Firewall and HIPS modes explained

- Comodo Client Security features two modules which are important to the security of your endpoints - the Firewall, and the Host Intrusion Prevention System (HIPS).

- Both these modules have in-depth settings which let you customize their security levels and general behaviour.

- These settings also let you change the protection mode of either module. The mode determines which types of file are allowed network access or execution rights.

- This article explains how to view firewall and HIPS modes, and what each mode means.

- Use the following links to jump to the section that interests you:

    - Firewall modes

   - HIPS modes

Firewall modes

- Login to Comodo one / Dragon

- Click 'Applications' > 'Endpoint Manager'

- Click 'Configuration Templates' > 'Profiles'

- Open the Windows profile applied to your target devices

    - Open the 'Firewall' tab if it has already been added to the profile

        OR

    - Click 'Add Profile Section' > 'Firewall' if it hasn't yet been added:
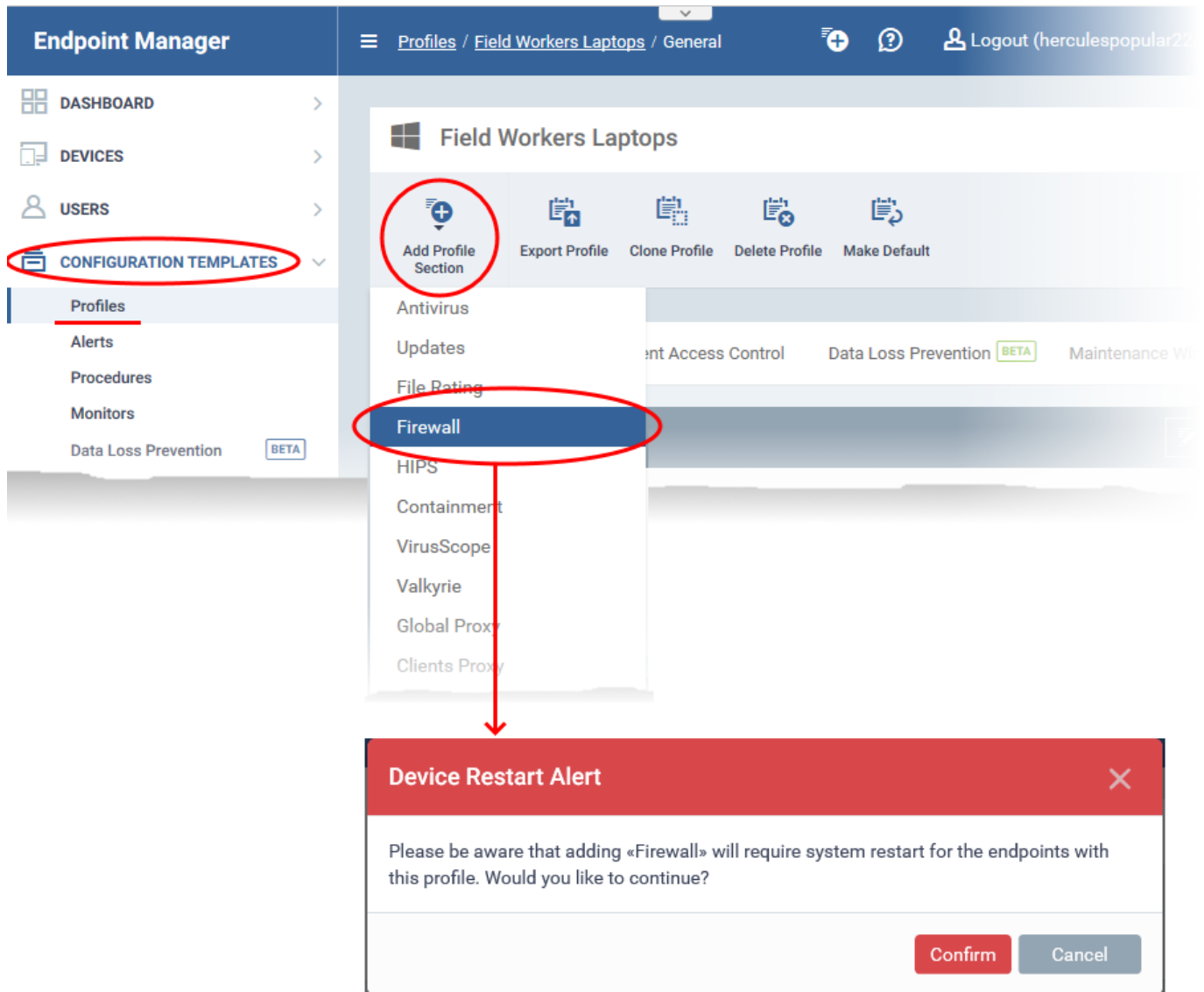
- The firewall section requires that target endpoints are restarted on application.

- Click 'Confirm' to continue

- Click the 'Firewall Settings' tab

- The upper section lets you activate the firewall and choose the firewall mode:
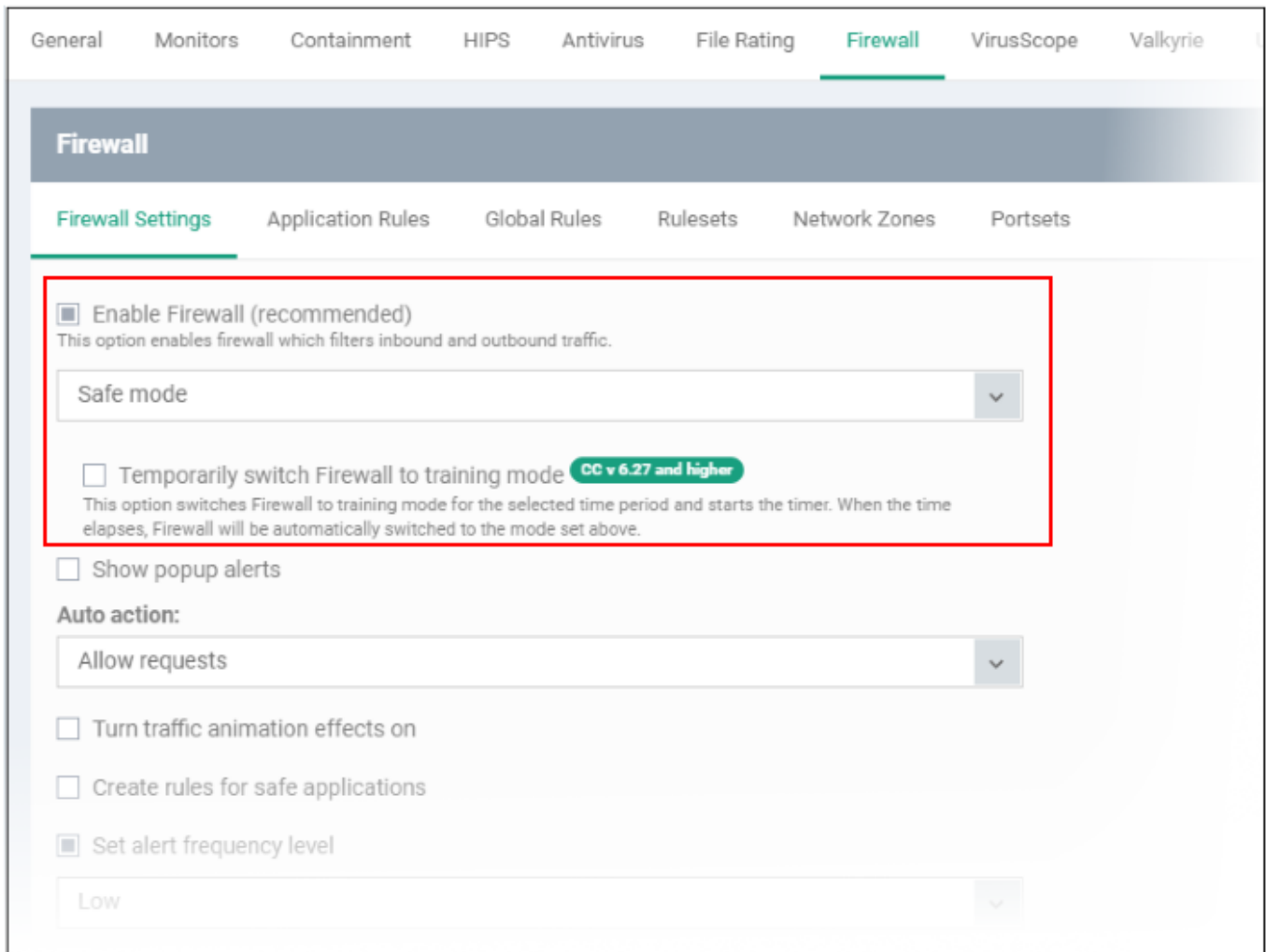
Safe Mode *(default)*

'Safe Mode' is the recommended setting for most users - combining a very high level of security with a manageable number of connection alerts.

- If 'Create rules for safe applications' is enabled, the firewall automatically adds rules to allow traffic from programs Comodo has certified as 'Safe'. 'Create rules for safe applications' can be found elsewhere on the settings page.

- You will receive alerts if unknown applications attempt to access the network/internet. You can grant access by choosing 'Treat as a Trusted Application' at the alert.

- Enable 'Do not show popup alerts' if you don't want endpoint users to see these alerts. You can choose a default action that the firewall should take instead.

Custom Ruleset

- The firewall applies ONLY the firewall rules that you have created. It will only allow traffic from applications that you have authorized in a rule.

- Users will see alerts for connection attempts by applications which are not covered by a rule. This applies even to applications on the Comodo safe list.

- Enable 'Do not show popup alerts' if you don't want endpoint users to see these alerts. You can then

choose a default action that the firewall should take instead.

Training Mode

- The firewall monitors network traffic and creates 'Allow' rules for all applications that request network access. This will continue until you come out of training mode.

- You will not receive any alerts in this mode. Only choose this mode if you are sure all applications on the endpoint are trustworthy.

- This mode is typically deployed for short periods to create a 'baseline' of trusted files on a network. Files which request network access during this period are assumed safe.

- This reduces the number of alerts during the initial deployment phase on networks with many unknown files. However, staying in training mode for extended periods can create an excessive number of rules, which may lead to endpoint performance issues.

- You can switch back to safe mode or custom mode after the baselining period is over.

**Temporarily switch Firewall to training mode**

- Place the firewall in training mode for a specific length of time. CCS will automatically revert to the mode in the drop-down when the training period is over.

- Note - Make sure you select 'Safe Mode' or 'Custom Ruleset' in the drop-down.

HIPS modes

- Login to Comodo one / Dragon

- Click 'Applications' > 'Endpoint Manager'

- Click 'Configuration Templates' > 'Profiles'

- Open the Windows profile applied to your target devices

  - Open the 'HIPS' tab if it has already been added to the profile

    OR

  - Click 'Add Profile Section' > 'HIPS' if it hasn't yet been added:
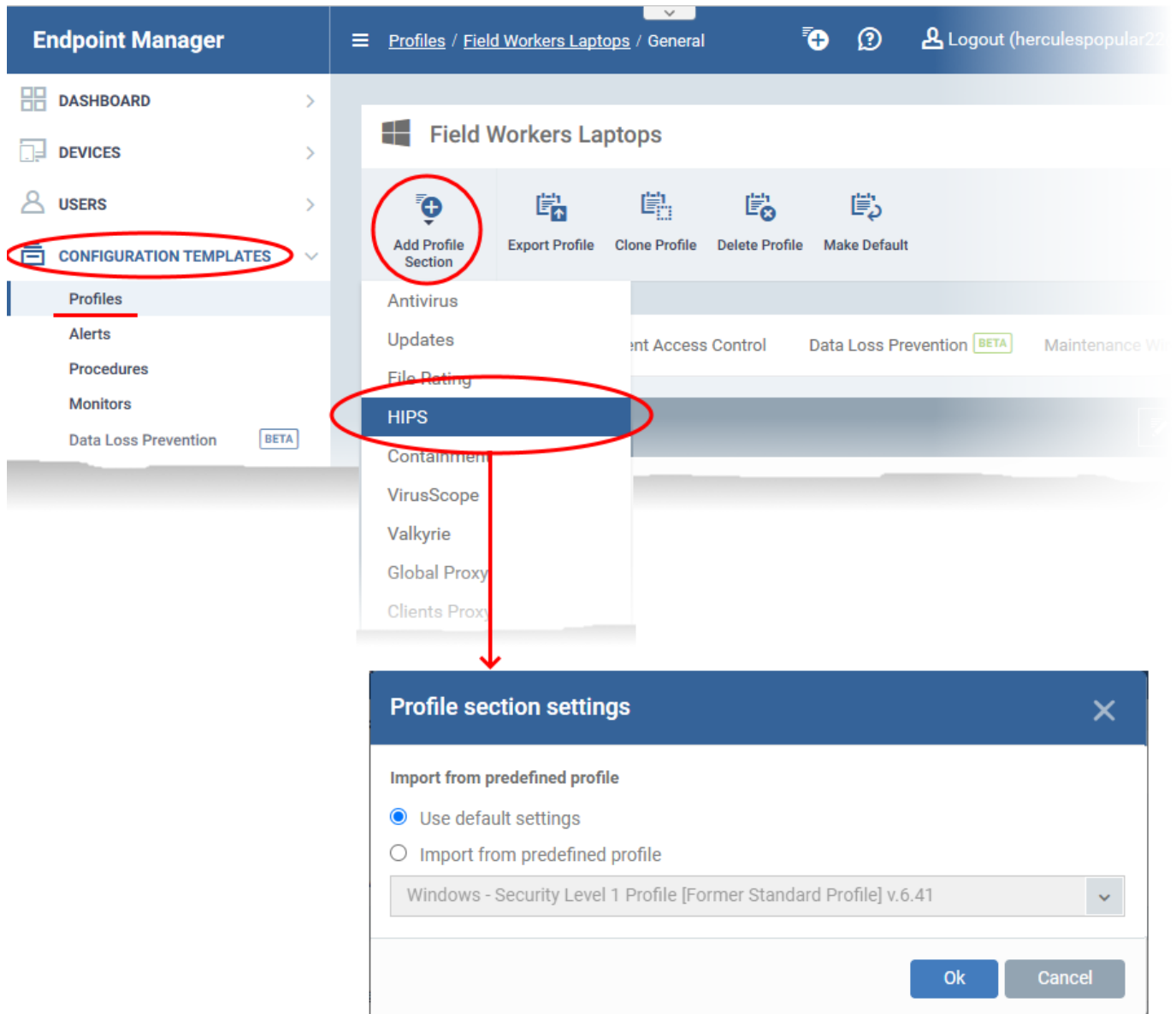
You can use the default HIPS settings or import them from a predefined profile:

- The default settings differ slightly from those in the various profiles. For example, there are two HIPS rules in the security level 1 profile, but there are no rules in the default settings.

- In either case, you can always modify the HIPS settings later as required.

- Make your selection then click 'Ok'.

- Click the 'HIPS Settings' tab

- The upper section lets you activate the firewall and choose the HIPS mode:

Paranoid Mode

- Highest security setting. HIPS will apply security controls to all files except those you have deemed safe. HIPS only obeys your configuration settings.

- HIPS does not attempt to learn the behaviour of applications, even those on the Comodo safe list. Nor does it create 'Allow' rules for them.

- Alerts are generated whenever an application attempts an unauthorized action. You can disable these alerts by selecting 'Do not show popup alerts' elsewhere on this page.

- Paranoid mode generates the highest number of alerts and is recommended for advanced users who want to complete awareness of system activity.

Safe Mode *(default)*

- Safe mode is recommended for most users and combines a high level of security with an easy-to-manage number of alerts.

- In safe mode, HIPS automatically learns the behaviour of applications on the Comodo safe list.

- 'Create rules for safe applications' is disabled by default for all predefined Endpoint Manager profiles. If 'Create rules for safe applications' is enabled on this page, then this mode also adds 'Allow' rules for safe apps.

- Users will see alerts whenever an unknown application attempts to run. They can add the app to the safe list by choosing 'Treat this application as Trusted' at the alert.

- Enable 'Do not show popup alerts' if you don't want endpoint users to see these alerts. You can choose a default action that CCS should take instead.

Training Mode

- HIPS learns the behaviour of every application and automatically creates 'Allow' rules for them. This includes any files with 'unknown' trust rating. This will continue until you come out of training mode.

- You will not receive any alerts in this mode. Only choose this mode if you are sure all applications on the endpoint are trustworthy.

- This mode is typically deployed for short periods to create a 'baseline' of trusted files on a network. Files which execute during this period are assumed safe.

- This reduces the number of alerts during the initial deployment phase on networks with many unknown files. However, staying in training mode for extended periods can create an excessive number of rules, which may lead to endpoint performance issues.

- You can switch back to safe mode or paranoid mode after the baselining period is over.

Temporarily switch HIPS to training mode

- Place HIPS in training mode for a specific length of time. CCS will automatically revert to the mode in the drop-down when the training period is over.

- Note - Make sure you select 'Safe Mode' or 'Paranoid Mode' in the drop-down.