

# How to clone and customize a profile then apply to devices or users

Click 'Configuration Templates' > 'Profiles'

- Configuration profiles let you specify a device's network access rights, overall security policy, scan schedule and other general settings.
- Once created, profiles can be applied to devices/device groups, and users/user groups.
- You can use a 'Default' profile shipped with Endpoint Manager, or configure your own custom profile.
- 'Cloning' a profile is a fast way to create a custom profile without starting from scratch. You can just edit the cloned profile to implement the specific settings you want.

Use the links below to jump to the section you need help with:

- [Clone a profile](#)
- [Customize the profile](#)
- [Apply the profile to devices](#)
- [View profiles associated with a device](#)
- [Default profiles](#)
- [Further reading](#)

## Clone a profile

- Log into ITarian
- Click 'Applications' > 'Endpoint Manager'
- Click 'Configuration Templates' > 'Profiles'



The screenshot shows the Endpoint Manager interface. On the left is a navigation menu with 'CONFIGURATION TEMPLATES' highlighted in a red box. The main area is titled 'Profiles' and shows a 'Default Profiles' section. Below this section are several action buttons: 'Create', 'Import', 'Export Profile', 'Clone Profile', 'Delete Profile', and 'Export'. A table lists various profiles with columns for 'OS', 'NAME', and 'CREATED BY'.

OS	NAME	CREATED BY
	Windows - Containment Only Profile 7.1	admin
	[cloned] Windows - Security Level 1 Profile v.7.1	comodo-pm-support@yopmail.com
	cloned[cloned] [cloned] Windows - Security Level 1 Profile v.6...	comodo-pm-support@yopmail.com
	[cloned] Windows - Security Level 1 Profile v.7.0	comodo-pm-support@yopmail.com
	[cloned] Windows - Security Level 1 Profile v.6.44	comodo-pm-support@yopmail.com
	[cloned] Windows - Security Level 1 Profile v.6.42	comodo-pm-support@yopmail.com
	TNS Monitors	comodo-pm-support@yopmail.com
	sample_prof_without_default	comodo-pm-support@yopmail.com
	sample_prof_with_default	comodo-pm-support@yopmail.com

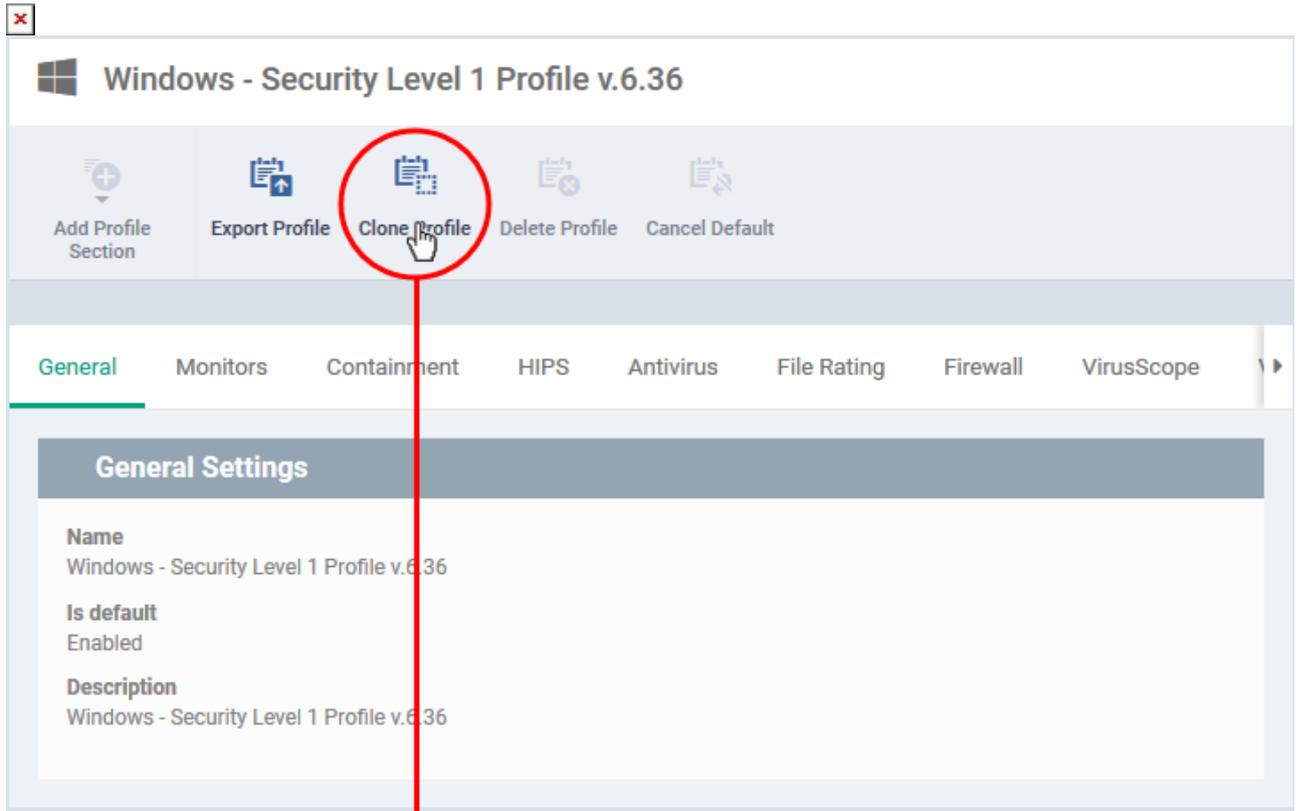
- Click 'Default Profiles' if you want to use a Xcitium preset profile as your template. See [Default profiles](#) at the end of this page to know more about default and pre-configured profiles shipped with EM.
  - See [this page](#) to know about the settings in the pre-configured profiles.

This screenshot shows a close-up of the 'Default Profiles' section. The 'Default Profiles' tab is circled in red. Below the tab is an 'Export' button with a dropdown arrow and a funnel icon on the right. A table lists profiles with columns for 'OS', 'NAME', 'CREATED BY', and 'UPDATED AT'.

OS	NAME	CREATED BY	UPDATED AT
	Linux - Security Level 1 Profile v.6...	admin	Not updated
	Windows - Security Level 1 Profil...	admin	Not updated
	macOS - Security Level 1 Profile v...	admin	Not updated
	Android - Security Level 1 Profile ...	admin	Not updated
	iOS - Security Level 1 Profile v.6.36	admin	Not updated

- Click on a profile name to open its configuration interface. Make sure the profile you select is designed for the OS of your target devices
  - You can filter profiles by clicking the funnel icon on the right

- Click the 'Clone Profile' button:

A screenshot of the "Clone Windows Profile" dialog box. The dialog has a blue header with the title "Clone Windows Profile" and a close button (X). Below the header are two text input fields. The first field is labeled "Name \*" and contains the text "[cloned] Windows - Security Level 1 Profile v.6.36". The second field is labeled "Description" and contains the text "Description". At the bottom right of the dialog is a blue button labeled "Clone".

- Enter a name and description for the profile then click 'Clone'.
- Your new profile is now ready for customization and deployment.



The screenshot shows a web-based configuration interface for a Windows profile. At the top, the title is "Windows profile for new staff". Below the title is a toolbar with five icons and their corresponding labels: "Add Profile Section", "Export Profile", "Clone Profile", "Delete Profile", and "Make Default". A horizontal menu below the toolbar contains several tabs: "General", "Monitors", "Containment", "HIPS", "Antivirus", "File Rating", "Firewall", and "VirusScope". The "General" tab is currently selected and highlighted with a green underline. Below the tabs is a "General Settings" section with a dark header bar containing the text "General Settings" and an "Edit" button with a pencil icon. The main content area of the "General Settings" section displays the following information:

- Name:** Windows profile for new staff
- Is default:** Disabled
- Description:** Windows - Security Level 1 Profile v.6.36

### Customize the profile

- Click 'Configuration Templates' > 'Profiles'
- Click the name of the profile you just cloned. This will open the profile configuration screen:



- You can now configure the profile as you see fit
- Click 'Add Profile Section' button if you wish to add a new module.
  - You can find help on specific profile settings in other articles in this wiki. Try searching for the item you need help with at <https://wiki.xcitium.com/frontend>.
  - The Endpoint Manager user guide also has lots of help with profile settings. [Click here](#) to view.
- Click 'Save'.

## Deploy the profile to devices

There are 4 ways you can assign the profile to device:

- The profile can now be deployed to devices directly, to the users, user groups or device groups.

1) Assign the profile to the device owner, aka the 'user'.

- Click 'Users' > 'User List' > click a username > 'Manage Profiles' > 'Add Profiles'

2) Assign the profile to a user group. Make the user (device owner) a member of the group

- Click 'Users' > 'User Groups' > click a group name > 'Manage Profiles' > 'Add Profiles'

See [How to apply a profile to users and user groups](#) for help to assign profiles to user and user groups

3) Assign the profile to the device itself.

- Click 'Devices' > 'Device List' > click a device name > 'Manage Profiles' > 'Add Profiles'

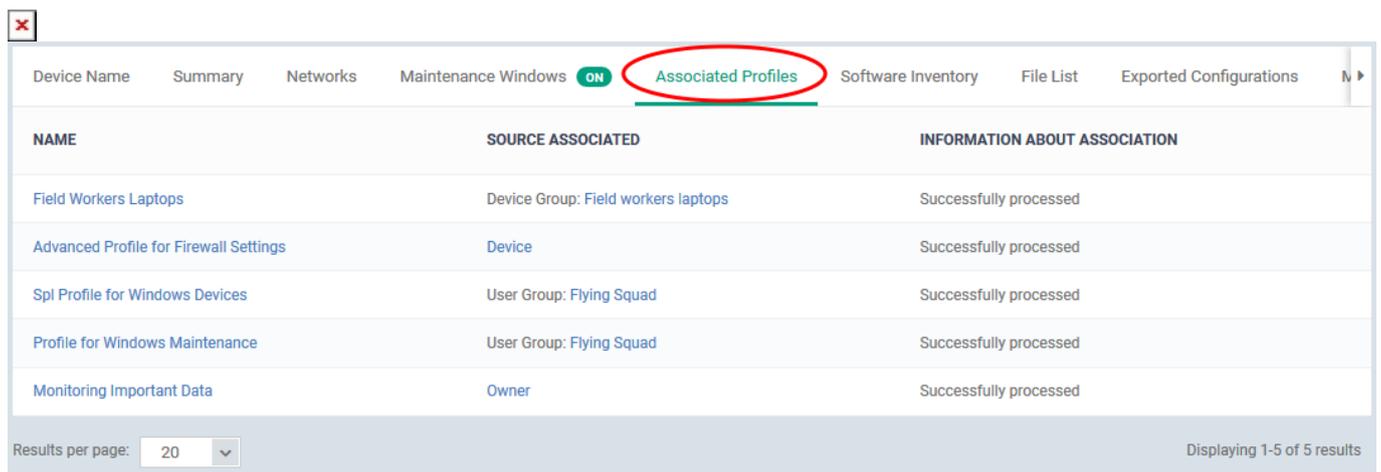
4) Assign the profile to a device group. Make the device a member of the group.

- Click 'Devices' > 'Device List' > 'Group Management' tab > click a group name > 'Manage Profiles'

See [How to apply a profile to devices and device groups](#) for help to assign profiles to user and user groups.

### View profiles associated with a device

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab in the top menu
  - Select a company or a group to view just their devicesOR
  - Select 'Show all' to view every device enrolled to EM
- Click the name of the device to open its device details interface
- Click the 'Associated Profiles' tab



NAME	SOURCE ASSOCIATED	INFORMATION ABOUT ASSOCIATION
<a href="#">Field Workers Laptops</a>	Device Group: <a href="#">Field workers laptops</a>	Successfully processed
<a href="#">Advanced Profile for Firewall Settings</a>	Device	Successfully processed
<a href="#">Spl Profile for Windows Devices</a>	User Group: <a href="#">Flying Squad</a>	Successfully processed
<a href="#">Profile for Windows Maintenance</a>	User Group: <a href="#">Flying Squad</a>	Successfully processed
<a href="#">Monitoring Important Data</a>	Owner	Successfully processed

Results per page: 20  Displaying 1-5 of 5 results

The 'Associated Profiles' tab lists all active configuration profiles on an endpoint applied through different sources.

See [How to view profiles active on a device](#) to read more.

### Default profiles:

- Click 'Configuration Templates' > 'Profiles' > 'Default Profiles'

The default profiles tab shows the list of pre-configured profiles that ship with EM. You can also mark any custom profiles as default. These profiles are automatically assigned to new devices which match their operating system IF no user / user-group profile or device group exists for the OS. The default profiles are replaced on the devices if you apply any profiles on them through the user, user group, device or device group channels.

Endpoint Manager ships with the following default profiles:

- Windows - Security Level 1 Profile
- Mac OS - Security Level 1 Profile
- Android - Security Level 1 Profile
- iOS - Security Level 1 Profile
- Linux - Security Level 1 Profile

Each of the profiles above provides good, baseline security for managed devices. These profiles cannot be modified or deleted, but may be replaced on devices by another profile.

Endpoint Manager also ships with three, non-default, profiles for Windows:

- Windows - Security Level 1 Profile [Former Standard Profile]
- Windows - Security Level 2 Profile
- Windows - Security Level 3 Profile

See [this page](#) to know about the settings in the pre-configured profiles.

**Further reading:**

[How to apply a profile to devices and device groups](#)

[How to apply a profile to users and user groups](#)

[How to view profiles active on a device](#)

[How to enroll devices using the on-boarding wizard](#)