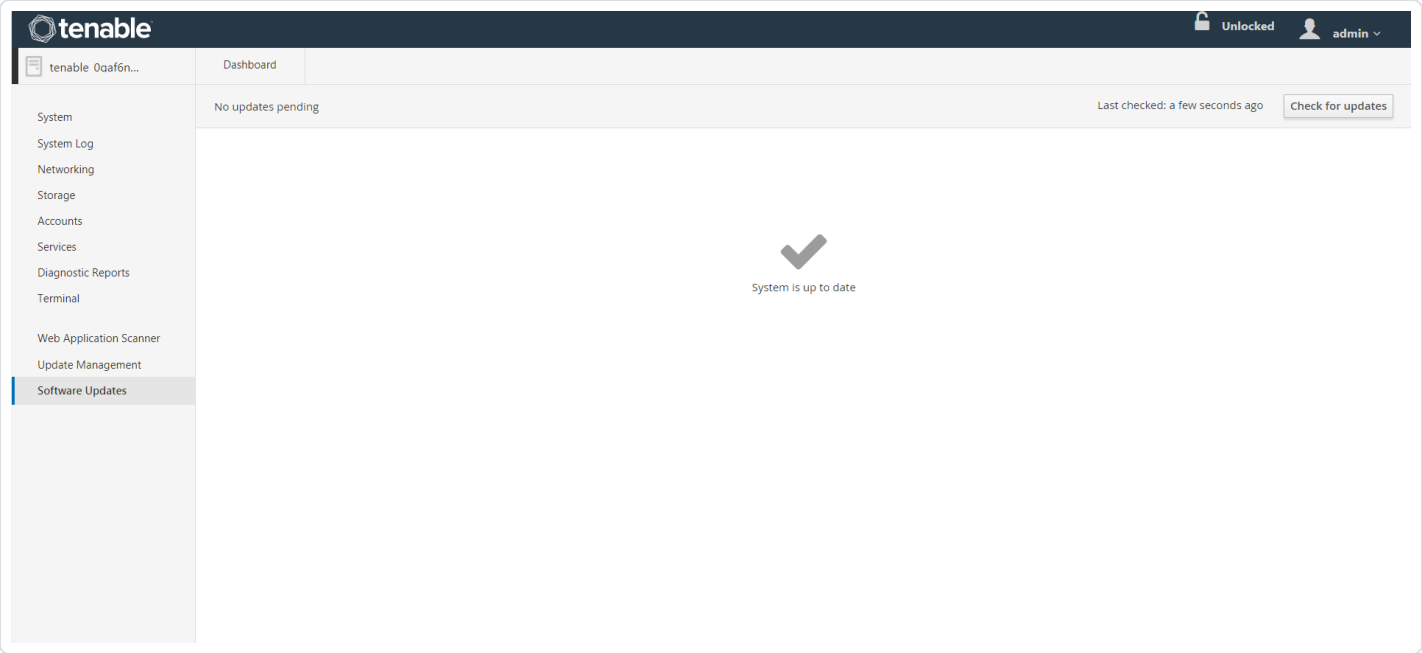
Proxy Configuration

The Proxy Configuration section provides the option for configuring a proxy server if a proxy server is needed for internet access. Enter the proxy information and click the **Save Proxy** button to complete the configuration.



Software Updates

The **Software Updates** page provides information for necessary system updates. Click the **Check for Updates** button to scan the system for uninstalled updates.



If updates are found, an **Install all updates** button will appear at the top of the page. Click the button to install the updates.