# Chapter 8 Application Protection

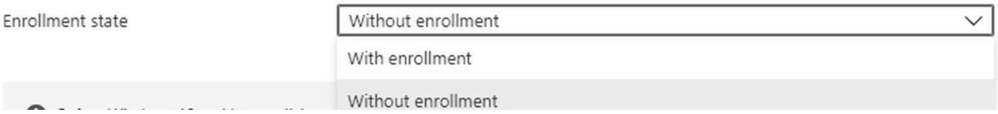
In Chapter 6, Conditional Access Policies, we touched upon Application Protection policies when we configured a session control that required a paired Application Protection policy for its functionality. As we saw then, we can configure an application to conform to various security parameters such as not allowing the corporate data the app generates to be saved other than in a corporate location. There is a lot that you can do with those settings.

Application Protection policies are configured in EndPoint Manager under Apps.

There’s another aspect to Application Protection to be explored and that is the automatic removal of corporate data when a condition is met.

## Examples

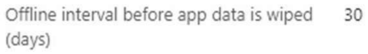
### Example 1: Remove OneDrive if Device is offline too long



Enrollment state: Without enrollment

When creating a new Application Protection policy, you will notice that you are prompted to choose whether the policy will apply to a device With enrollment or Without enrollment. This refers to the device status in EndPoint Manager. If you want a policy to apply to both enrolled and not enrolled devices, BYOD for example, then you will need to create two policies.

Once we’ve created the policy next, select the app that it will apply to. For this example, choose OneDrive. Then further down in the list of available settings choose the number of days that you will allow the device to keep local sync’d data without checking in.



Offline interval before app data is wiped (days) 30