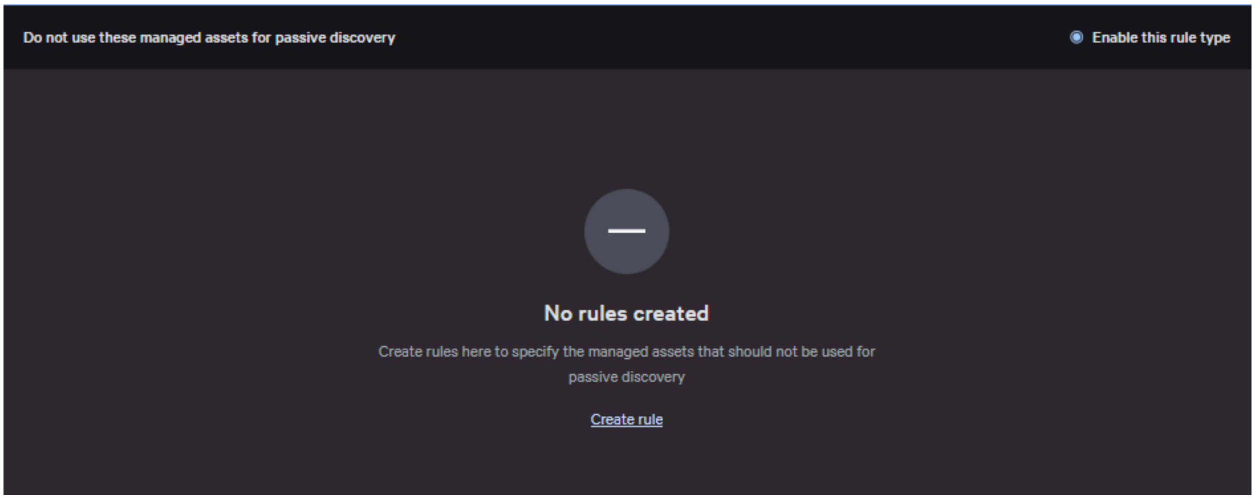
Passive Discovery Configuration in Crowdstrike

Passive Discovery is a tool in Exposure Management that provides visibility into assets that don't currently have Crowdstrike installed. Passive Discovery works by pulling IP and MAC address information from assets that share a network with one or more managed assets and classifying these assets as Unmanaged (a device that could potentially run Crowdstrike) or Unsupported (IoT or other devices that cannot run Crowdstrike). This asset information can be valuable, but since Crowdstrike has no way of knowing whether these Unmanaged or Unsupported assets are managed by you, devices that frequently connect off-site can start generating noise by populating the list with assets you don't manage or care about.

To address this concern, Crowdstrike has recently added the ability to configure Passive Discovery to allow or block devices from doing passive discovery. We're going to walk through how to set this up.

1) In the Crowdstrike console, go to **Exposure Management>Setup>Passive Discovery**.
2) Rules can either be configured as a blocklist ('Do not use these managed assets for passive discovery') or an allowlist ('Use only these assets for passive discovery'). Decide which rule type works best for your situation, and start by creating a rule.



Do not use these managed assets for passive discovery

● Enable this rule type

No rules created

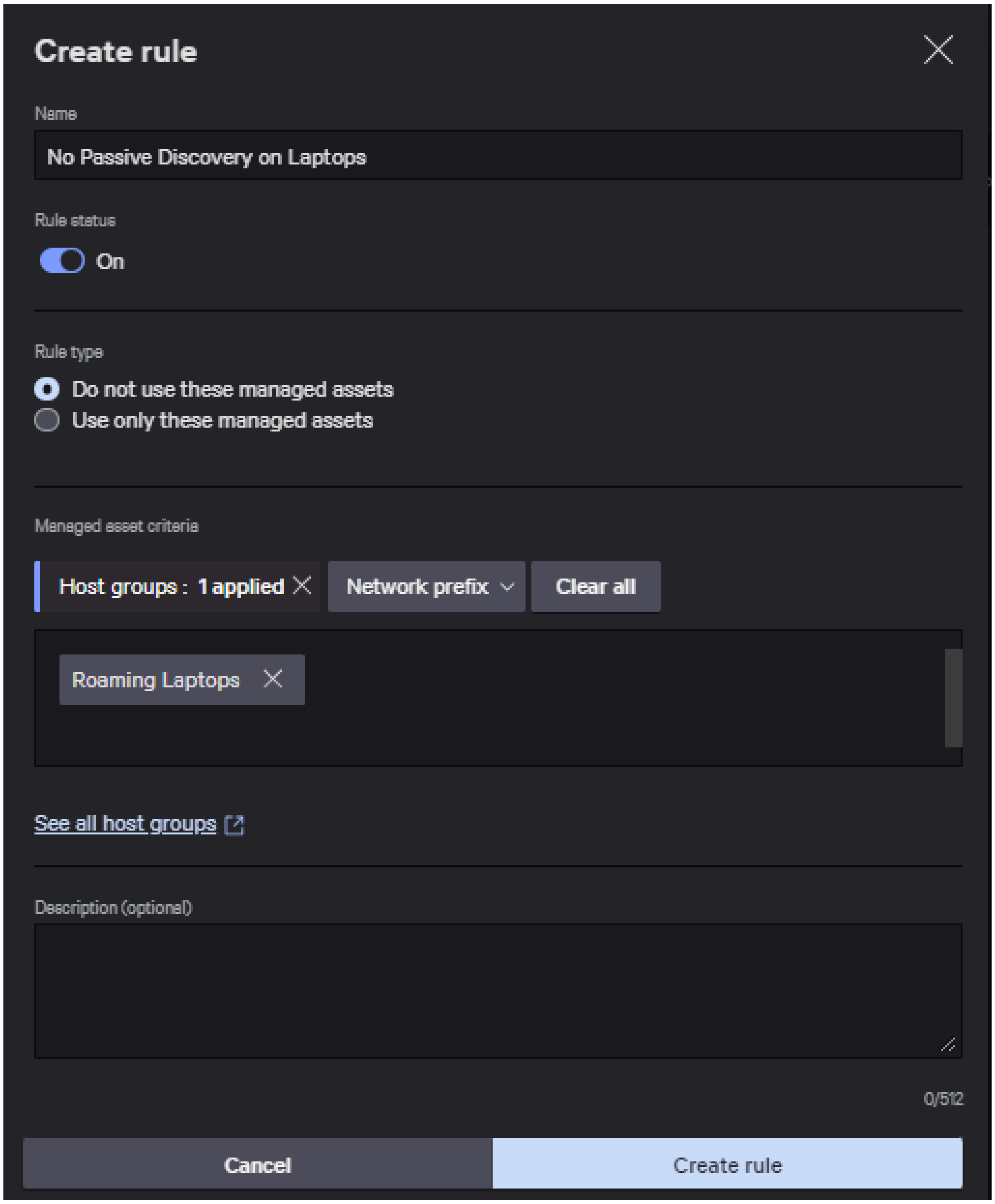
Create rules here to specify the managed assets that should not be used for passive discovery

Create rule

3) Name the rule, make sure the rule type matches what you're trying to achieve, and select the host group or network prefix you want to use:

Example A: You have a group of laptops that frequently travel off-campus, so you'd like to stop those assets from ever doing Passive Discovery.

Note: Only MCNC has the ability to create groups because an inadvertent group misconfiguration could impact Crowdstrike's protection in your environment. If you'd like to create a Passive Discovery rule based on a group that doesn't exist, please contact MCNC SecOps for assistance.



Create rule

Name: No Passive Discovery on Laptops

Rule status: On

Rule type

● Do not use these managed assets

○ Use only these managed assets

Managed asset criteria

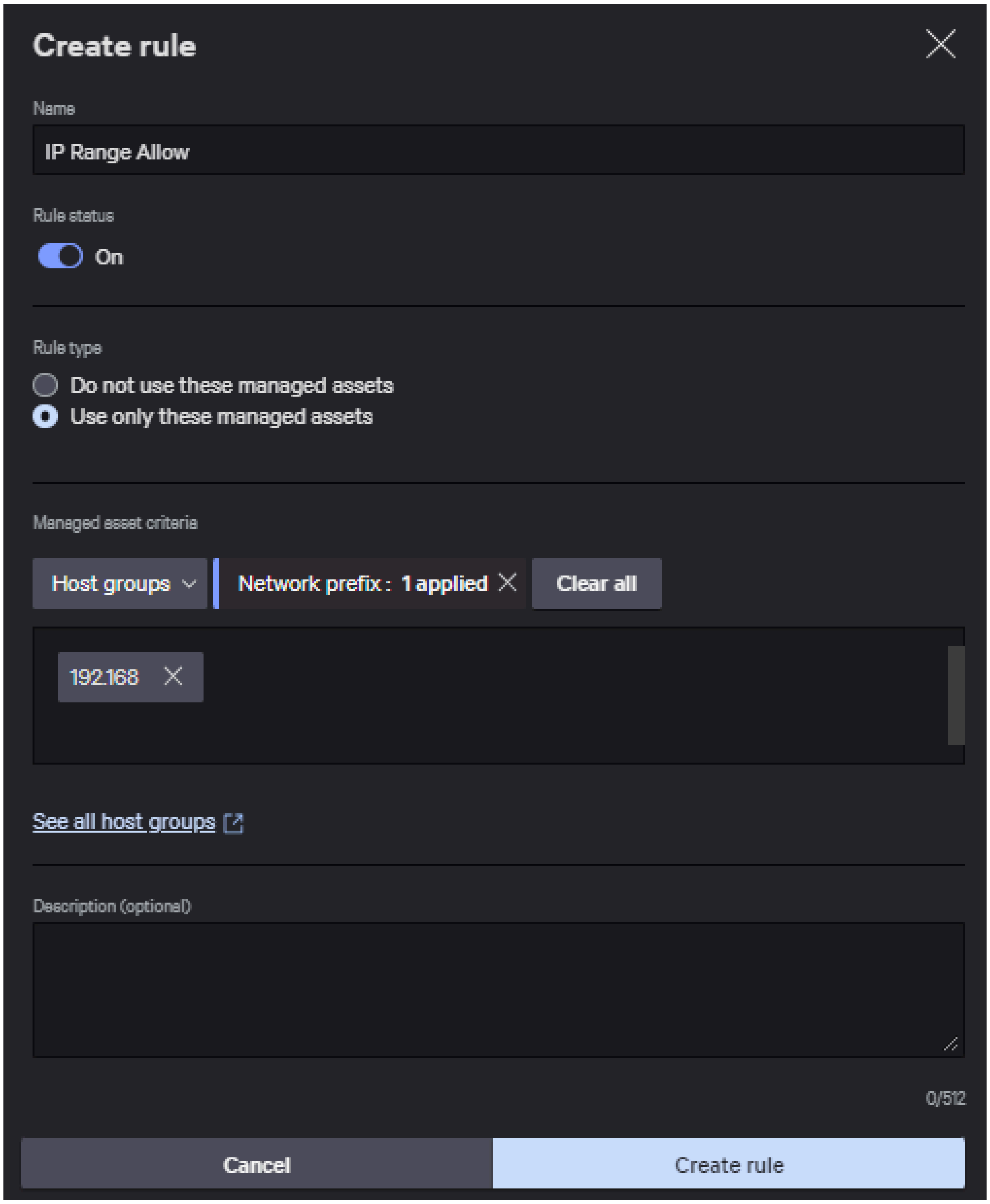
Host groups : 1 applied

Roaming Laptops

Description (optional)

0/512

Example B: You know you only use 192.168.x.x addresses on your work network, so you can create a rule that only allows Passive Discovery when managed assets have an IP in that range.



Create rule

Name: IP Range Allow

Rule status: On

Rule type

○ Do not use these managed assets

● Use only these managed assets

Managed asset criteria

Network prefix : 1 applied

192.168

Description (optional)

0/512

4) You're all done! Hopefully this gives you some ideas for how to configure Passive Discovery in your environment to get the most out of the tool.