Policies in ESET Security Management Center (7.x)

Anish | ESET Nederland - 2018-09-14 - Reacties (0) - ESET Security Management Center

Solution

How are policies applied to client workstations?

In ESET Security Management Center (ESMC) 7.x, policies are defined by the product. More specific policies generally overwrite less specific policies; however, you now have the ability to force a given policy setting so that it cannot be overwritten by a child policy in its own hierarchy. Groups to which a policy is applied are displayed next to it in ESMC, you can view information about which policies are being applied and the resulting configuration on each client computer.

- Groups and computers can have several policies assigned to them, and can also inherit policies from groups above their home group in heirarchy. The most important component in determining how policy rules are applied on a given device is the hierarchy of the group where that device resides.

- For devices in static groups, policies are applied in the order that groups are arranged.

- For dynamic groups, child dynamic group policies are applied first. This allows you to apply policies with greater impact at the top of the group tree and apply more specific policies for subgroups. For more detailed information about policy and group ordering, see the Online Help topic Ordering Groups.

- ESET recommends that you assign more generic policies (for example, general settings such as update servers) to groups that are higher in the groups tree. More specific policies (for example device control settings) should be assigned deeper in the groups tree. The lower policy usually overrides the settings of the upper policies when merging (unless defined otherwise with policy flags—see below for policy flag configurations). For more detailed information about merging policies, see Merging policies.

For more information on creating policies and assigning them to workstations, see Create a new policy and assign it to a group.

Force and Apply configuration settings

If the **Apply** or **Force** flag is not set, a policy setting will be applied according to the group hierarchy described in the section above. Use the **Apply** or **Force** features to define how active configuration parameters are adopted by child policies:

- **Force** —Settings with the ☒ **Force** flag have priority and cannot be overwritten by a policy set with a higher hierarchy (even if that policy has a **Force** flag). This assures that this setting will not be changed by additional policies when merging.
- **Apply** — Settings with the ☒ **Apply** flag will be sent to the client. However, when merging policies, this policy setting can be ovewritten by a different policy. When a policy is applied to a client computer, and a particular setting has the Apply flag, that setting is changed regardless of the client's local configuration. Because this setting is not forced it can be changed by other policies later on.
- **Not apply** — Settings with the flag ☒ **Not apply** are not set by policy. Because this setting is not forced it can be changed by other policies later on.

When creating policies, you can configure additional rules. These rules allow you to arrange the same settings in various policies:

- **Replace** — The default rule used when merging policies. This rule replaces the settings set by the former policy. In ERA 6.4 and earlier, **Replace** is the default and only available rule.
- **Append** — Used when applying the same setting in various policies, you can append the setting with this rule. The setting will be placed at the end of the list which was created by merging policies.
- **Prepend** — Used when applying the same setting in various policies, you can prepend the setting with this rule. The setting will be placed at the beginning of the list which was created by merging policies.

ESMC 7.x and the recent ESET security products support merging of local and remote lists in policies in a new way.

Examples:

- How policies are merged when applying flags and rules in Online Help.
- How can Administrator allow users to see all policies.

KB Solution ID: KB6830 |Document ID: 25734|Last Revised: August 17, 2018