

## Chapter 4 Endpoint Manager base setup

In this chapter we will setup the items in Endpoint Manager that are in the main menu. These policies and settings, for the most part, could be considered prerequisites for the bulk of the customization of your devices to come.

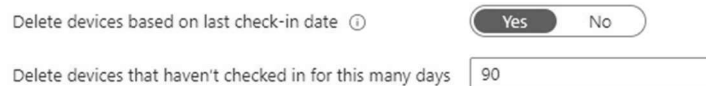
### Device Clean-up

Endpoint Manager gives you the opportunity to automate the removal of devices that aren't active in your domain any longer. It's quite easy to lose track of machines that went out for repair and were never re-deployed or that were cycled out for some reason but then everyone was busy and the step to remove that machine from Azure AD was missed. You can now stop that from happening by making inactive device removal automatic.

### Examples

#### Remove inactive devices automatically

To remove devices automatically, in the Endpoint Manager portal, down at the bottom of the list in the Other category you'll find Device clean-up rules.



The screenshot shows two configuration options for device clean-up rules. The first option is "Delete devices based on last check-in date" with a help icon (i) and a toggle switch set to "Yes". The second option is "Delete devices that haven't checked in for this many days" with a text input field containing the number "90".

Set the Delete devices base on last check-in date to Yes. Set the Delete devices that haven't checked in for this many days number to 30 or some other number of days that is reasonable for your environment.

### Apple MDM Push Certificate

To accept management from Endpoint Manager, Apple devices require that an MDM push certificate be installed. This certificate authorizes Endpoint Manager to provide configuration to the device. This certificate is obtained from Apple, and it must be renewed annually so be sure to put that task onto your calendar.

During this process you will also be setting up an Apple ID for the corporation. Document and store that account information in a safe place. You will need it at renewal time next year.