# Copyright Statement

This document is from [SyntaxBearror.io](https://www.syntaxbearror.io/) and is provided to the greater IT community. It may include elements from others which are governed under their respective copyright standards.

This work is under a [*Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International license*](http://creativecommons.org/licenses/by-nc-sa/4.0/). You may use this work for internal use only in your organization. If you make improvements to it, you are encouraged to share those with the community, and you will be rightfully attributed. We ask you submit your improvements to syntaxbearror.io.

For-profit uses of this work in part or whole are prohibited.

**Last Modified Date**

March 7, 2021

**Contributors**

Christopher Clai of [SyntaxBearror.io](https://www.syntaxbearror.io/)

Table of Contents

[Copyright Statement 1](#_Toc72073052)

[Resetting a System 3](#_Toc72073053)

[Re-Synchronizing a System 4](#_Toc72073054)

[Creating a Configuration Profile 5](#_Toc72073055)

[Modifying Configuration Profiles 6](#_Toc72073056)

[Creating a Compliance Policy 7](#_Toc72073057)

[Modifying Compliance Policies 8](#_Toc72073058)

[Setting Up an Application 9](#_Toc72073059)

[Modifying an Application 10](#_Toc72073060)

[Creating an App Protection Policy 12](#_Toc72073061)

[Modifying an App Protection Policy 13](#_Toc72073062)

# Resetting a System

|  |  |
| --- | --- |
| **Step 1** | Login to the Microsoft Endpoint Manager Admin Center  <https://endpoint.microsoft.com/#home> |
| **Step 2** | Click on Devices on the left-side menu. |
| **Step 3** | Click on All devices on the Devices Overview page. |
| **Step 4** | Search for the system, or locate it in the device listing, and then click on it to open the properties of the device. |
| **Important!** | Before proceeding with this step make sure that the user is in front of the computer, and that they have the setup documents available to them on another system, on their mobile device, or printed out. Verify with the user that the device is connected via Ethernet to their switch or router and that it is not using wireless. If using wireless, you cannot proceed until an ethernet connection can be made to the device. |
| **Step 5** | On the properties of the system, you have several options along the header of the screen. To fully reset a system back to deployment default, click on Fresh Start. |
| **Step 6** | A prompt will appear below that asks if you want to retain user data. By default, we do not want to retain user data, but if we need to, make sure that option is checked before you click Yes. |
| **Step 7** | Advise the user the command was sent. If the device does not go for reboot or notify the user it is about to be rebooted within 5 minutes, have the user follow the instructions provided to them on how to sync their device to the cloud. |

# Re-Synchronizing a System

|  |  |
| --- | --- |
| **Step 1** | Login to the Microsoft Endpoint Manager Admin Center  <https://endpoint.microsoft.com/#home> |
| **Step 2** | Click on Devices on the left-side menu. |
| **Step 3** | Click on All devices on the Devices Overview page. |
| **Step 4** | Search for the system, or locate it in the device listing, and then click on it to open the properties of the device. |
| **Step 5** | On the properties of the system, you have several options along the header of the screen. To force a policy sync, click on the Sync command. |
| **Step 6** | Confirm with the user that a toast notification has appeared on their notification bar or on the lower right corner of the screen advising them that the device policy is updating. If after 5 minutes this does not appear, have the user follow the instructions provided to them on how to sync their device to the cloud. |

# Creating a Configuration Profile

|  |  |
| --- | --- |
| **Step 1** | Login to the Microsoft Endpoint Manager Admin Center  <https://endpoint.microsoft.com/#home> |
| **Step 2** | Click on Devices on the left-side menu. |
| **Step 3** | In the left-hand menu of the *Devices Overview* page, click configuration profiles. |
| **Step 4** | Click on Create Profile located along the top of the *Device Configuration Profiles overview* page. This will open a blade on the right side of your screen. |
| **Step 5** | Select the *platform* that the profile is intended to target. |
| **Step 6** | Select the Profile type that the profile is intended to target. Typical profile types we use are:  Administrative Templates  Custom  Domain Join  Delivery Optimization  Device Restrictions Endpoint Protection  Identity protection  To understand all the available types, visit: [*https://docs.microsoft.com/en-us/mem/intune/configuration/device-profile-create*](https://docs.microsoft.com/en-us/mem/intune/configuration/device-profile-create)  Follow the prompts from that point to complete the profile configuration. |

# Modifying Configuration Profiles

|  |  |
| --- | --- |
| **Step 1** | Login to the Microsoft Endpoint Manager Admin Center  <https://endpoint.microsoft.com/#home> |
| **Step 2** | Click on Devices on the left-side menu. |
| **Step 3** | In the left-hand menu of the *Devices Overview* page, click configuration profiles. |
| **Step 4** | Click on the target configuration profile in the list, and this will take you to the profiles overall page. |
| **Step 5** | Click Properties on the profile’s overall page. |
| **Step 6** | From there click Edit adjacent to the section you want to modify. Here is what each section means:  *Basics* – Here you can change the name and description of the profile. Profile platforms and types cannot be edited. A new profile must be created.  *Configuration Settings* – In this section you can edit the actual settings that apply to the systems.  *Scope Tags* – This is where you can edit the tags associated with the profile, to align them with other objects within Intune that have a similar tag.  *Assignments –* To add or remove groups or users that the profile applies to.  *Applicability Rules –* To further narrow down assignment of the profile to specific types of systems, though we currently do not employ this feature. |

# Creating a Compliance Policy

|  |  |
| --- | --- |
| **Step 1** | Login to the Microsoft Endpoint Manager Admin Center  <https://endpoint.microsoft.com/#home> |
| **Step 2** | Click on Devices on the left-side menu. |
| **Step 3** | In the left-hand menu of the *Devices Overview* page, click compliance policies. |
| **Step 4** | Click on Create Policy located along the top of the *Device compliance policies* *overview* page. This will open a blade on the right side of your screen. |
| **Step 5** | Select the *platform* that the profile is intended to target, then click Create. |
| **Step 6** | Follow the prompts from that point to complete the policy configuration. |

# Modifying Compliance Policies

|  |  |
| --- | --- |
| **Step 1** | Login to the Microsoft Endpoint Manager Admin Center  <https://endpoint.microsoft.com/#home> |
| **Step 2** | Click on Devices on the left-side menu. |
| **Step 3** | In the left-hand menu of the *Devices Overview* page, click compliance policies. |
| **Step 4** | Click on the target compliance policy in the list, and this will take you to the policies overall page. |
| **Step 5** | Click Properties on the policy’s overall page. |
| **Step 6** | From there click Edit adjacent to the section you want to modify. Here is what each section means:  *Basics* – Here you can change the name and description of the profile. Profile platforms and types cannot be edited. A new profile must be created.  *Compliance Settings* – In this section you can edit the actual settings that will be audited to determine compliance.  *Actions for Noncompliance* – This is what will occur to devices that are found not in compliance.  *Scope Tags* – This is where you can edit the tags associated with the profile, to align them with other objects within Intune that have a similar tag.  *Assignments –* To add or remove groups or users that the profile applies to. |

# Setting Up an Application

|  |  |
| --- | --- |
| **Step 1** | Login to the Microsoft Endpoint Manager Admin Center  <https://endpoint.microsoft.com/#home> |
| **Step 2** | Click on Apps on the left-side menu. |
| **Step 3** | Select the platform that the application targets. |
| **Step 4** | On the specific platform’s app page, click on Add. |
| **Step 5** | Select the appropriate *app type* based on the platform selected, click Select, and follow the prompts from there to complete an app setup. |

# Modifying an Application

|  |  |
| --- | --- |
| **Step 1** | Login to the Microsoft Endpoint Manager Admin Center  <https://endpoint.microsoft.com/#home> |
| **Step 2** | Click on Apps on the left-side menu. |
| **Step 3** | Select the platform that the application targets. |
| **Step 4** | On the specific platform’s app page, click on the application you want to modify. |
| **Step 5** | Click on Properties on the specific apps overview page. |
| **Step 6** | From there click Edit adjacent to the section you want to modify. Here is what each section means:  *App Information* – The core details about the application that will be shown to users.  *Program* – This is only shown on uploaded package installations. This is for changing the package file, install or uninstall instructions, and to adjust the return codes.  *Requirements* – This is not shown on all types, but if it is, these would be the minimum requirements you want the system to have to install the application.  *Detection Rules* – This is only shown on uploaded package installations. This is the rules that define what files, folders or registry keys Intune should look for to verify an app is installed.  *Dependencies* – This is only shown on uploaded package installations. This is similar in requirements, as you are defining if any frameworks must be installed prior.  *Scope Tags* – This is where you can edit the tags associated with the app, to align them with other objects within Intune that have a similar tag.  *Assignments –* To add or remove groups or users that the application is required for or available to in the appropriate app store. |

# Creating an App Protection Policy

|  |  |
| --- | --- |
| **Important!** | App Protection Policies develop an effective sandbox between supported applications and only one should be applied per system to avoid issues. |
| **Step 1** | Login to the Microsoft Endpoint Manager Admin Center  <https://endpoint.microsoft.com/#home> |
| **Step 2** | Click on Apps on the left-side menu. |
| **Step 3** | Click on App Protection Policies on the left-side menu of the Apps overview page. |
| **Step 4** | Click on Create Policy located along the top of the page and select the appropriate platform you are targeting. |
| **Step 5** | Follow the steps in the wizard to complete the creation of the policy. |

# Modifying an App Protection Policy

|  |  |
| --- | --- |
| **Step 1** | Login to the Microsoft Endpoint Manager Admin Center  <https://endpoint.microsoft.com/#home> |
| **Step 2** | Click on Apps on the left-side menu. |
| **Step 3** | Click on App Protection Policies on the left-side menu of the Apps overview page. |
| **Step 4** | Click on the policy in the listing that you want to modify. |
| **Step 5** | On the policy’s overview page, click on Properties. |
| **Step 6** | Click on Edit adjacent to which section you want to modify. Here is what each section means:  *Basics* – Here you can change the name and description of the profile. Profile platforms and types cannot be edited. A new profile must be created.  *Targeted Apps* – The apps which this policy applies to.  *Required Settings* – Whether Windows Information Protection and corporate-specific identifiers are used.  *Advanced Settings* – Additional settings related to defining a network perimeter for the applications, and how data protection should function.  *Assignments –* To add or remove groups or users that the profile applies to.  *Scope Tags* – This is where you can edit the tags associated with the profile, to align them with the systems that have a similar tag. |