Host Management and Retention

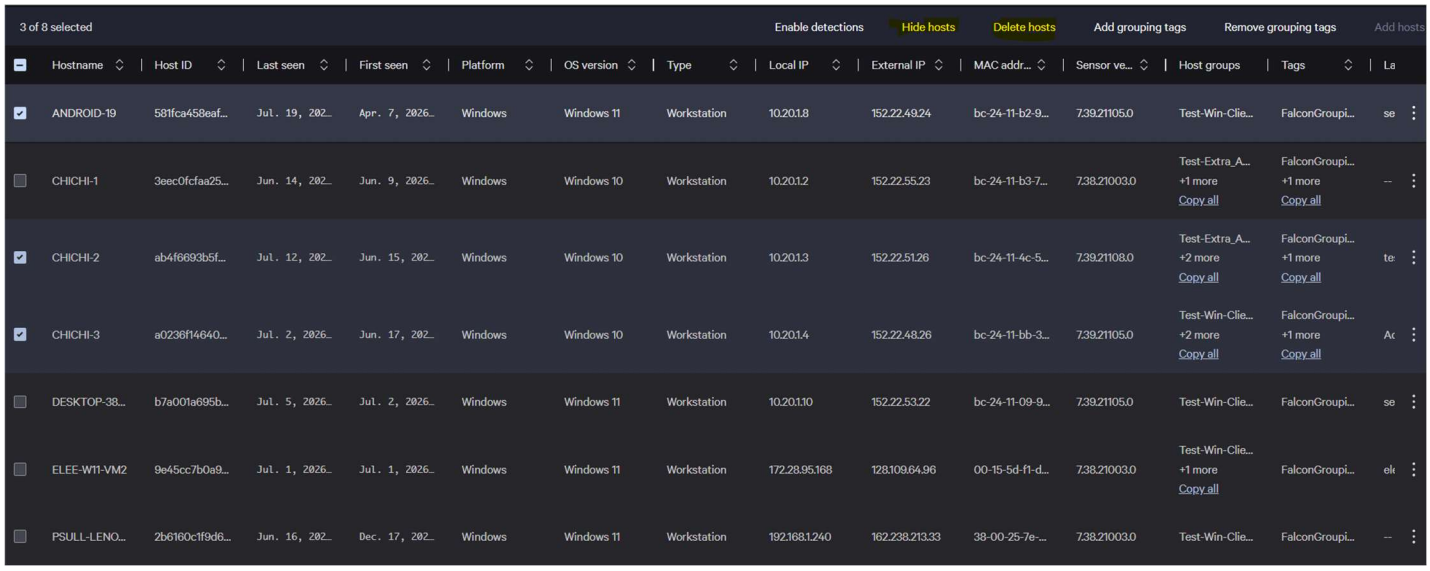
The Host Management view in Crowdstrike displays information about all of your active hosts. By default this includes all hosts running Crowdstrike that have been observed online at least once in the past 45 days. However, there may be scenarios where you'd like to remove hosts without waiting that long. This document discusses various methods for manually and automatically removing hosts from your inventory.

A Quick Note about 'Removal'

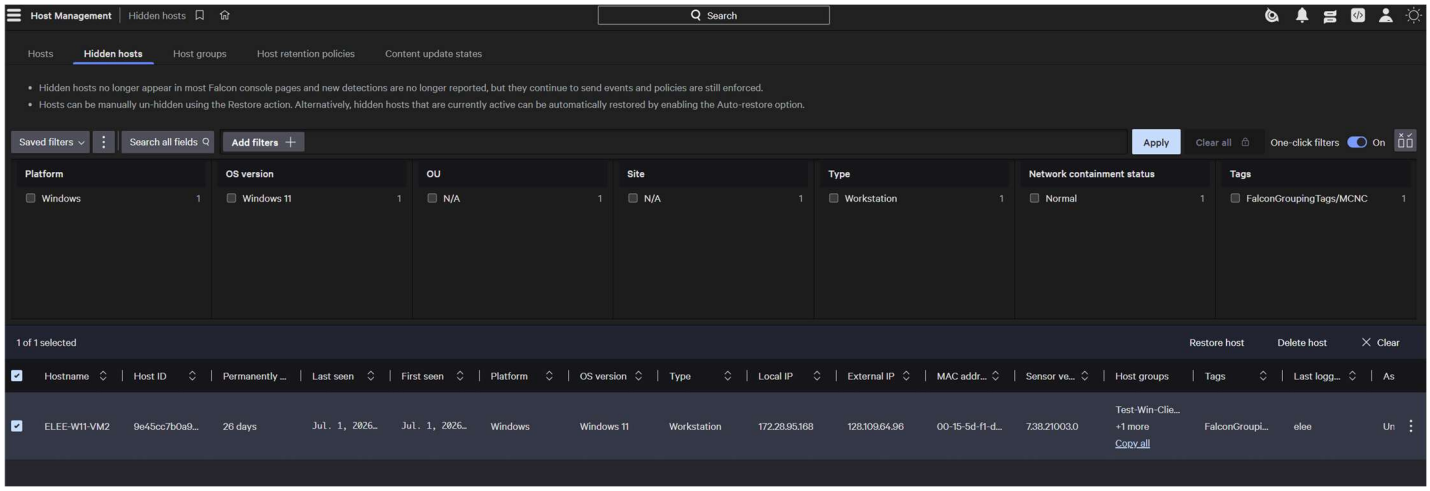
Removing hosts from view can be helpful to reduce noise, take action on recently decommissioned hosts, and focus on your active assets. However, it's important to note that removing hosts from the console *does* ***not*** *uninstall Crowdstrike or disable the sensor.* Hosts that are removed from the console will continue to detect and respond to malicious activity, and in some situations the host will return to Host Management the next time it is seen online. To remove Crowdstrike from a device you will need to provide a valid maintenance token from Host Management and uninstall the sensor on the device itself via Control Panel or command line. For more information consult the Crowdstrike Documentation.

Manual Removal

Hosts can be manually removed from Host Management view (Host Setup and Management>Host Management). After checking the box next to one or more hosts you will see menu options to Hide and Delete Hosts (we'll look at the differences below).



You can view hosts that are currently hidden via the Hidden Hosts menu in the top left. From here you can restore hosts or permanently delete them. Hidden hosts are automatically deleted after 45 days offline.



Hide vs Delete

Hiding and deleting hosts are similar in that they both remove hosts from your active Host Management list, but there are a few key differences that may affect which will better meet your needs. Comprehensive information is available in the documentation, but here's a quick comparison:

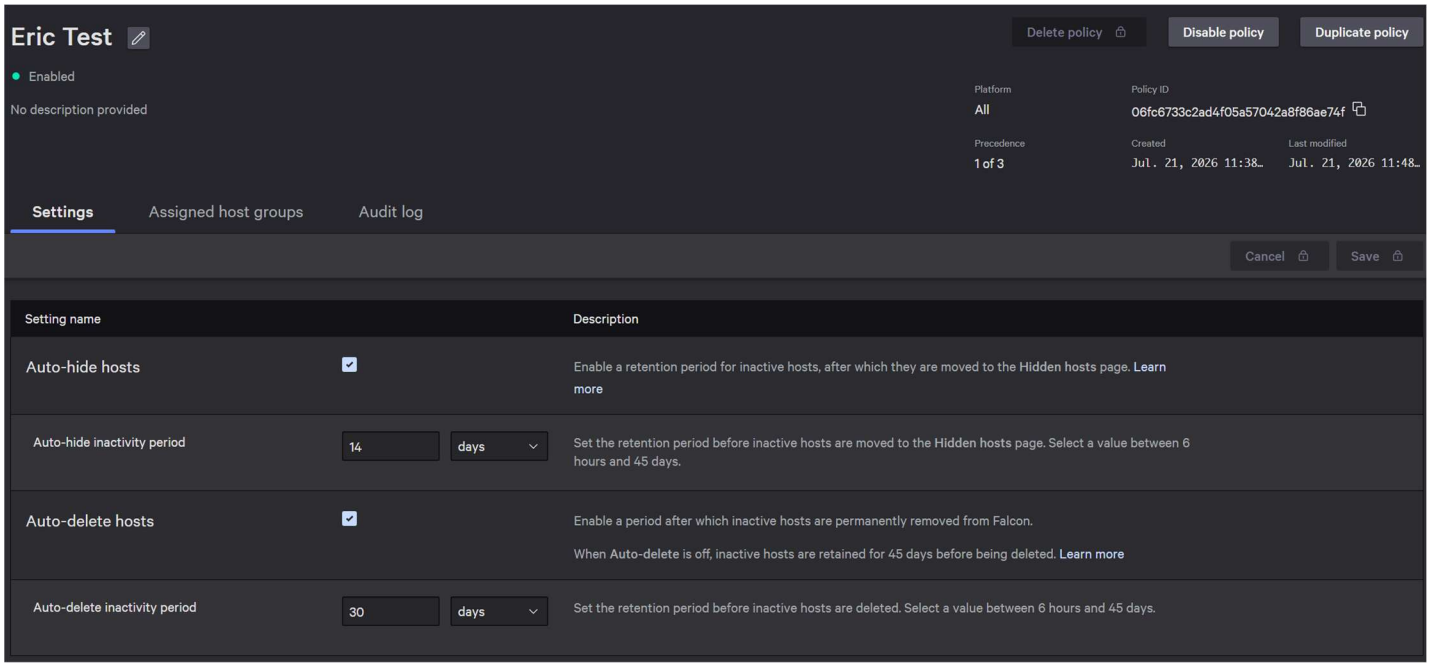
- Hidden hosts will be moved to the Hidden Hosts list and can be restored if needed. Deleted hosts can not be restored from the console, though they will reappear if they return online.
- If a host is reobserved online, a hidden host remains in the hidden list until restored, while a deleted host is restored automatically.

Host Retention Policy

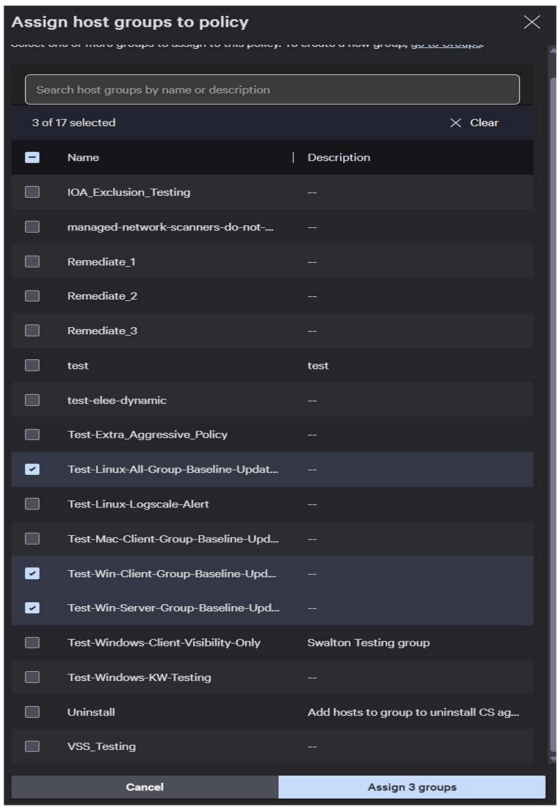
By default hosts are deleted from the console after 45 days. In addition to hiding or deleting hosts manually, Crowdstrike also allows you to create a Host Retention Policy for some or all of your assets. This policy can hide or remove assets at whatever cadence you choose, from 45 days to as little as 6 hours. For example, if you are using Crowdstrike on virtual hosts that are frequently deployed and decommissioned, you may want to auto-delete hosts in a 'VM' OU after only 7 days to keep your host list as up to date as possible.

Set Up a Host Retention Policy:

1) Go to 'Host setup and management>Host retention policies'
2) Select 'Create Policy'.
3) Configure the policy to fit your needs by choosing when hosts are auto-hidden and/or auto-deleted. The screenshot below shows a configuration where inactive hosts will be auto-hidden after 14 days before being auto-deleted at 30 days.



4) Save policy changes and go to ‘Assigned host groups’. Here you will choose which of your groups receive this Host Retention Policy. You can select some or all of your host groups. For assistance setting up a new group (for instance, if you want to apply a Host Retention policy to a specific OU, device type, or grouping tag), please contact MCNC Support.



5) Once configuration is complete, make sure to click the ‘Enable Policy’ button
6) Policies are applied based on precedence, so if there are multiple Host Retention rules only the first rule that applies to that host will be enforced. Ensure that precedence is set up to apply your policy as expected. For example, if you have a rule that applies to a subset of Windows Servers and a rule that applies to all Windows hosts, the more narrow rule should typically take precedence.

