How to password protect clients and enable local configuration

Click ‘Configuration Templates’ > ‘Profiles’ > click the name of a Windows profile > 'Add Profile Section' > 'Client Access Control'

Password Protection:

- The client access control section of a profile lets you set password protection for CCS and the communication client on an endpoint.
- Once set, users will need to enter a password to access important areas of the interfaces.
- This stops users from opening the clients locally and making changes to important tasks and settings.

Local Configuration:

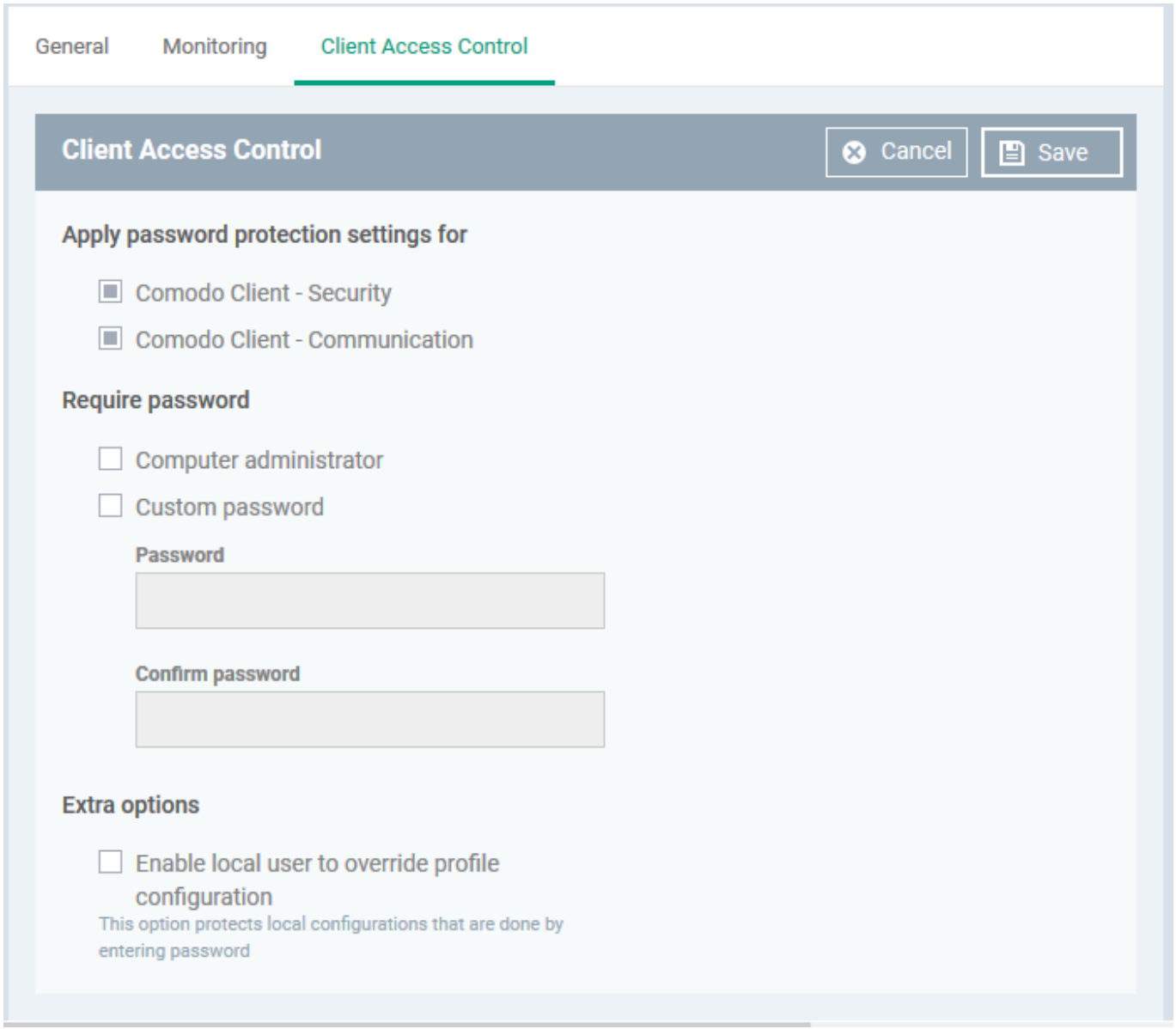
- Under normal conditions, Endpoint Manager checks managed devices every 5 minutes to make sure the local settings match the profile settings. It will reinstate the profile settings if it discovers any deviation, undoing any local changes.
- The client access control section lets you disable the process described above. This means local configuration changes will not get overruled by the profile settings. This is useful if you want the freedom to configure devices locally.

You must enable password protection if you want to enable local configuration.

Configure client access control settings

- Login to Comodo One / Xcitium
- Click 'Applications' > 'Endpoint Manager'
- Click 'Configuration Templates' > 'Profiles'
- Open the Windows profile applied to your target devices
    - Open the 'Client Access Control' tab if it has already been added to the profile

      OR
    - Click 'Add Profile Section' > 'Client Access Control' if it hasn't yet been added



- **Apply password protection settings for** - Specify which clients you want to password protect.
    - Comodo Client - Security - Password protects the settings interface, and the 'Tasks' interfaces for antivirus, firewall, HIPS, and containment.
- Users can still run some limited tasks. These include run an on-demand virus scan, open the virtual desktop, and run programs in the container.
- **Communication Client** - Password protects important settings, including the ability to configure a proxy for the client to connect to Endpoint Manager.
- **Require Password** - Select the type of password required to access CCS and/or CC:
    - **Computer administrator** - Admins can access the local interfaces by providing their domain admin password. If the admin is already logged into the machine then they can open the interface without a password.
    - **Custom password** - Specify a unique string to access the CCS / CC interfaces.

If you select ‘Custom password’ but not ‘Computer administrator’, then even admins will need to enter the custom password to access the clients.

The tables below summarize how the passwords work together for admins and regular users:

Admin logged-in			
Admin password enabled	Yes	No	Yes
Custom password enabled	Yes	Yes	No
Requirements	No password needed	Custom password required	No password needed

Admin not logged-in / Standard user logged-in			
Admin password enabled	Yes	No	Yes
Custom password enabled	Yes	Yes	No
Requirements	Either password	Custom password required	Admin password required

- **Enable local user to override profile configuration** - Endpoint Manager will not reverse local settings that are different to those in the endpoint's profile. You must enable password protection if you want to use this option.

- Click 'Save' to apply your changes to the profile.