

Click 'Configuration Templates' > 'Profiles' > open a Windows profile > Click 'Add Profile Section' > 'Updates'

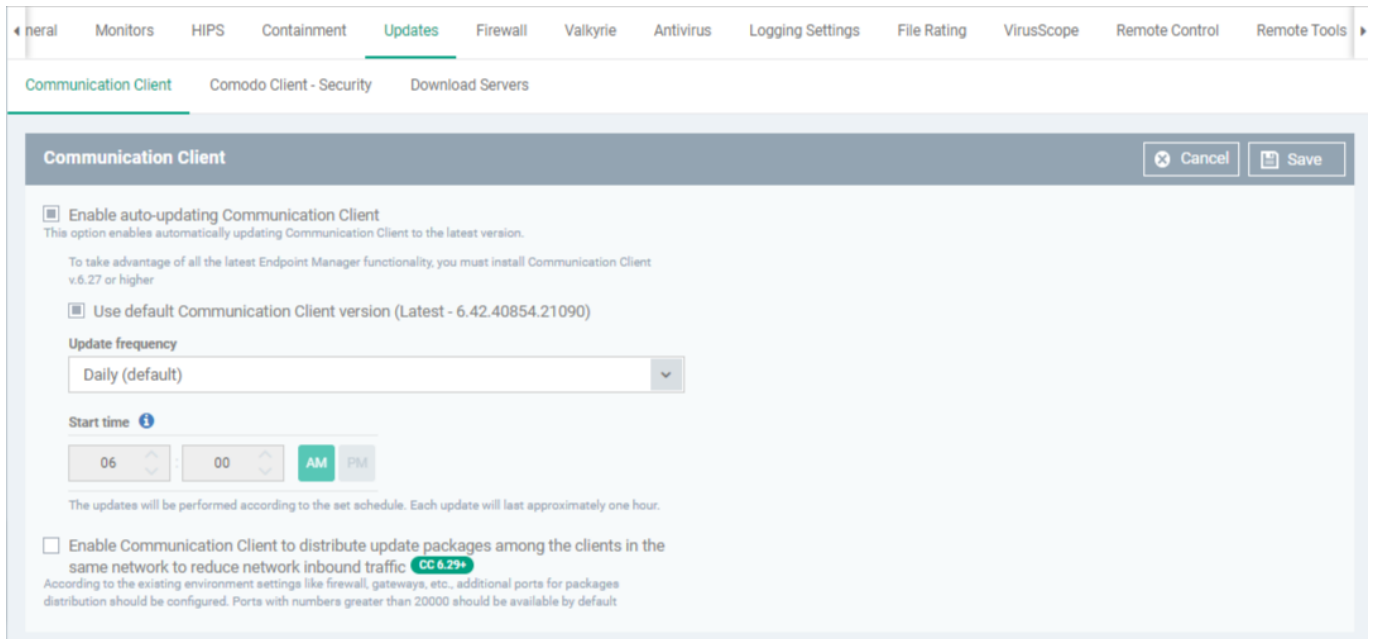
- The updates section of a Windows profile lets you configure how and when managed devices should check for client updates.
- Endpoint Manager uses two types of clients:
 - **Communication Client (CC)** - The communication client is an agent installed on your managed devices. It receives commands and tasks from the Endpoint Manager and implements them on those devices. The client also informs the Endpoint Manager of the endpoint's status.
 - **Comodo Client - Security (CCS)** - This is the security software. CCS provides advanced endpoint protection such as antivirus, firewall, threat-containment, web-filtering, and more.
- You can enable automatic updates, specify which version to install, choose update frequency, and enable local updates.
- This article explains how to add and configure an 'Updates' section on a configuration profile.

Use the following links to jump to the task you need help with:

- [Add 'Updates' section to a profile](#)
- [Update settings for the communication client \(CC\)](#)
- [Update settings for the Comodo Client Security \(CCS\)](#)
- [Setup local download servers](#)
- [Global CC settings](#)

Add 'Updates' section to a profile

- Login to ITarian
 - Click 'Applications' > 'Endpoint Manager'
 - Click 'Configuration Templates' > 'Profiles'
 - Click the 'Profiles' tab
 - Open the Windows profile applied to your target devices
 - Open the 'Updates' tab
- OR
- Click 'Add Profile Section' > 'Updates', if it hasn't yet been added

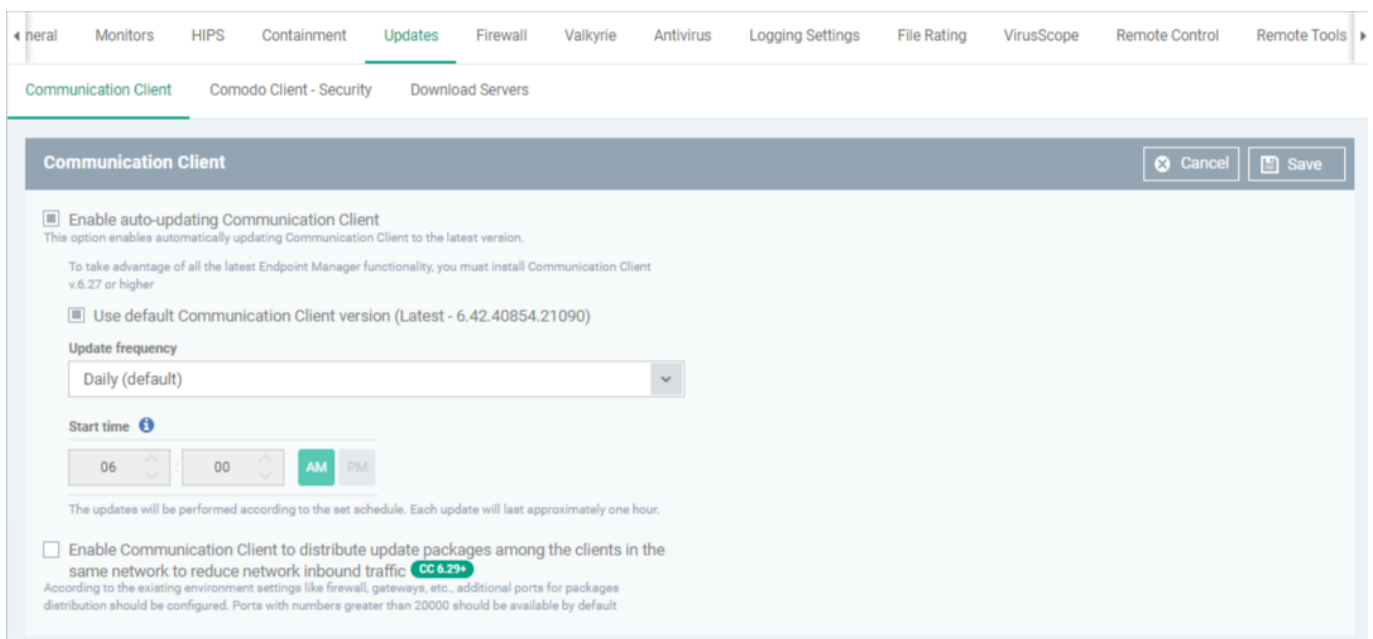


There are three tabs:

- [Communication Client](#) - Enable automatic updates for CC.
- [Comodo Client - Security](#) - Enable automatic updates for CCS
- [Download Servers](#) - Specify a proxy server from which managed endpoints should collect updates.

Update settings for the communication client (CC)

- Open the 'Updates' section of a profile
- Click the 'Communication Client' tab, then 'Edit':



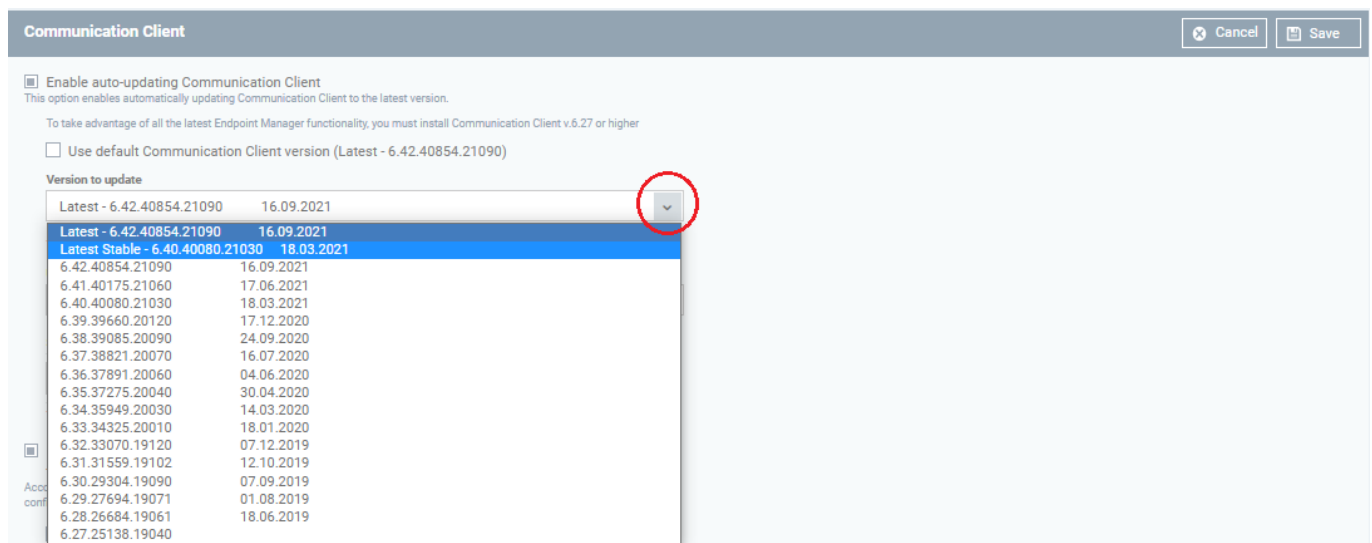
- **Enable auto-updating Communication Client** - Forces the endpoint to check for and install CC program updates at the selected frequency. You can set the location of the download server in the

'Download Servers' tab. Deselect if you want to disable auto-updates

- You can also manually update clients by clicking 'Devices' > 'Device List' > select your target devices > Click 'Install or Update Packages' button.
- See this [help page](#) if you want more assistance with manual updates.
- **Use default Communication Client version** - Choose whether or not to always update to the 'default' version.
 - **Enabled** - The client will always update to the default version (**Default**). Under normal conditions, the default version is the latest version.
 - **Disabled** - You choose the version to which the client updates. Make sure you choose a higher version than already installed.

Note 1. You can change the 'default' version in 'Settings' > 'Portal Set-up' > 'Client Settings' > 'Windows' > 'Comodo Client'.

Note 2. You can only change the version if 'Change version while updating' is enabled in 'Settings' > 'Portal Set-up' > 'Client Settings' > 'Windows' > 'Comodo Client'. If it is not enabled, then the default version is automatically deployed. You will be able to choose "Latest Stable Version" if there are any issues with the latest versions of the CCC.



See [Global CC settings](#) at the end of this page to read more.

- **Update Frequency** - Choose how often CC should check for updates:
 - **Daily (Default)** - The client checks for updates every day at 6:00 am.
 - **Daily (custom)** - The client checks for updates every day at the time you specify
 - **Weekly** - Select the days and times that you want the client to check for updates
 - **On selected days** - Choose one or more days in a month to check for updates. For example,

you might want to update on the first and third Wednesdays of every month.

- **Monthly** - Select the date and time in a month to check for updates

Use default Communication Client version
(Latest - 6.33.33567.20010)

Update frequency

Weekly

Start time ⓘ

11 : Minutes AM PM

The updates will be performed according to the set schedule.
Each update will last approximately one hour.

Days of the week [Select All](#) | [Reset](#)

Sunday Monday Tuesday Wednesday **Thursday** Friday Saturday

Enable Communication Client to distribute updates to other endpoints in the network

- **Enable Communication Client to distribute updates to clients in the same network** - Download updates to a managed endpoint, then use that endpoint as the source from which other endpoints collect their updates.

This saves internet bandwidth and accelerates updates in large networks.

If enabled, your endpoint clients will follow this process at update time:

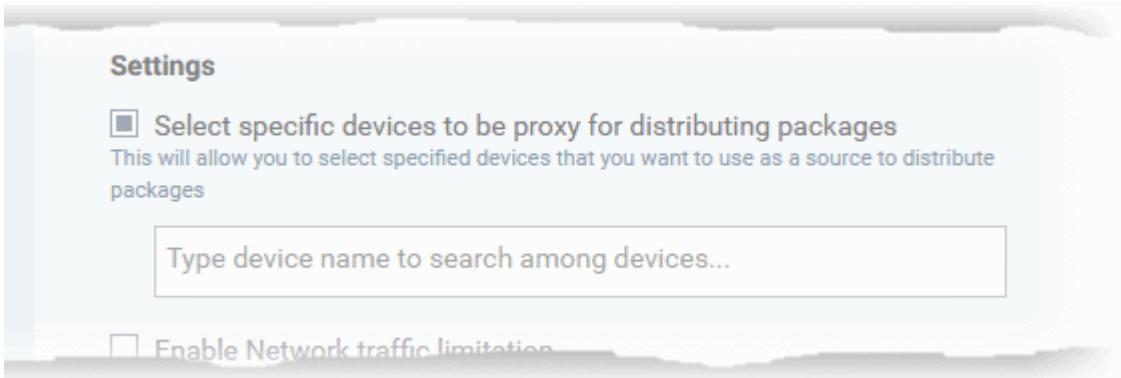
- The endpoint first checks other endpoints to see if the update is installed on them
- If available, the client fetches the update from the local endpoint
- If not available, the client downloads the update from the server set in the '[Download Servers](#)' tab
- This endpoint becomes the source from which other endpoints collect their updates.

You can also choose the types of updates that use this mechanism:

- **Communication Client updates** (Version 6.29 or higher)
- **Comodo Client Security updates** (Version 11.4 or higher)
- **Antivirus Database updates** (Version 11.4 or higher)



- **Select specific devices to be proxy for distributing packages** - Choose specific devices from which endpoints should collect updates. If you do not enable this option then any device in the local network can act as a source.
 - Enter the names of the target devices in the field provided.
 - You can add multiple devices as sources. Endpoints will collect from the first source they find which has the update.



- **Enable Network traffic limitation** - The maximum % of network bandwidth that can be used to share updates. (Default = 30%)
- **Enable device count limitation** - The maximum number of devices with which the client is allowed to simultaneously share updates. (Default = 10, Maximum = 20).
- **Use download servers directly in case of any communication issue** - If the endpoint cannot contact other endpoints it will instead collect the update from the server in the 'Download Servers' tab.
- Click 'Save'.

The following table shows how clients will collect updates in different scenarios:

| | Option | | | Client fetches update from: |
|------------|---|---|---|---|
| | Enable Communication Client to distribute ... | Select specific devices to be proxy ... | Use download servers directly in case ... | |
| Scenario 1 | ✓ | X | X | Any local device which already has the update |
| Scenario 2 | ✓ | ✓ | X | Only from selected devices |
| Scenario 3 | ✓ | X | ✓ | 1. Any device in the local network 2. Download servers |
| Scenario 4 | ✓ | ✓ | ✓ | 1. Selected devices 2. Download servers |

Update settings for the Comodo Client Security (CCS)

- Open the 'Updates' section of a profile
- Click the 'Comodo Client - Security' tab then 'Edit':

The screenshot shows the 'Updates' tab of the Comodo Client Security settings. The window title is 'Comodo Client - Security' and it has 'Cancel' and 'Save' buttons. The settings are organized into two main sections: 'Application Updates' and 'Virus database updates'.

Application Updates

- Enable auto-updating Comodo Client - Security
This option enables automatically updating CCS to the latest version.
- Update frequency**
Daily (default)
- Start time** ⓘ
7 : Minutes AM PM
- Skip updates if the device is offline
- Reboot options**
 - Force the reboot in
5 minutes
 - Suppress the reboot ⓘ
 - Warn about the reboot and let users postpone it
- Reboot message**
Enter a message that the device owner will get before the reboot

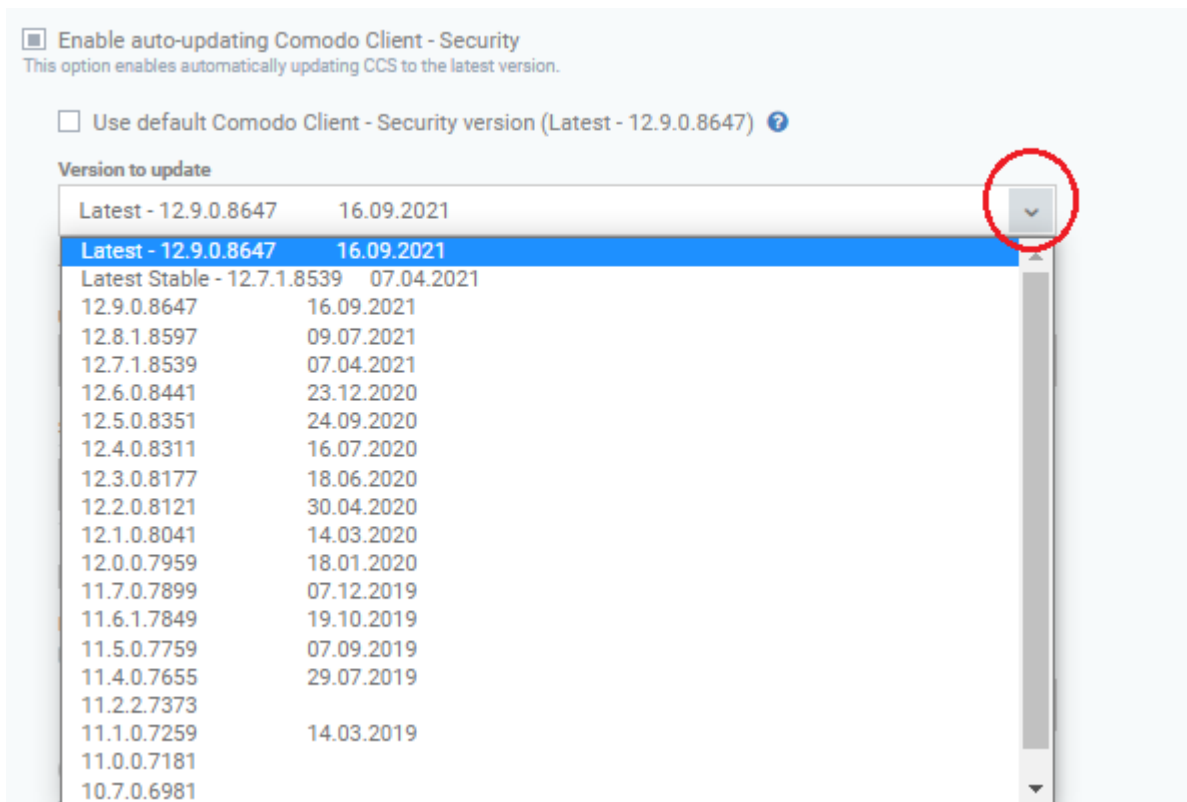
Virus database updates

- Check for database update every
1 Hours
- Do not check for updates if running on battery
- Check for updates during Windows Automatic Maintenance
Applies to Windows 8 and higher

- **Enable auto-updating Comodo Client - Security** - Forces the endpoint to check for and install CCS program updates at the selected frequency. You can set the location of the download server in the

'Download Servers' tab. Deselect if you want to disable auto-updates.

- **Use default Comodo Client - Security version** - Choose whether or not to always update to the 'default' version.
 - **Enabled** = The client will always update to the default version (Default)
 - **Disabled** = You can choose the version to which the client updates. Make sure you choose a higher version than already installed. You cannot install a lower version than the current version.



Note 1. You can configure the default version in 'Settings' > 'Portal Set-up' > 'Client Settings' > 'Windows' > 'Comodo Client'. Under normal conditions, the default version is the latest version.

Note 2. You can only change the version if 'Change of version while updating' is enabled in 'Settings' > 'Portal Set-up' > 'Client Settings' > 'Windows' > 'Comodo Client - Security'.

- **Update Frequency** - Choose how often CCS should check for updates. The available options are:
 - **Daily (Default)** - The client checks for updates every day at 6:00 am.
 - **Daily (custom)** - The client checks for updates every day at the time you specify
 - **Weekly** - Select the days and times that you want the client to check for updates
 - **On selected days** - Choose one or more days in a month to check for updates. For example, you might want to update on the first and third Wednesdays of every month.

- **Monthly** - Select the date and time in a month to check for updates
- **Skip updates if the device is offline** - Updates will not be installed if the endpoint is not connected to EM.
- **Reboot Options** - Configure how the endpoint should restart after the update is installed:
 - **Force the reboot in** - Restart the endpoint for a certain period of time after installation. You can choose 5, 10, 15 or 30 minutes. Enter a message in the field provided to inform users about the reboot.
 - **Suppress the reboot** - Do not restart the machine after the updates. CCS will only become fully functional after the device is restarted.
 - **Warn about the reboot and let users postpone it** - Show an alert to the user which advises them that their computer needs to be restarted. Please type the message in the space provided.

The alert lets end-users restart the endpoint immediately or postpone the restart till later.

- **Virus database Updates** - Choose when the endpoint should check for and download virus signature updates
 - **Check for database update every** - Specify how often CCS should check for and install virus updates.
 - **Do not check for updates if running on battery** - Only check for updates if the computer is connected to the mains supply. Useful for laptops and other battery-driven devices.
 - **Check for updates during Windows Automatic Maintenance** - CCS will check for virus updates when Windows enters maintenance mode. The check will run at maintenance time *in addition* to the configured schedule. Only applies to Windows 8 and later.
- Click 'Save'.

Setup local download servers

The download servers tab lets you configure proxy servers from which endpoints should collect updates.

Local proxies can help save bandwidth and accelerate the update process when a large number of endpoints are involved.

You can configure different servers for Comodo Client Security and Comodo Client Communication.

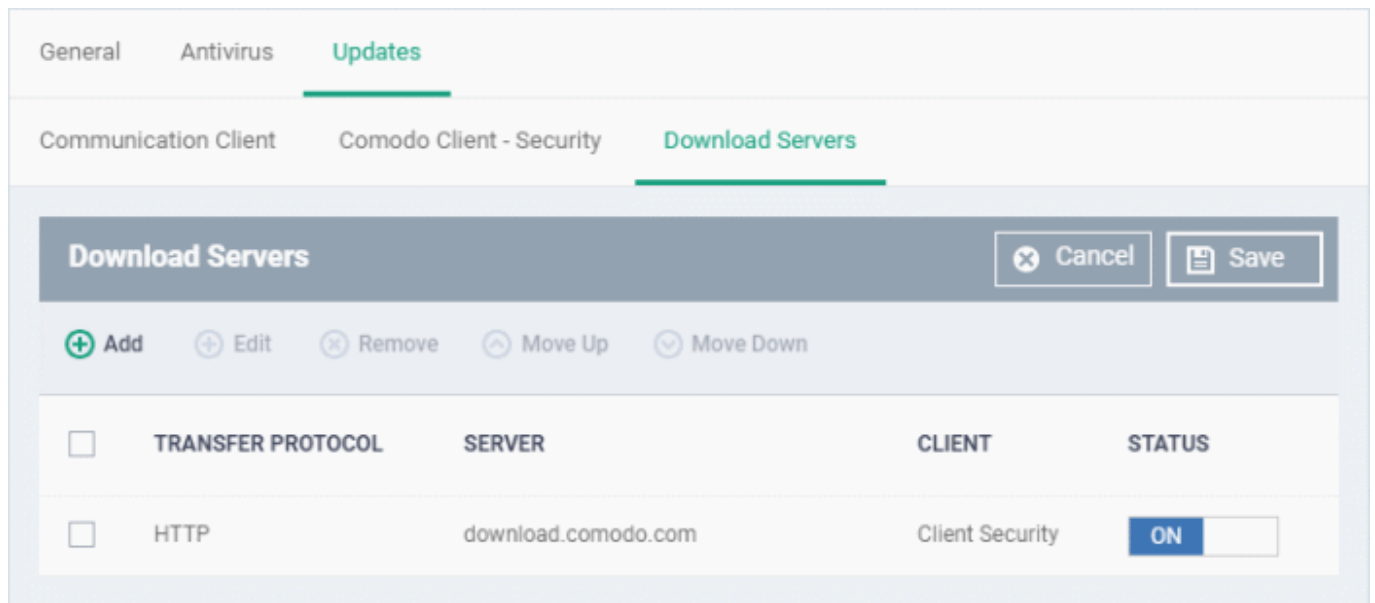
Prerequisite - You need to install 'ESM Update Mirror' on your proxy to collect the initial update files from Comodo servers. Your endpoints will then download the updates from the proxy.

- Download the setup file from <https://drive.google.com/file/d/0B4qKr5xfENWBS0FOUHM2VDFQMnc/view>.
- Run the setup file on a Windows server and follow the installation wizard.
- Ensure that the service has started:

- 'Run' > Enter 'services.msc' > locate 'Apache2.2'.
- Click the 'Start' link on the left if the service is not running.

Configure download servers

- Open the 'Updates' section of a profile
- Click the 'Download Servers' tab then 'Edit':



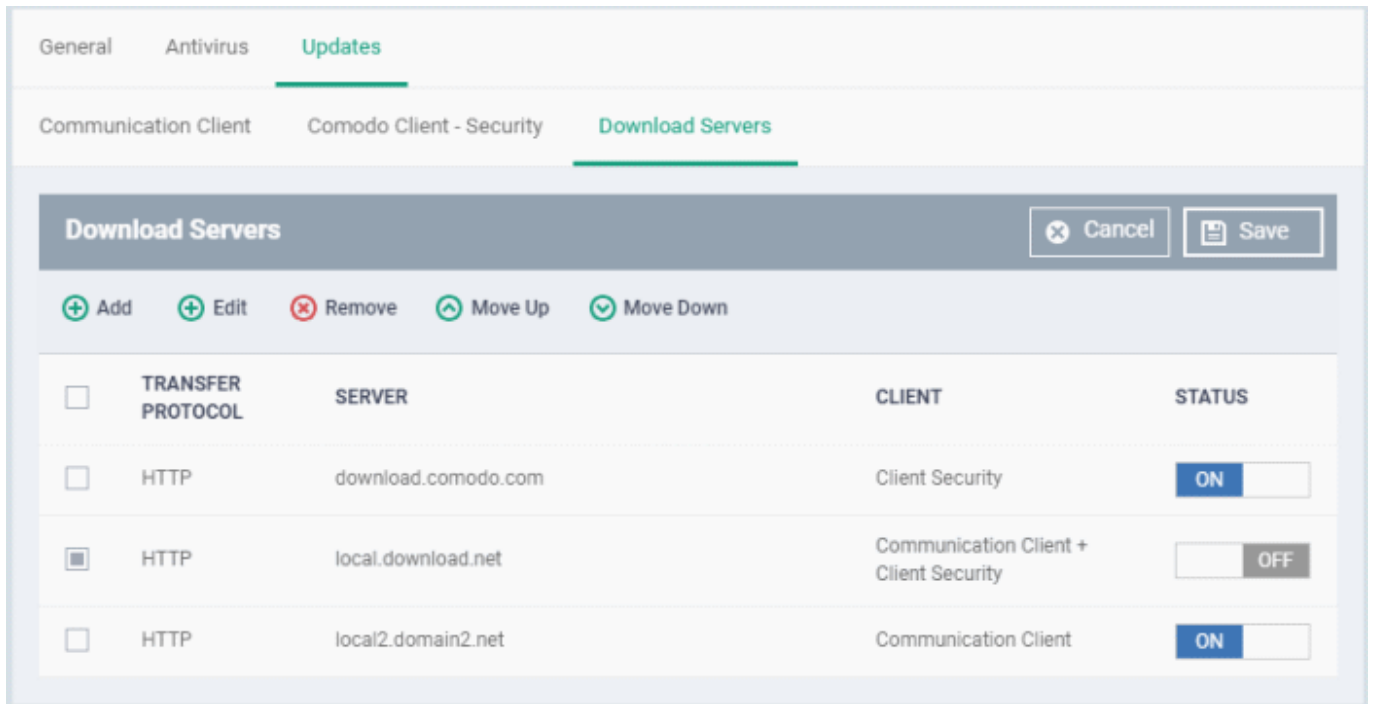
By default, endpoints will download updates from Comodo servers (download.comodo.com). You can add your local proxy servers here and enable/disable servers as required.

- Click 'Add'



- **Transfer Protocol** - Select HTTP or HTTPS
- **Host** – Enter the IP address or hostname of your proxy
- **Client** - Select which items should be collected from the proxy:
 - **Communication Client** - Endpoints will collect communication client (CC) updates from the proxy server.
 - **Client Security** - Endpoints will collect security client (CCS) updates from the proxy server, including virus database updates.
 - **Communication Client + Client Security** - Endpoints will collect both CC and CCS updates from the proxy.
- Click 'Add'.

- Repeat the process to add more servers.



- Use the 'on-off' switch to enable or disable a server. You need to enable the server in order for endpoints to use it
- Endpoints will request updates from servers in the order they appear in this list, with the server at the top getting consulted first.
- You can re-prioritize the list by selecting a server then clicking 'Move Up' or 'Move Down'
- Click 'Save' your changes take effect

Global CC settings

Click 'Settings' > 'Portal Set-Up' > 'Client Settings' > 'Windows' > 'Communication Client'

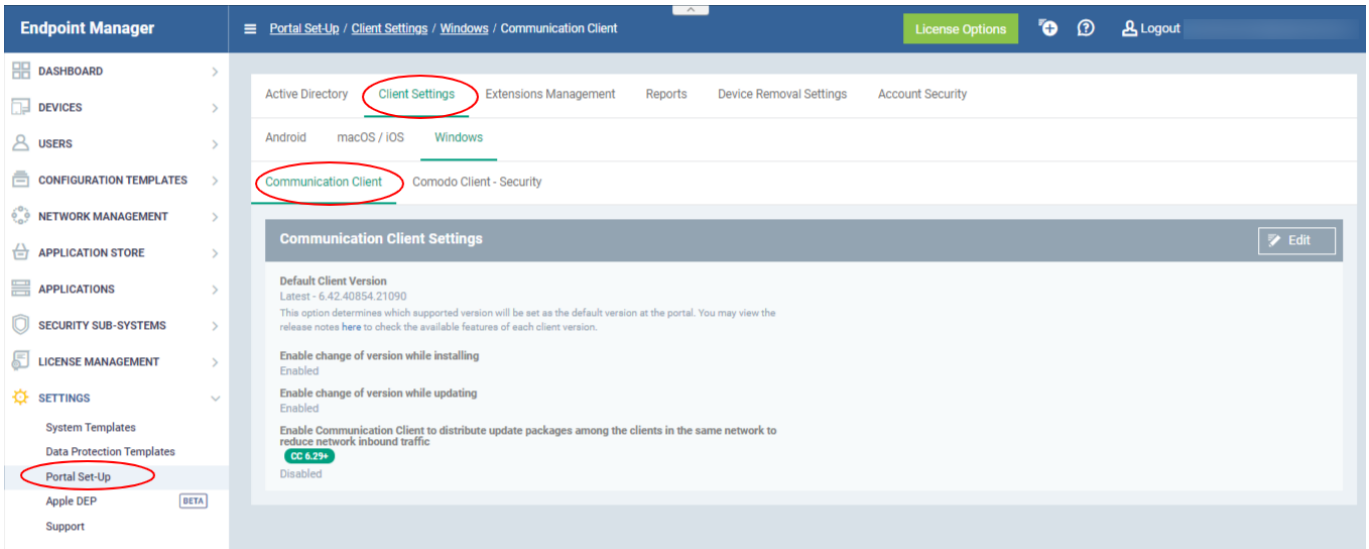
The settings area lets you:


- Configure update intervals
- Set the 'Default client version' which is installed on your endpoints. This is set to always fetch and install the latest version unless you specify otherwise.
- Specify whether admins can change the version of the client installed on an endpoint.
- Choose whether to use an endpoint as the source from which other endpoints collect their updates. This can save time and bandwidth versus each endpoint downloading directly from the server.

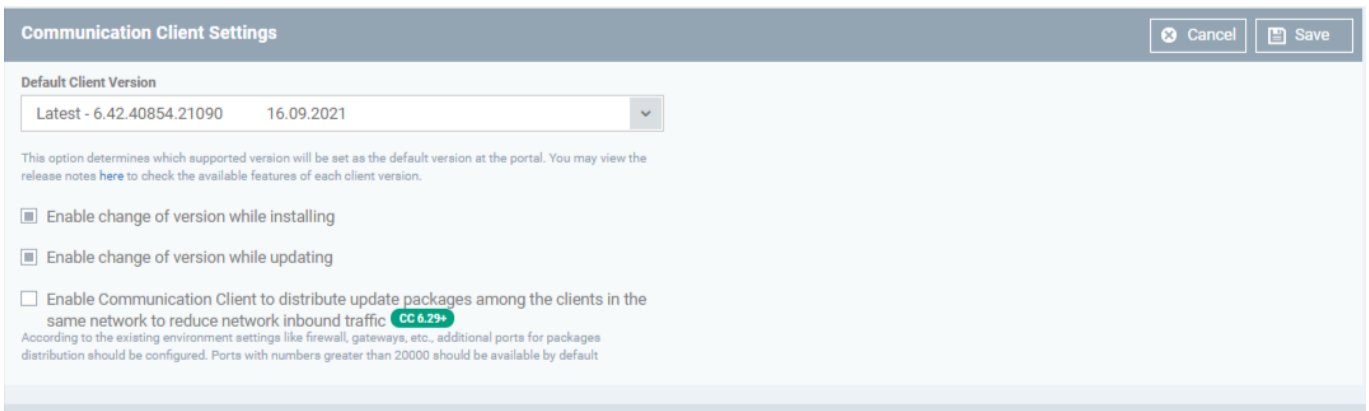
Configure the communication client

- Click 'Settings' > 'Portal Set-Up' > 'Client Settings'

- Click the 'Windows' tab > 'Communication Client'



- Click the edit button  on the right to modify the default settings



Default Client Version - Determines which agent version should be installed on endpoints.

- Choose the default agent version from the drop-down. (Default = 'Latest').
- You will be able to choose “Latest Stable Version” if there are any issues with the latest versions of the CCC.

Enable change of version while installing – Choose whether installation wizards allow admins to change the version of the client that gets installed.

If enabled, admins can choose the version of the client they want to install in the following wizards:

- **Enroll devices** - 'Devices' > 'Device List' > 'Enroll Device'
- **Bulk installation** - 'Devices' > 'Bulk Installation Package'

Enable change of version while updating – Choose whether admins can update a client to a version other than the 'Default' version. (Default = Disabled)

If enabled, admins can choose the version of the client they want to update to in the following wizards:

- **Update additional packages** - 'Devices' > 'Device List' > 'Install or Update Packages' > 'Update Additional Packages'
- **Updates section of Windows profile** - 'Configuration Templates' > 'Profiles' > 'Windows Profile' > 'Updates' profile section

Note - Make sure to upgrade to a higher version. Installing a lower version than the existing agent is not supported.

Enable Communication Client to distribute update packages among the clients in the same network to reduce network inbound traffic - Download updates to a managed endpoint, then use that endpoint as the source from which other endpoints collect their updates.

This saves internet bandwidth usage and accelerates updates in large networks.

If enabled, your endpoint clients will follow this process at update time:

- The endpoint first checks other endpoints to see if the update is installed on them
- If available, the client fetches the update from the local endpoint
- If not available, the client downloads the update from the default download servers
- This endpoint then becomes the source from which other endpoints collect their updates.
- You can choose the type of updates that use this mechanism:
 - **Communication Client updates** (Version 6.29 or higher)
 - **Comodo Client Security updates** (Version 11.4 or higher)
 - **Antivirus Database updates** (Version 11.4 or higher)

Enable Communication Client to distribute update packages among the clients in the same network to reduce network inbound traffic **CC 6.29+**

According to the existing environment settings like firewall, gateways, etc., additional ports for packages distribution should be configured. Ports with numbers greater than 20000 should be available by default

Communication Client packages

Comodo Client - Security packages **CCS 11.4+**

Comodo Client - Security Antivirus Database packages **CCS 11.4+**

Settings

Enable Network traffic limitation
This setting enables you to define maximum amount of network traffic to be used for distribution of packages

Less than or equal to (%)

30

Enable device count limitation
This setting enables you to define maximum number of devices to be used for distribution of packages

Less than or equal to

10

Use download servers directly in case of any communication issue
This option enables you to use download servers that is listed in Download Servers Tab in profiles under Updates section in case of any communication issue with ditribution mechanism. Please note that if this is not selected, in

- **Enable Network traffic limitation** - The maximum % of network bandwidth that can be used to share updates. (Default = 30%)
- **Enable device count limitation** - The maximum number of devices with which the client is allowed to share updates. Default = 10.
- **Use download servers directly in case of any communication issue** - If the endpoint cannot contact other endpoints, it will collect the update from the main server.
- Click 'Save' to apply your changes.

Notes:

- The settings described in this section are 'global' settings that apply to all endpoint clients. However, you can also configure client update settings in the 'Updates' section to profile.
- There is one overlapping item between these two - '[Enable the communication client to distribute packages to other clients in the network](#)'.
- Endpoint Manager prioritizes this setting as follows:
 - If you *do not add* an update section to the profile, then the global settings apply
 - If you *do add* an update section, then Endpoint Manager will ignore the '...distribute...' settings in global settings

