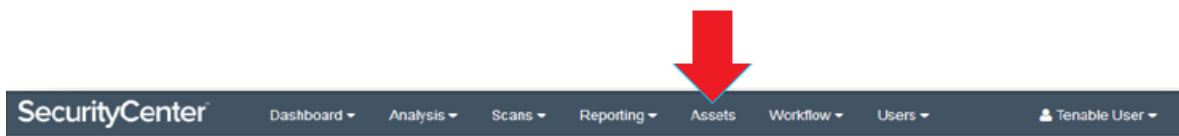


How to Add Assets to SecurityCenter

SecurityCenter allows you to focus dashboards and reports on specific network segments, systems, or repositories that you want to analyze. One way to do this is through the use of assets.

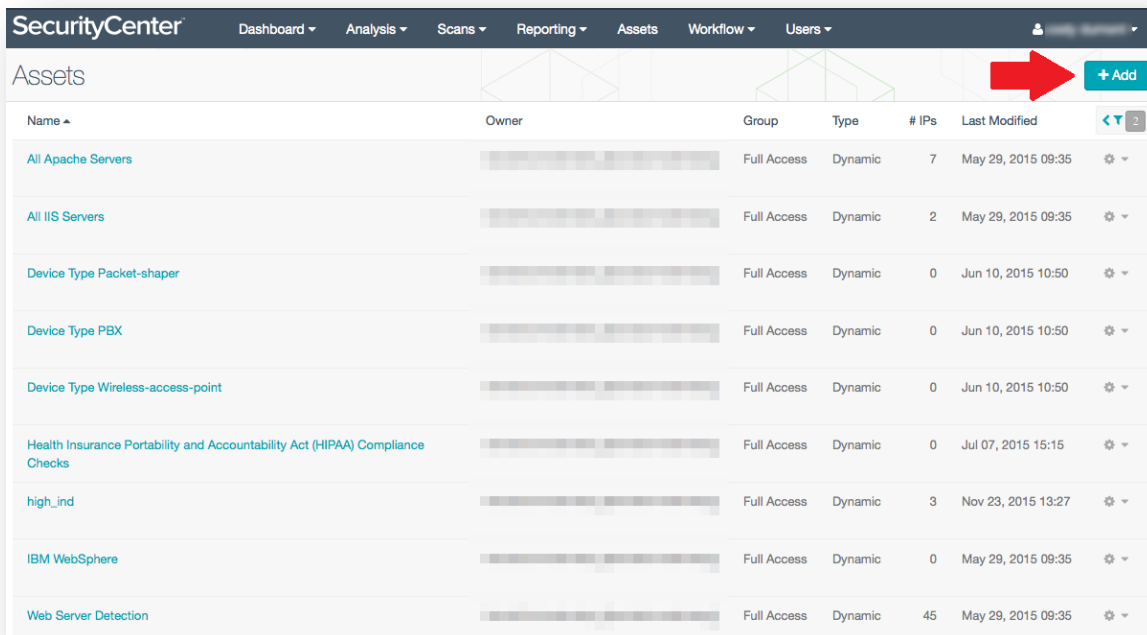
There are several types of assets; however, this guide will discuss two: dynamic and custom. Dynamic assets are dynamically discovered using filters to identify systems with similar characteristics, such as all systems with critical severity vulnerabilities discovered. Static assets are manually entered by an administrator and can be based on IP address, subnet, or range of IP addresses.

All assets can be added or accessed through the top-level menu in SecurityCenter:

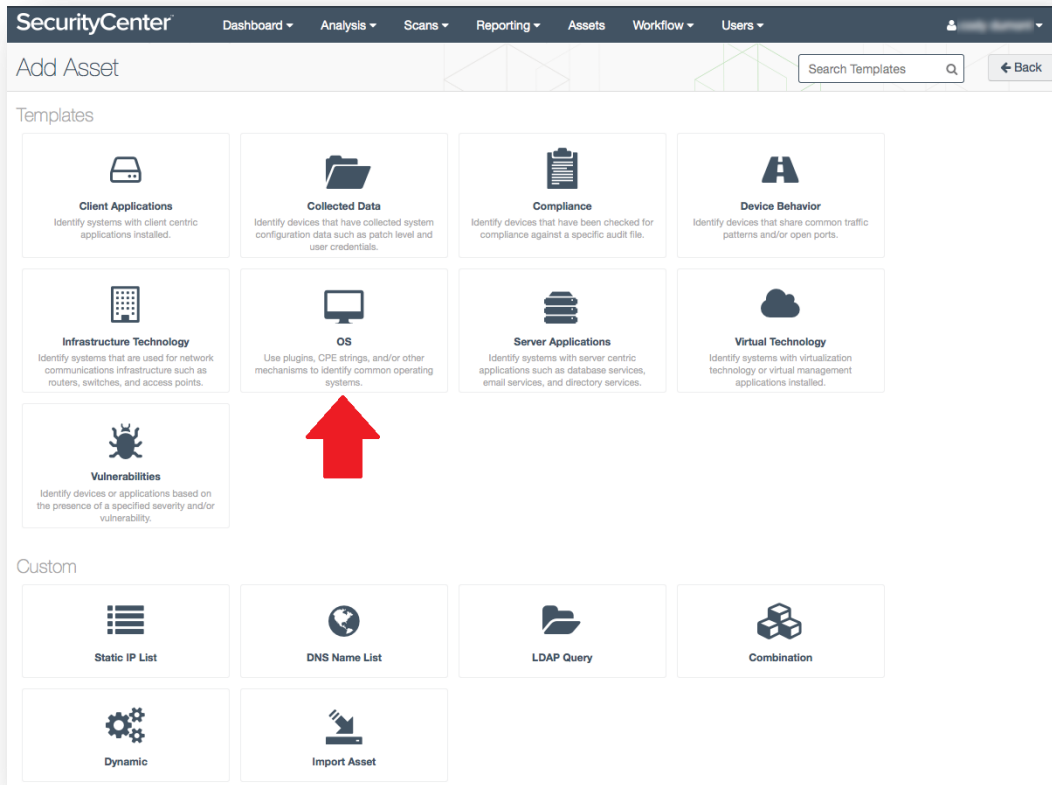


Adding a Dynamic Asset

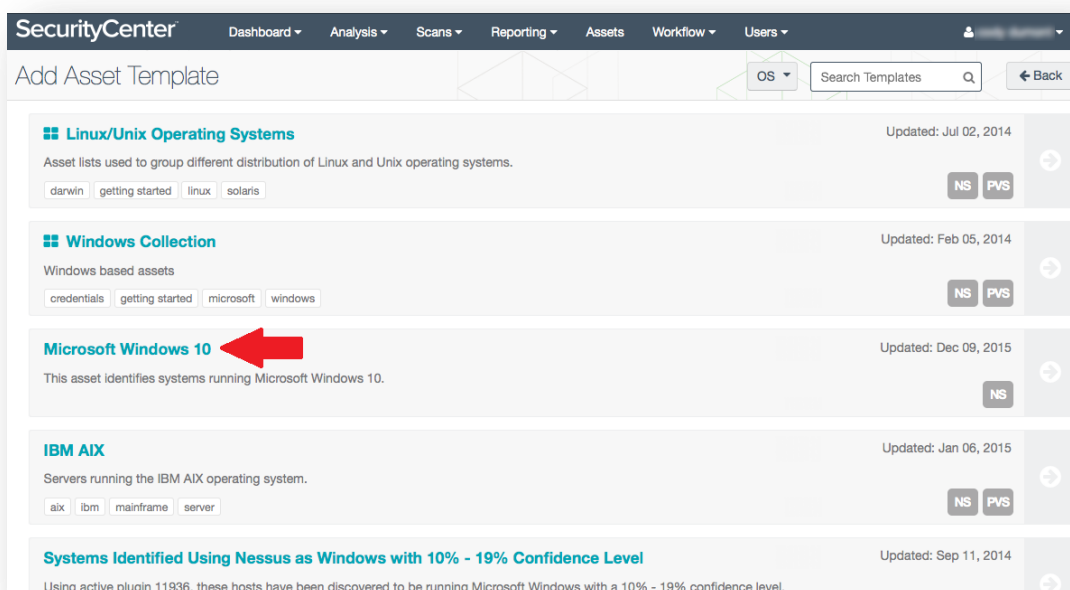
The Assets page will show you a list of all your current assets. To add a dynamic asset simply click on the **Add** button at the top right of the screen.



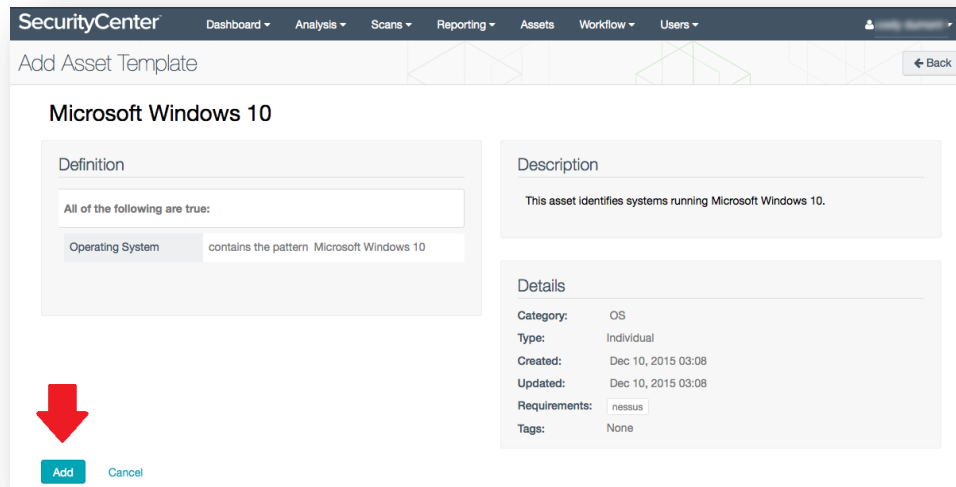
On the next screen, pick the type of asset to add. In this case, we want to add Microsoft Windows 10 systems, so we'll click on OS.



This will bring up the **Add Asset Template**, which shows a list of all OS-based asset templates available in the feed. To add an asset template for Windows 10 systems, we click on **Microsoft Windows 10**.

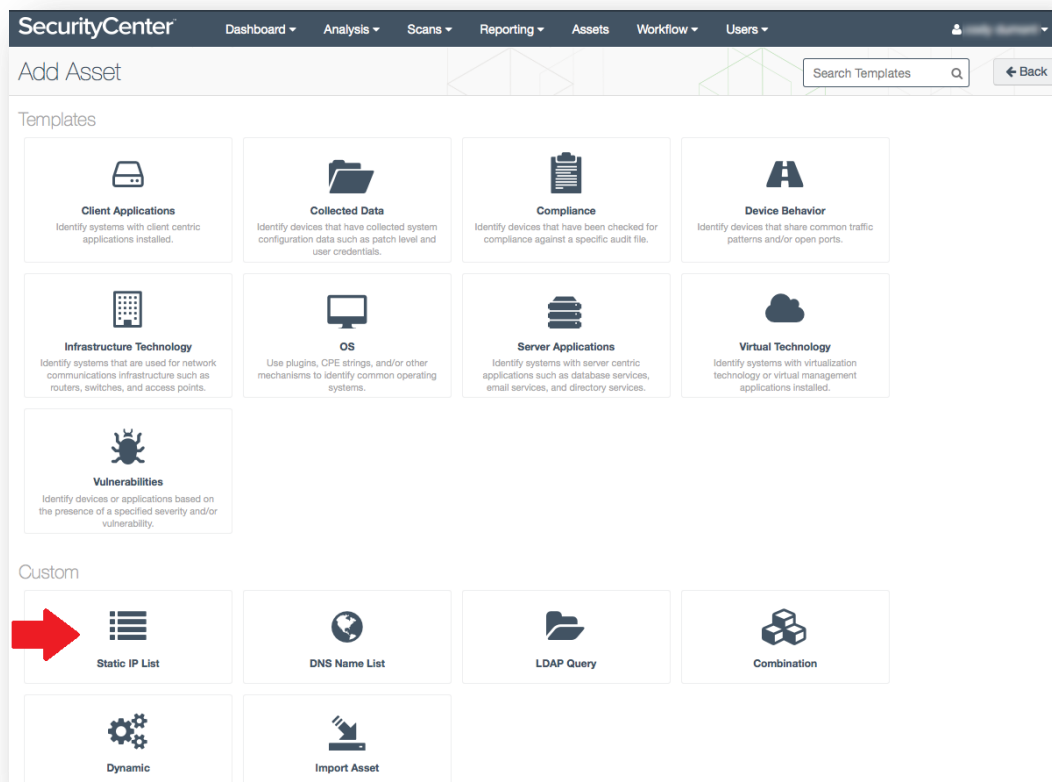


On the following page, click **Add** and your dynamic asset is added.



Adding a Custom Asset

To add a custom asset, navigate to the Assets page and click on **Add** in the upper right-hand corner of the screen. However, when the Add Asset screen appears, you'll select an option under the **Custom** heading. You can add custom assets by IP address list, DNS name list, LDAP query, and more. For this example, we'll be adding a **Static IP List** asset.



Click on **Static IP List** to bring up the **Add Static IP List Asset** screen. Here you will enter the asset name you want to create and the relevant IP address(es), then click **Submit**. In this case, we are creating an asset named “LAN 113”.

SecurityCenter Dashboard Analysis Scans Reporting Assets Workflow Users

Add Static IP List Asset

General

Name* LAN 113

Description Subnet 10.31.113.0/24

IP Addresses* 10.31.113.0/24 Choose File Clear IPs

Include Unmanaged Hosts

Submit Cancel

You will see your newly created custom asset in your Asset List within a few minutes.

SecurityCenter Dashboard Analysis Scans Reporting Assets Workflow Users

Assets

+ Add

Name	Owner	Group	Type	# IPs	Last Modified
LAN 104		Full Access	Static IP List	256	2 days ago
LAN 113		Full Access	Static IP List	256	2 days ago
LAN 31.100		Full Access	Static IP List	256	2 days ago

For More Information

If you would like more information about adding and using assets with dashboards, see our [“How to Use Assets with Dashboards”](#) how-to guide. You can also visit the [SecurityCenter Discussion Forum](#) and [SecurityCenter Dashboard blog](#), or refer to your SecurityCenter User Guide.



About Tenable Network Security

Tenable Network Security transforms security technology for the business needs of tomorrow through comprehensive solutions that provide continuous visibility and critical context, enabling decisive actions to protect your organization. Tenable eliminates blind spots, prioritizes threats, and reduces exposure and loss. With more than one million users and more than 20,000 enterprise customers worldwide, organizations trust Tenable for proven security innovation. Tenable's customers range from Fortune Global 500 companies, to the Department of Defense, to mid-sized and small businesses in all sectors, including finance, government, healthcare, higher education, retail, and energy. Transform security with Tenable, the creators of Nessus and leaders in continuous monitoring, by visiting tenable.com.