

Cisco Stealthwatch

Host Group Automation Service

Automate Host Groups for precise Stealthwatch optimization

Cisco Stealthwatch® provides network visibility and detection to help protect your organization against advanced threats. By having knowledge of who is on the network and what they are doing, your organization can implement smarter assessments of your network to ensure that it is customized to your business needs. Automating host groups is an ideal way to keep Stealthwatch operating at its best and ensures that your network and security personnel receive timely and accurate data. It allows your security team to receive more accurate alerts, providing them with a high degree of confidence that alarms are meaningful by reducing false positives.

As a result, you will receive:

- Ability to proactively deploy, design, and manage integrations with external data sources using a high-fidelity graphical user interface
- Reduced operational overhead to lower operating costs while reducing errors and superfluous alerts and job notifications
- Ability to maintain proper configuration of your host group structure

Benefits

- Tackle dynamic server behavior of constantly changing IP addresses and automate host groups to make the policies on your dynamic host groups more effective.
- Manage constantly changing IP addresses in real time so you can mitigate erroneous alarms when communicating to malicious hosts.
- Automate updating host groups to keep your Stealthwatch system operating at maximum efficiency for optimal protection against wide-ranging threats.

What's included

- Integrate up to three custom data sources
- Include data from IPAM, CMDB, internal or external threat feeds, ASNs, or static datasheets using pre-defined and custom connectors
- Professional service engineer creates custom automation rules via an advanced graphical user interface hosted on the Cisco® Service Delivery Platform (CSDP) to deliver Host Group Automation to your Stealthwatch system

Next steps

To learn more about Cisco security services and how our Stealthwatch host group automation services can benefit your business, contact your local account representative or authorized Cisco reseller. For more information on how Cisco can help you protect your organization from today's dynamic threats, visit <https://www.cisco.com/go/services/security>.

Read the [Cisco Security Stealthwatch Host Group Automation Service description](#) to learn about the terms and conditions of this service.

Host Groups Provide Contextual Visibility

Host groups are essential to the operating structure of Stealthwatch. Well defined host groups ensure you receive proper alarm notifications and give you additional context when analyzing NetFlow records. They allow you to separate network devices by location or function so, when you view NetFlow records, you see IP traffic that you can correlate to devices within a specific physical location or work function within your network. Cisco Stealthwatch Host Group Automation Service allows you to update your Stealthwatch host groups with data from authoritative IP address management (IPAM) systems. By keeping Stealthwatch host groups synchronized with your network infrastructure, you reduce overhead and optimize your Stealthwatch operation.

Ensure Accuracy with Automation

This service provides you with a logical means of categorizing network assets for improved visibility and control. Host groups are critical to Stealthwatch performance so keeping them up to date is necessary. Since so many devices are added to your network frequently, it can be overwhelming to manually keep your host groups up to date. By automating this process, you ensure that your host groups are regularly updated with the latest data possible ensuring they are classified and sorted correctly. This optimizes your Stealthwatch system performance and reduces excess consumption of your team's resources since they do not have to manually organize every asset on your network in to the appropriate host group.

Increase Alarm Fidelity

Since automating your host group structure eliminates human error, you decrease false-positive alarms and give your security teams a high degree of confidence that when an alarm fires, it warrants investigation. By automating your host group synchronization, you maintain accurate groupings so you're assured that items on your network are assigned correctly for compliance and security policies.

“The Stealthwatch Professional Services team helped automate our host group configuration. We now have insights to where all of our network segments reside on our physical footprint.”

Security Manager

Education