

## Episode Title: Configure and manage Windows Defender Application Control

### Objectives:

At the end of this episode, I will be able to:

1. Understand how applications can be restricted by using Windows Defender Application Control
2. Deploy Application Control by using Group Policy
3. Identify feature differences based on the operating system version

### Key Points:

#### Key Point 1

Windows Defender Application Control allows you to restrict applications that can be ran on a computer. These restrictions can be by codesigning certificates, application binanries, or Microsoft Intelligent Security Graph.

#### Key Point 2

The policies that you define with Application Control can be deployed at-scale using Group Policy. The .XML file will need to be accessible by the computers that need to have their settings changed.

#### Key Point 3

The operating system that is being targeted with Application Control has different features. Be aware of the different features that are available per OS.

- If additional resources are used during the episode, they can be obtained using the download link on the overview episode (e.g. diagrams, no powerpoints)

---

### External Resources:

If external resources were used during this episode, you can reference the following external resources for supplementary tools and information, if none were used, then this section will be blank:

- Windows Defender Application Control  
: <https://learn.microsoft.com/en-us/windows/security/application-security/application-control/windows-defender-application-control/wdac-and-applocker-overview>