Frequently Asked Questions

HYAS **Protect Policy Management**

Contents

Did I lose my existing policies with this update?

Not at all! Your existing policies are still safe and sound under the **Default** policy. Just head over to Protect Policy Management, find Default under Your Protection Policies, and click on it. You'll see all your pre-update policies right there—unchanged and still protecting your organization.

How is Policy Management different now?

The new Policy Management framework is a significant foundational upgrade. Organizations can now create multiple policies, each made up of Categories and Rules, and apply them to specific network assets.

Initially, policy assignment is limited to Source Networks, but future updates will introduce support for custom groups based on the HYAS Protect Agent and Local Active Directory integration.

As for rules—rulesets are no longer used. What you configure are now simply rules, giving you more direct and flexible control over your protection settings.

How does the Default policy work?

The Default policy acts as a fallback—it automatically applies to any network assets that don't have another specific policy assigned. It doesn't override other policies; instead, it ensures that every asset is covered, even if no custom policy has been set for it.

How do I create a new policy?

Creating a new policy is easy! Just go to **Protect Policy Management** and click the "+" next to **Your Protection Policies**. Then, give your policy a name, add a description, and choose the categories and rules you want to apply. That's it—you're ready to protect specific network assets with your custom policy.

How do I apply a policy to a Source Network?

To apply a policy to a source network, click the **Source Networks** icon in the left-hand menu. Find the one you want to update, then use the dropdown under Assigned Policy to select your desired policy. Click Save, and you're done!

Note: Each Source Network can only have one policy assigned at a time.

Why are Threat categories always locked?

Threat categories are locked by default in HYAS Protect to ensure you're automatically protected from high-risk threats like phishing, malware, and command-and-control activity—right out of the box. It's our way of guaranteeing a strong baseline of protection without requiring any initial configuration.

In which order are policies applied?

Policies are applied in a **top-down** manner. This means the order of policies listed under **Your Protection Policies** matters—whichever policy appears highest on the list and applies to a given asset will take precedence. Once a matching policy is applied, no other policies are evaluated for that asset.

What is MSSP Policy Inheritance and what's new in this release?

MSSP Policy Inheritance allows MSSPs to create policies—including **categories and lists**—that can be inherited by their child organizations. This ensures consistent protection across all orgs while reducing redundant configuration.

With this release, MSSPs gain **granular control** over policy inheritance. Previously, there was no way to restrict child organizations from creating their own policies that could override MSSP-defined ones. Now, MSSPs can:

- Enable or disable policy inheritance.
- Decide whether child organizations can create their own policies.
- Select which specific organizations are allowed to do so.

How do I enable/disable Policy Inheritance?

To configure policy inheritance, navigate to **Settings > MSSP Settings > Policy Inheritance**.

As an MSSP, how do I configure a standard policy that applies to my desired organizations?

To configure a standard policy for inheritance:

1. Go to the **MSSP** icon in the left-hand menu.

2. Select either **Categories** or **Lists**, and make your desired configuration updates.

Once saved, the configured policy will be inherited by any organization you've enabled policy inheritance for.

How do I enable/disable Policy Inheritance?

To configure policy inheritance, navigate to **Settings > MSSP Settings > Policy Inheritance**. From here, you can enable/disable Policy Inheritance, as well as defining whether to allow only specified orgs to create policies or to all orgs by default.

How do I select which organizations can/cannot create their own policies?

First, make sure **Policy Inheritance** is enabled (see instructions above). Then:

1. Navigate to the organization in question.
2. Click on **Protect Policy Management**.
3. In the top-right corner, locate the **"Permission to Create"** setting.
4. Toggle this setting based on your preference:
    - **Enabled** – The organization *can* create its own policies.
    - **Disabled** – The organization *cannot* create its own policies.

Where do I get additional information?

For more information, please see our product documentation at docs.hyas.com or reach out to support@hyas.com