## Introduction

Congratulations on starting your trial of Nessus Professional, the de-facto industry standard vul- nerability assessment solution for security practitioners! Nessus Professional is the most com- prehensive vulnerability assessment solution on the market today, designed to simplify assessments, save time, and provide accurate visibility into your networks.

This guide will assist you to ensure you get the most out of your trial. This guide is intended to be a starting point as you familiarize yourself with the interface, features, and capabilities of Nessus Pro- fessional. For an in-depth guide into all the options available in Nessus Professional, see the full [Nes-](https://docs.tenable.com/nessus/Content/GettingStarted.htm) [sus User Guide](https://docs.tenable.com/nessus/Content/GettingStarted.htm).

## Trial License vs Full License

During your Nessus Professional trial, you can try out some of the product’s functionality, including conducting scans for up to 32 IP addresses and exporting reports. When you purchase the full Nessus Professional license, you will unlock expanded functionality and additional features, including scan- ning for unlimited IP addresses, scan scheduling, compliance and auditing tools, product support, and more. You can explore all of the features available in Nessus Professional by checking out the [inter-](https://www.tenable.com/nessus-demo) [active Nessus Professional demo](https://www.tenable.com/nessus-demo).

# Get Started

## Trial Email

Register for Nessus Professional Free trial account. <https://www.tenable.com/products/nessus/nessus-professional>

After signing up for a Nessus trial, you should receive an email with instructions for how to activate your Tenable Community account. You will be prompted to create a log-in password and start your trial.

If you have already successfully activated your Tenable Community account, you can navigate to your Nessus trial management page. You should see your license key, as well as a link to **Download Nes- sus to Start Trial**.

## Download and Install Nessus

To download Nessus, click **Download Nessus to Start Trial** in your Tenable Community account page or go directly to the Nessus downloads page: [www.tenable.com/downloads/nessus](http://www.tenable.com/downloads/nessus).

There is a single Nessus package per operating system and processor. Download the appropriate pack- age for your operating system. In our case we have installed Nessus on our Kali Linux Instance.

**Note:** You cannot download a Nessus trial on a VMware Virtual Appliance.

Download the Kali Linux package based on your processor architecture, for example

###### Example Nessus package file names and descriptions

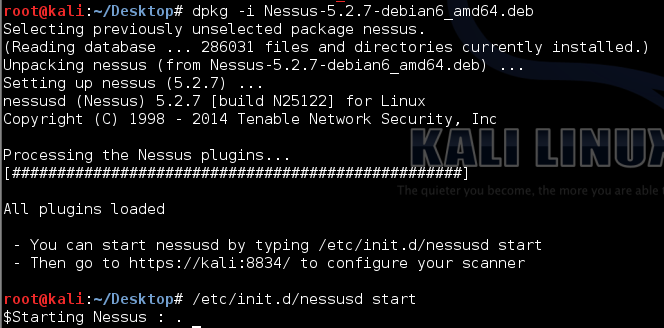
|  |  |
| --- | --- |
| **Nessus Packages Package Descriptions** | |
| Nessus-<version number>- Win32.msi | Nessus <version number> for Windows 7, 8, and 10 - i386 |
| Nessus-<version number>- x64.msi | Nessus <version number> for Windows Server 2008, Server 2008 R2\*, Server 2012, Server 2012 R2, 7, 8, and 10 - x86-64 |
| Nessus-<version number>- debian6\_amd64.deb | Nessus <version number> for Debian 6 and 7 / Kali Linux - AMD64 |
| Nessus-<version num- ber>.dmg | Nessus <version number> for Mac OS X 10.8, 10.9, and 10.10 - x86- 64 |

|  |  |
| --- | --- |
| **Nessus Packages Package Descriptions** | |
| Nessus-<version number>- fc20.x86\_64.rpm | Nessus <version number> for Fedora 20 and 21 - x86\_64 |
| Nessus-<version number>- suse10.x86\_64.rpm | Nessus <version number> for SUSE 10.0 Enterprise - x86\_64 |
| Nessus-<version number>- ubuntu1110\_amd64.deb | Nessus <version number> for Ubuntu 11.10, 12.04, 12.10, 13.04,  13.10, and 14.04 - AMD64 |

**Install and Configure Nessus**

Install Nessus

Once you've downloaded the appropriate Nessus Debian package to your Kali Linux installation, run the following commands to install and start Nessus (it is assumed that your Kali Linux is configured with access to the Internet)



Now you have to start nessusd by typing /etc/init.d/nessusd start.

Each time you restart the machine you must start nessusd first then only you can access Nessus.

Now you can access nessus from your browser by hitting url provided after installation of nessus.

For ex in above case: <https://kali:8834/>

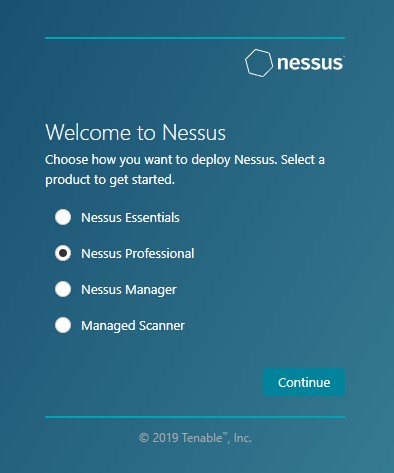
## Configure Nessus

###### Before You Begin

When you access Nessus in a web browser, a warning appears regarding a connection privacy prob- lem, an untrusted site, an unsecure connection, or a related security certificate issue. This is expected and normal behavior. Nessus provides a self-signed SSL certificate.

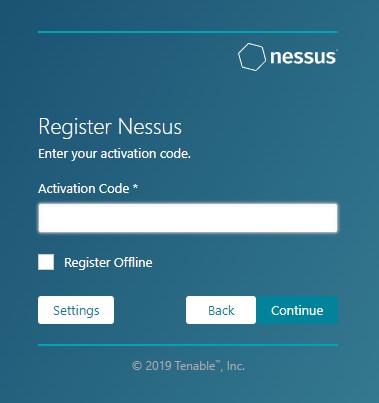
###### To configure Nessus:

1. On the **Welcome to Nessus** screen, select **Nessus Professional**.



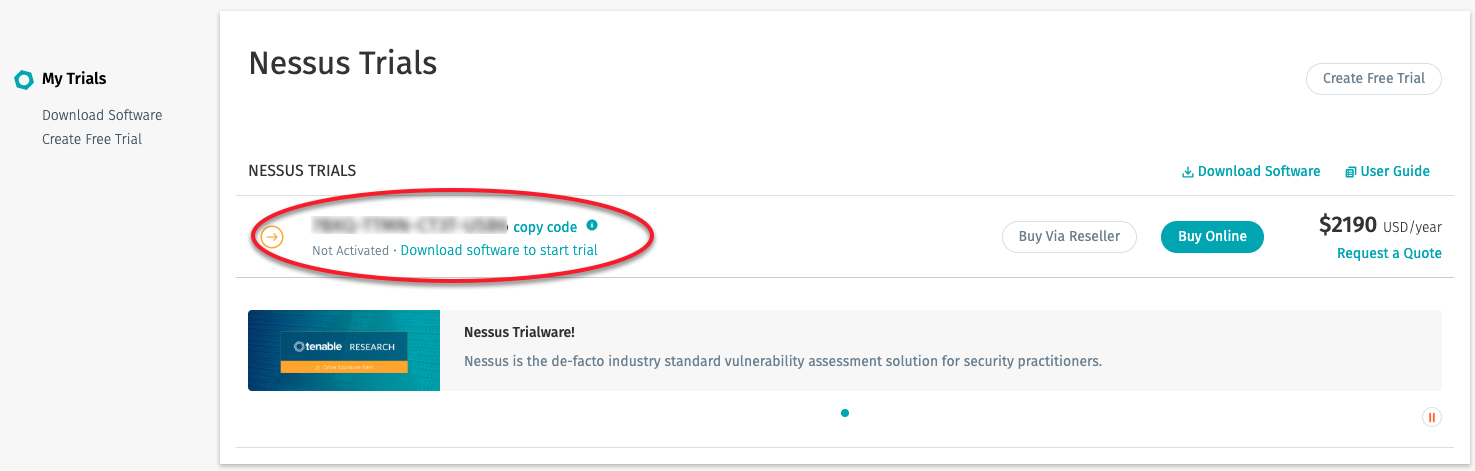
1. Click **Continue**.

The **Register Nessus** screen appears.



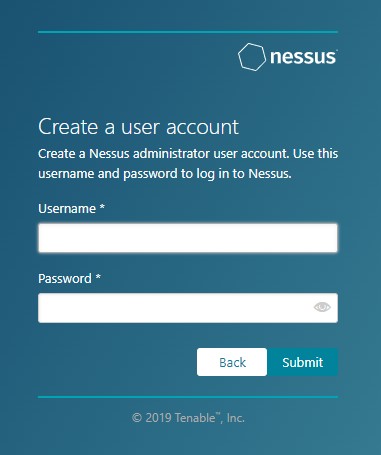
1. Type your **Activation Code**.

The activation code is available on your Tenable Community account page.



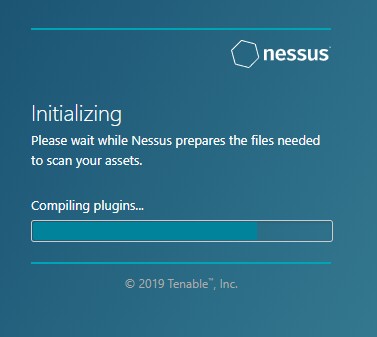
1. Click **Continue**.

The **Create a user account** screen appears.



1. Create a Nessus administrator user account that you use to log in to Nessus:
   1. In the **Username** box, enter a username.
   2. In the **Password** box, enter a password for the user account.
2. Click **Submit**.

Nessus finishes the configuration process, which may take several minutes.



1. Using the administrator user account, you created, **Sign In** to Nessus.

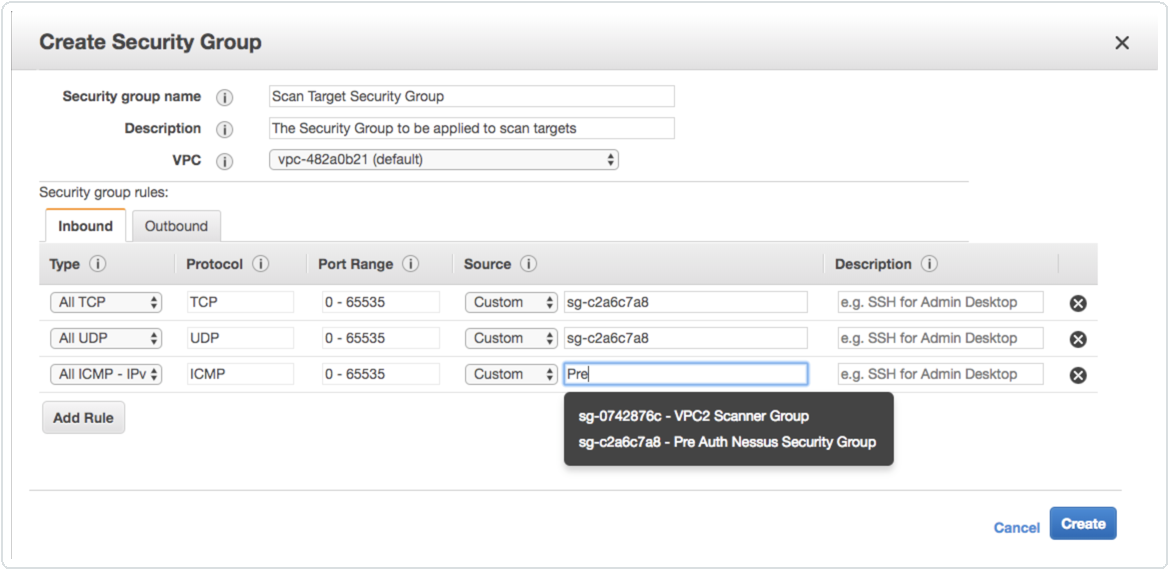


**Modify Security Group to Permit Scanning**

The following steps describe how to create a security group that allows all inbound access from the Nessus scan-ner. Any EC2 instance that this security group is applied to can be scanned by Nessus scanner.

1. In the left-hand menu, click **Security Groups**.
2. Select the appropriate security group which you have used while deployment.
3. In the **Security group** create entries for **TCP, UDP, ICMP** as shown in below image.

Enter private IP of Kali Linux instance as source.



1. Click **Create**.

# Navigate Nessus

The top navigation bar displays links to the two main pages: **Scans** and **Settings**. You can perform all Nessus primary tasks using these two pages. Click a page name to open the corresponding page.



|  |  |
| --- | --- |
| **Item Description** | |
|  | Toggles the **Notifications** box, which displays a list of noti- fications, successful or unsuccessful login attempts, errors, and system information generated by Nessus. |
| Username | Displays a drop-down box with the following options: **My Account**, **What's New**, **Documentation**, and **Sign Out**. |

# Settings

The **Settings** page contains the information and settings related to your Nessus installation and license.

For the purposes of your trial, you can leave most settings at their default value. From the **Settings** page, you can do the following:

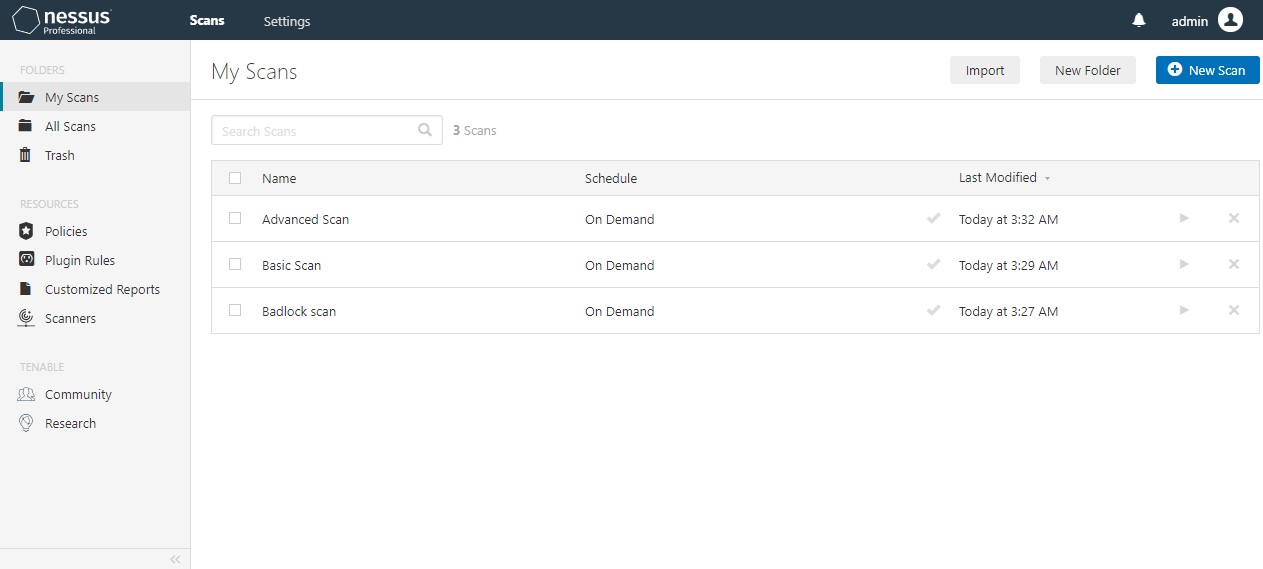
* View information such as the license expiration date and software version.
* (Optional) Configure proxy settings if you skipped it during initial configuration or need to change the settings.
* Change your password.
* View scanner health.

For more information on configuring settings, see [Settings](https://docs.tenable.com/nessus/Content/Settings.htm) in the *Nessus User Guide*.

On the **Scans** page, you can create, view, and manage scans and resources.

To access the **Scans** page, in the top navigation bar, click **Scans**. The left navigation bar displays the

**Folders** and **Resources** sections.



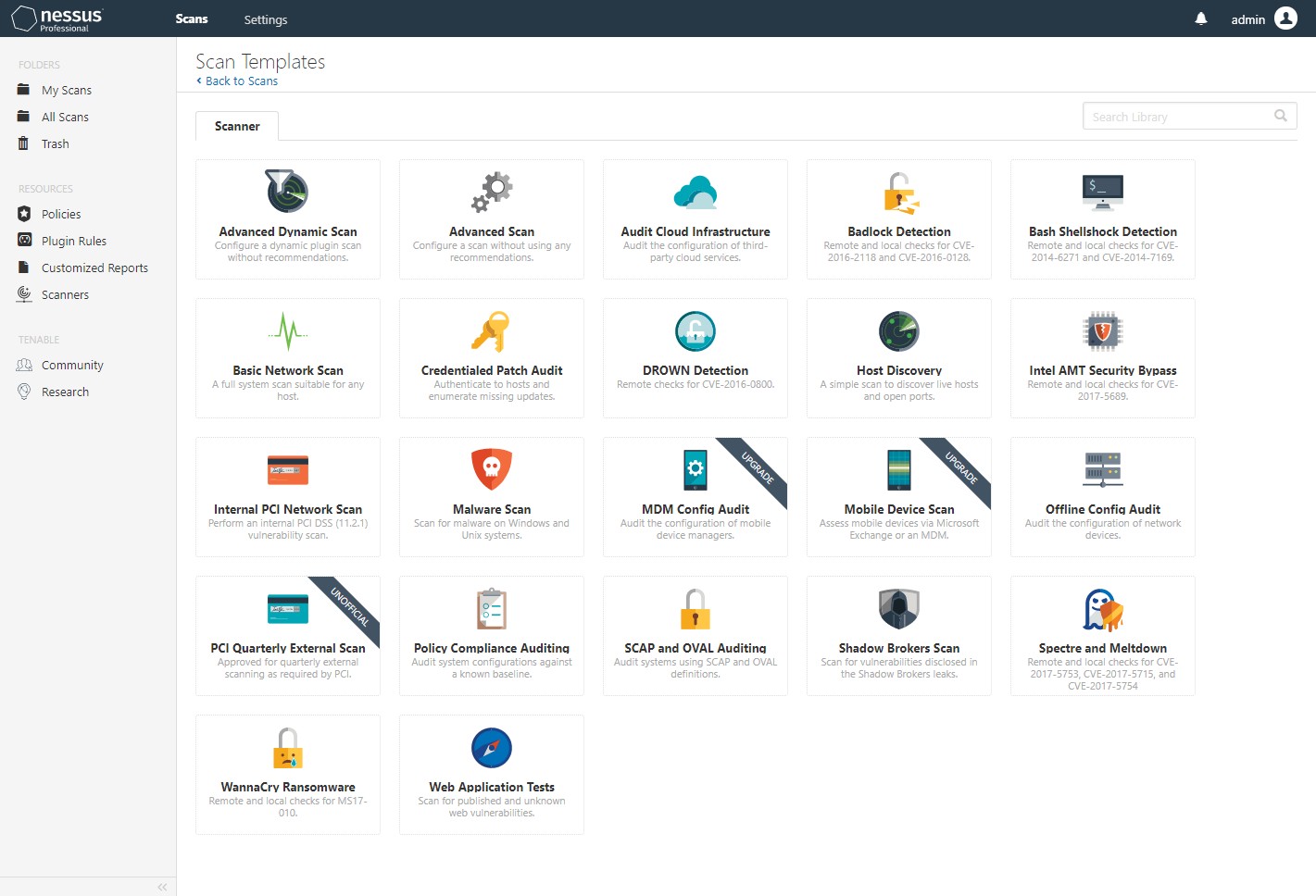
1. In the top navigation bar, click **Scans**. The **My Scans** page appears.
2. In the upper right corner, click the **New Scan** button. The **Scan Templates** page appears.
3. Click the scan template that you want to use.
4. Configure the scan's [settings](#_bookmark7).
5. If you want to launch the scan later, click the **Save** button.

The scan is saved.

-or-

If you want to launch the scan immediately, click the  button, and then click **Launch**. The scan is saved and launched.

Templates facilitate the creation of scans and policies.



The Nessus interface provides brief explanations of each template in the product. Some templates may not be available during a trial and are available when you purchase a fully-licensed copy of Nessus Pro- fessional. To see a full list of the types of templates that are available in Nessus, see [Scan and Policy](https://docs.tenable.com/nessus/Content/ScanAndPolicyTemplates.htm) [Templates](https://docs.tenable.com/nessus/Content/ScanAndPolicyTemplates.htm) in the *Nessus User Guide*.

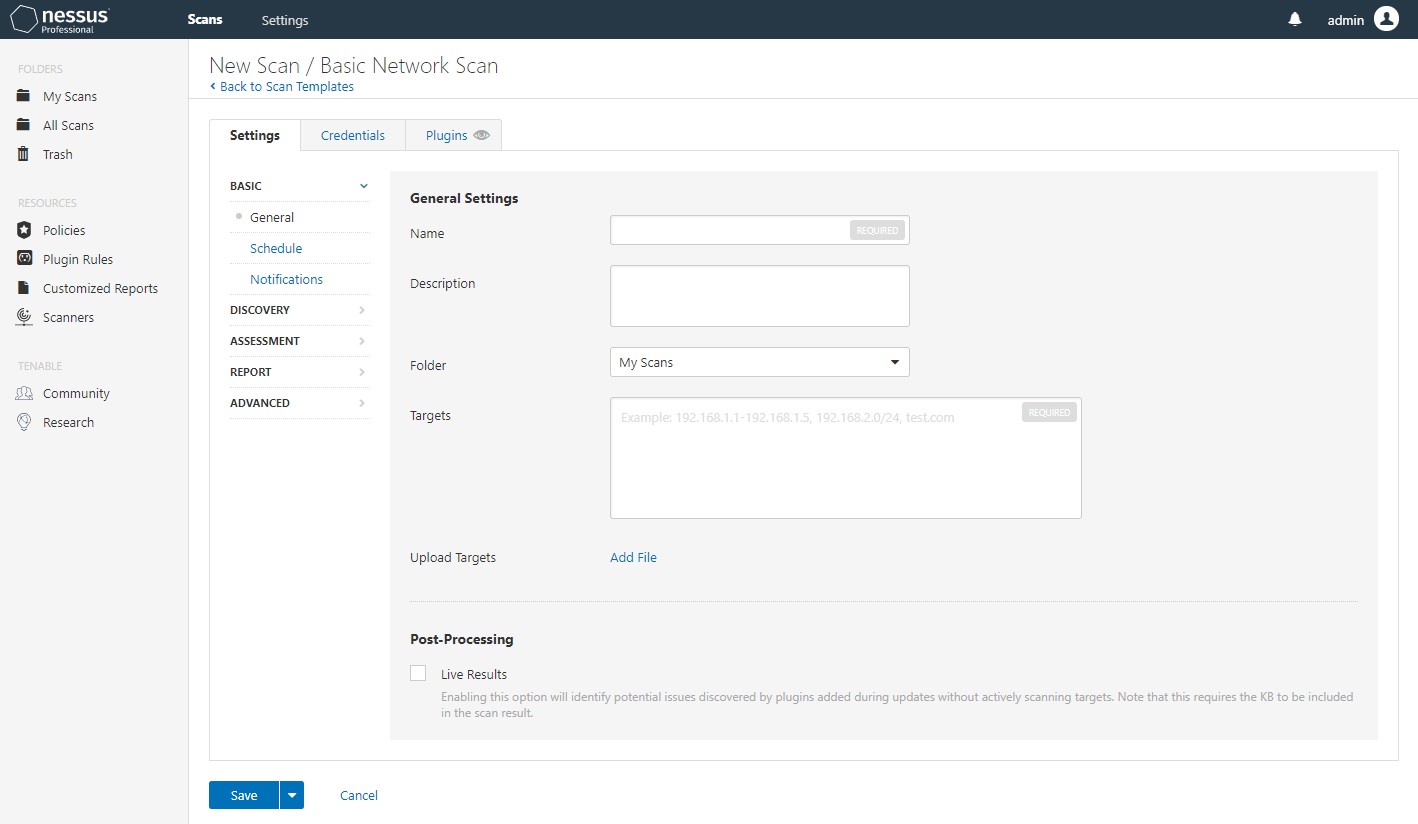
The template you choose determines what settings are configurable and how they can be set. For a detailed explanation of scan settings, refer to [Scan and Policy Settings](https://docs.tenable.com/nessus/Content/TemplateSettings.htm) in the *Nessus User Guide*.

A policy is a set of predefined configuration options related to performing a scan. After you create a policy, you can select it as a template in the User Defined tab when you create a scan. For more inform- ation, see [Create a Policy](https://docs.tenable.com/nessus/Content/CreateAPolicy.htm) in the *Nessus User Guide*.

# Example: Configure a Basic Network Scan

For your trial period, Tenable recommends using the **Basic Network Scan** template. This template has several default settings preconfigured, which allows you to quickly perform your first scan and view results without a lot of effort. This example walks you through configuring a basic network scan.

###### Configure Basicsettings section.



The following table describes the **Basic** settings:

|  |  |
| --- | --- |
| **Setting Description** | |
| **Name** | The name of the scan or policy. The name appears in the Nessus interface. |
| **Description** | (Optional) A description of the scan or policy. |
| **Folder** | The folder where the scan appears after you save it. |
| **Targets** | Specifies one or more targets to be scanned. If you select a target group or upload a targets file, you are not required to specify additional targets. |

**Note:** For your trial period, you can scan up to 32 targets total. A fully- licensed installation of Nessus Professional allows you to scan an unlimited number of targets.

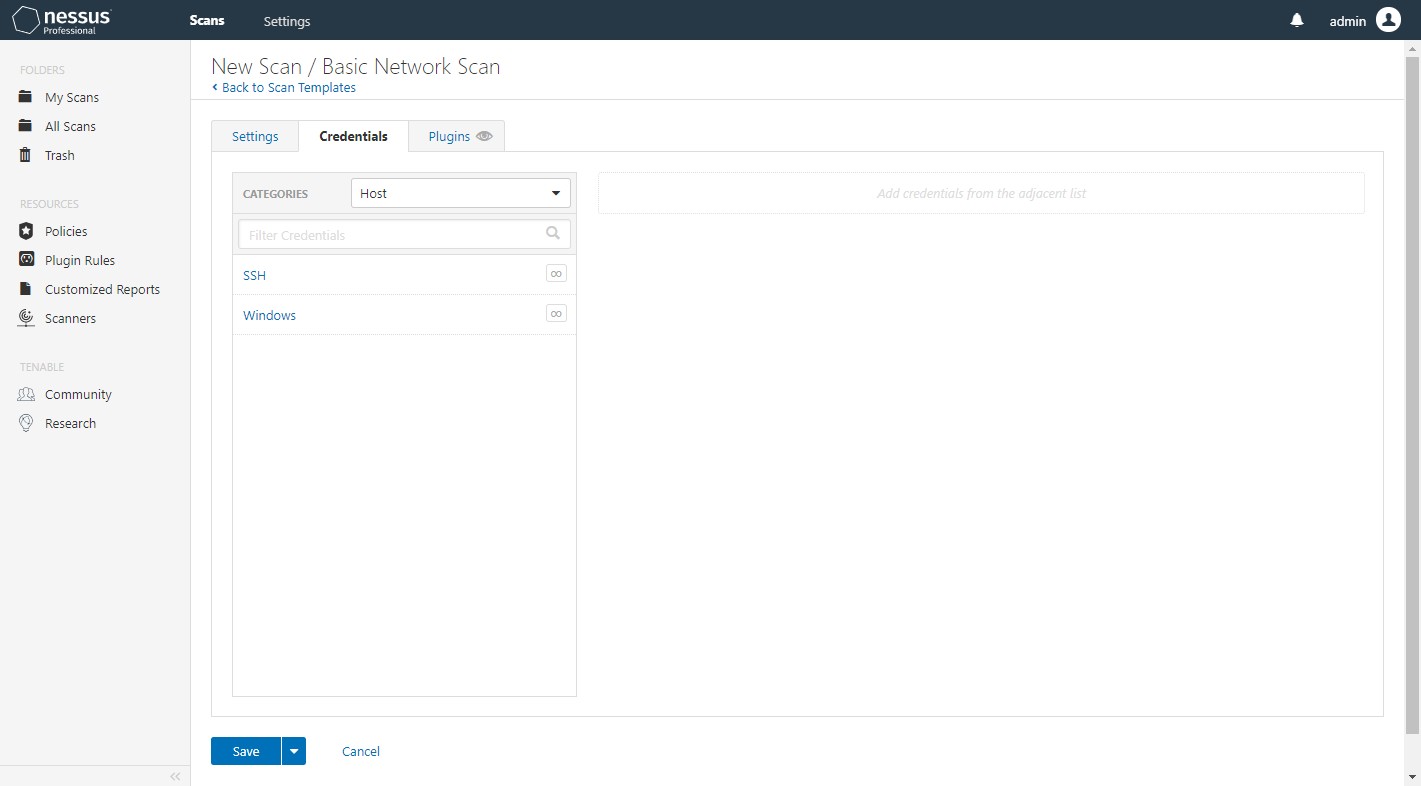
###### Configure remaining settings.

Although you can leave the remaining settings at their preconfigured defaults, Tenable recom- mends reviewing the **Discovery**, **Assessment**, **Report**, and **Advanced** settings to ensure that they are appropriate for your environment.

For more information, see the [Scan Settings](https://docs.tenable.com/nessus/Content/TemplateSettings.htm) documentation in the *Nessus User Guide.*

###### Configure credentials.

To configure **Credentials** for a scan, click the **Credentials** tab.



This allows credentialed scans to run, which can result in much more complete results and a more thorough evaluation of the vulnerabilities in your environment.

3.1 Click on SSH option provided on left side in credentials tab.

3.2 After this you’ll get options to enter username and SSH private key file which is used to SSH into machine.

3.3 Here each deployment/service is deployed using Bosh and user named vcap is automatically gets created. We must enter username as vcap and SSH private key in order to get detailed results.

In our case all the services are deployed using Bosh hence, bosh private keys can be used to SSH into deployments. These keys are stored on S3 buckets.

3.4 You must ensure that proper keys are passed to scan as it will not throw any error, while performing scans. But you’ll get an error in reports in plugin output section.

###### Launch scan.

After you have configured all your settings, save and launch the scan.

The time it takes to complete a scan involves many factors such as network speed and con- gestion, so the scan may take some time to run.

# Scan Results

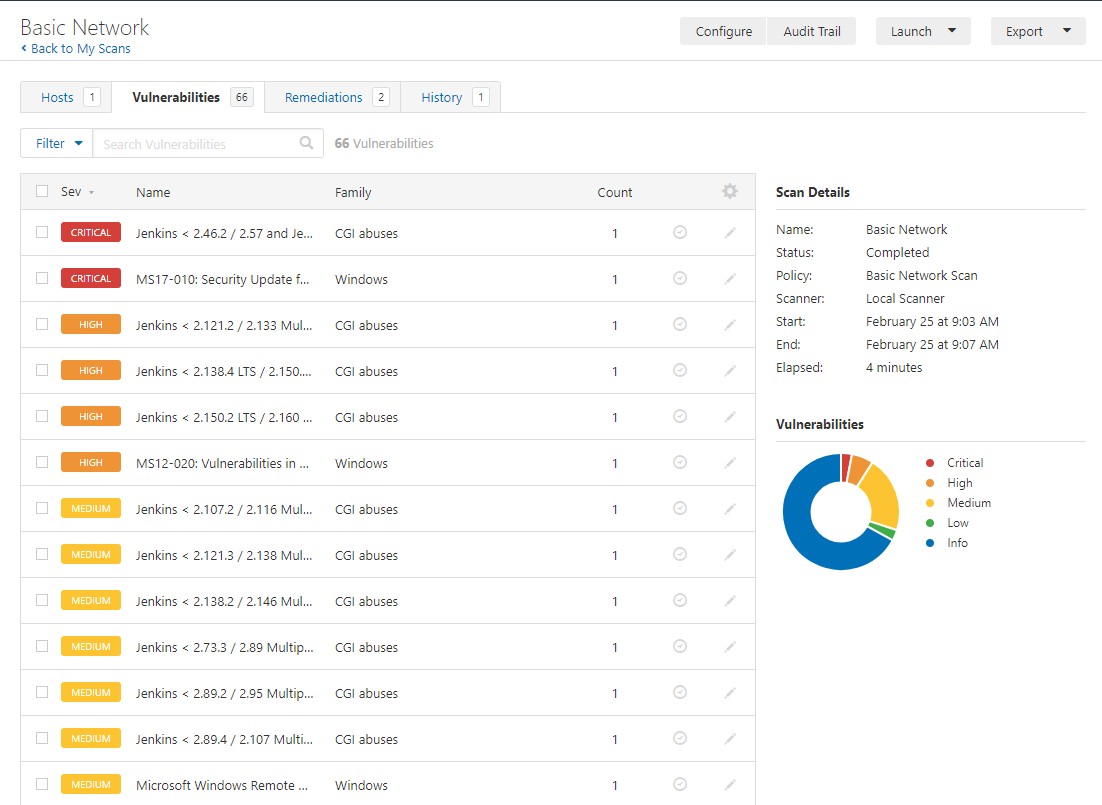
You can view scan results to help you understand your organization’s security posture and vul- nerabilities. Color-coded indicators and customizable viewing options allow you to customize how you view your scan’s data.

You can view scan results in one of several views:

|  |  |
| --- | --- |
| **Page Description** | |
| Hosts | Displays all scanned targets. |
| Vulnerabilities | Lists identified vulnerabilities, sorted by severity. |
| Remediations | If the scan's results include **Remediation** information, this list displays sug- gested remediations that address the highest number of vulnerabilities. |
| Notes | Displays additional information about the scan and the scan’s results. |
| History | Displays a listing of scans: **Start Time**, **End Time**, and the **Scan Statuses**. |

Viewing scan results by vulnerabilities gives you a view into potential risks on your assets.

# View Vulnerabilities

You can view vulnerabilities found by a scan, or vulnerabilities found on a specific host by a scan. When you drill down on a vulnerability, you can view information such as plugin details, description, solution, output, risk information, vulnerability information, and reference information.

###### To view vulnerabilities:

1. In the top navigation bar, click **Scans**. The **My Scans** page appears.
2. Click the scan for which you want to view vulnerabilities. The scan's results page appears.
3. Do one of the following:
   * Click a specific host to view vulnerabilities found on that host.
   * Click the **Vulnerabilities** tab to view all vulnerabilities. The **Vulnerabilities** tab appears.
4. To view details for the vulnerability, click the vulnerability row.

The vulnerability details page appears, displaying plugin information and output for each instance on a host.

# Create a Scan Report

You can create a scan report to help you analyze the vulnerabilities and suggested remediations on affected hosts. You can create a scan report in PDF, HTML, or CSV format, and customize it to contain only certain information.

When you create a scan report, it includes the results that are currently visible on your scan results page. You can also select certain hosts or vulnerabilities to further narrow your report.

To export a scan in Nessus or Nessus DB format, which allows you to import the scan into another Nes- sus instance or Tenable product, see [Export a Scan](https://docs.tenable.com/nessus/Content/ExportAScan.htm) in the *Nessus User Guide*.

###### To create a scan report:

1. In the top navigation bar, click **Scans**. The **My Scans** page appears.
2. Click a scan.

The scan's results page appears.

1. (Optional) To create a scan report that includes specific scan results, do the following:
   * Search to narrow your scan results.
   * Use filters to narrow your scan results.
2. In the upper-right corner, click **Report**.
3. From the drop-down box, select the format in which you want to export the scan results.
4. Configure the report for your selected format:

**CSV**

1. Select the check boxes for the columns you want to appear in the CSV report.

**Note:** To select all columns, click **Select All**. To clear all columns, click **Clear**. To reset columns to the system default, click **System**.

1. (Optional) To save your current configuration as the default for CSV reports, select the

**Save as default** check box.

1. Click **Generate Report**.

Nessus creates the scan report.

### HTML or PDF

Do one of the following:

* + Create a high-level summary scan report:
  1. Select **Executive Summary**.
  2. Click **Generate Report**.

Nessus creates the scan report.

* + Create a custom scan report:

1. Select **Custom**.
2. Configure the following settings:
   * **Data** — Select **Vulnerabilities Remediations** to include that information in the report.
   * **Group Vulnerabilities By** — From the drop-down box, select whether vul- nerabilities should be grouped by **Host** or **Plugin**.
     + If you group by **Host**, select whether to include **Scan Information** and

**Host Information**.

* + If your report includes **Vulnerabilities**, select the **Vulnerabilities Details** that you want to include. If a vulnerability does not have available data for the details you selected, Nessus omits it for that result.
  + **Formatting Options** (PDF only) — Select whether to **Include page breaks between vulnerability results**.

1. (Optional) To save your current configuration as the default for HTML reports, select the **Save as default** check box.
2. Click **Generate Report**.

**Nessus creates the scan report.**