How to set Remote control options in a profile

- ITarian Remote Control lets you take-over Windows and Mac OS devices to solve issues, install third party software and run system maintenance.
- You can also transfer files and folders between your computer and the remote computer (Windows devices only).
- You can take remote control of a device as follows:
    - Click ‘Devices’ > ‘ Device List’ > 'Device Management'
    - Select the device you want to control
    - Click the 'Remote Control' button above the table
        - Install the remote control application if required
    - Login to the application with your Comodo One/ Dragon username and password
    - Connect to the target device
- This tutorial explains how to configure remote control preferences in a profile. The settings you choose will apply when you connect to devices that use the profile.

Process in brief:

- Login to Comodo One/ Dragon
- Click ‘Applications’ > ‘Endpoint Manager’
- Click ‘Configuration Templates’ > ‘Profiles'
- Click the name of the Windows or MAC profile that you want to work on
- Open the **‘Remote Control’** tab (or click **‘Add Profile Section’ > ‘Remote Control’**)
- Configure the settings
- Click **'Save'**

Process in detail

- Login to Comodo One/ Dragon
- Click ‘Applications’ > ‘Endpoint Manager’
- Click ‘Configuration Templates’ > ‘Profiles'
- Click the name of the Windows or MAC profile that you want to work on
- Open the ‘Remote Control’ tab and click 'Edit' (or click ‘Add Profile Section’ > ‘Remote Control’)

- The configuration screens are different for Windows and Mac OS profile. Use the links below for help on each:
    - Windows Profile
    - ??Mac OS Profile

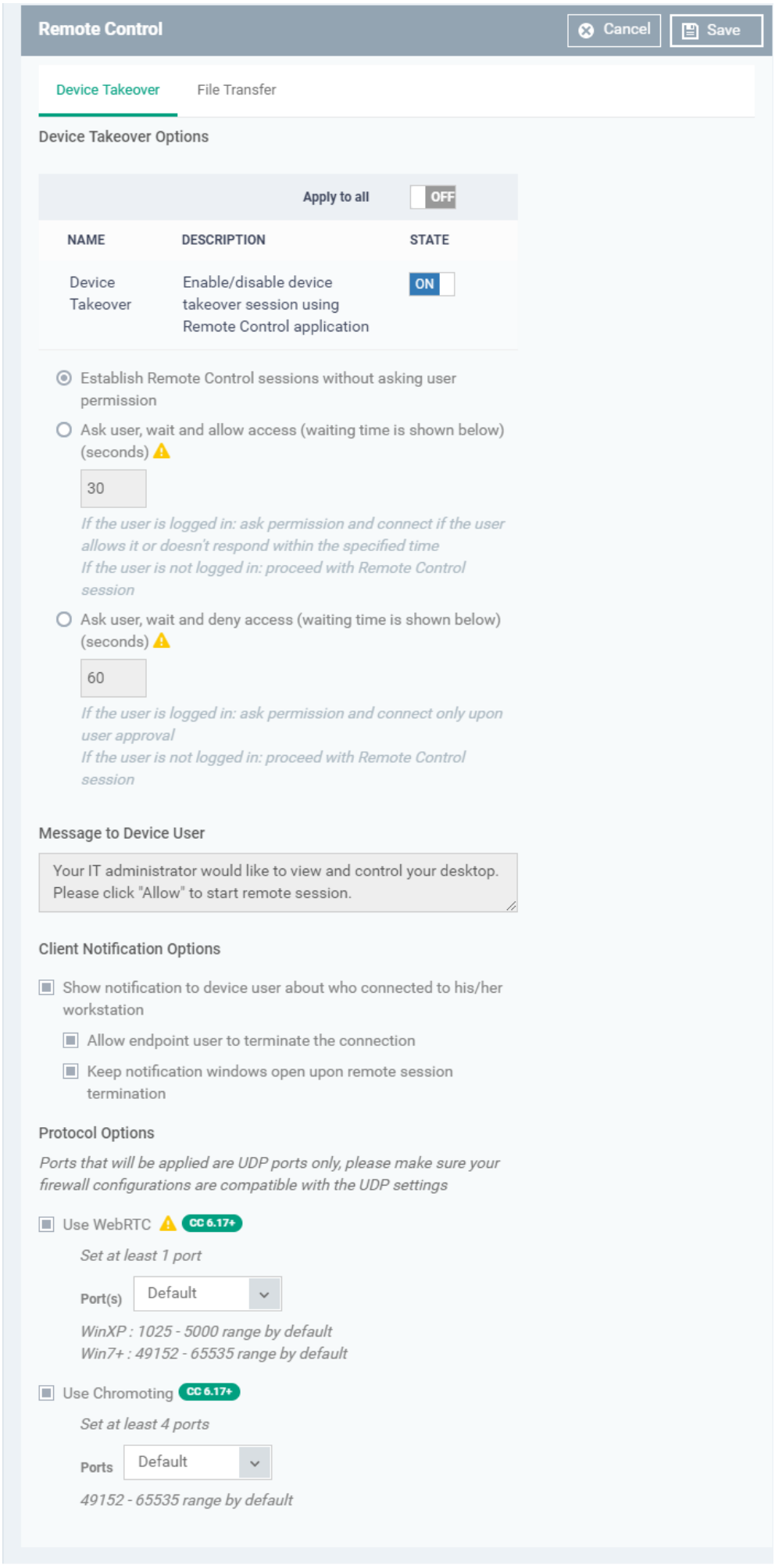
Windows Profile

The remote control configuration screen has two tabs:

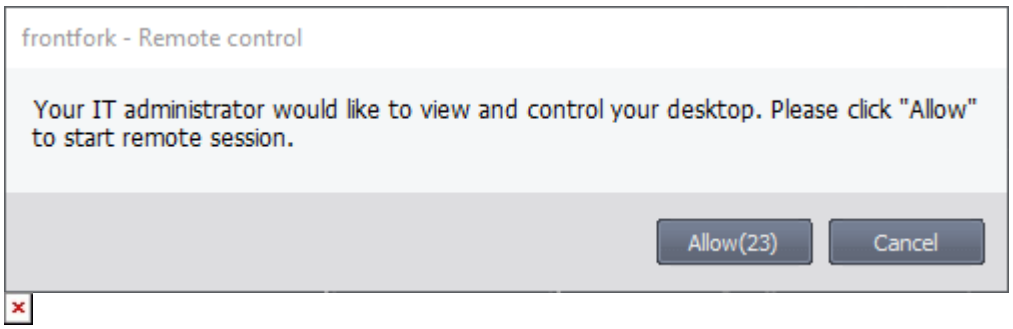
- Device Takeover
- File Transfer

Device Takeover

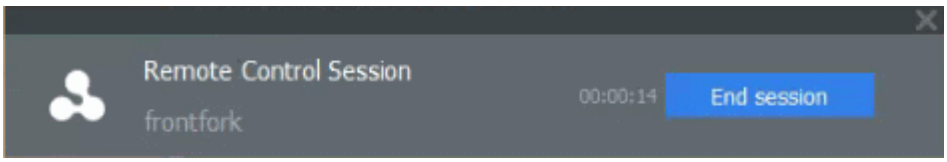
- ‘Device Takeover’ gives you full control of the remote device like a traditional RDP connection.
- For example, you can move your mouse around the remote desktop, open programs, configure the control panel, etc.
- Click the 'Device Takeover' tab and configure the options below:


Remote Control
Cancel
Save
Device Takeover
File Transfer
Device Takeover Options
Apply to all
OFF
NAME
DESCRIPTION
STATE
Device Takeover
Enable/disable device takeover session using Remote Control application
ON
Establish Remote Control sessions without asking user permission
Ask user, wait and allow access (waiting time is shown below) (seconds)
30
If the user is logged in: ask permission and connect if the user allows it or doesn't respond within the specified time
If the user is not logged in: proceed with Remote Control session
Ask user, wait and deny access (waiting time is shown below) (seconds)
60
If the user is logged in: ask permission and connect only upon user approval
If the user is not logged in: proceed with Remote Control session
Message to Device User
Your IT administrator would like to view and control your desktop. Please click "Allow" to start remote session.
Client Notification Options
Show notification to device user about who connected to his/her workstation
Allow endpoint user to terminate the connection
Keep notification windows open upon remote session termination
Protocol Options
Ports that will be applied are UDP ports only, please make sure your firewall configurations are compatible with the UDP settings
Use WebRTC
CC 6.17+
Set at least 1 port
Port(s)
Default
WinXP : 1025 - 5000 range by default
Win7+ : 49152 - 65535 range by default
Use Chromoting
CC 6.17+
Set at least 4 ports
Ports
Default
49152 - 65535 range by default

- **Device Takeover -** Use the ‘ON/OFF’ switch to allow or disable remote control of devices that use this profile.
- **Establish Remote Control without asking permission –** Take control without notifying the end-user.
- **Ask user, wait and allow access** – Show a message to the user which requests them to accept the connection. The connection will be established if the user doesn’t respond within the timeout period.
    - Enter the timeout period (in seconds)
    - Users will see the following message each time you attempt to take over their device:



    - **Ask user, wait and deny access** - Show a message to the user which requests them to accept the connection (as shown above). The connection attempt will be abandoned if the user does not respond within the timeout period.
        - Enter the timeout period (in seconds)
- **Message to Device User**
    - Enter the text of the connection request message. For example, “Your administrator would like to take control of your desktop. Click 'Allow' to accept the connection request.”
    - You can only enter a message if you chose one of the ‘Ask...’ options above.
- **Show notification to device user about who connected to his/her workstation** - Enable or disable the notification shown on the endpoint when a remote session is active:



??????????????**Allow endpoint user to terminate the connection** - Choose whether or not the 'End Session' button is shown in the notification box above. If enabled, the end-user will be able to close the connection.

    - **Keep notification windows open upon remote session termination** – The notification box is shown even after the remote takeover session is closed. The user can close the box at their discretion.
- **Protocol Options**

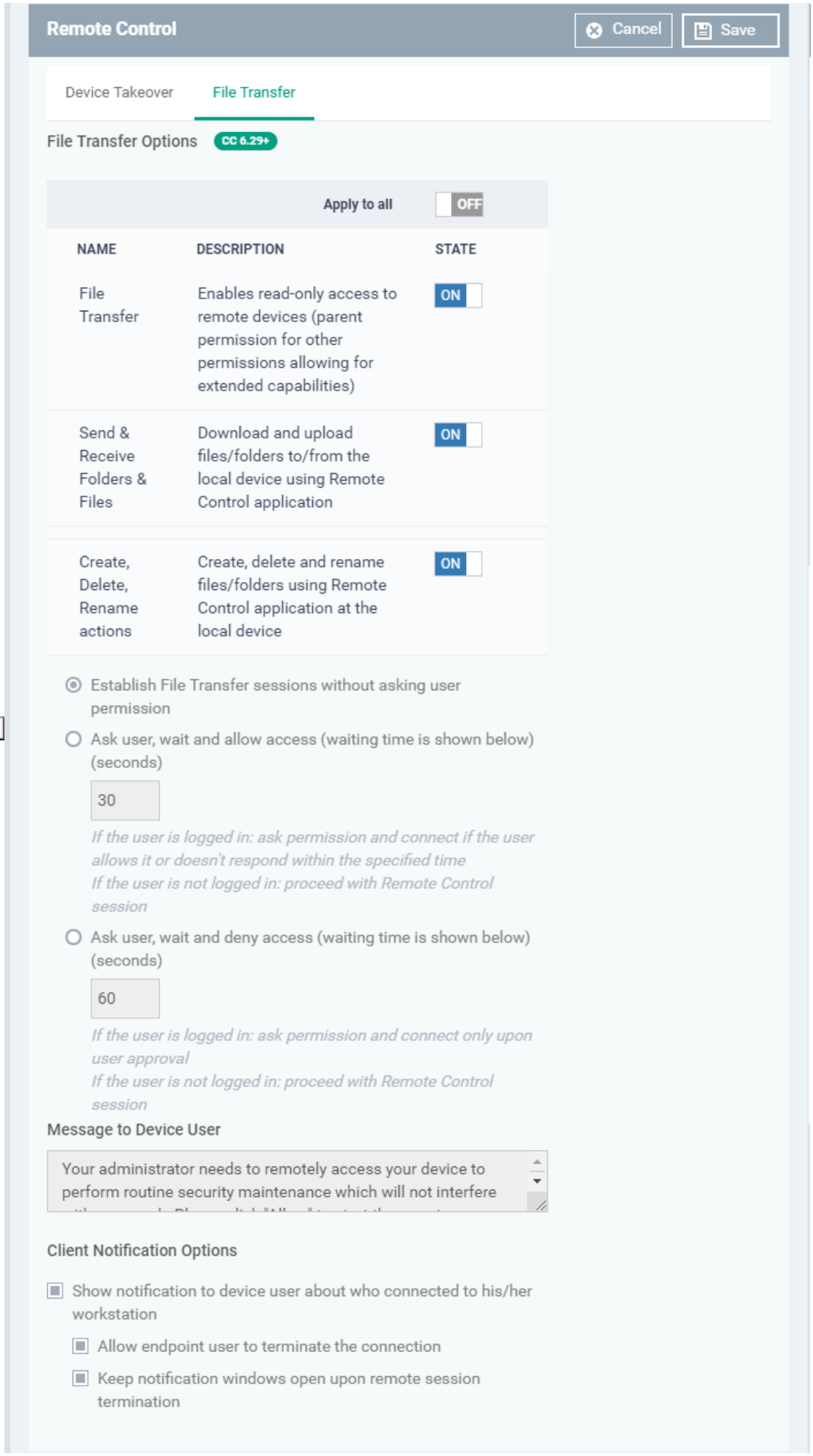
These options let you configure the protocol used for the remote takeover session.

- These settings apply to version 6.17+ of the RC tool.
- Please make sure you do not assign well-known special ports. We recommend the following port range for custom use: 49152-65535.
- You can also specify custom ports to be used by the protocol for an additional layer of safety. This lets you keep specific ports open while blocking other ports for security.

- **Use WebRTC** – The remote control tool uses the WebRTC protocol to connect to the device. This option is mandatory and cannot be deselected.
  ????
- **Ports** - Select the ports used by the WebRTC protocol. The options are:
  - **Default** - WebRTC will use port range 1025 - 5000 for Windows XP, and 49152 - 65535 for Windows 7 and above.
  - **Custom** - Specify a single custom port to be used by WebRTC
  - **Custom Range** - Specify a custom range to be used by WebRTC
- ???????**Use Chromoting** – The Chromoting protocol provides stable, high quality connections to remote devices. It is supported by Windows 7 and later (and by all MAC devices).
  - Enabled - The tool will use Chromoting to connect to devices running Windows 7 or above. It will use WebRTC to connect to Windows XP/Vista devices.
  - Disabled – The tool will use WebRTC to connect to all Windows devices.
    - **Ports**
      - **Default** - Chromoting will use the port range 49152 – 65535
      - **Custom Range** - Specify a port range to be used by Chromoting. Enter a range covering at least 4 ports.

???????
??????????????????????????????**File Transfer**

- The file transfer feature lets you perform file operations on the remote computer. For example, it allows you to copy files to and from the remote computer, and create/delete/rename items.


Remote Control
Cancel
Save
Device Takeover
File Transfer
File Transfer Options
CC 6.29+
Apply to all
OFF
NAME
DESCRIPTION
STATE
File Transfer
Enables read-only access to remote devices (parent permission for other permissions allowing for extended capabilities)
ON
Send & Receive Folders & Files
Download and upload files/folders to/from the local device using Remote Control application
ON
Create, Delete, Rename actions
Create, delete and rename files/folders using Remote Control application at the local device
ON
Establish File Transfer sessions without asking user permission
Ask user, wait and allow access (waiting time is shown below) (seconds)
30
If the user is logged in: ask permission and connect if the user allows it or doesn't respond within the specified time
If the user is not logged in: proceed with Remote Control session
Ask user, wait and deny access (waiting time is shown below) (seconds)
60
If the user is logged in: ask permission and connect only upon user approval
If the user is not logged in: proceed with Remote Control session
Message to Device User
Your administrator needs to remotely access your device to perform routine security maintenance which will not interfere
Client Notification Options
Show notification to device user about who connected to his/her workstation
Allow endpoint user to terminate the connection
Keep notification windows open upon remote session termination

File Transfer Options:

- **File Transfer** - Allows admins to view files/folders on remote devices. You can enable this setting in isolation if you only want admins to have read-access to the remote device.
  You must enable this setting in order to enable the two more powerful settings below:
- **Send & Receive Folders & Files** - Enable admins to transfer files/folders between the admin computer and the remote computer.
- **Create, Delete, Rename actions** – Enable admins to perform file operations on the remote computer.

User Permission Settings

The user permission settings are the same, or very similar, to those described in the 'Device Takeover' section above.

Click the following links to read about each setting:

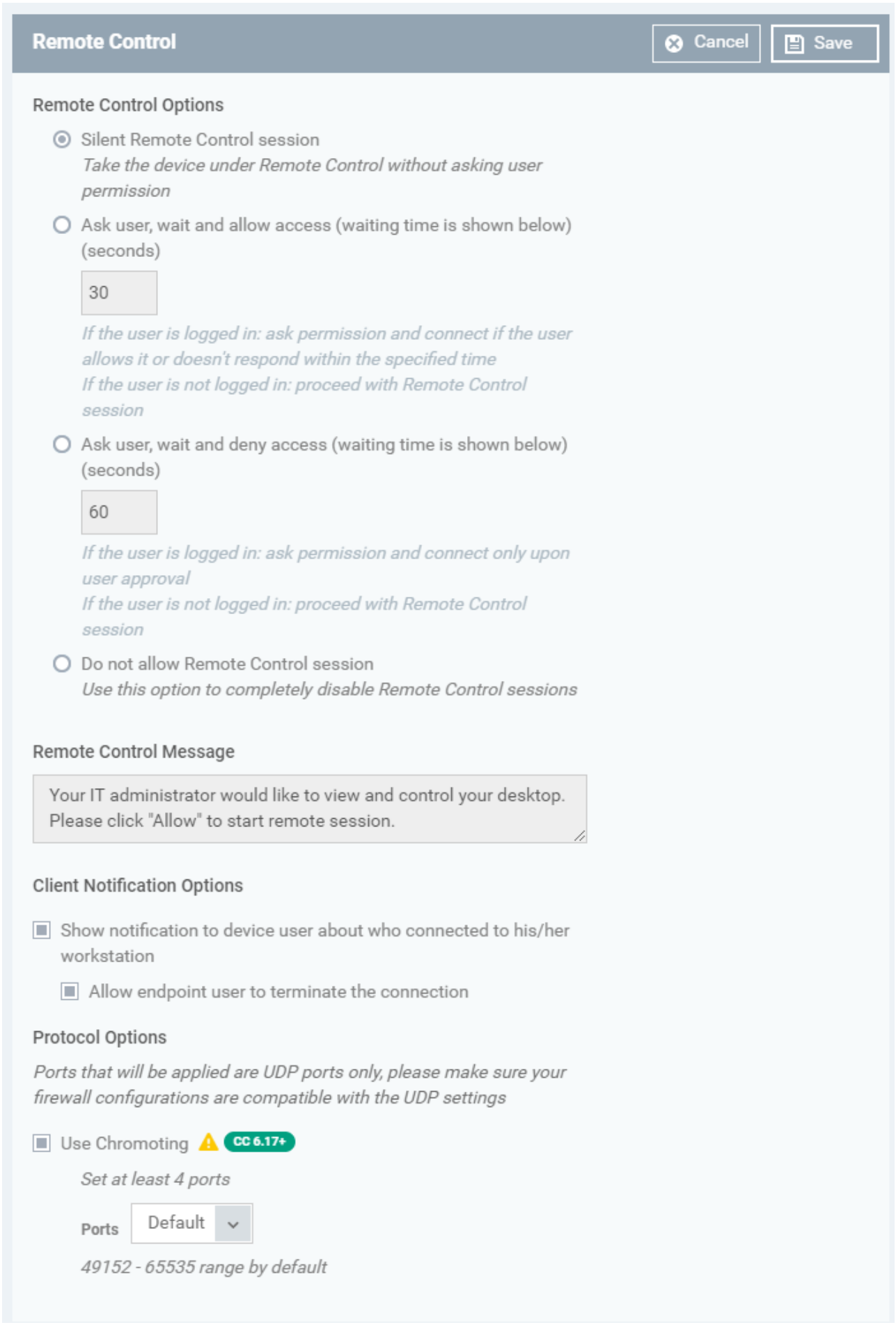
- Establish File Transfer sessions without asking user permission
- Ask user, wait and allow access
- Ask user, wait and deny access
- Remote Control Message
- Show notification to device user about who connected to his/her workstation
    - Allow endpoint user to terminate the connection
    - Keep notification windows open upon remote session termination

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

Mac OS Profile

- The remote control tool lets admins take full control of a remote MAC device.
- For example, you can move your mouse around the remote desktop, open programs, configure the control panel, etc.
  ???????
  The settings in the remote control area are similar to those described in the Windows section earlier. Please click the following links to read more about each.
- Silent Remote Control Session – Same as 'Establish without notification' in a Windows profile
- Ask user, wait and allow access
- Ask user, wait and deny access
- Do not allow remote control session – Same as choosing 'Off' for device takeover in Windows profile
- Remote Control Message
- Show notification to device user about who connected to his/her workstation
    - Allow endpoint user to terminate the connection

- Use Chromoting – Note – Chromoting is the mandatory connection protocol for MAC devices.



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

???????