# Table of Contents

Welcome to Tenable Core + Tenable.io Web Application Scanning .............................................................. 6
Get Started .................................................................................................................................................. 7
Tenable Core Requirements ...................................................................................................................... 9
   System Requirements ............................................................................................................................... 10
   Access Requirements ............................................................................................................................... 12
   Default Security Configuration Standards ............................................................................................. 14
Deploy or Install Tenable Core .................................................................................................................. 19
   Deploy Tenable Core in VMware ............................................................................................................ 20
   Deploy Tenable Core in Hyper-V ............................................................................................................ 22
   Deploy Tenable Core in Microsoft Azure ................................................................................................ 24
   Deploy Tenable Core in Microsoft Azure via the Portal ......................................................................... 25
   Deploy Tenable Core in Microsoft Azure via the CLI ............................................................................ 27
Install Tenable Core on Hardware ............................................................................................................ 29
   Edit the Network Configuration ............................................................................................................ 31
   Edit the Proxy Configuration .................................................................................................................. 33
Disk Management ........................................................................................................................................ 35
   Add or Expand Disk Space ....................................................................................................................... 36
Manually Configure a Static IP Address .................................................................................................... 38
Create an Initial Administrator User Account ......................................................................................... 42
Create a Password for the Initial Administrator User Account ................................................................. 44
Link Tenable Core to Tenable.io ............................................................................................................... 46
Log In to Tenable Core .............................................................................................................................. 47
<table>
<thead>
<tr>
<th>Configure and Manage</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>View the Dashboard</td>
<td>51</td>
</tr>
<tr>
<td>Add a Server</td>
<td>52</td>
</tr>
<tr>
<td>Edit a Server</td>
<td>53</td>
</tr>
<tr>
<td>Delete a Server</td>
<td>54</td>
</tr>
<tr>
<td>Synchronize Accounts</td>
<td>55</td>
</tr>
<tr>
<td>Manage the System</td>
<td>56</td>
</tr>
<tr>
<td>Change Performance Profile</td>
<td>58</td>
</tr>
<tr>
<td>Restart Tenable Core</td>
<td>59</td>
</tr>
<tr>
<td>Shut Down Tenable Core</td>
<td>60</td>
</tr>
<tr>
<td>Edit Your Tenable Core Hostname</td>
<td>61</td>
</tr>
<tr>
<td>Edit Your Time Settings</td>
<td>62</td>
</tr>
<tr>
<td>View the System Log</td>
<td>63</td>
</tr>
<tr>
<td>Filter the System Log</td>
<td>64</td>
</tr>
<tr>
<td>Manage System Networking</td>
<td>65</td>
</tr>
<tr>
<td>Add a Bonded Interface</td>
<td>67</td>
</tr>
<tr>
<td>Add a Team of Interfaces</td>
<td>69</td>
</tr>
<tr>
<td>Add a Bridge Network</td>
<td>70</td>
</tr>
<tr>
<td>Add a VLAN</td>
<td>71</td>
</tr>
<tr>
<td>Manage System Storage</td>
<td>72</td>
</tr>
<tr>
<td>Rename a Filesystem</td>
<td>73</td>
</tr>
<tr>
<td>Delete a Filesystem</td>
<td>74</td>
</tr>
<tr>
<td>Manage User Accounts</td>
<td>75</td>
</tr>
<tr>
<td>Create New User Account</td>
<td>76</td>
</tr>
<tr>
<td>Topic</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Edit a User Account</td>
<td>77</td>
</tr>
<tr>
<td>Delete a User Account</td>
<td>81</td>
</tr>
<tr>
<td>Manage Services</td>
<td>82</td>
</tr>
<tr>
<td>Create a Timer</td>
<td>85</td>
</tr>
<tr>
<td>Generate a Diagnostic Report</td>
<td>86</td>
</tr>
<tr>
<td>Access the Terminal</td>
<td>87</td>
</tr>
<tr>
<td>Manage Tenable.io Web Application Scanning in Tenable Core</td>
<td>88</td>
</tr>
<tr>
<td>Configure a Proxy Server</td>
<td>90</td>
</tr>
<tr>
<td>Start, Stop, or Restart Your Application</td>
<td>91</td>
</tr>
<tr>
<td>Manage Updates</td>
<td>92</td>
</tr>
<tr>
<td>Configure Automatic Updates</td>
<td>93</td>
</tr>
<tr>
<td>Configure Your Automatic Update Schedule</td>
<td>95</td>
</tr>
<tr>
<td>Update On Demand</td>
<td>96</td>
</tr>
<tr>
<td>Update Tenable Core Offline</td>
<td>98</td>
</tr>
<tr>
<td>Manage Certificates</td>
<td>99</td>
</tr>
<tr>
<td>Manage the Server Certificate</td>
<td>100</td>
</tr>
<tr>
<td>Upload a Custom Server Certificate</td>
<td>101</td>
</tr>
<tr>
<td>Remove a Custom Server Certificate</td>
<td>104</td>
</tr>
<tr>
<td>Upload a Certificate for a Trusted Certificate Authority</td>
<td>105</td>
</tr>
<tr>
<td>Use Different Certificates for Tenable Core and Your Application</td>
<td>107</td>
</tr>
<tr>
<td>Application Data Backup and Restore</td>
<td>108</td>
</tr>
<tr>
<td>Configure a Remote Storage Host</td>
<td>110</td>
</tr>
<tr>
<td>Perform an On-Demand Backup</td>
<td>112</td>
</tr>
<tr>
<td>Change the Scheduled Backup Time</td>
<td>113</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Restore a Backup</td>
<td>115</td>
</tr>
<tr>
<td>SNMP Agent Configuration</td>
<td>117</td>
</tr>
<tr>
<td>Configure an SNMP Agent via the User Interface</td>
<td>118</td>
</tr>
<tr>
<td>Configure an SNMP Agent via the CLI</td>
<td>121</td>
</tr>
<tr>
<td>Take a Virtual Machine Snapshot</td>
<td>122</td>
</tr>
</tbody>
</table>
Welcome to Tenable Core + Tenable.io Web Application Scanning

You can use the Tenable Core operating system to run an instance of Tenable.io Web Application Scanner in your environment. After you deploy Tenable Core + Tenable.io Web Application Scanning, you can monitor and manage your Tenable.io Web Application Scanner processes through the secure Tenable Core platform.

To quickly get started with Tenable Core + Tenable.io Web Application Scanning, see Get Started.

Features

- Secure, stable platform that reduces the time to your first scan.
- Provides automatic application installation and updates via Tenable public repositories.
- Built on CentOS 7.
- Targets Center for Internet Security (CIS) standards for RedHat 7 with SELinux enabled. For more information, see Default Security Configuration Standards.
- Root access enabled on builds.

Other Tenable Core Configurations

To run a different Tenable application on Tenable Core, see:

- Tenable Core + Nessus
- Tenable Core + Nessus Network Monitor
- Tenable Core + Tenable.sc
- Tenable Core + Tenable.ot

Note: Tenable does not recommend deploying multiple applications on a single instance of Tenable Core. If you want to deploy several applications on Tenable Core (for example, Tenable.sc and Tenable.io Web Application Scanning), deploy a unique instance for each application.
Get Started

Tenable recommends the following sequence to deploy and get started with Tenable Core + Tenable.io Web Application Scanning.

To get started with Tenable Core:

1. Confirm that your environment meets the requirements in Tenable Core Requirements. If necessary, prepare to increase your disk space after you deploy.

2. **Deploy or install** Tenable Core + Tenable.io Web Application Scanning.

3. (Optional) If you want to increase your disk space to accommodate your organization's data storage needs, do one of the following:
   - If you are deploying Tenable Core + Tenable.io Web Application Scanning as a virtual machine or on hardware, see Disk Management.
   - If you are deploying Tenable Core + Tenable.io Web Application Scanning in a cloud environment, refer to your cloud platform's documentation for information about increasing disk space.

4. (Optional) If Dynamic Host Configuration Protocol (DHCP) is not available on the network where you deployed Tenable Core, configure an IP address for your Tenable Core + Tenable.io Web Application Scanning deployment.

5. (Optional) If necessary, log in as a wizard user and create an administrator account, as described in Create an Initial Administrator User Account.

   **Note:** You must create an administrator account if you deployed Tenable Core + Tenable.io Web Application Scanning via one of the following methods:
   - As a virtual machine
   - On hardware

   If you deployed Tenable Core + Tenable.io Web Application Scanning in a cloud environment and you did not create a password during deployment, you must create a password for your administrator account.

6. **Log In to Tenable Core** with your new administrator credentials.

7. (Optional) If you want to create more user accounts, see Create New User Account.
8. (Optional) If you want to configure Tenable Core to use a proxy server, see Configure a Proxy Server.

9. Configure WAS to meet the specifications you want for your application.

   For more information about configuring and operating Tenable.io Web Application Scanner, see the Tenable.io Web Application Scanning User Guide.

10. Configure and manage Tenable Core. To access the application interface, see Configure and Manage.
Tenable Core Requirements

You can deploy Tenable Core + Tenable.io Web Application Scanning on any system that meets the following Tenable Core and Tenable.io Web Application Scanner environment requirements.

**Note:** Tenable does not recommend deploying multiple applications on a single instance of Tenable Core. If you want to deploy several applications on Tenable Core (for example, Tenable.sc and Tenable.io Web Application Scanning), deploy a unique instance for each application.

System Requirements
Access Requirements
Default Security Configuration Standards
System Requirements

To install and run Tenable Core + Tenable.io Web Application Scanning, your system must meet the following hardware requirements established for Tenable.io Tenable.io Web Application Scanning. For more information about Tenable.io requirements, see Tenable.io in the General Requirements User Guide.

**Note:** Tenable Support does not assist with issues related to your CentOS 7 operating system, even if you encounter them during installation or deployment.

<table>
<thead>
<tr>
<th>Environment</th>
<th>Tenable Core File Format</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Machine</td>
<td>VMware</td>
<td>.ova file</td>
</tr>
<tr>
<td></td>
<td>Microsoft Hyper-V</td>
<td>.zip file</td>
</tr>
<tr>
<td>Cloud</td>
<td>Microsoft Azure</td>
<td>n/a</td>
</tr>
<tr>
<td>Hardware</td>
<td>.iso image</td>
<td>Install Tenable Core on Hardware</td>
</tr>
</tbody>
</table>

**Note:** While you could use the packages to run Tenable Core in other environments, Tenable does not provide documentation for those procedures.

Tenable.io Web Application Scanning Hardware Requirements

**Note:** Tenable does not recommend deploying multiple applications on a single instance of Tenable Core. If you want to deploy several applications on Tenable Core (for example, Tenable.sc and Tenable.io Web Application Scanning), deploy a unique instance for each application.

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Hardware Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>WAS Scanning up to 4 concurrent web applications</td>
<td><strong>CPU:</strong> (4) 2 GHz cores</td>
</tr>
<tr>
<td></td>
<td><strong>Core Ram:</strong> 16GB RAM</td>
</tr>
</tbody>
</table>
Access Requirements

Your Tenable Core + Tenable.io Web Application Scanning deployment must meet the following requirements.

- **Internet Requirements**
- **Port Requirements**

Internet Requirements

You must have internet access to download Tenable Core files.

After you transfer a file to your machine, internet access requirements to deploy or update Tenable Core vary depending on your environment.

<table>
<thead>
<tr>
<th>Environment</th>
<th>Tenable Core Format</th>
<th>Internet Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Machine</td>
<td>VMware .ova file</td>
<td>You do not need internet access to deploy or update Tenable Core.</td>
</tr>
<tr>
<td></td>
<td>Microsoft Hyper-V .zip file</td>
<td></td>
</tr>
<tr>
<td>Cloud</td>
<td>Microsoft Azure n/a</td>
<td>Requires internet access to install or update Tenable Core.</td>
</tr>
<tr>
<td>Hardware</td>
<td>.iso image</td>
<td></td>
</tr>
</tbody>
</table>

**Tip:** You do not need access to the internet when you install updates to Tenable Core + Tenable.io Web Application Scanning via an offline .iso file. For more information, see [Update Tenable Core Offline](#).

Port Requirements

Your Tenable Core deployment requires access to specific ports for inbound and outbound traffic.

**Inbound Traffic**

You must allow inbound traffic to the following ports.
<table>
<thead>
<tr>
<th>Port</th>
<th>Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP 22</td>
<td>Inbound SSH connections.</td>
</tr>
<tr>
<td>TCP 8000</td>
<td>Inbound HTTPS communications to the Tenable Core interface.</td>
</tr>
<tr>
<td>TCP 8090</td>
<td>Inbound HTTPS communications for restoring backups.</td>
</tr>
<tr>
<td></td>
<td>Inbound communications with the file upload server.</td>
</tr>
</tbody>
</table>

### Outbound Traffic

You must allow outbound traffic to the following ports.

<table>
<thead>
<tr>
<th>Port</th>
<th>Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP 22</td>
<td>Outbound SSH connections, including remote storage connections.</td>
</tr>
<tr>
<td>TCP 443</td>
<td>Outbound communications to the appliance.cloud.tenable.com server for system updates.</td>
</tr>
<tr>
<td>UDP 53</td>
<td>Outbound DNS communications for Tenable.io Web Application Scanning and Tenable Core.</td>
</tr>
</tbody>
</table>
Default Security Configuration Standards

By default, Tenable Core applies security configurations based on the following Center for Internet Security (CIS) standards. For more information about CIS standards, see cisecurity.org.

**Note:** SELinux is enabled by default on the Tenable Core operating system.

CIS Standards

**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 1.7.1.* (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 3.5.* (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
  • 4.2.4 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
- 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
## Deploy or Install Tenable Core

You can run Tenable Core + Tenable.io Web Application Scanning in the following environments.

**Note:** Tenable Support does not assist with issues related to your CentOS 7 operating system, even if you encounter them during installation or deployment.

<table>
<thead>
<tr>
<th>Environment</th>
<th>Tenable Core File Format</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Machine</td>
<td>VMware</td>
<td>.ova file</td>
</tr>
<tr>
<td></td>
<td>Microsoft Hyper-V</td>
<td>.zip file</td>
</tr>
<tr>
<td>Cloud</td>
<td>Microsoft Azure</td>
<td>n/a</td>
</tr>
<tr>
<td>Hardware</td>
<td></td>
<td>.iso image</td>
</tr>
</tbody>
</table>

**Note:** While you could use the packages to run Tenable Core in other environments, Tenable does not provide documentation for those procedures.
Deploy Tenable Core in VMware

To deploy Tenable Core + Tenable.io Web Application Scanning as a VMware virtual machine, you must download the Tenable Core + Tenable.io Web Application Scanning .ova file and deploy it on a hypervisor.

Before you begin:

- Confirm your environment will support your intended use of the instance, as described in System Requirements.
- Confirm your internet and port access will support your intended use of the instance, as described in Access Requirements.

To deploy Tenable Core + Tenable.io Web Application Scanning as a VMware virtual machine:

1. Download the Tenable Core WAS VMware Image file from the Tenable Downloads page.
2. Open your VMware VM in the hypervisor.
3. Import the Tenable Core + Tenable.io Web Application Scanning VMware .ova file from your computer to your virtual machine. For information about how to import a .ova file to your virtual machine, see VMware Documentation.
4. In the setup prompt, configure the VM to meet your organization’s storage needs and requirements, as well as those described in System Requirements.
5. Launch your Tenable Core + Tenable.io Web Application Scanning instance.

The VM boot process appears in a terminal window.

**Note:** The boot process may take several minutes to complete.

Tenable Core + Tenable.io Web Application Scanning is fully deployed when the virtual machine boot process completes.

What to do next:
• Continue getting started with Tenable Core + Tenable.io Web Application Scanning, as described in Get Started.
Deploy Tenable Core in Hyper-V

To deploy Tenable Core + Tenable.io Web Application Scanning as a Microsoft Hyper-V virtual machine, you must download the Tenable Core + Tenable.io Web Application Scanning .zip file and deploy it on the host where you want to launch Tenable Core + Tenable.io Web Application Scanning.

Note: After you download the .zip file, you can use an external storage device to deploy it on another machine. You do not need internet access on the machine hosting Tenable Core.

Before you begin:

- Confirm your environment will support your intended use of the instance, as described in System Requirements.
- Confirm your internet and port access will support your intended use of the instance, as described in Access Requirements.

To deploy Tenable Core + Tenable.io Web Application Scanning as a Hyper-V virtual machine:

1. Download the Tenable Core WAS VMware Image file from the Tenable Downloads page.
2. Navigate to your Hyper-V Manager on the machine where you want to deploy Tenable Core + Tenable.io Web Application Scanning.
3. Extract the .zip file you previously downloaded. Extracting may take a few minutes.
4. In your Hyper-V Manager, create a new virtual machine.
   The Hyper-V Manager wizard appears.
5. In the setup wizard, adjust the virtual machine configurations to meet your organization's storage needs, and the requirements described in System Requirements.

Note: Tenable recommends that you select Generation 1 when the Hyper-V Manager wizard prompts you during the configuration.
6. When prompted to Connect to a Virtual Hard Disk in the wizard, select **Use an existing virtual hard disk**.

7. Click **Browse** and select the .vhd file.

8. Click **Finish**.

   The Hyper-V setup completes.

9. (Optional) If you want to increase the number of CPUs on your virtual machine:
   a. In the **Virtual Machines** table, right-click the row for your machine and click **Settings**.
      The settings window appears.
   b. In the **Hardware** section, click **Processor**.
   c. Modify the settings as necessary.
   d. Click **Ok**.

10. In the **Virtual Machines** table, right-click the row for your machine and click **Start** or **Connect**.

    The virtual machine load process appears in a console. The load process may take several minutes to complete.

**What to do next:**

- Continue getting started with Tenable Core + Tenable.io Web Application Scanning, as described in **Get Started**.
Deploy Tenable Core in Microsoft Azure

It is typically simplest to create and configure Tenable Core + Tenable.io Web Application Scanning using the Microsoft Azure portal, as described in Deploy Tenable Core in Microsoft Azure via the Portal.

In some cases, you may prefer to use the Microsoft Azure CLI to deploy Tenable Core in Azure, as described in Deploy Tenable Core in Microsoft Azure via the CLI.
Deploy Tenable Core in Microsoft Azure via the Portal

It is typically simplest to create and configure Tenable Core + Tenable.io Web Application Scanning using the Microsoft Azure portal.

In some cases, you may prefer to use the Microsoft Azure CLI to deploy Tenable Core in Azure, as described in Deploy Tenable Core in Microsoft Azure via the CLI.

Before you begin:

- Confirm your environment will support your intended use of the instance, as described in System Requirements.
- Confirm your internet and port access will support your intended use of the instance, as described in Access Requirements.

To deploy a Tenable Core + Tenable.io Web Application Scanning VM via the Azure portal:

1. Log in to the Microsoft Azure portal. For more information, see the AWS Documentation.
2. Create a new resource by searching for the TenableCore WAS template.
3. Configure all desired options.

**Note:** If you want Tenable Core + Tenable.io Web Application Scanning to automatically link to Tenable.io on first boot, enter the following in the advanced settings using the custom data box:

```
#cloud-config
runcmd:
  # Link WAS to tenable.io
  - /usr/libexec/tenablecore/was_rest_client.py
  - "--set-link"
  - "--scanner-name"
  - <The name of your scanner as you want it to appear in Tenable.io>
  - "--linkkey"
  - <Your Tenable.io linking key>
  - "--iohost"
  - "https://cloud.tenable.com"
```
4. Start the VM deployment.

Azure begins the VM deployment. Azure displays a success message when finished.

What to do next:

- Continue getting started with Tenable Core + Tenable.io Web Application Scanning, as described in [Get Started](#).
Deploy Tenable Core in Microsoft Azure via the CLI

It is typically simplest to create and configure Tenable Core + Tenable.io Web Application Scanning using the Microsoft Azure portal, as described in [Deploy Tenable Core in Microsoft Azure via the Portal](#).

In some cases, you may prefer to use the Microsoft Azure CLI to deploy Tenable Core in Azure.

Before you begin:

- Confirm your environment will support your intended use of the instance, as described in [System Requirements](#).
- Confirm your internet and port access will support your intended use of the instance, as described in [Access Requirements](#).

To deploy a Tenable Core + Tenable.io Web Application Scanning VM via the Azure CLI:

1. In a text editor, open a new file.
2. If you want Tenable Core + Tenable.io Web Application Scanning to automatically link to Tenable.io on first boot, copy and paste the following configuration variables:

   ```
   #cloud-config
   runcmd:
   # Link WAS to tenable.io
   - /usr/libexec/tenablecore/was_rest_client.py
   - "--set-link"
   - "--scanner-name"
   - <The name of your scanner as you want it to appear in Tenable.io>
   - "--linkkey"
   - <Your Tenable.io linking key>
   - "--iohost"
   - "https://cloud.tenable.com"
   ```
3. Save and close the configuration file.
4. Log in to the Azure CLI.

5. Run the `az vm create` command to deploy the file, using the variables defined below.

   **Tip:** For more information about the Azure CLI, see the *Microsoft Azure CLI Documentation*.

   The system deploys your Tenable Core + Tenable.io Web Application Scanning VM.

What to do next:

- Continue getting started with Tenable Core + Tenable.io Web Application Scanning, as described in [Get Started](#).
Install Tenable Core on Hardware

You can install Tenable Core + Tenable.io Web Application Scanning directly on hardware using an .iso image. When you install Tenable Core via an .iso image on your computer, Tenable Core replaces your existing operating system with the Tenable Core operating system.

Before you begin:

- Confirm your environment will support your intended use of the instance, as described in System Requirements.
- Confirm your internet and port access will support your intended use of the instance, as described in Access Requirements.

To install Tenable Core + Tenable.io Web Application Scanning on hardware:

1. Download the Tenable Core WAS VMware Image file from the Tenable Downloads page.
2. Boot the .iso. For more information, see your environment documentation.

Caution: Booting the .iso replaces your existing operating system with the Tenable Core operating system.

Tip: To monitor the progress of the installation, select Install TenableCore using serial console from the boot menu. For more information about the Tenable.ot serial console, see the Tenable.ot User Guide.

The installer installs Tenable Core + Tenable.io Web Application Scanning on your hardware.

If there are no configuration errors, the installation begins.

If there are configurations errors, the Installation menu appears.

If you need to resolve configuration errors [l] with your 4) Installation source and/or 5) Software selection settings, you will need to Edit the Network Configuration or Edit the Proxy Configuration.

Caution: Do not enter any other menus or modify any other settings.

The installation runs and the server restarts.

What to do next:
• Continue getting started with Tenable Core + Tenable.io Web Application Scanning, as described in Get Started.
Edit the Network Configuration

During installation, you may need to edit the network configuration settings. Perform this procedure to resolve errors [!] with your 4) Installation source and/or 5) Software selection settings.

Caution: Do not enter any other menus or modify any other settings.

To edit the network configuration:

1. From the Installation menu, press the 8 key.
2. Press the Enter key.
   The Network Configuration menu appears.
3. Press the 2 key.
4. Press the Enter key.
   The Device Configuration menu appears.
5. Review the 1) IPv4 address or "dhcp" for DHCP, 2) IPv4 netmask, 3) IPv4 gateway, and 6) Nameservers settings and, if necessary, edit them.
   For example, you must edit these settings if you are installing Tenable Core on a static network without DHCP.
6. Check 8) Apply configuration in installer.
7. Press the c key until you return to the Installation menu.
8. Press the r key to refresh the menu.
9. Confirm that settings 1-7 show an [x]. If the settings all show an [x] proceed to step 11.
10. If 4) Installation source still shows a [!]:
   Refresh the repository URL:
   a. Press the 4 key.
   b. Press the Enter key.
   The Installation Source menu appears.
c. Press the 3 key.
d. Press the Enter key.
   The Installation Source submenu appears.
e. Press the 2 key.
f. Press the Enter key.
   The Specify Repo Options menu appears.
g. Press the c key.
h. Press the Enter key.
   The system refreshes the repository URL and the Installation menu appears.

11. Press the r key to refresh the menu.
12. Press the c key until you return to the Installation menu.
Edit the Proxy Configuration

During installation, you may need to edit the proxy configuration settings to identify the proxy you want to use for internet access.

**Caution:** Do not enter any other menus or modify any other settings.

To edit the proxy configuration:

1. From the **Installation** menu, press the 3 key.
2. Press the **Enter** key.
   
The **Proxy Configuration** menu appears.
3. Type the proxy you want to use. For example, `https://username:password@192.0.2.221:3128`.
   
   **Note:** If your password includes a special character, the special character must be HTML URL encoded.
4. Press the **Enter** key.
5. If your proxy is a man-in-the-middle proxy that intercepts SSL traffic, a prompt appears.
   
   **In the prompt:**
   
   1. Type yes.
   
   2. Press the **Enter** key.
      
      The system temporarily disables SSL verification. The system automatically re-enables SSL verification after the installation completes.
      
      The **Installation** menu appears.
6. Press the 4 key.
7. Press the **Enter** key.
   
   The **Installation Source** menu appears.
8. Press the 3 key.
9. Press the **Enter** key.
The **Installation Source** submenu appears.

10. Press the **2** key.

11. Press the **Enter** key.

   The **Specify Repo Options** menu appears.

12. Press the **c** key.

13. Press the **r** key, then the **Enter** key.

14. If necessary, continue pressing the **r** key, then the **Enter** key until 4) **Installation source** no longer says **(Processing...)**.

   The system refreshes the repository URL.
Disk Management

You can use the Tenable Core interface to manage some aspects of your Tenable Core machine disk space. Tenable Core uses Linux logical volume management (LVM) for disk management.

Disk management via the Tenable Core interface assumes you understand basic LVM terminology:

- **Volume group** – A group of one or more physical volumes.
- **Physical volume** – A hard disk, hard disk partition, or RAID unit.
- **Logical volume** – A block of space on the volume group sized to mirror several or all of your physical volumes.
- **File system** – The file system on the logical volume.
- **Mount point** – The location where you mounted the file system in your operating system.

For more information about these concepts, see general documentation for Linux.

Tenable Core Partitions

Tenable Core installs or deploys with the following preconfigured partitions:

- `/boot`
- `Swap`
- `/`
- `/var/log`
- `/opt`

To add more storage space to Tenable Core (typically, in `/opt`), add a disk or expand a disk as described in [Add or Expand Disk Space](#).
Add or Expand Disk Space

If you need more space in Tenable Core to meet the requirements, add space to your machine by expanding an existing disk or adding a new disk. For general information about Tenable Core disk management, see Disk Management.

Caution: You cannot reassign disk space after you have assigned the space to a file system.

To add or expand existing disk space on your Tenable Core machine:

1. Power down your machine, as instructed by your local administrator or the documentation for your local environment.

2. Add a new disk or expand an existing disk in your machine configuration, as instructed by your local administrator or the documentation for your local environment.

3. Power up your machine, as instructed by your local administrator or the documentation for your local environment.

4. Log in to Tenable Core.

   The System page appears.

5. In the left navigation bar, click Storage.

   The Storage page appears.

6. In the Filesystems section, locate the file system with /opt as the Mount Point and note the file system Name (e.g., /dev/vg0/00).

   Tip: Typically, you want to add space to /opt. To add more storage space to a less common partition (for example, / or /var/log), locate the file system for that partition.

7. Click the row for the file system Name that includes your preferred partition as the Mount Point.

   The Volume Group page appears.

8. In the Physical Volumes section, click the + button.

   The Add Disks window appears.
9. Click the check box for the space you added.

10. Click **Add**.

   The **Volume Group** page appears, updated to show the added space in the **Physical Volumes** section.

11. In the **Logical Volumes** section, expand the section for the file system **Name** that includes your preferred partition as the **Mount Point**.

12. Click **Grow**.

   The **Grow Logical Volume** window appears.

13. Use the slider to increase the size of the file system to your desired size (typically, to the new maximum).

14. Click **Grow**.

   The system expands the logical volume and the file system.

   The **Volume Group** page appears, refreshed to reflect the new size.
Manually Configure a Static IP Address

If you deploy Tenable Core in an environment where DHCP is configured, Tenable Core automatically receives network configurations (including your IP address). If DHCP is not configured, you must manually configure a static IP address in Tenable Core.

For more information about the default NIC configuration in your environment, see System Requirements.

Before you begin:

- Deploy or install Tenable Core + Tenable.io Web Application Scanning, as described in Deploy or Install Tenable Core.
- Contact your network administrator and obtain your network’s netmask and the IP address for your Tenable Core + Tenable.io Web Application Scanning deployment.

To manually configure a static IP address:

1. In the command line interface (CLI) in Tenable Core, type the following to log in as a wizard user:

   ```bash
tenable-y3u1xwh1 login: wizard
   Password: admin
   ```

   A prompt appears asking if you want to configure a static IP address.

2. Press the **y** key.

   (Optional) If the prompt does not appear, in the command line interface (CLI) in Tenable Core, run the following command to access the configuration user interface:

   ```bash
   nmtui edit
   ```

   The list of connections page appears.

3. Select the connection you want to configure.

4. Press **Tab** to select **Edit**.
5. Press **Enter**.

   The **Edit Connection** window appears.

6. In the **IPv4 Configuration** row, press **Tab** to select **Automatic**.

7. Press **Enter**.

8. Select **Manual** from the drop-down box.

9. Press **Enter**.

10. Press **Tab** to select **Show**.

11. Press **Enter**.

   Additional configuration fields appear.

   **Note**: Type the value for each configuration field as four numbers separated by a period. Refer to the examples for each field.

12. In the **Addresses** field, type the IPv4 IP address for your Tenable Core + Tenable.io Web Application Scanning deployment, followed by a forward slash and your netmask.

    Example:

    ```
    192.0.2.57
    ```

13. In the **Gateway** field, type your gateway IP address.

    Example:

    ```
    192.0.2.177
    ```

14. In the **DNS servers** field, type your DNS server IP address.

    Example:

    ```
    192.0.2.176
    ```
15. Press **Tab** to select **<Add...>**.

**Note:** Complete steps 12-15 only if you have additional DNS server IP addresses to add. Repeat for each IP address.

16. Press **Enter**.

An empty box appears in the **DNS servers** row.

17. In the new row, type your second DNS server IP address.

Example:

```
192.0.2.8
```

18. Select the check box in the **Require IPv4 addressing for this connection** row.

19. Press **Tab** to select **<OK>**.

The list of connections appears.

20. Press **Tab** to select **<Quit>**.

21. Press **Enter**.

If you log in with a wizard, a prompt appears asking if you want to create an administrator account.

To create an administrator account, see **Create a First-Time User Account**.

You will be logged out of the wizard account.

22. Log into the CLI using the administrator account.

23. Restart the connection. In the command line interface (CLI) in Tenable Core, run the following command:

```
$ nmcli connection down "Wired connection 1" && nmcli connection up "Wired connection 1"
```

**Note:** Restarting the connection enables the system to recognize your static IP address. You can reboot the system instead to trigger the response.

What to do next:
• Confirm that the Tenable Core **nic1** MAC address matches the NIC MAC address in your VMware passive scanning configuration. If necessary, modify your VMware configuration to match your Tenable Core MAC address. For more information, see [System Requirements](#).
Create an Initial Administrator User Account

The first time you access Tenable Core + Tenable.io Web Application Scanning, you log in as a wizard user.

Then, you create an initial administrator account.

**Tip:** If you delay creating an initial administrator account, after a few minutes, the system locks you out of the wizard user account. You will need to reboot Tenable Core to proceed with the initial administrator account creation.

Before you begin:

- Deploy or install Tenable Core + Tenable.io Web Application Scanning, as described in [Deploy or Install Tenable Core](#).

To create an initial administrator user account:

1. Navigate to the URL for your Tenable Core VM.
   
   The login page appears.

2. In the **User name** field, type **wizard**.

3. In the **Password** field, type **admin**.

4. Click **Log In**.
   
   The **Create New Administrator** window appears.

5. In the **Username** field, type the username you want to use for your administrator account.

6. In the **Password** field, type a new password for your administrator account.

7. Click **Create Account**.
   
   A confirmation window appears.

8. Click **Finish Setup**.
   
   Tenable Core creates your user account.

9. Click **Log Out**.
   
   Tenable Core logs you out.
What to do next:

- (Optional) If you want to log in again, see [Log In to Tenable Core](#).
- (Optional) If you want to create another user account, see [Create New User Account](#).

**Note:** You must log back in again before you can create a new user account.
Create a Password for the Initial Administrator User Account

If you deployed Tenable Core + Tenable.io Web Application Scanning in a [cloud environment](#) and did not create a password during deployment, you cannot access the Tenable Core interface. You must create a password for your administrator account via SSH before you can access the Tenable Core interface.

You do not need to create a password via SSH when deploying Tenable Core + Tenable.io Web Application Scanning in any of the other supported environments.

Before you begin:

- Confirm you have an SSH client installed that can access your Tenable Core server.

To create a password for the initial administrator user account:

1. Open a connection to Tenable Core with your SSH client via one of the following methods:
   - If your SSH client uses a command line interface (CLI), run the following command:

     ```
     ssh <your administrator username>@<your Tenable Core hostname or IP address>
     ```

   - If your SSH client uses a user interface, open the interface and follow the prompts to connect to Tenable Core via SSH.

     Tenable Core connects to your SSH client.

2. When prompted, provide your Tenable Core username via one of the following methods:
   - If you deployed in Amazon Web Service (AWS), type `ec2-user` as your username.
   - If you deployed in Microsoft Azure, type the username you configured during your deployment.

3. Run the `sudo passwd` command.

   ```
   sudo passwd "$USERNAME"
   ```

   The SSH client prompts you to provide a password.
4. Type the password you want to use for your administrator account.

5. Press **Enter**.

   Tenable Core assigns the password to your administrator account.

6. Run the `exit` command to log out of Tenable Core.

What to do next:

- Continue getting started with Tenable Core + Tenable.io Web Application Scanning, as described in [Get Started](#).
Link Tenable Core to Tenable.io

After you deploy your instance of Tenable Core + Tenable.io Web Application Scanning, you can configure your Web Application Scanner to Tenable.io.

Before you begin:

- Log in to Tenable Core in a browser, as described in Log In to Tenable Core.
- (Optional) If you want to connect Tenable Core + Tenable.io Web Application Scanning to Tenable.io via a proxy, configure a proxy connection to the internet, as described in Configure a Proxy Server.

To configure Tenable.io Web Application Scanning in Tenable Core:

1. In the left navigation menu, click Web Application Scanner.

   The Tenable.io Link window appears.

   Tip: Click the icon next to the Tenable.io Link URL: option to reopen the window.

2. In the Link Key: box, type your Tenable.io linking key.

   Note: To retrieve your Tenable.io linking key, log in to Tenable.io and navigate to Scans>Agents. On the Linked Agents tab, your linking key appears.

3. In the Scanner Name: box, type a name for your scanner as you want it to appear in Tenable.io.


5. (Optional) If you configured a proxy for Tenable Core to connect to Tenable.io, select the Connect Using Proxy: check box.

6. Click Activate Scanner.

   A success message appears.

Your Web Application Scanner appears in the scanner list on Tenable.io. For more information, see Web Application Scans in the Tenable.io Web Application Scanning User Guide.
Log In to Tenable Core

Log in to Tenable Core to configure and manage your Tenable Core + Tenable.io Web Application Scanning instance in the Tenable Core interface.

Before you begin:

- Deploy Tenable Core + Tenable.io Web Application Scanning, as described in Deploy or Install Tenable Core.

To log in to Tenable Core:

1. Navigate to the URL for your Tenable Core VM.
   
The login page appears.

2. In the User name field, type your username.

3. In the Password field, type your password.

4. Select the Reuse my password for privileged tasks check box.

   **Note:** You cannot configure or manage your instance of Tenable Core + Tenable.io Web Application Scanning if you do not select the Reuse my password for privileged tasks check box.

5. Click Log in.

   Tenable Core logs you in to the user interface.
Configure and Manage

You can use the Tenable Core user interface to configure and manage Tenable Core + Tenable.io Web Application Scanning.

View the Dashboard

Add a Server

Edit a Server

Delete a Server

Synchronize Accounts

Manage the System

Change Performance Profile

Restart Tenable Core

Shut Down Tenable Core

Edit Your Tenable Core Hostname

Edit Your Time Settings

View the System Log

Filter the System Log

Manage System Networking

Add a Bonded Interface

Add a Team of Interfaces

Add a Bridge Network

Add a VLAN

Manage System Storage

Rename a Filesystem

Delete a Filesystem
Manage User Accounts
   Create New User Account
   Edit a User Account
   Delete a User Account

Manage Services
   Create a Timer

Generate a Diagnostic Report

Access the Terminal

Manage Tenable.io Web Application Scanning in Tenable Core

Configure a Proxy Server

Start, Stop, or Restart Your Application

Manage Updates
   Configure Automatic Updates
   Update On Demand
   Update Tenable Core Offline

Manage Certificates
   Manage the Server Certificate
   Upload a Certificate for a Trusted Certificate Authority
   Use Different Certificates for Tenable Core and Your Application

Application Data Backup and Restore
   Configure a Remote Storage Host
   Perform an On-Demand Backup
   Change the Scheduled Backup Time
   Restore a Backup
SNMP Agent Configuration

Configure an SNMP Agent via the User Interface

Configure an SNMP Agent via the CLI

Take a Virtual Machine Snapshot
View the Dashboard

You can use the Dashboard page to view usage statistics and manage your attached servers.

To view the Tenable Core dashboard:

1. Log in to Tenable Core via the user interface, as described in Log In to Tenable Core.

   The System page appears.

2. Hover over the left navigation bar and click Dashboard.

   The Dashboard page appears.

You can:

<table>
<thead>
<tr>
<th>Section</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data graphs</td>
<td>• View a graph of the CPU usage on your instance.</td>
</tr>
<tr>
<td></td>
<td>• View a graph of the Memory usage on your instance.</td>
</tr>
<tr>
<td></td>
<td>• View a graph of the Network bandwidth usage on your instance.</td>
</tr>
<tr>
<td></td>
<td>• View a graph of the Disk I/O bandwidth usage on your instance.</td>
</tr>
<tr>
<td></td>
<td>• To change the time range for data displayed in the graph:</td>
</tr>
<tr>
<td></td>
<td>1. In the top-right corner of the graph, click the drop-down box.</td>
</tr>
<tr>
<td></td>
<td>2. Select a time range.</td>
</tr>
<tr>
<td></td>
<td>The system refreshes the graph.</td>
</tr>
<tr>
<td>Servers table</td>
<td>• Add a server, as described in Add a Server.</td>
</tr>
<tr>
<td></td>
<td>• Edit a server, as described in Edit a Server.</td>
</tr>
<tr>
<td></td>
<td>• Delete a server, as described in Delete a Server.</td>
</tr>
<tr>
<td></td>
<td>• Synchronize user accounts, as described in Synchronize Accounts.</td>
</tr>
<tr>
<td></td>
<td>• To view detailed information about a server, click a server row. For</td>
</tr>
<tr>
<td></td>
<td>more information, see System.</td>
</tr>
</tbody>
</table>
Add a Server

To add a server:

**Note:** You can add as many servers to the Dashboard as you want.

1. Hover over the far-left navigation bar.
   The left navigation plane appears.
2. Click **Dashboard**.
   The **Dashboard** page appears.
3. Click the **+** icon.
   The **Add Machine to Dashboard** window appears.
4. In the **Address** field, type the IP address or host name for the server you want to add.
5. In the **Color** field, click the color you want to represent the server.
6. Click **Add**.
   A confirmation window appears.
   **Note:** If Tenable Core cannot establish authentication, the Unknown Host window appears. Contact your administrator to confirm your server’s name or IP address.
7. Click **Connect**.
   A credentials window appears.
8. Type your credentials in the **User name** and **Password** fields.
   **Note:** To synchronize your accounts so that your account information and passwords are the same across multiple servers, click the **synchronize accounts and passwords** link. Refer to **Synchronize Accounts** for more information.
9. Click **Log In**.
   Tenable Core adds the server to your list of servers in the **Servers** table.
   **Note:** If the server does not appear in the list right away, refresh the browser.
Edit a Server

To edit a server:

1. From the top bar in the **Servers** table, click the icon.
   
   A pencil icon (-pencil) and a trashcan icon (trash) appear next to each server name.

2. Click the icon.
   
   The **Edit Server** window appears.

3. Do any of the following:
   
   - In the **Host Name** box, type the name you want for your server.
   
   - Update the server color:
     
     - In the **Color** box, click the color bar.
     
     A color menu appears.
     
     - Click the color you want to represent the server.
     
     The server color changes.

4. Click **Set**.
   
   Tenable Core updates your server information.
Delete a Server

To delete a server:

1. From the top bar in the **Servers** table, click the check mark icon.
   
   A pencil icon and a trashcan icon appear next to each server name.

2. Click the trashcan icon.
   
   The server disappears from the server list.
Synchronize Accounts

If you have multiple user accounts but do not want to manage credentials for each one, you can synchronize your accounts, which allows you to seamlessly navigate between accounts without providing a different user name and password for each account.

**Note:** You can synchronize accounts while either adding or editing servers in the Dashboard.

To synchronize accounts:

1. While either adding or editing a server, click the **Synchronize users** link in the dialogue box. The **SYNCHRONIZE USERS** dialogue box appears with a list of your accounts.

   **Note:** If you are adding a server, the linked text in the dialogue box is **synchronize accounts and passwords**.

2. Check the boxes next the accounts you want to synchronize.

3. Click **Synchronize**.
## Manage the System

You can use the **System** page to view usage statistics and manage system settings.

To manage the Tenable Core system:

1. Log in to Tenable Core via the user interface, as described in [Log In to Tenable Core](#).

   The **System** page appears.

You can:

<table>
<thead>
<tr>
<th>Section</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>System details section</td>
<td>• View summary information about your Tenable Core instance.</td>
</tr>
<tr>
<td></td>
<td>• Change the performance profile for your instance, as described in <a href="#">Change Performance Profile</a>.</td>
</tr>
<tr>
<td></td>
<td>• Restart or shut down your instance, as described in <a href="#">Restart Tenable Core</a> and <a href="#">Shut Down Tenable Core</a>.</td>
</tr>
<tr>
<td></td>
<td>• Edit the hostname for your instance, as described in <a href="#">Edit Your Tenable Core Hostname</a>.</td>
</tr>
<tr>
<td></td>
<td>• Edit the time and time zone settings for your instance, as described in <a href="#">Edit Your Time Settings</a>.</td>
</tr>
<tr>
<td>Data graphs</td>
<td>• View a graph of the <strong>CPU</strong> usage on your instance.</td>
</tr>
<tr>
<td></td>
<td>• View a graph of the <strong>Memory &amp; Swap</strong> usage on your instance.</td>
</tr>
<tr>
<td></td>
<td>• View a graph of the <strong>Disk I/O</strong> bandwidth usage on your instance.</td>
</tr>
<tr>
<td></td>
<td>• View a graph of the <strong>Network Traffic</strong> bandwidth usage on your instance.</td>
</tr>
<tr>
<td></td>
<td>• To change the time range for data displayed in the graphs:</td>
</tr>
<tr>
<td></td>
<td>1. In the top-right corner of the graph, click the drop-down box.</td>
</tr>
<tr>
<td></td>
<td>2. Select a time range.</td>
</tr>
</tbody>
</table>
The system refreshes the graph.
Change Performance Profile

To change the performance profile for your Tenable Core instance:

1. Log in to Tenable Core via the user interface, as described in Log In to Tenable Core.
   The System page appears.

2. In the left navigation pane, click the System option. The System page displays.

3. Click on the link next to the Performance Profile option in the information list that is left of the graph charts. A new window will appear displaying Performance Profile options.

4. Select the desired Performance Profile. The recommended profile is labeled in the list.

5. Click Change Profile to confirm the new selection.
Restart Tenable Core

To restart your Tenable Core instance:

1. Log in to Tenable Core via the user interface, as described in Log In to Tenable Core.
   
   The System page appears.

2. In the left navigation pane, click the System option.
   
   The System page displays.

3. Next to the Power Options item, click the Restart button or select it from the drop-down box.
   
   A new window will appear.

4. Enter a message for the users in the text box.

5. Select the delay time from the drop down menu. This is the time that the restart will start.
   
   Choose from one of the minute increments or enter a specific time. There is also an option to restart immediately with no delay.

6. Click the Restart button to initiate and save the updated information.
Shut Down Tenable Core

To shut down your Tenable Core instance:

1. Log in to Tenable Core via the user interface, as described in Log In to Tenable Core.
   The System page appears.

2. In the left navigation pane, click the System option.
   The System page displays.

3. Next to the Power Options item, click the arrow by Restart to display the drop down menu.
   Select Shut Down.
   A new window will appear.

4. Enter a message for the users in the text box.

5. Select the delay time from the drop down menu. This is the time that the shut down will start.
   Choose from one of the minute increments or enter a specific time. There is also an option to
   Shut Down immediately with no delay.

6. Click Shut Down to initiate and save the updated information.

![Shut Down window](image)
Edit Your Tenable Core Hostname

To edit the hostname for your Tenable Core instance:

1. Log in to Tenable Core via the user interface, as described in Log In to Tenable Core.

   The System page appears.

2. In the left navigation pane, click the System option.

   The System page displays.

3. Click the link next to the Host Name option in the information list that is left of the graph charts.

   A new window will appear with the options to enter/edit the Pretty Host Name and Real Host Name.

4. Enter the Pretty Host Name for the machine.

   The Real Host Name will update as the Pretty Host Name is entered.

5. Click Change to update the name.

   The new name will be displayed next to the Hostname option.

---

<table>
<thead>
<tr>
<th>Change Host Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pretty Host Name</td>
</tr>
<tr>
<td>Real Host Name</td>
</tr>
</tbody>
</table>

---
Edit Your Time Settings

To edit the system time and time zone settings for your Tenable Core instance:

1. Log in to Tenable Core via the user interface, as described in Log In to Tenable Core. The **System** page appears.

2. Next to **System Time**, click the link. The **Change System Time** window appears.

3. In the **Time Zone** drop-down box, select your time zone.
   
   **Tip:** Type the first few letters of the desired time zone to filter the list.

4. In the **Set Time** drop-down box, select your preferred method for time synchronization.
   
   **Tip:** By default, Tenable Core is set to **Automatically using NTP**.

5. Click **Change**.

   Tenable Core saves the change.
View the System Log

You can use the **System Log** page to view 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.
Filter the System Log

Several log type filters are available. The **Everything** option is selected by default. Select another option using the drop down menu at the top of the page. The logs are listed with the most recent entry displayed first. Previous days are divided into sections with the corresponding date displayed in the header.

The logs can be filtered using the drop down menu. Click on the date to display the filter options for the logs.
Manage System Networking

You can use the Networking page to view real-time system network traffic information, interface connection options, and logs.

To manage Tenable Core system networking:

1. Log in to Tenable Core via the user interface, as described in [Log In to Tenable Core](#).

   The System page appears.

2. In the left navigation bar, click Networking.

   The Networking page appears.

You can:

<table>
<thead>
<tr>
<th>Section</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Graphs</strong></td>
<td>• View a graph of the <strong>Sending</strong> (outbound) network traffic on your instance.</td>
</tr>
<tr>
<td></td>
<td>• View a graph of the <strong>Receiving</strong> (inbound) network traffic on your instance.</td>
</tr>
<tr>
<td><strong>Firewall</strong></td>
<td>• View Firewall rules.</td>
</tr>
<tr>
<td>section</td>
<td>• Add Zones.</td>
</tr>
<tr>
<td></td>
<td>• Add Allowed Services.</td>
</tr>
<tr>
<td><strong>Interfaces</strong></td>
<td>• Aggregate multiple network interfaces into a single bonded interface, as described in <a href="#">Add a Bonded Interface</a>.</td>
</tr>
<tr>
<td>table</td>
<td>• Add a team of interfaces, as described in <a href="#">Add a Team of Interfaces</a>.</td>
</tr>
<tr>
<td></td>
<td>• Add a bridge to create a single aggregate network from multiple communication networks, as described in <a href="#">Add a Bridge Network</a>.</td>
</tr>
<tr>
<td></td>
<td>• Add a VLAN, as described in <a href="#">Add a VLAN</a>.</td>
</tr>
<tr>
<td>Networking Logs table</td>
<td>View a log of activity for the system network.</td>
</tr>
</tbody>
</table>
Add a Bonded Interface

You can add a bond to aggregate multiple network interfaces into a single bonded interface.

To add a bonded interface to Tenable Core:

1. In the left navigation pane, click the **Networking** option. The **Networking** page displays.
2. In the **Interfaces** heading, click the **Add Bond** button on the **Interfaces** section. A new window appears.
3. Enter a **Name** for the bond.
4. Select the members (interfaces) to bond to in the **Members** section.
5. Select an option for **MAC**.
6. Select the **Mode**.
7. Select a **Primary**.
8. Select the type of **Link Monitoring**. The recommended type is labeled in the drop down list.
9. Enter the **Monitoring Intervals** with options to link up or down delay increments.

<table>
<thead>
<tr>
<th>Name</th>
<th>bond0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Members</td>
<td>ens160 en32</td>
</tr>
<tr>
<td>MAC</td>
<td></td>
</tr>
<tr>
<td>Mode</td>
<td>Active Backup</td>
</tr>
<tr>
<td>Primary</td>
<td></td>
</tr>
<tr>
<td>Link Monitoring</td>
<td>MIL (Recommended)</td>
</tr>
<tr>
<td>Monitoring Interval</td>
<td>100</td>
</tr>
<tr>
<td>Link up delay</td>
<td>0</td>
</tr>
<tr>
<td>Link down delay</td>
<td>0</td>
</tr>
</tbody>
</table>

[Image of Bond Settings Table ]
Add a Team of Interfaces

To add a team of interfaces to Tenable Core:

1. In the left navigation pane, click the Networking option. The Networking page displays.
2. In the Interfaces heading, click the Add Team button on the Interfaces section. A new window will appear.
3. Enter the Team Name.
4. Select the Ports needed for the new team.
5. Select the Runner and Link Watch from the drop down list.
6. Enter the Link up and Link down delay increments.
Add a Bridge Network

You can add a bridge to create a single aggregate network from multiple communication networks.

To add a bridge network to Tenable Core:

1. In the left navigation pane, click the **Networking** option. The **Networking** page displays.
2. In the **Interfaces** heading, click the **Add Bridge** button on the **Interfaces** section. A new window will appear.
3. Enter a **Name** for the bridge.
4. Select the **Ports** that will connect to the bridge.
5. Click the box next to **Spanning Tree Protocol (STP)** to get additional STP options.
6. Click **Apply** to add the new bridge.

### Bridge Settings

<table>
<thead>
<tr>
<th>Name</th>
<th>bridge0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ports</td>
<td>ens192</td>
</tr>
<tr>
<td></td>
<td>ens192.1</td>
</tr>
</tbody>
</table>

**Spanning Tree Protocol (STP)**

- **STP Priority**: 32768
- **STP Forward delay**: 15
- **STP Hello time**: 2
- **STP Maximum message age**: 20

[Apply] [Cancel]
Add a VLAN

To add a VLAN to Tenable Core:

1. Click the **Add VLAN** button on the Interfaces section. A new window will appear.
2. Select the **Parent** from the drop down list.
3. Enter the **VLAN Id** and name.
4. Click **Apply** to confirm add the **VLAN**.
5. The new **VLAN** will display in the **Interface** list.

### VLAN Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parent</td>
<td>ens192</td>
</tr>
<tr>
<td>VLAN Id</td>
<td>1</td>
</tr>
<tr>
<td>Name</td>
<td>ens192.1</td>
</tr>
</tbody>
</table>
Manage System Storage

You can use the Storage page to view real-time system storage graphs, filesystem information, and logs. For more information, see Disk Management.

To manage Tenable Core storage:

1. Log in to Tenable Core via the user interface, as described in Log In to Tenable Core.

   The System page appears.

2. In the left navigation bar, click Storage.

   The Storage page appears.

You can:

<table>
<thead>
<tr>
<th>Section</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Graphs</td>
<td>- View a graph of the Reading storage activity on your instance.</td>
</tr>
<tr>
<td></td>
<td>- View a graph of the Writing storage activity on your instance.</td>
</tr>
<tr>
<td><strong>Filesystems</strong></td>
<td><strong>table</strong></td>
</tr>
<tr>
<td></td>
<td>- View information about each filesystem.</td>
</tr>
<tr>
<td></td>
<td>- Click a row to view additional details about the filesystem.</td>
</tr>
<tr>
<td></td>
<td>- Rename a filesystem, as described in Rename a Filesystem.</td>
</tr>
<tr>
<td></td>
<td>- Delete a filesystem, as described in Delete a Filesystem.</td>
</tr>
</tbody>
</table>
Rename a Filesystem

To rename a filesystem in Tenable Core:

1. In the left navigation pane, click Storage.
   
   The Storage page appears.

2. In the File Systems section, click on the individual file in the file systems list.
   
   The details page appears.

3. Click the Rename button in the upper right section of the window.
   
   A new window appears.

4. Enter the new name for the File System.

5. Click Create.
   
   The new name appears on the page.
Delete a Filesystem

To delete a filesystem in Tenable Core:

1. In the left navigation pane, click the **Storage** option. The **Storage** page displays.

2. In the **File System** section, click the individual file in the files systems list. The details page will appear.

3. Click the red **Delete** button in the system heading.

4. Confirm that you want to delete the **File System**.

5. **Caution:** Deleting a volume group will erase all data on it.
Manage User Accounts

You can use the Accounts page to manage user accounts for your Tenable Core instance.

To manage Tenable Core user accounts:

1. Log in to Tenable Core via the user interface, as described in Log In to Tenable Core.
   The System page appears.
2. In the left navigation bar, click Accounts.
   The Accounts page appears.

Do any of the following:

- Create a new user account, as described in Create New User Account.
- Edit a user account, as described in Edit a User Account.
- Delete a user account, as described in Delete a User Account.
Create New User Account

**Required User Role:** Administrator

You can create a new user account from the Accounts page.

To create a new user account:

1. Log in to Tenable Core, as described in [Log In to Tenable Core](#).
2. In the left navigation bar, click Accounts.
   - The Accounts page appears.
3. Click Create New Account.
   - The Create New Account window appears.
4. In the Full Name box, type the user's full name.
5. In the User Name box, type a username for the user account.
6. In the Password box, type a password for the user account.
7. In the Confirm box, retype the password.
8. Click Create.
   - Tenable Core creates the new account and displays it on the Accounts page.

What to do next:

- (Optional) If you want to configure the user account, see [Edit a User Account](#).
- (Optional) If you want to delete the user account, see [Delete a User Account](#).
Edit a User Account

**Required User Role:** Administrator

You can edit a user account configuration, including the user's full name, password, roles, access, and public SSH keys.

Before you begin:

**To edit a user account:**

1. Log in to Tenable Core, as described in [Log In to Tenable Core](#).
2. In the left navigation bar, click Accounts.
   - The Accounts page appears.
3. Click the user account you want to edit.
   - The account page for the user account appears.
4. On the user account page, you can:

<table>
<thead>
<tr>
<th>Section</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Name</td>
<td>Type a name for the user account.</td>
</tr>
<tr>
<td>Roles</td>
<td>- To grant the user account administrator access, select the <strong>Server Administrator</strong> check box.</td>
</tr>
<tr>
<td></td>
<td>- To remove administrator access from the user account, clear the <strong>Server Administrator</strong> check box.</td>
</tr>
<tr>
<td>Access</td>
<td>- To lock the user account, select the <strong>Lock Account</strong> check box to lock the user account.</td>
</tr>
<tr>
<td></td>
<td>- To unlock the user account, clear the <strong>Lock Account</strong> check box to unlock the user account.</td>
</tr>
<tr>
<td></td>
<td>- To configure the account to remain unlocked indefinitely:</td>
</tr>
</tbody>
</table>

**Note:** If you do not configure the account to remain unlocked indefinitely:
Tenable Core automatically locks the account on the set expiration date.

1. Click **Never lock account**.
   
   The **Account Expiration** window appears.

2. Select the **Never lock account** option.

3. Click **Change**.
   
   Tenable Core sets the account to remain unlocked indefinitely.

- **Select an expiration date for the account:**

  1. Click **Never lock account**.
     
     The **Account Expiration** window appears.

  2. Select the **Lock account on** option.

  3. Click the box next to the **Lock account on** option.
     
     A calendar drop-down box appears.

  4. In the calendar drop-down box, select the date when you want the account to expire.

  5. Click **Change**.
     
     Tenable Core sets the expiration date for the user account.

**Password**

- To set a new user account password:

  1. Click **Set Password**.
     
     The **Set Password** window appears.

  2. In the **New Password** box, type the password you want to use for the account.

  3. Click **Set**.
Tenable Core updates the user account password.

- To force a user to change their user account password:
  1. Click **Force Change**.
     
     The **Force password change** window appears.
  2. Click **Reset**.
     
     Tenable Core disables the password for the user account. The user must change the password on the next log in attempt.

- Configure the user account password to remain active indefinitely:
  
  **Note:** If you do not configure the password to remain active indefinitely, Tenable Core automatically expires the password on the set expiration date.

  1. Click **Never expire password**.
      
     The **Password Expiration** window appears.
  2. Select the **Never expire password** option.
  3. Click **Change**.
     
     Tenable Core sets the password to remain active indefinitely.

- Select an expiration date for the user account password:
  1. Click **Never expire password**.
      
     The **Password Expiration** window appears.
  2. Select the **Require password change every [blank] days** option.
  3. In the **Require password change every [blank] days** sec-
4. Click **Change**.

Tenable Core sets the expiration date for the user account password.

**Authorized Public SSH Keys**

- To add a public SSH key to the user account:
  1. In the **Authorized Public SSH Keys** table, click the icon.

    The **Add public key** window appears.

  2. In the text box, type or paste your public SSH key.

  3. Click **Add key**.

    Tenable Core adds the SSH key to the user account.

- To remove a public SSH key:
  1. In the **Authorized Public SSH Keys** table, next to the key you want to remove, click the icon.

    Tenable Core removes the SSH key from your account.
Delete a User Account

**Required User Role:** Administrator

You can delete a user account from the Accounts page.

To delete a new user account:

1. Log in to Tenable Core in a browser, as described in Log In to Tenable Core.

2. In the left navigation bar, click Accounts.
   
   The Accounts page appears.

3. Click the user account you want to delete.
   
   The account page for the user account appears.

4. In the upper-right corner, click Delete.
   
   The delete window for the user account appears.

5. (Optional), if you want to permanently delete files attached to the user account, select the Delete Files check box.

   **Note:** If you do not delete them, the files remain attached to the Tenable Core instance, along with their existing access permissions. Users who were previously granted access can still access the files.

6. Click Delete.
   
   Tenable Core delete the user account.
Manage Services

You can use the **Services** page to view information about targets, system services, sockets, timers, and paths.

To manage Tenable Core services:

1. Log in to Tenable Core via the user interface, as described in [Log In to Tenable Core](#).
   
   The **System** page appears.

2. In the left navigation bar, click **Services**.
   
   The **Services** page appears.

You can:

<table>
<thead>
<tr>
<th>Tab</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Targets</strong></td>
<td>1. Click <strong>Stop, Start, Restart</strong>, or <strong>Reload</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Restarting a service will completely stop and restart the service. Reloading a service will only reload the service's configuration files.</td>
</tr>
<tr>
<td></td>
<td>The system changes the status of the service.</td>
</tr>
<tr>
<td><strong>System Services</strong></td>
<td>• View a list of system services.</td>
</tr>
<tr>
<td></td>
<td>• Click a row to view detailed information about a service.</td>
</tr>
<tr>
<td></td>
<td>• To change the status of a service:</td>
</tr>
<tr>
<td></td>
<td>1. Click a row.</td>
</tr>
<tr>
<td></td>
<td>The service details page appears.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Stop, Start, Restart</strong>, or <strong>Reload</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Restarting a service will completely stop and restart the service. Reloading a service will only reload the service's configuration files.</td>
</tr>
<tr>
<td></td>
<td>The system changes the status of the service.</td>
</tr>
</tbody>
</table>
| Sockets | • View a list of socket services.  
• Click a row to view detailed information about a service.  
• To change the status of a service:  
  1. Click a row.  
    The service details page appears.  
  2. Click **Stop, Start, Restart, or Reload**.  
    **Note:** Restarting a service will completely stop and restart the service. Reloading a service will only reload the service's configuration files.  
    The system changes the status of the service. |
|---|---|
| Timers | • View a list of timer services.  
• Click a row to view detailed information about a service.  
• Create a new timer, as described in [Create a Timer](#).  
• To change the status of a service:  
  1. Click a row.  
    The service details page appears.  
  2. Click **Stop, Start, Restart, or Reload**.  
    **Note:** Restarting a service will completely stop and restart the service. Reloading a service will only reload the service's configuration files.  
    The system changes the status of the service. |
| Paths | • View a list of path services.  
• Click a row to view detailed information about a service.  
• To change the status of a service:  

1. Click a row.

   The service details page appears.

2. Click **Stop, Start, Restart, or Reload**.

   **Note**: Restarting a service will completely stop and restart the service. Reloading a service will only reload the service's configuration files.

   The system changes the status of the service.
Create a Timer

To create a timer:

1. In the left navigation pane, click the **Services** option. The **Services** page displays.
2. In the **Services** page heading, click the **Create Timers** button. A new window appears.
3. Enter the **Service Name**, **Description**, **Command**, and **Run** information.
4. Click **Save**. The new timer will display in the enabled section of the list.
Generate a Diagnostic Report

You can use diagnostic reports to assist with troubleshooting Tenable Core.

To generate a diagnostic report for troubleshooting:

1. Log in to Tenable Core via the user interface, as described in Log In to Tenable Core.
   The System page appears.

2. In the left navigation bar, click Diagnostic Reports.
   The Diagnostic Reports page appears.

3. Click the Create Report button.

4. A new window with a status bar will appear as the report generates.

5. When the report is complete, the status will display Done.

6. Click the Download Report button to save and print the report.
Access the Terminal

The **Terminal** page provides a console to access a user-specific command line interface.
Manage Tenable.io Web Application Scanning in Tenable Core

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**.
Configure a Proxy Server

If your organization configured a proxy server to conceal your IP address, share an internet connection on your local network, or control internet access on your network, set the proxy configuration in Tenable Core.

Before you begin:

- Log in to Tenable Core in a browser, as described in Log In to Tenable Core.

To configure a proxy server:

1. In the left navigation bar, click **Update Management**.
   
   The **Updates** page appears.

2. In the **Proxy Host** box, type the hostname and port for your proxy server in the format **hostname:port** (e.g., https://192.0.2.1:2345).

3. (Optional) In the **Proxy Username** box, type a username for your proxy server.

4. (Optional) In the **Proxy Password** box, type a password for the proxy.

5. Click **Save Proxy**.

   The system initiates your proxy configuration.
Start, Stop, or Restart Your Application

To start, stop, or restart your application via the UI:

1. Log in to Tenable Core via the user interface, as described in Log In to Tenable Core.
   The System page appears.
2. In the left navigation bar, click Tenable.io Web Application Scanning.
   The application page appears.
3. In the Installation Info section, click Start, Stop, or Restart.

To start, stop, or restart your application via the CLI:

1. Log in to Tenable Core via the Terminal page or command line interface (CLI).
   The command line appears.
2. To change the status of your application, do one of the following:
   • To start, run the following command:
     
     `pkexec systemctl start nessus-was-scanner.service`
   • To stop, run the following command:
     
     `pkexec systemctl stop nessus-was-scanner.service`
   • To restart, run the following command:
     
     `pkexec systemctl restart nessus-was-scanner.service`
   The command runs.
Manage Updates

You can use the **Updates Management** page and the **Software Updates** page to manage your Tenable Core and application updates.

If your deployment is online, Tenable recommends:

- Configuring automatic updates. For more information, see [Configure Automatic Updates](#).
- Performing on-demand updates, as needed. For more information, see [Update On Demand](#).

If your deployment is offline, you can perform offline updates. For more information, see [Update Tenable Core Offline](#).
Configure Automatic Updates

By default, automatic updates are enabled on Tenable Core.

If Tenable Core is installed or deployed in an online environment, Tenable recommends keeping automatic updates enabled. When performing an automatic update, Tenable Core retrieves and installs:

- The latest version of Tenable.io Web Application Scanner.
- The latest version of CentOS included in Tenable Core.
- The latest version of any additional packages required by Tenable Core.
- The latest version of any additional CentOS packages you installed.

To configure automatic updates:

1. Log in to Tenable Core via the user interface, as described in Log In to Tenable Core.
   
The System page appears.

2. In the left navigation pane, click Update Management.
   
The Update Management page appears.

3. In the AUTOMATIC UPDATES section, click the link in Scheduled updates can be enabled/disabled Here.
   
The Services details page appears, displaying the details for the tenablecore.update.timer service.

4. Confirm that Automatic Startup is enabled.

   **Note:** Tenable does not recommend disabling automatic updates or otherwise modifying Automatic Startup for the tenablecore.update.timer service.

5. Review the schedule for the automatic updates and modify, if needed, as described in Configure Your Automatic Update Schedule.

What to do next:
• If the update included any of the following packages, restart Tenable Core as described in Start, Stop, or Restart Your Application.
  
  • kernel
  • glibc
  • linux-firmware
  • systemd
Configure Your Automatic Update Schedule

By default, automatic updates are enabled on Tenable Core.

If Tenable Core is installed or deployed in an online environment, Tenable recommends keeping automatic updates enabled.

To configure the schedule for your automatic updates:

1. Log in to Tenable Core via the user interface, as described in Log In to Tenable Core.
   
   The System page appears.

2. In the left navigation pane, click Update Management.

   The Update Management page appears.

3. In the AUTOMATIC UPDATES section, click the link in Timer Config Line.

   The Edit Timer Configuration window appears.

4. Modify the schedule.

   **Note:** If you set both a Day of week and a Day of month, the system only performs updates on days when those two parameters are true. For example, if you set Wednesday as the Day of week and 8 as the Day of month, Tenable Core performs automatic updates only on the 8th of the month if it is a Wednesday.

   **Tip:** Tenable Core uses Eastern Time as your default time zone, unless you modify it as described in Edit Your Time Settings.

5. Click Save.

   Tenable Core modifies the schedule for automatic updates.
Update On Demand

If Tenable Core is installed or deployed in an online environment, you can perform updates on demand. When updating on demand, Tenable Core retrieves and installs:

- The latest version of Tenable.io Web Application Scanner.
- The latest version of CentOS included in Tenable Core.
- The latest version of any additional packages required by Tenable Core.
- The latest version of any additional CentOS packages you installed.

Before you begin:

- Manually refresh the packages:
  a. Log in to Tenable Core via the Terminal page or command line interface (CLI).
    The command line appears.
  b. In the command line interface (CLI) in Tenable Core, run the following command:

        ```
        sed -i.orig '/self.cache_age == 0/s/=/>/' /usr/share/PackageKit/helpers/yum/yumBackend.py
        ```

To update on demand:

1. Log in to Tenable Core via the user interface, as described in Log In to Tenable Core.
   The System page appears.

2. In the left navigation pane, click Software Updates.
   The Software Updates page appears.

3. Click Check for Updates.
   The page refreshes and displays available updates.

4. If updates are available, click Install all updates.
   Tenable Core performs the updates.
What to do next:

- If the update included any of the following packages, restart Tenable Core as described in Start, Stop, or Restart Your Application.
  - kernel
  - glibc
  - linux-firmware
  - systemd
Update Tenable Core Offline

Tenable recommends applying all offline updates, in order, to your offline Tenable Core machine. Do not skip offline updates.

For information about the contents of individual offline update files, see the Tenable Core Release Notes.

To upload a Tenable Core offline update .iso file:

1. Navigate to the Tenable Core Offline Update ISO section of the Tenable Downloads page.
2. Click and download the offline update .iso file.
3. Rename the offline update .iso file as tenable-offline-updates.iso.
4. Upload the file via scp. For example:

   ```
   scp local-is0-file.iso user@host:/srv/tenablecore/offlineiso/tenable-offline-updates.iso
   ```

   **Note:** The target line may vary; however, the destination must be the following path:
   `/srv/tenablecore/offlineiso/tenable-offline-updates.iso`

After the upload, updates are applied automatically at the configured time or on the next Tenable Core reboot. You can also manually install updates.

**Note:** Once the .iso file is uploaded, no further action is needed. However, you can make subsequent updates by replacing the existing .iso file if desired.
Manage Certificates

From the SSL/TLS Security Certificates page, you can manage the certificates used by Tenable Core and your application.

- Manage the Server Certificate
- Upload a Certificate for a Trusted Certificate Authority
- Use Different Certificates for Tenable Core and Your Application
Manage the Server Certificate

When you first deploy or install Tenable Core, Tenable provides a default server certificate for accessing the Tenable Core and application interfaces.

Tip: By default, Tenable Core uses the same certificates for Tenable Core as well as Tenable.io Web Application Scanner. To use a different server certificate for Tenable.io Web Application Scanner, see Use Different Certificates for Tenable Core and Your Application.

Note: The default certificate is not signed by a recognized certificate authority (CA). If your browser reports that the Tenable Core or application server certificate is untrusted, Tenable recommends uploading a custom server certificate signed by a trusted certificate authority (CA) for Tenable Core and application use. For more information, see Upload a Custom Server Certificate. Alternatively, you can download the Tenable-provided CA certificate (cacert.pem) for your server certificate and upload it to your browser.

If you upload a custom server certificate signed by a custom CA, you must also provide certificates in the chain to validate your custom server certificate.

For more information, see:

- Upload a Custom Server Certificate
- Remove a Custom Server Certificate
Upload a Custom Server Certificate

If you do not want to use the Tenable-provided server certificate, you can upload a custom server certificate to Tenable Core. For more information, see Manage the Server Certificate.

You cannot upload multiple custom server certificates to Tenable Core. Uploading a new file replaces the existing file.

**Tip:** By default, Tenable Core uses the same certificates for Tenable Core as well as Tenable.io Web Application Scanner. To use a different server certificate for your application, see Use Different Certificates for Tenable Core and Your Application.

Before you begin:

- Confirm your custom server certificate and key files use the *.der, *.pem, or *.crt extension.
- Move the custom server certificate and key files to a location accessible from your browser.

To upload a custom server certificate for Tenable Core:

1. Log in to Tenable Core via the user interface, as described in Log In to Tenable Core.

   The System page appears.

2. In the left navigation pane, click SSL/TLS Certificates.

   The SSL/TLS Certificates page appears.

3. Click the System Certificate tab.

4. Locate the Update Certificate section in the SERVER CERTIFICATES section.
5. **Provide your Server Certificate.**
   
a. Click **Choose File**.
   
The upload window appears.

   b. Browse to and select the file.
   
   Tenable Core loads the file.

6. **Provide your Server Key.**
   
a. Click **Choose File**.
   
The upload window appears.

   b. Browse to and select the file.
   
   Tenable Core loads the file.

7. **(Optional) If your custom server certificate is signed by a custom CA that requires an intermediate certificate to validate the custom server certificate, provide your Intermediate Certificate.**
   
a. Click **Choose File**.
   
The upload window appears.
b. Browse to and select the file.

Tenable Core loads the file.

8. (Optional) If your custom server certificate is signed by a custom CA, upload your **Custom Root CA Certificate**.
   
   a. Click **Choose File**.
      
      The upload window appears.
   
   b. Browse to and select the file.
      
      Tenable Core loads the file.

9. Click **Install Server Certificates**.

   Tenable Core uploads the files. A success message appears to confirm the upload succeeded.

10. In the left navigation pane, click **Services**.

    The **Services** page appears.

11. Restart the **Cockpit** service, as described in **Manage Services**.

    The **Cockpit** service restarts and enables the new certificate.
Remove a Custom Server Certificate

If you no longer want to use your custom server certificate for Tenable Core, you can remove the certificate and revert to using a Tenable-provided server certificate. For more information, see Manage the Server Certificate.

To remove a custom server certificate and revert to the Tenable-provided default certificate:

1. Log in to Tenable Core via the user interface, as described in Log In to Tenable Core.
   
The System page appears.

2. In the left navigation pane, click SSL/TLS Certificates.

   The SSL/TLS Certificates page appears.

3. Click the System Certificate tab.

4. In the SERVER CERTIFICATES section, in the Update Certificate section, click Reset Server Certificates.

   A confirmation window appears.

5. Click Reset.

   A success message appears to confirm the reset succeeded.
Upload a Certificate for a Trusted Certificate Authority

You can upload a trusted certificate authority (CA) certificate for any of the following purposes:

- You want to use certificate authentication for user accounts on Tenable.io Web Application Scanner.

You do not need to upload a trusted CA certificate for any other reasons. You can upload any number of trusted CA certificates to Tenable Core.

Note: By default, Tenable Core uses the same certificates for Tenable Core as well as Tenable.io Web Application Scanner. To decouple the certificates used for your Tenable Core system and your application, see Use Different Certificates for Tenable Core and Your Application.

If you decouple the certificates, Tenable Core disregards the custom CA certificate configuration on the System Certificate tab. Tenable Core does not use custom CA certificates for reasons other than the application use.

To view details about an existing certificate, click to expand the Filename section for a certificate. To remove an existing certificate, select the certificate and click the Delete button.

Before you begin:

- Confirm the trusted CA certificate is in .der, .pem, or .crt format.
- Move the trusted CA certificate to a location accessible from your Tenable Core server.

Upload a trusted CA certificate:

1. Log in to Tenable Core via the user interface, as described in Log In to Tenable Core.

   The System page appears.

2. In the left navigation pane, click SSL/TLS Certificates.

   The SSL/TLS Certificates page appears.

3. Click the System Certificate tab.

4. In the TRUSTED CERTIFICATEAuthorities section, in the Add Certificate Authority section, next to Certificate, click Choose File.
The upload window appears.

5. Browse to and select the certificate file. Tenable Core uploads the certificate file.

6. Click **Install Certificate Authority**.

   A success message appears to confirm the upload succeeded.
Use Different Certificates for Tenable Core and Your Application

By default, Tenable Core uses the same certificates for Tenable Core as well as Tenable.io Web Application Scanner. If needed, you can decouple your system and application certificates and customize them independently.

Before you begin:

- Upload a custom server certificate for Tenable Core, as described in [Upload a Custom Server Certificate](#).

To decouple and customize your application certificates:

1. Log in to Tenable Core via the user interface, as described in [Log In to Tenable Core](#).
   
   The **System** page appears.

2. In the left navigation pane, click **SSL/TLS Certificates**.
   
   The **SSL/TLS Certificates** page appears.

3. Click the application tab.
   
   The application tab appears.

   
   The application tab refreshes to display the settings in edit mode.

5. Remain on the application tab and configure the settings for your application-specific server certificate, as described in [Upload a Custom Server Certificate](#).

6. Remain on the application tab and configure the settings for one or more custom certificate authority (CA) certificate, as described in [Upload a Certificate for a Trusted Certificate Authority](#).

**Note:** If you upload a custom CA certificate on the application tab, Tenable Core disregards the custom CA certificate configuration on the **System Certificate** tab. Tenable Core does not use custom CA certificates for reasons other than the application use described in [Upload a Certificate for a Trusted Certificate Authority](#).
Application Data Backup and Restore

Backup and restore requires a connection to a remote storage host. When Tenable Core begins a scheduled or on-demand backup, your files are temporarily stored in `/opt/tenablecore/backup/spool` before being sent to the configured remote storage host.

Later, you can restore your backup data by uploading your backup file to Tenable Core.

For more information, see:

- Configure a Remote Storage Host
- Perform an On-Demand Backup
- Change the Scheduled Backup Time
- Restore a Backup

If you want to enable or disable a scheduled backup, click [Scheduled backups can be configured Here.](#)

**Note:** During a backup or a restore, Tenable Core stops the Tenable.io Web Application Scanner application service. You cannot use Tenable.io Web Application Scanner or the Tenable.io Web Application Scanner interface during this time.

After the backup or restore completes, your services restart and Tenable.io Web Application Scanner resumes normal function.

**Tip:** A VM snapshot backs up the entire VM (application installed files, application data, OS files and configurations.) To take a snapshot of your VM, see Take a Snapshot.

Remote Storage Host Requirements

The location where you store your backups must:

- Have rsync installed.
- Have an SSH server installed and running.
- Have sufficient storage space to hold your application’s backup data. While application data size and file compression varies, you could safely size your remote storage host by doubling...
the disk space currently in use on your application.

- Have a user with write permissions to manage the remote storage host location.

**Note:** Tenable Core does not manage your remote storage system. If you are concerned about space on your remote storage system, remove backup files manually when you no longer need them.
Configure a Remote Storage Host

Before you back up application data, you must establish a remote storage host with SSH key authentication and configure that host in Tenable Core.

Before you begin:

- Confirm your SSH private key for authenticating to the remote storage host is in OpenSSH key format.
- Prepare your remote storage host environment, as described in the Remote Storage Host Requirements.
- Confirm that you can log in to your remote storage host using SSH key authentication.

To configure your remote storage host:

1. Log in to Tenable Core via the user interface, as described in Log In to Tenable Core.

   The System page appears.

2. In the left navigation bar, click Remote Storage.

   The Remote Storage Configuration page appears.

3. In the Remote Host box, type the hostname for the remote storage host where you want to store your backup files.

4. In the Remote Path: box, type the location on the remote host where you want to store your backup files.

5. In the User box, type the username for a user on the remote host with edit permissions for the remote path location.

6. In the SSH private key box, paste the SSH private key for authenticating to the remote storage host.

7. Click Save Configuration.

What to do next:
• Perform a backup, as described in Perform a Backup on Demand.

• (Optional) Change your automatic backup schedule, as described in Change Your Automatic Backup Schedule.

• (Optional) Restore a backup, as described in Restore a Backup.
Perform an On-Demand Backup

Perform a backup of your application data anytime between scheduled backups. For more information about scheduled backups, see Change the Scheduled Backup Time.

Note: During a backup or a restore, Tenable Core stops the Tenable.io Web Application Scanner application service. You cannot use Tenable.io Web Application Scanner or the Tenable.io Web Application Scanner interface during this time.

After the backup or restore completes, your services restart and Tenable.io Web Application Scanner resumes normal function.

Before you begin:

- Configure your remote storage host, as described in Configure Remote Storage Host.

To perform an on-demand backup:

1. Log in to Tenable Core via the user interface, as described in Log In to Tenable Core.

   The System page appears.

2. In the left navigation bar, click Backup/Restore.

   The Backup/Restore page appears.

3. In the AVAILABLE MODULES section, select the box next to the application you want to back up.

4. Click Take Backup Now.

   The BACKUP IN PROGRESS window appears. The window disappears after the system completes the backup.

What to do next:

- (Optional) Restore the backup, as described in Restore a Backup.
Change the Scheduled Backup Time

By default, Tenable Core backs up your applications daily at 2:30 AM local time. You can edit your schedule preferences in Tenable Core to change the time and frequency of your scheduled backups.

For more information about managing your time preferences, see Edit Your Time Settings.

**Note:** Tenable Core cannot perform a backup (scheduled or on-demand) until you configure a remote storage host on your computer. For more information, see Configure a Remote Storage Host.

To change the scheduled backup time:

1. Log in to Tenable Core via the user interface, as described in Log In to Tenable Core.
   
   The System page appears.

2. In the left navigation bar, click Backup/Restore.

   The Backup/Restore page appears.

3. In the AUTOMATIC BACKUPS table, locate the Timer Config Line row.

4. Click Edit.

   The EDIT TIMER CONFIGURATION window appears.

5. On the EDIT TIMER CONFIGURATION window, update the configuration based on your desired backup frequency:

   **Note:** If you specify a day of the week and a day of the month for your scheduled backups, Tenable Core performs the backups only when those values overlap. For example, if you specify Monday and 15, Tenable Core performs your backups only on Mondays that fall on the 15th day of the month.

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Daily</td>
<td>• In the <strong>Day of Week</strong> and <strong>Day of Month</strong> boxes, type an asterisk (*).</td>
</tr>
<tr>
<td></td>
<td>• In the <strong>Hour</strong> box, type the hour when you want Tenable Core to perform a backup as an integer between 0 and 23.</td>
</tr>
<tr>
<td></td>
<td>• In the <strong>Minute</strong> box, type the minute when you want Tenable Core</td>
</tr>
</tbody>
</table>
### Performing Scheduled Backups

To perform a backup as an integer between 0 and 59.

<table>
<thead>
<tr>
<th><strong>Weekly</strong></th>
<th><strong>Monthly</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• In the <strong>Day of Week</strong> box, type the day of the week when you want Tenable Core to perform a backup (e.g., <em>Monday</em> or <em>Mon</em>).</td>
<td></td>
</tr>
<tr>
<td>• In the <strong>Day of Month</strong> box, type an asterisk (*).</td>
<td></td>
</tr>
<tr>
<td>• In the <strong>Hour</strong> box, type the hour you want Tenable Core to perform a backup as an integer between 0 and 23.</td>
<td></td>
</tr>
<tr>
<td>• In the <strong>Minute</strong> box, type the minute you want Tenable Core to perform a backup as an integer between 0 and 59.</td>
<td></td>
</tr>
<tr>
<td>• In the <strong>Day of Week</strong> box, type an asterisk (*).</td>
<td></td>
</tr>
<tr>
<td>• In the <strong>Day of Month</strong> box, type the day of the month when you want Tenable Core to perform a backup as an integer (e.g., 15).</td>
<td></td>
</tr>
<tr>
<td>• In the <strong>Hour</strong> box, type the hour you want Tenable Core to perform a backup as an integer between 0 and 23.</td>
<td></td>
</tr>
<tr>
<td>• In the <strong>Minute</strong> box, type the minute you want Tenable Core to perform a backup as an integer between 0 and 59.</td>
<td></td>
</tr>
</tbody>
</table>

6. Click **Save**.

Your scheduled backup time updates.

**What to do next:**

- (Optional) Perform an on-demand backup, as described in [Perform a Backup On Demand](#).
- (Optional) Restore the backup, as described in [Restore a Backup](#).
Restore a Backup

You can restore a backup to return an application to a prior state.

**Note:** During a backup or a restore, Tenable Core stops the Tenable.io Web Application Scanner application service. You cannot use Tenable.io Web Application Scanner or the Tenable.io Web Application Scanner interface during this time.

After the backup or restore completes, your services restart and Tenable.io Web Application Scanner resumes normal function.

Before you begin:

- Check your firewall settings and confirm that your computer can access port 8090 on Tenable Core, as described in [Access Requirements](#).

To restore an application backup:

1. Log in to Tenable Core via the user interface, as described in [Log In to Tenable Core](#).
   
   The **System** page appears.

2. In the left navigation bar, click **Backup/Restore**.
   
   The **Backup/Restore** page appears.

3. In the **UPLOAD AND RESTORE** section, click **Choose a file**.
   
   Your file explorer appears.

4. Select the desired backup file.

5. Click **Open**.

   A details window for the backup appears.

6. If prompted, confirm that you want to upgrade or downgrade your current Tenable Core application version to match the application version from your backup file.

   a. Click **Install Correct Version**.

      A confirmation window appears.
b. Click **Replace**.

Tenable Core installs the correct version of your application.

The restore widow appears.

7. Click **Restore**.

The system restores your backup to Tenable Core.

**Note**: Do not log out of Tenable Core or close your browser until after the **Uploading the archive** task is complete. If you end your session early, the restore fails.

When the restore finishes, a success message appears.

**Tip**: If the restore attempt fails, an error message appears with details and remediation instructions. Resolve the errors and click **Retry**.
SNMP Agent Configuration

If your organization uses a Simple Network Monitoring Protocol (SNMP) network management station (NMS) for device monitoring, you can install a `net-snmp` agent onto Tenable Core to report device data to your NMS.

You can use the user interface to configure common SNMPv2 or SNMPv3 settings. To configure other advanced or uncommon SNMP settings, use the CLI.

- Configure an SNMP Agent via the User Interface
- Configure an SNMP Agent via the CLI

To stop, start, restart, or reload the SNMP service in Tenable Core, or to view SNMP logs, see Manage Services.
Configure an SNMP Agent via the User Interface

**Required User Role:** Administrator with *Reuse my password for privileged tasks* enabled

If your organization uses a Simple Network Monitoring Protocol (SNMP) network management station (NMS) for device monitoring, you can install a `net-snmp` agent onto Tenable Core to report device data to your NMS.

You can use the user interface to configure common SNMPv2c or SNMPv3 settings. To configure other advanced or uncommon SNMP settings, use the CLI as described in [Configure an SNMP Agent via the CLI](#).

To install and configure an SNMP agent on Tenable Core via the user interface:

1. Log in to Tenable Core via the user interface, as described in [Log In to Tenable Core](#).
   
   The **System** page appears.

2. In the left navigation bar, click **SNMP**.
   
   If you already installed an SNMP agent on Tenable Core, the **SNMP** page appears. If you do not have an SNMP agent installed on Tenable Core, the **Install SNMP Packages** window appears.

3. (Optional) In the **Install SNMP Packages** window, click **Install SNMP** to install the SNMP service.
   
   Tenable Core installs the SNMP service and opens inbound ports 161 and 162 on Tenable Core.
   
   The **SNMP** page appears.

4. In the **SNMP common setup** section, configure the contact properties you want to appear on your NMS for this instance of Tenable Core.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact</td>
<td>A name, email address, or other identifier for the person you want to list as the contact for questions about this instance of Tenable Core.</td>
</tr>
</tbody>
</table>
5. If you want to grant an SNMPv2c NMS access to Tenable Core, in the **SNMPv2c access control setup** section, configure one or both of the settings:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>read-only access community name</td>
<td>Specifies the read-only community string for the SNMPv2c NMS.</td>
</tr>
<tr>
<td>read-write access community name</td>
<td>Specifies the read-write community string for the SNMPv2c NMS.</td>
</tr>
</tbody>
</table>

6. If you want to grant an SNMPv3 NMS read-only access to Tenable Core, in the **SNMPv3 access control setup** section, configure the settings:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read-only Hash algorithm</td>
<td>Specifies the read-only hash algorithm for the SNMPv3 NMS.</td>
</tr>
<tr>
<td>Read-only access username</td>
<td>Specifies the username and password for an account on the SNMPv3 NMS.</td>
</tr>
<tr>
<td>Read-only access user password</td>
<td></td>
</tr>
</tbody>
</table>

7. If you want to grant an SNMPv3 NMS read-write access to Tenable Core, in the **SNMPv3 access control setup** section, configure the settings:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read-write Hash algorithm</td>
<td>Specifies the read-write hash algorithm for the SNMPv3 NMS that you want to grant read-write access on Tenable Core.</td>
</tr>
<tr>
<td>Read-write</td>
<td>Specifies the username and password for an account on the</td>
</tr>
<tr>
<td>access username</td>
<td>SNMPv3 NMS.</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Read-write access user password</td>
<td></td>
</tr>
</tbody>
</table>

8. Click **Save Configuration**.

Tenable Core saves your SNMP configuration.
**Configure an SNMP Agent via the CLI**

**Required User Role:** Root user

If your organization uses a Simple Network Monitoring Protocol (SNMP) network management station (NMS) for device monitoring, you can install a net-snmp agent onto Tenable Core to report device data to your NMS.

To install and configure an SNMP agent on Tenable Core via the CLI:

1. Prepare the net-snmp agent configuration file and add it to Tenable Core, as described in the Net-SNMP Documentation.
2. Log in to Tenable Core via the [Terminal page](#) or command line interface (CLI).
   - The command line appears.
3. In the /etc/snmp/ directory, open the snmpd.local.conf file.
   - The file opens.
4. Locate the IncludeFile line in the file.
5. Comment out the IncludeFile line to instruct Tenable Core to ignore all current and future configurations on the SNMP page of the Tenable Core user interface.
   - Tenable Core ignores SNMP configurations in the Tenable Core user interface.
Take a Virtual Machine Snapshot

You can take a snapshot to back up the your entire machine, including application-installed files, application data, OS files and configurations.

Before you begin:

- Stop your instance of Tenable Core + Tenable.io Web Application Scanning, as described in Start, Stop and Restart Tenable Core.

To take a snapshot of Tenable Core:

1. Take a snapshot, as described in the documentation for your environment.