Tenable for ServiceNow

Last Updated: March 19, 2018

Table of Contents

Introduction

This document describes how to deploy SecurityCenter for integration with ServiceNow Security Operations. Please email any comments and/or suggestions to support@tenable.com.

As the leader in IT Service Support Management (ITSSM), ServiceNow's cloud platform and form-based workflow engine enables its customers to overcome the increasing challenges faced within IT service delivery. ServiceNow's ability to automate the service management process through the use of a single system of record and automated workflow helps IT, operations, and business users increase efficiency and productivity while lowering costs.

Tenable Network Security has partnered with ServiceNow to allow ServiceNow customers and partners the ability to leverage Tenable™ vulnerability data. Through the use of a ServiceNow MID server, calls are made to SecurityCenter APIs to retrieve specific vulnerability data. The Tenable™ vulnerability data is then automatically imported into ServiceNow Security Operations allowing for enhanced visibility and context of the vulnerabilities within your organization. The result is a stronger security posture through improved workflows, reporting, and automated action.

Integration Requirements

The following are required in order to integrate SecurityCenter with ServiceNow Security Operations:

Note: Customers upgrading from the existing 1.0 version should uninstall the existing connector before installing the new 1.1 version.

- ServiceNow subscription to Security Operations (Premium Option)

  http://www.servicenow.com/products/security-operations.html

- ServiceNow MID server installed and registered within your ServiceNow instance

  http://wiki.servicenow.com/index.php?title=MID_Server_Configuration#gsc.tab=0

- Tenable for Security Operations application

  https://store.servicenow.com

- Tenable SecurityCenter version 5.x or higher
- Valid Security Manager user account on Tenable SecurityCenter with access to the appropriate repositories (Scan Results you wish to import).
- Operators of the Tenable for Security Operations application use the ServiceNow Security Operations tables in addition to its own.

Integration Configuration

The following steps outline the configuration process to allow ServiceNow, through the use of the Tenable application, to poll and retrieve vulnerability data from Tenable SecurityCenter. You must be logged in with a ServiceNow account that has the x_tsirm_tenable.admin role to perform the setup process.

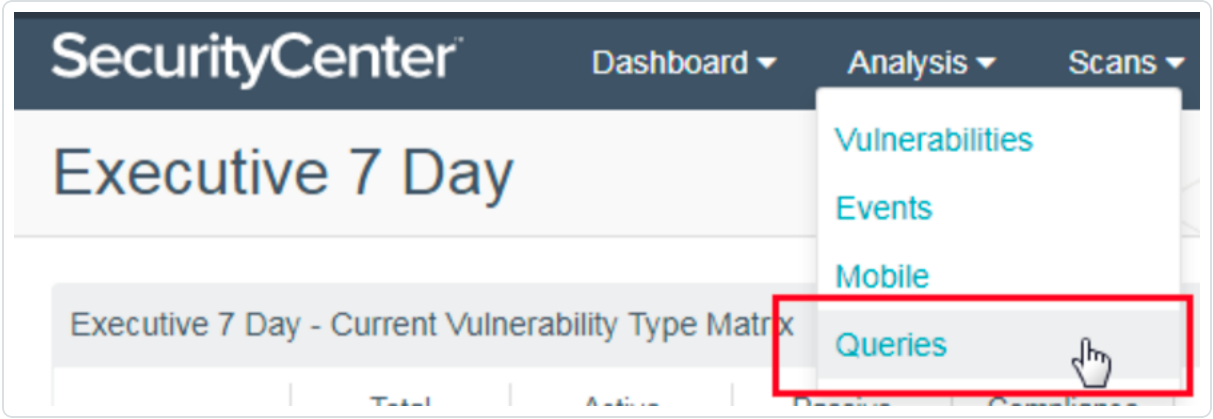
The setup process involves these major steps, spelled out below in greater detail:

- Setting up NIST NVD data (CVE) import
- Entering SecurityCenter credentials into ServiceNow via the **Connectors** page
- Creating a query via SecurityCenter to control the vulnerability data entering ServiceNow
- Creating a scheduled import
- Configuring the CMDB matching rules, which governs how vulnerabilities get tied to assets in your CMDB
- Configuring the CMDB target list feature to push a target list from ServiceNow to SecurityCenter to bring existing assets into the scope of future SecurityCenter scans

To begin the configuration, confirm you have a working ServiceNow MID server with access to SecurityCenter. Consult ServiceNow documentation for added details.

Set up a Query in SecurityCenter

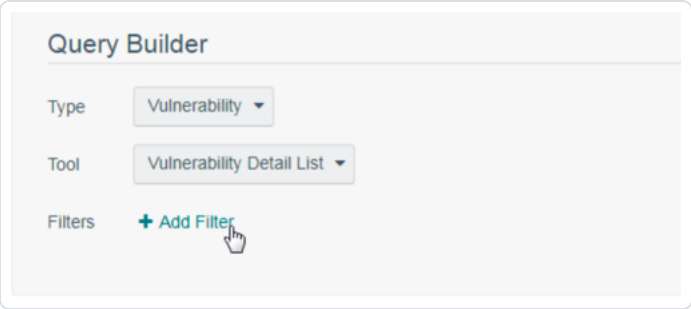
1. In SecurityCenter, navigate to **Analysis.**
2. Under **Analysis** select **Queries**.



3. Click **Add**.
4. In the **Name** field, type a name for the query.

5. Optionally, in the Description field, type a description of the query.
6. Optionally, from the Tag, drop-down menu, select a tag for the query.
7. From the **Type** drop-down menu, select **Vulnerability**.
8. From the **Tool** drop-down menu, select **Vulnerability Detail List**.
9. Optionally, in the **Filter** section, add any desired filters to the query.

   Note: Queries may use the Last Observed filter, but this filter is ignored. The integration uses it internally to import only vulnerabilities that have changed, for efficiency reasons.

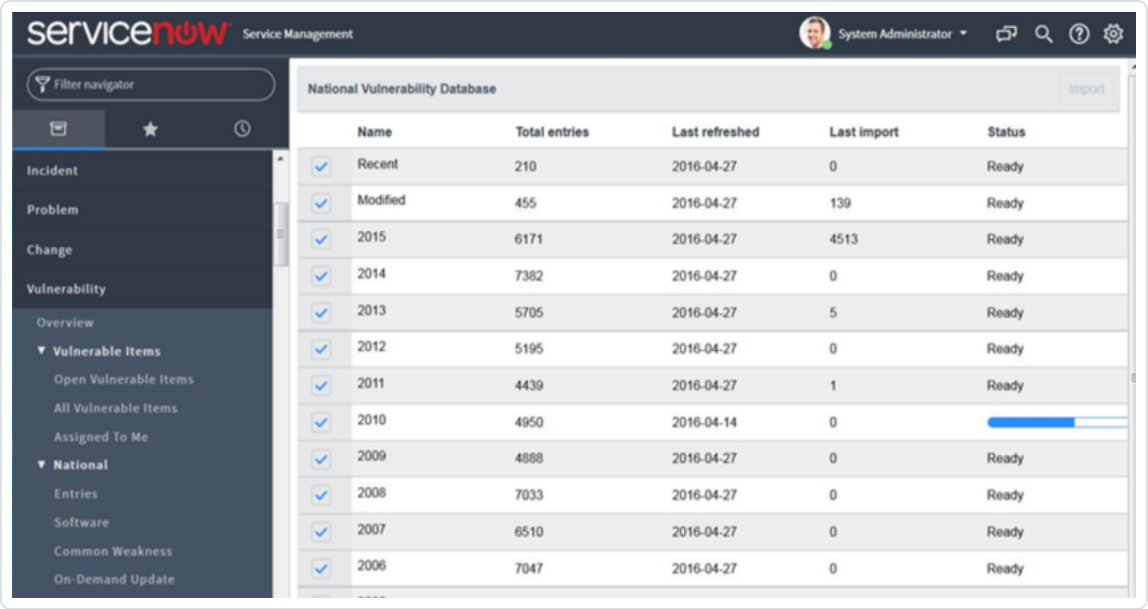
   

10. Click **Submit**.

Configure ServiceNow and SecurityCenter Connector

1. In your ServiceNow platform, navigate to the **Vulnerability** menu.
2. Under **Administration**, select **On-Demand Update**.
3. Check all of the check boxes.
4. Click **Import** to populate the National Vulnerability Database.

   Note: This process can take anywhere from a few minutes to an hour. You should perform this update on a regular basis as described in your ServiceNow Security Operations guidelines.



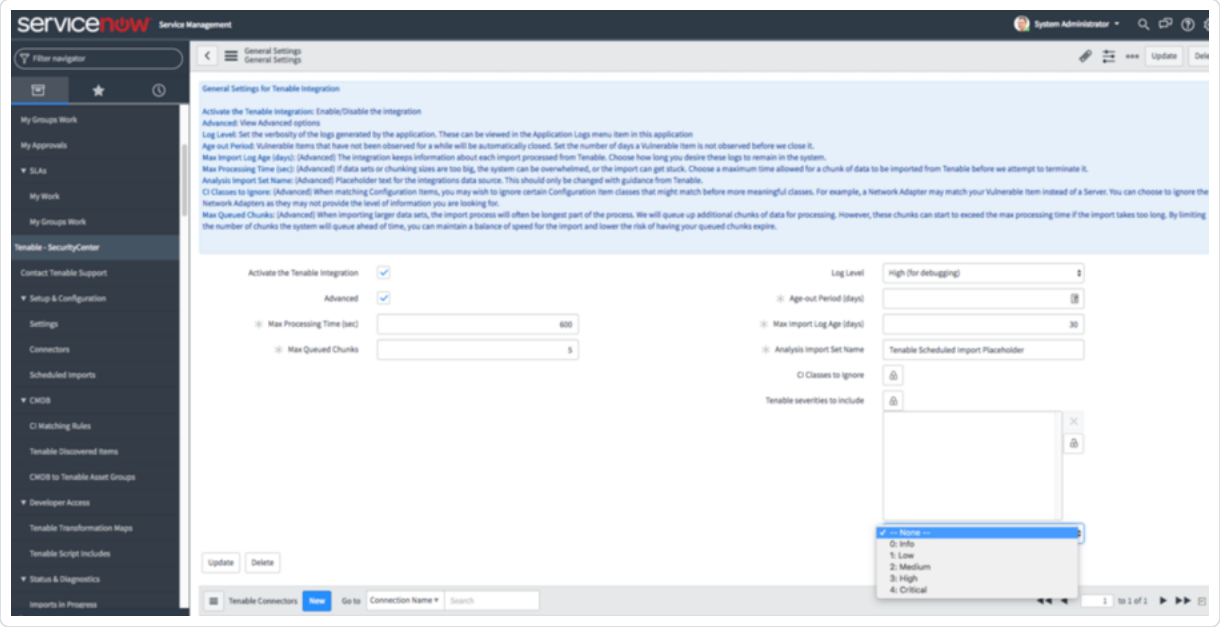
5. Log into SecurityCenter.

6. Create a security administrator account dedicated for use with this ServiceNow application. This account is used by ServiceNow to connect to SecurityCenter to retrieve vulnerability data.

   Note: This account must have access to the repositories containing the report data you wish to import. For further explanations of SecurityCenter, please consult the SecurityCenter User Guide.

7. Log into the ServiceNow console.

8. In the left-hand pane, click **Tenable** to expand the menu options.



9. Under **Setup and Configuration**, click **Settings**.
10. Activate the application. This toggle can be used at any point if the application needs to be suspended temporarily.

11. Under **Tenable**, select **Connectors**.
12. In the **Tenable Connections** section, click **New**.
13. In the **Connection Name** field, enter the name you wish to see when looking at running imports.

> **Tip:** If you're unsure, use the domain name of your SecurityCenter installation.

14. In the **Endpoint** field, enter the URL to access SecurityCenter.

> **Tip:** Be sure to include the https://, such as: https://securitycenter.example.com/

15. In the **API Username** and **Password** fields, enter the credentials used to access SecurityCenter.
16. If your SecurityCenter installation is not on the public internet, then in the **MID Server** section

select the MID Server to use.

> **Note:** If you do not see this field, ensure you have the **agent_admin** role.

17. Click **Test the Connector**.

    The connector's settings save and are tested. If you do not see a `Connection was successful` message, it may be because the default certificate used by SecurityCenter is not trusted by ServiceNow. See the Support and Troubleshooting section for steps to diagnose and resolve this issue.

18. Click **Update Queries for this Connector** to make the previously configured query available in ServiceNow.

Create a Scheduled Import Job

1. In the left hand pane under the **Tenable** menu, navigate to **Scheduled Imports**.
2. Click **New** to create a scheduled import job.
3. In the **Import Name** field, enter a name for the import.

   > **Tip:** If you're unsure, use the name of the SecurityCenter query.

4. In the **Initial Run - Historical Data** field, specify how far back (in days) to import when this Scheduled Import runs for the first time. For example, if Within 30 days is selected, vulnerabilities that were observed 15 or 25 days ago are imported into ServiceNow. After the first import, Tenable for Security Operations only requests as many days as needed to catch up with SecurityCenter as a matter of efficiency.
5. From the **Tenable Connector** drop-down menu, select the connector for the import.
6. From the **Tenable Query** drop-down menu, select the previously configured query.

   > **Note:** This is the primary method to control what types of vulnerabilities you want to see in ServiceNow. Any query created in SecurityCenter with **Type** of **Vulnerability** and **Tool** of **Vulnerability Detail List** can be used by this integration. If you do not see any queries available, navigate back to the Connector and click **Update Queries for this Connector** to fetch them, or ensure that you are logged in with the user account associated with the connector, as SecurityCenter does not allow query sharing between users.

7. In the **Schedule** section, in the Run and Time fields, select how often to request new vulnerability data from SecurityCenter.
8. Click **Submit** to save the scheduled import.
9. If you want to begin the import now, visit the new scheduled import and click **Execute Now**.

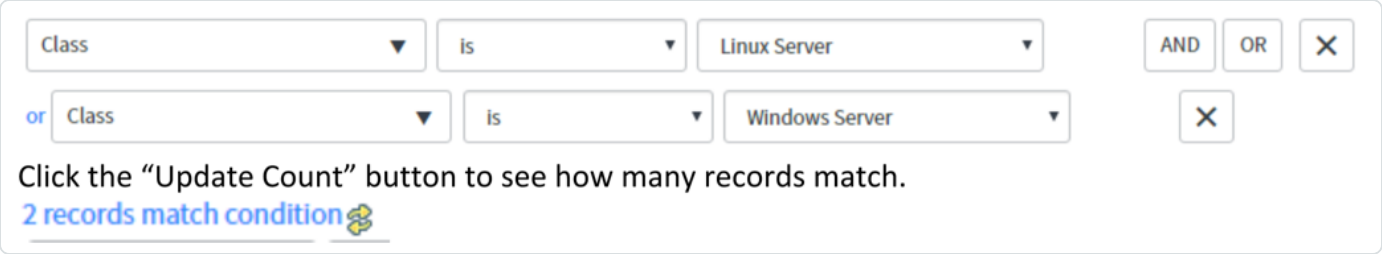
> **Tip:** You can click **Test the Query** to estimate how many records are imported and (if you have run any other imports) how long the process takes.

Set up CI Matching Rules

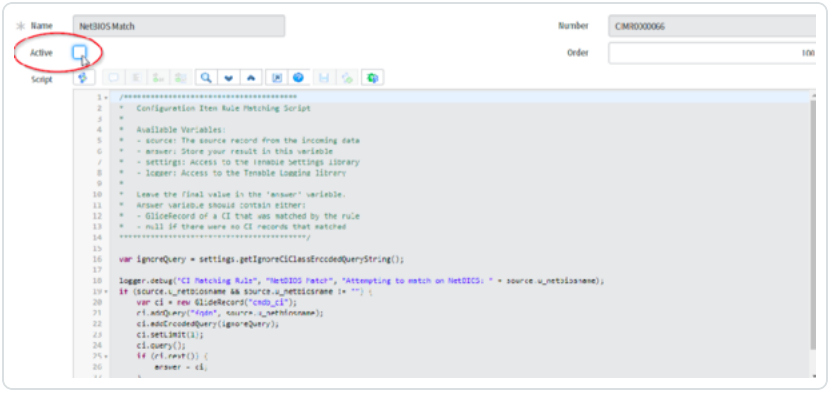
1. In the left-hand pane under the **Tenable** menu, navigate to **CMDB**.
2. Under **CMDB**, select **CI Matching Rules**.

> **Note:** These control how vulnerabilities get matched up to assets in your CMDB. There are a number of built-in rules that cover most types of assets. For every incoming vulnerability, each of these matching rules is tried in turn until one matches. The first rule that matches an asset “wins”.

3. In the left-hand pane under the **Tenable** menu, navigate to **CMDB**.
4. Click the **Show/Hide** Filter button.
5. In the **Filter** section, select what CMDB records are used.



6. Deactivate any rules you do not want to be used for matching. For example, if you do not want to ever match based on NetBIOS name, you can click on that rule and uncheck the **Active** checkbox.

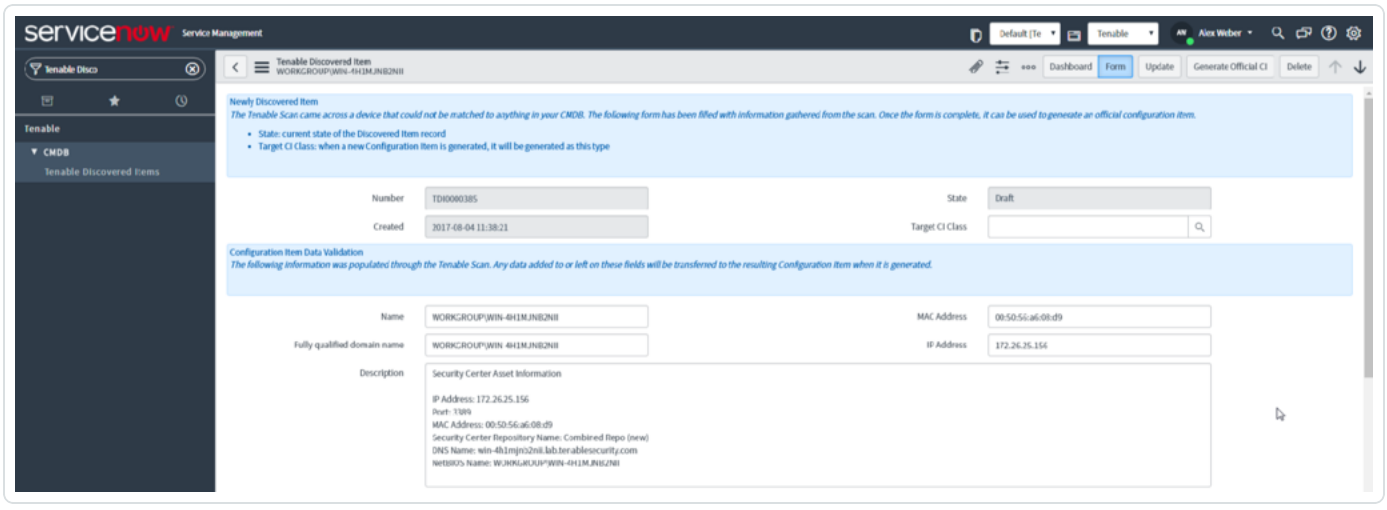


7. To reorder the matching rules, edit their **Order** fields. Match rules are tried in ascending order (lowest to highest). For example: if you changed **NetBIOS Match** to have an order of 700, it would be sorted after all other rules since default rules have values between 100 and 600. Because the first rule to match wins, and the NetBIOS match rule is now the last to be tried, a vulnerability only matches to a CI by NetBIOS name if no other rule found a match first.

Tenable Discovered Items

If a vulnerability does not match any of the CMDB Matching Rules, a special class of CI is created called a **Tenable Discovered Item**. To publish these items to your CMDB:

1. Under **CMDB**, select **Tenable Discovered Items**.
2. Click on the item you wish to publish to the CMDB.
3. In the **CI Target Class** field, type a target CI class for the item.
4. Click **Generate Official CI**. All vulnerabilities tied to this **Tenable Discovered Item** are moved to the new CI.

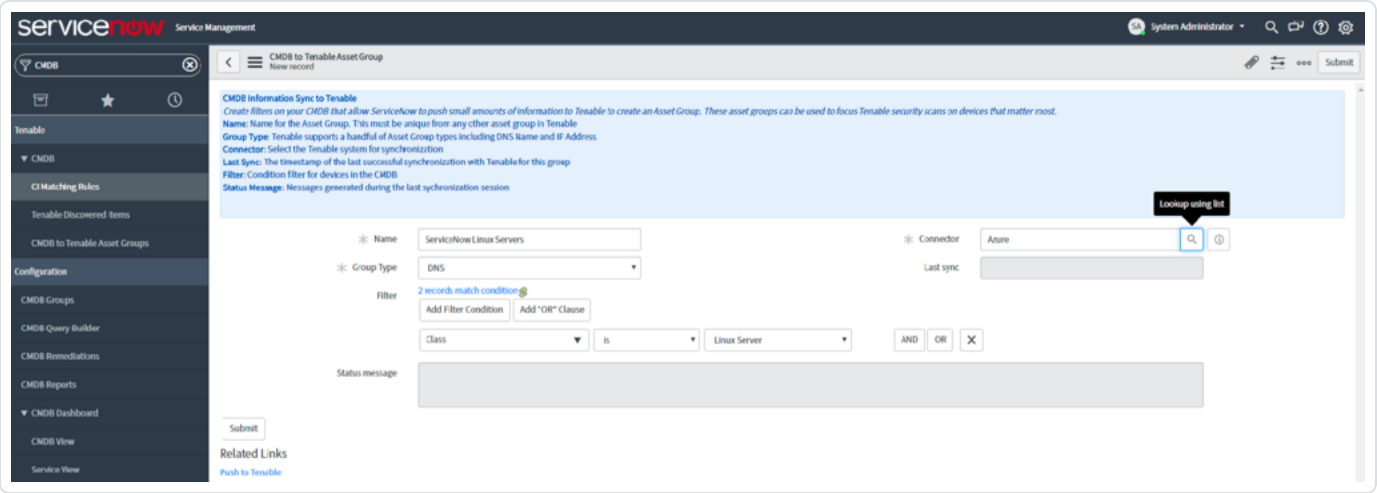


Note: If you're seeing **Tenable Discovered Items** imported that you wish to ignore, then in the **CI Classes to Ignore** section, add them to the Ignored list.

Create Tenable Asset Group

1. Under **CMDB**, select **CMDB to Tenable Asset Groups**.
2. Click **New**.

   Note: This feature is supported on Istanbul and later only.

3. In the **Name** field, enter the name for the asset group in SecurityCenter.

   Note: The sysid of this record idadded to the end, to ensure uniqueness. It is not possible to use an existing Asset Group.

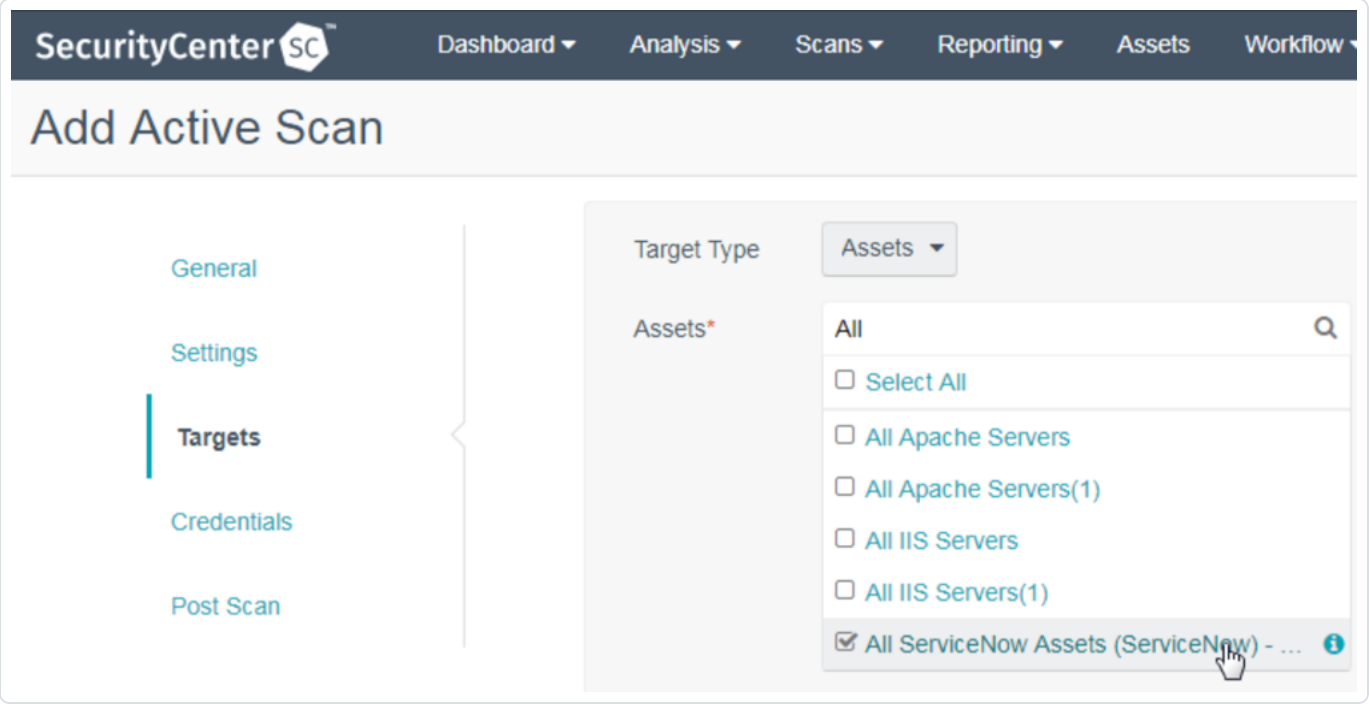
4. In the **Connector** field, enter the SecurityCenter instance to which you want to push the asset group.
5. From the **Group Type** drop-down menu, select whether the asset group is composed of DNS names or IP Addresses.
6. In the Filter section, add any desired filters to the group.
7. Click **Submit**.

   The asset group is created and appears in the **Assets** section of SecurityCenter.

Note: This asset list is synced to SecurityCenter every 24 hours. Contact Tenable support if you need to sync more often than this.

Create an Active Scan for the Asset Group

1. In SecurityCenter, navigate to the **Scans** section.
2. Under **Scans**, select **Active Scans**.
3. Click **Add**.
4. Under **Targets**, locate and select the newly created asset list.



The integration is configured.

Note: In the left hand pane under the **Tenable** menu, click Support to open a direct link to the Tenable Support Portal. For more information on support, please see the Support and Troubleshooting section.

About Tenable

Tenable Network Security provides continuous network monitoring to identify vulnerabilities, reduce risk, and ensure compliance. Our family of products includes SecurityCenter Continuous View™, which provides the most comprehensive and integrated view of network health, and Nessus®, the global standard in detecting and assessing network data. Tenable is relied upon by many of the world's largest corporations, not-for-profit organizations, and public sector agencies, including the entire U.S. Department of Defense. For more information, visit tenable.com.