Tenable.io Evaluation Workflow

Last Revised: November 06, 2018

Table of Contents

Welcome

Use this document to evaluate Tenable.io for your organization. For more comprehensive feature and configuration information, see the Tenable.io User Guide.

Before you begin:

- Sign up for a Tenable.io evaluation.

To get started in your evaluation period with Tenable.io:

Part 1

1. Create Users, Groups, and Access Groups
2. Create Target Groups
3. Create Exclusion Lists
4. Create an External Scan
5. Create an Internal Scan
6. (Optional) Use Agents

Part 2

7. Create and Customize Dashboards
8. Create and Customize Saved Searches
9. (Optional) Create Recast & Accept Risk Rules
10. (Optional) Create Scanner Groups (Scan Distribution)

Part One

1. Create Users, Groups, and Access Groups
2. Create Target Groups
3. Create Exclusion Lists
4. Create an External Scan
5. Create an Internal Scan
6. (Optional) Use Agents

Create Users, Groups, and Access Groups

1. Log in to Tenable.io.
2. Navigate to **Settings > Users**.
3. Create your first user and select the applicable permissions.

   > **Best Practice:** You will want to use the Standard role for most users.

4. Create your first group:
   a. Click **Groups**.
   b. Select **New Group**.
   c. Click **Submit**.
   d. Click **Manage Users**.
   e. Click **Add user** and select group members.

      > **Best Practice:** You will probably want to make yourself a user in this group if you are taking advantage of the Asset Isolation setting under Target Groups and Access Groups.

5. Create your first access group:

   > **Tip:** When initially viewing Access Groups, you will be greeted with a System Access Group. Click the System Access Group to view current permissions. The default setting for this group is enabled for all Users and Groups, which allows access to all assets by default.

   > **Best Practice:** The most secure practice is to disable this setting for the System Access Group. Then, create other access groups with unique network ranges to implement least privilege access control.

   a. Click **Access Groups**.
   b. Select **New Group**.
   c. Create an Access Group **Name**.
   d. Assign Asset Rules(s) for specific criteria (e.g., IP address, AWS Account ID, and FQDN).
   e. Click **Save**.

f. If you do not want to grant access to all users and groups, click **Add Users and Groups**. Then, search for and assign access to the appropriate user or group.

g. Click **Add** to finish adding users and groups.

h. Click **Create** to finish creating your access group.

Create Target Groups

Tip: *Target groups* are designed to limit scan permissions. *Access groups* are designed to limit vulnerability data view permissions.

1. Navigate to **Scans > Target Groups**.
2. Toggle on the **Asset Isolation** setting.
3. Begin creating the **Target Groups** that you will scan first.
4. Assign to either a specific user and/or group.

   Best Practice: Leave the default group set to **no access** in order to implement least privilege access control for the scan targets.

5. Set your new group to **Can Scan**.
6. Rinse and repeat for each specific target group.

   Best Practice: There are two settings for Target Groups, System, and User. System should be used by the main admin user. This will create these target groups as defaults for the subsequent users to see when they log in. The User target group should be specific to the end user themselves where they can break the System groups into smaller, relevant subsets specific to their area of responsibility.

   Tip: Subnet 10.0.0.0/24 is created as system group and then each user could create a user target group specific to their hosts within that larger subnet so User 1 is 10.0.0.0/28 and User 2 is 10.0.0.129/28.

Create Exclusion Lists

1. Create Exclusions as applicable (optional).

   You can use exclusions to restrict the scanning of specific hosts based on a selected schedule.

   > **Tip:** Exclusions without a schedule are set to *Always On*.

Create an External Scan

1. Navigate to **Scans > New Scan > Basic Network Scan**.
2. Input a *Scan Name* and ensure that an appropriate regional cloud scanner is selected.
3. Apply the appropriate **Target Group**.

   Best Practice: Edit the Permission settings and in the Data Sharing section define whether you want these results included in the Workbench or not. For User sharing, if this is a scan template/scan result that you want others on the team to utilize then apply this group permission to the appropriate group.

   Tip: This is typically done with *Can Control* permissions.
4. Make sure to leave **Default group** to *no access*.
5. Save and launch the scan.

Create an Internal Scan

1. Link and Configure Nessus Scanners
2. Create Centralized Credentials
3. Create the Scan

Link and Configure Nessus Scanners

1. Navigate to **Scans > Scanners**.
2. Download Nessus.
3. Run the Nessus installer on your local/internal system and create a local Nessus user.
4. Select **Managed by Tenable.io** and copy / paste the Linking key from your Tenable.io instance (located under the **Scanners** tab). Refer to Link your Nessus Scanner to Tenable.io in the Tenable.io user guide.
5. As soon as the scanner is linked, it will show up as an available scanner within Tenable.io (allow approximately 15-20 minutess for plugins to sync).

   > **Tip:** Plugins will continue to sync to the scanner(s) every 24 hours after initial linkage.

Create Centralized Credentials

1. Navigate to **Settings > Credentials**.
2. Click **Add** and select the type of Credentials (Window, SSH, etc.).
3. Add in your credentials and then select the appropriate permissions for the group/user that you also want to allow access to use.

> **Tip:** This is typically done with *Can Control* permissions.

Create the Scan

1. Navigate to **Scans > New Scan > Basic Network Scan**.
2. Input a *Scan Name* and ensure you select an internally linked scanner, and not a Cloud Scanner.
3. Apply the appropriate **Target Group**.

   Best Practice: Edit the Permission settings and in the Data Sharing section define whether you want these results included in the Workbench or not. For User sharing, if this is a scan template that you want others on the team to utilize then apply this group permission to the appropriate group.

   Tip: This is typically done with *Can Control* permissions.
4. Make sure to leave **Default group** to *no access*.
5. Click the **Credentials** tab and click **Add** under the **Add Managed Credentials** section.
6. Select the appropriate credential(s) created in the previous step.
7. Save and launch the scan.

(Optional) Use Agents

1. Link and Configure Agents
2. Create the Agent Scan

Link and Configure Agents

1. Navigate to **Scans > Agents**.
2. Similar to linking a scanner, download the OS-appropriate Nessus Agent package from the Tenable Downloads site.
3. Run the Nessus Agent installer and follow the Link an Agent steps in the Tenable.io user guide.
4. As soon as the Nessus Agentis linked, it'll show up as an available agent within Tenable.io.

   Tip: Plugins will continue to sync to the Agent(s) every 24 hours after initial linkage.

   Best Practice: Be sure to assign the Agent into an Agent Group when configuring Agents.

   Tip: You are required to scan via an Agent Group.

5. Create Agent group and then toggle on Add members and select the individual agents you want to be part of this group.

   Best Practice: Categorize Nessus Agents into Regional or OS-specific groups (or both).

Create the Agent Scan

1. Navigate to **Scans > New Scan**.
2. Click the **Agent** tab and select **Basic Agent Scan**.
3. Input a *Scan Name.*
4. Apply the appropriate **Agent Group**.
5. Choose an **Agent Scan Window**.

   > **Best Practice:** Set the Scan Window to 12 hours or more. This will ensure that the agent(s) have enough time to check into Tenable.io, receive the scan job, run the scan job, and report back the results

6. Configure the Permissions for the Scan.

   > **Best Practice:** Edit the Permission settings and in the Data Sharing section define whether you want these results included in the Workbench or not. For User sharing, if this is a scan template that you want others on the team to utilize then apply this group permission to the appropriate group (typically with “Can Control” permissions).

7. Make sure to leave **Default group** to *no access.*
8. Save and launch the agent scan.

Part Two

1. Create and Customize Dashboards
2. Create and Customize Saved Searches
3. (Optional) Create Recast & Accept Risk Rules
4. (Optional) Create Scanner Groups (Scan Distribution)

Create and Customize Dashboards

Tip: Review the Dashboard templates and determine which specific templates are best for your use case. You can then delete any unnecessary widgets which will move the template dashboard to the “My Dashboard” section. From there, you can continue to remove any widget(s) that aren’t applicable.

1. Navigate to **Dashboards**.
2. Select a Dashboard from the **Dashboard Templates** section.
3. Click **Configure** at the top right to adjust the Name of the dashboard.
4. Apply a specific Target Group.
5. Rinse and repeat but continue to re-apply these additional dashboard to other target groups as necessary.

   Tip: As an alternative you can also narrow a dashboard to one specific widget and title it accordingly. For example, “Top Ports per Regions”, and then duplicate that individual widget multiple times and apply a unique target group to each widget giving you the ability to see one topic over multiple regions in one view.

6. Click on the share icon at the top of the page to configure scheduled exports.

Create and Customize Saved Searches

1. Navigate to **Dashboards > Vulnerabilities Workbench**.
2. Click the **Advanced** tab at the top to configure query parameters.
3. Once satisfied with the query, click the Save icon at the top right.
4. Input a Saved Search Name.
5. Save the query.
6. Saved Searches will now be available under the Saved dropdown menu.

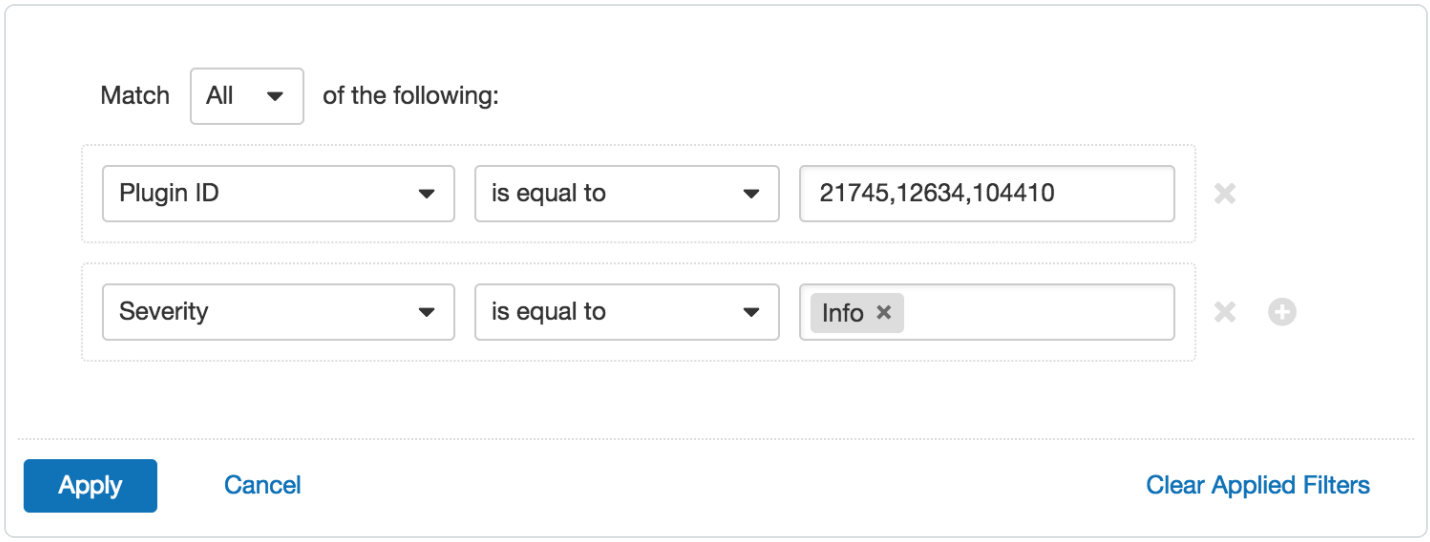
For more information, see Advanced Search Examples - Vulnerabilities Workbench and Advanced Search Examples - Asset Workbench.

Advanced Search Examples - Vulnerabilities Workbench

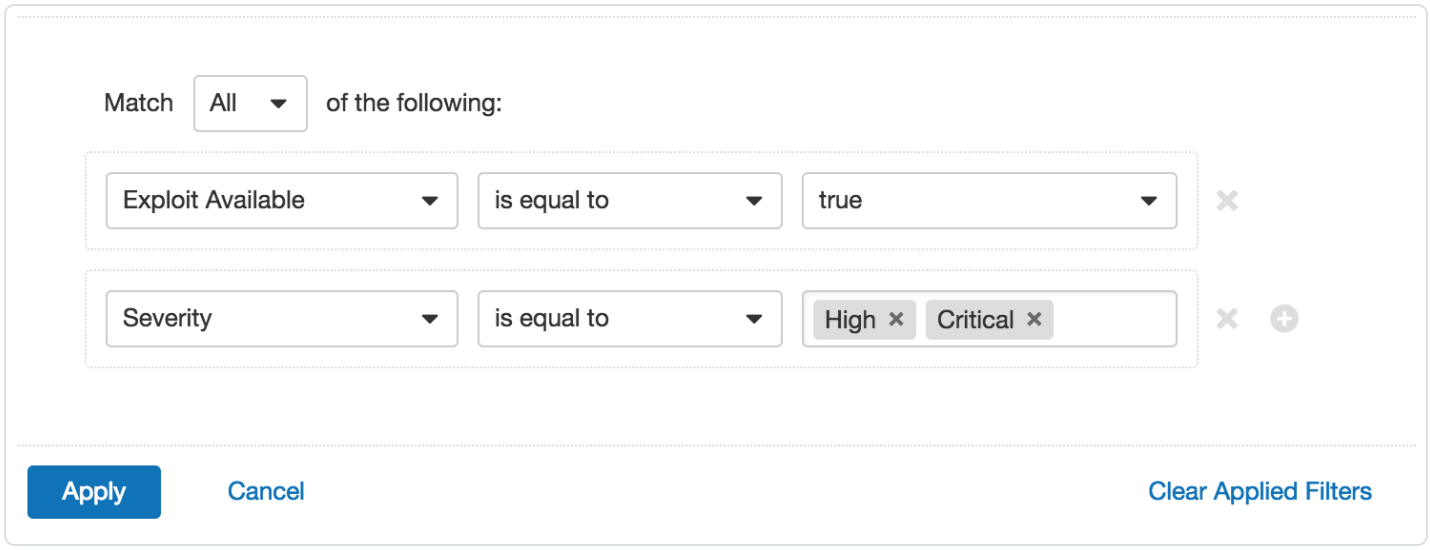
Tip: If any of your filters include informational results, then you must use the filter 'severity=info' in order to see those results. Info severity plugins will not automatically show in the search.

Tip: Don't forget the importance of the time period setting for each of these searches.

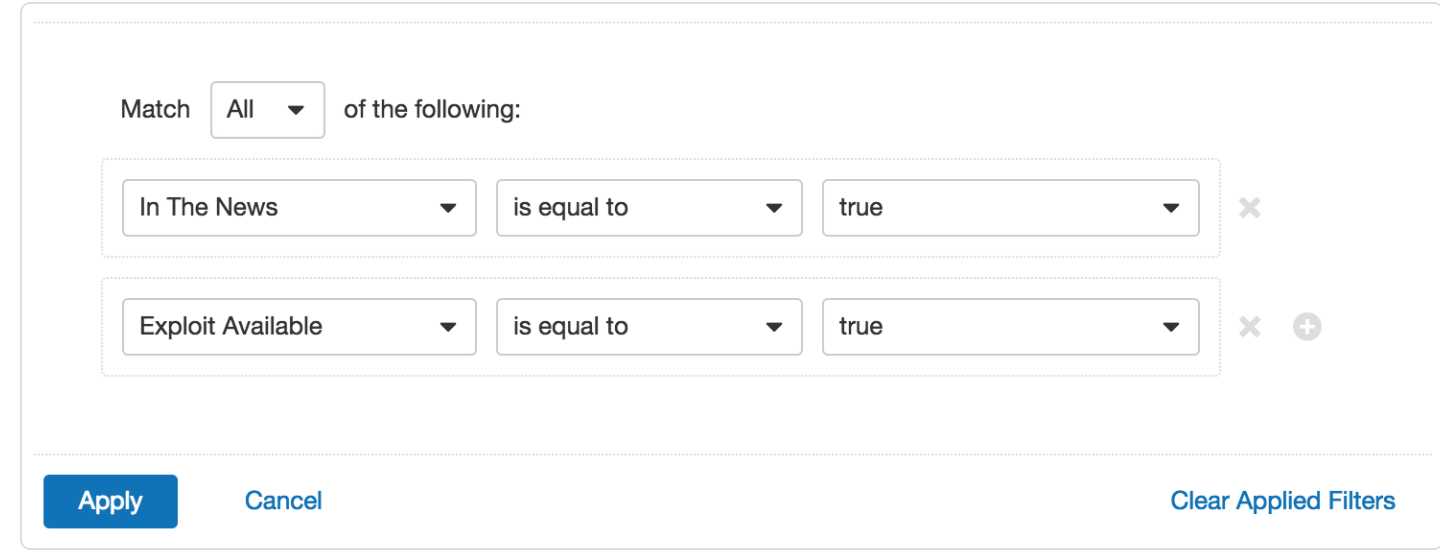
Authentication Failures



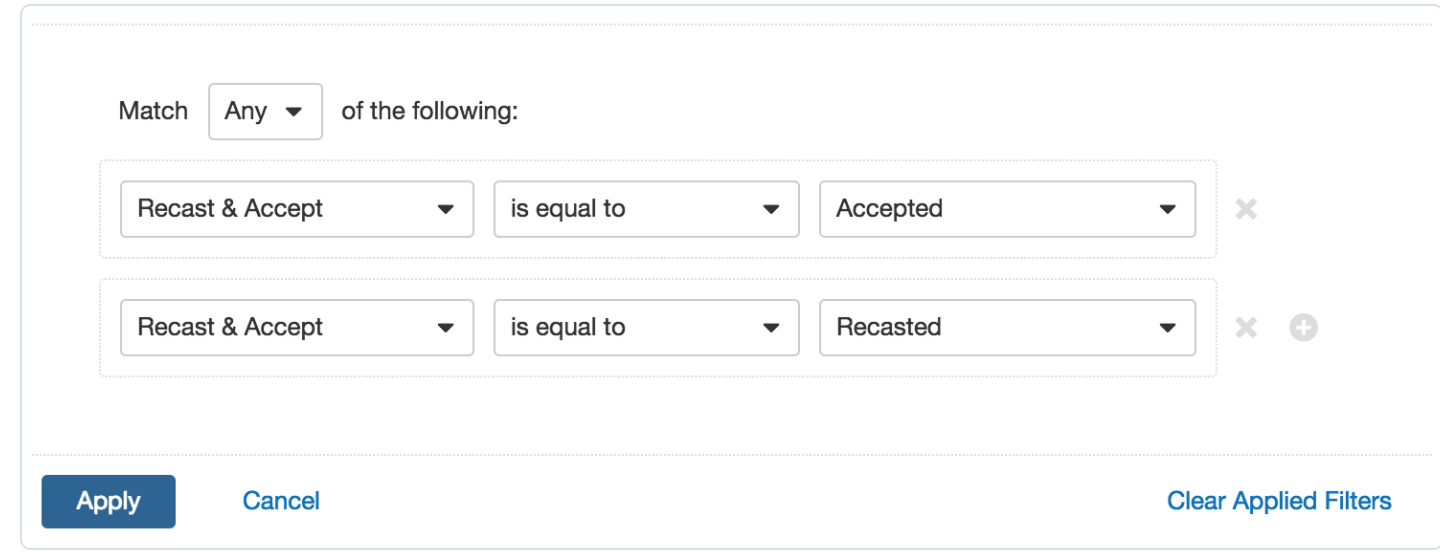
Critical and Exploitable



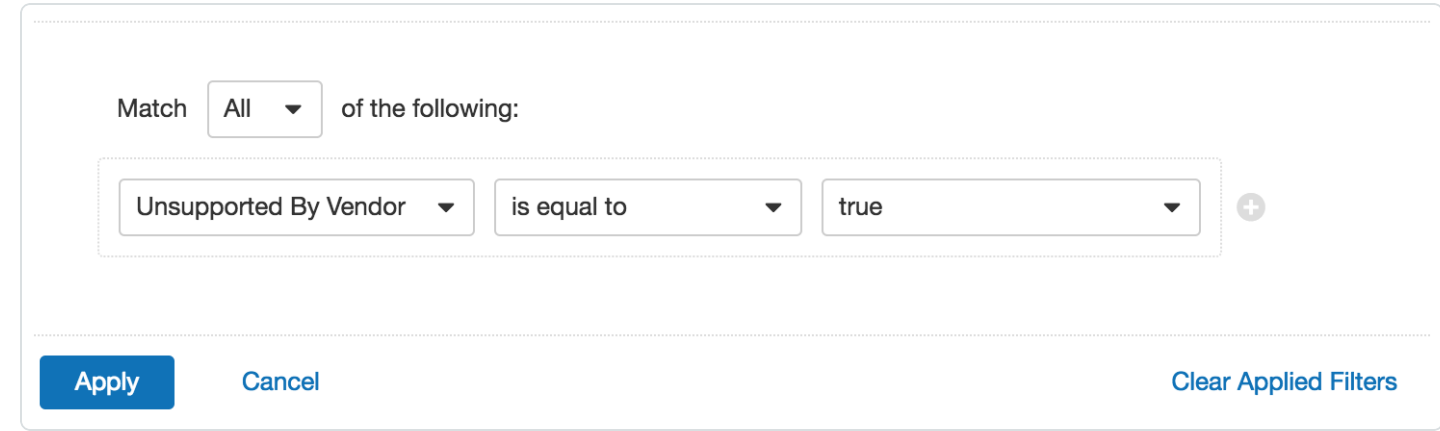
Newsworthy and Exploitable



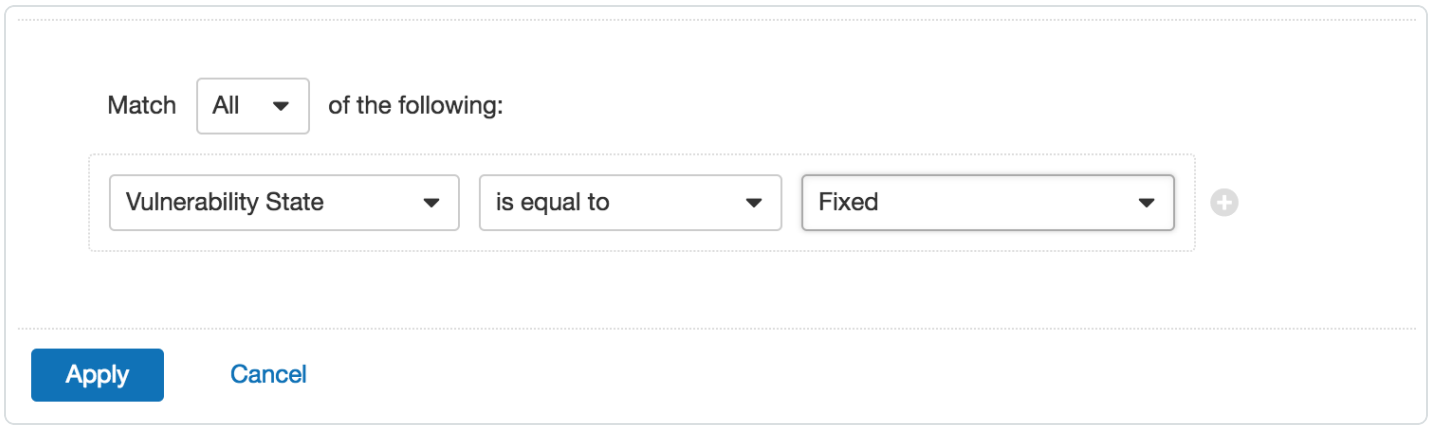
Recast and Accept Risk Rules



Unsupported software

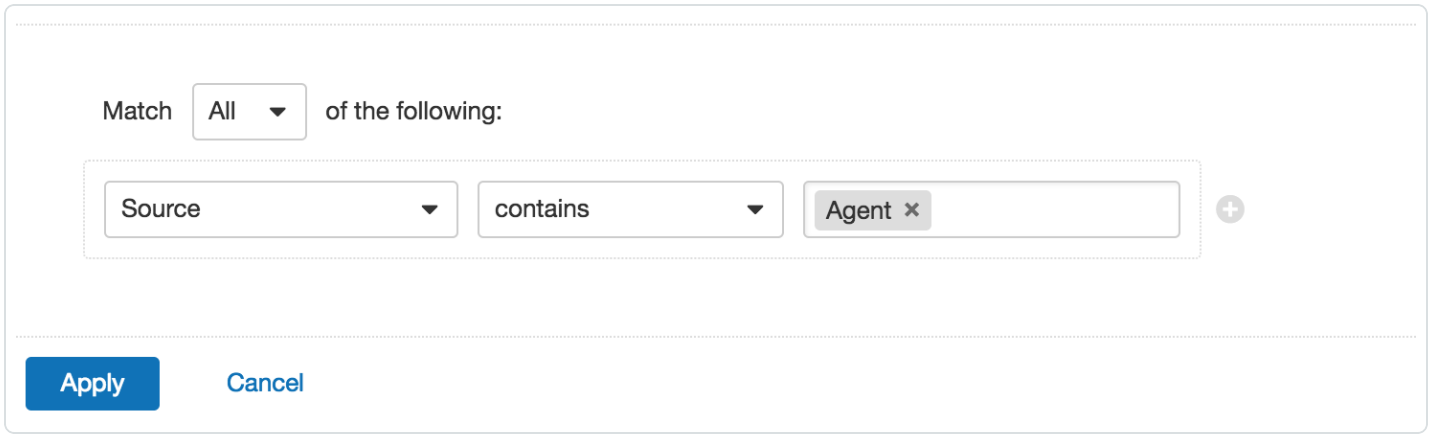


Mitigated Vulnerabilities

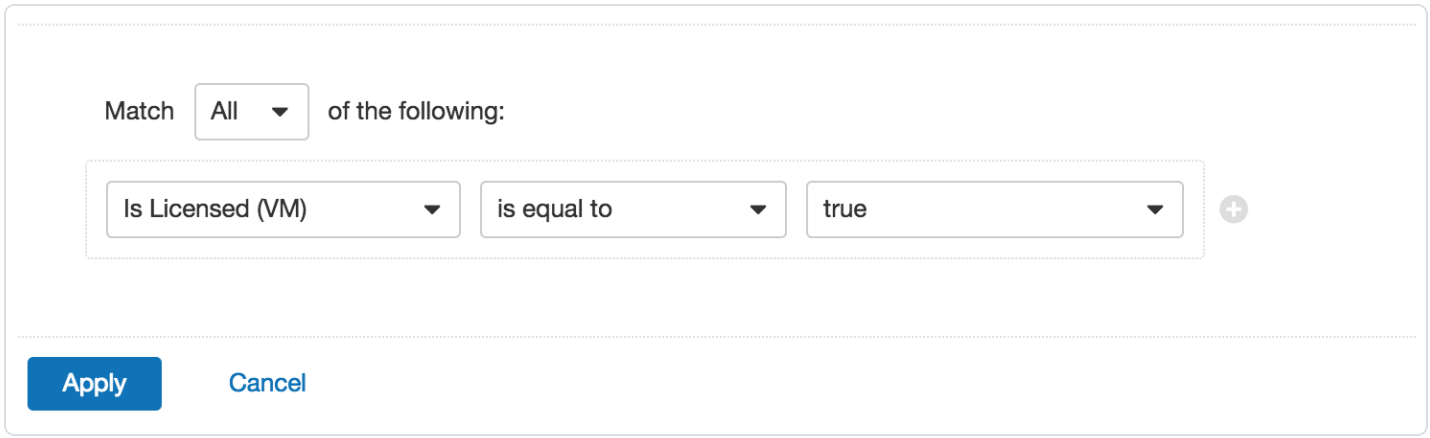


Advanced Search Examples - Asset Workbench

Agent Assets

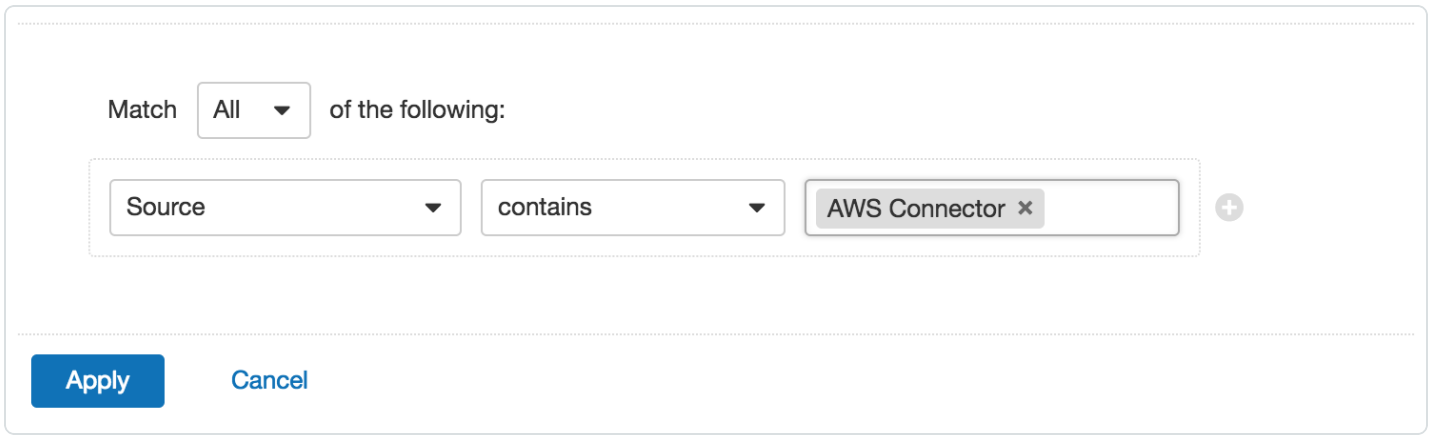


Understanding what is Licensed

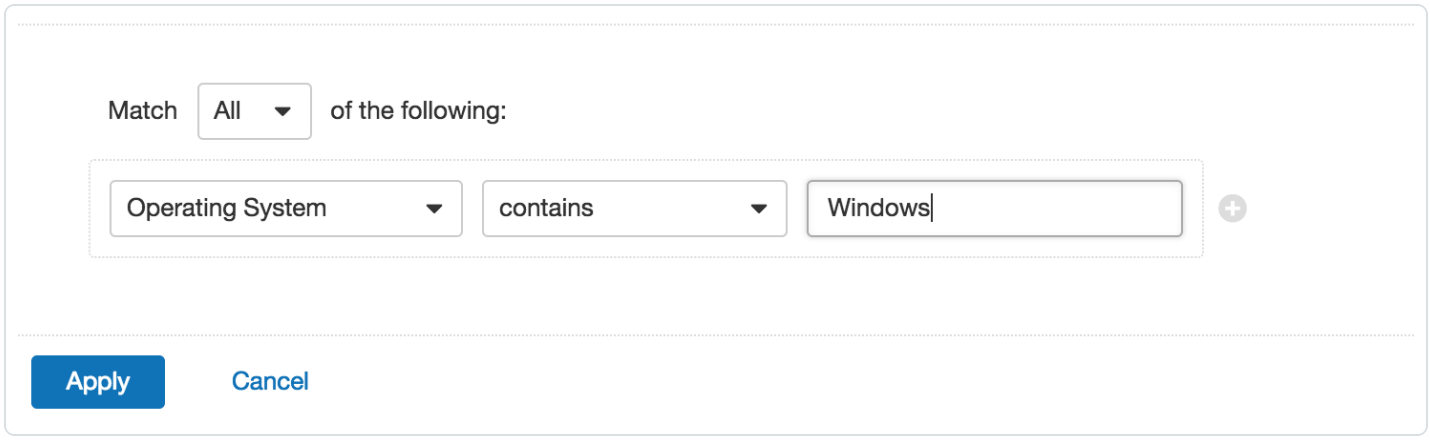


Tip: Make sure you change the time meter to Last 90 Days or another time period.

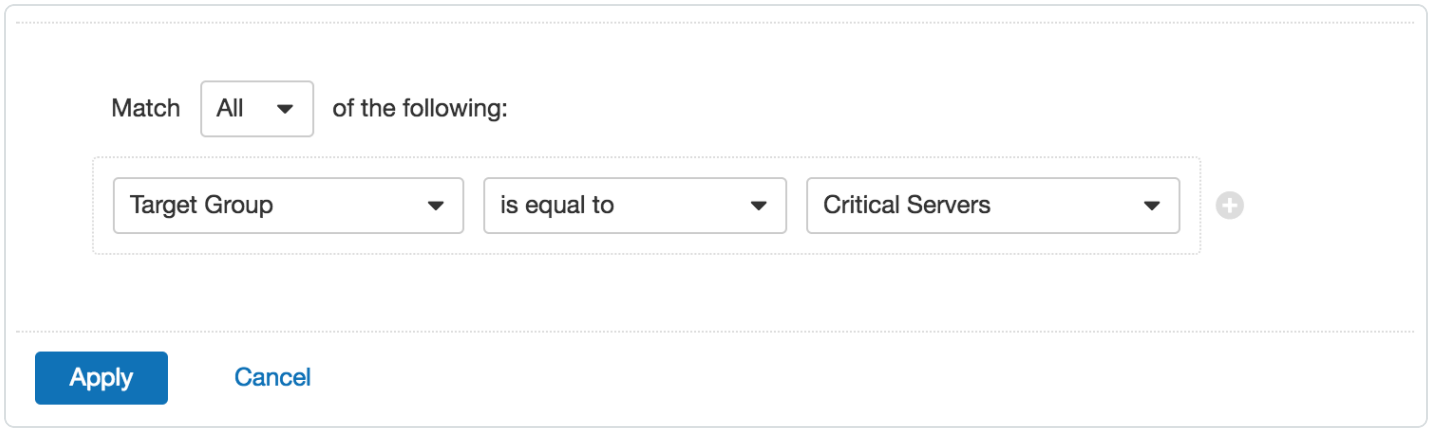
AWS Connector Discovered Assets



Windows Operating systems



Specific Target Group



(Optional) Create Recast & Accept Risk Rules

After going through the vulnerability results and beginning to disseminate your workflows you will start to have certain vulnerabilities arise that cannot be patched or that can be adjusted in severity based on existing compensating controls. To take advantage of our Risk Rules engine, assemble a list of plugins that fit this criteria and follow the steps below.

1. Navigate to **Settings > Recast Rules**.
2. Click **New Rule**.
3. Input the Plugin ID, Action, Target Group, and optional expiration settings.
4. Save the Recast Rule.

> **Tip:** Be sure to allow a few minutes for the newly created rule to go through the vulnerability database and apply itself accordingly, it will not immediately take effect.

(Optional) Create Scanner Groups (Scan Distribution)

For a comprehensive overview into how scan distribution functions, refer to About Scan Distribution in the Tenable.io user guide.

1. Navigate to **Scans > Scanners**.
2. Select New Group and input a Group Name.
3. Select multiple scanners from the Available Scanners list in order to assign them to the new Scanner Group.

   Best Practice: It's best practice to take advantage of scan distribution via scanner groups in order to realize a significant drop in scan completion time by distributing scan jobs/tasks across multiple available scanners

   Tip: It's important to apply scanners to a group that co-exists in the same geographical region. You wouldn't want to scan a target location with a scanner that can't reach said targets.
4. When creating / editing scans, simply select the Scanner Group as opposed to an single scanner to commit the change.