11 DP 101-Creating Auto Unprotect Task and Activating the Configuration Video Transcript

[00:00:01] **Data Protector 101: Creating a Task for Auto-Unprotect and Activating the Configuration.** Now that we have **Auto-Protect** configured, let's configure **Auto-Unprotect**. Coming down to the **Tasks** folder, right click and select **New Task** and we'll see that same wizard window appear that we used for the **Auto-Protect** process. So we're gonna start at the top and we're going to give it a name. **Auto-Unprotect**. Come over here choose **Create Folders** because those are **Source** and **Destination** folders have not been created just yet. I don't need any notes here at this point. The **Task Type** is our **File Change** and from here I'm going to go all the way down to the **Templates** and select my **Auto-Unprotect** template. Toggling the arrows we come down to (Auto-Protect you) **Auto-Unprotect UXP files** and then we're going to apply the template just like we did in the **Auto-Protect**. So you see those same shifts occurring. Some notes are supplied. The ***.uxl script** has been chosen. Our **Executable** and **Log Files** have been populated. The thing that we need to focus on is the **Executable**. This is essentially a placeholder script for our **Auto-Unprotect** process. If you recall we used the **MacMT Machine ID** in our **Auto-Protect** setup. So back when we created our **Machine ID**, we created those additional scripts as well. And one of those was a **ID specific Auto-Unprotect**. Well this is where you're going to apply that particular script because the **ID** that was used to protect the data needs to be authenticated against within the script that's auto unprotecting. So we need to definitively choose that script to allow **Auto-Unprotect** to properly execute. You can do it one of two ways. You can actually change this **ID r**ight here and type in manually type in in the **ID** name and ensure that the underscore stays put. The other option is you can simply browse for that script, which is what I'm going to choose to do here. It opens us up directly into the **Scripts** folder the one that we would see in our **Data Protector** window. And we can scroll down and find that script that we created for that specific **ID** for **Auto-Unprotect** and select it. It's gonna populate this box so that now our **Auto-Protect** and **Auto-Unprotect** processes can work together based on the **Identity.** So moving into the **File Processing Options**, we need to identify our **Source** folder. So we're gonna browse for that folder path. Coming onto the desktop, selecting **series one**. We see these two folders already in here. Those are the **Auto-Protect** necessary folders for **Source** and **Destination**. And so we're gonna leave it at this level and select. And then we're going to add on an additional folder on the end of this one. And I'm going to title it **Unprotect UXPs**.

[00:03:06] The **Include Filter** is simply one file type and that's the ***.UXP**. No other file types are needed. It's the only one that will be recognized by the **Auto-Unprotect** process.

[00:03:16] The **Exclude Filter** has been left blank. It isn't as essential to worry about the *.log and *.tmp files in this list of the attempt for unprotecting data. But if you'd like to type those in, you're certainly welcome to do so. We're going to move on past **Timer Options** because it's the same 30 minute scan which is fine with me at the moment. But before we go into **Script Parameters**, we're going to copy the file path. As if you recall, we don't have a browse key in this for the folder path that we've got to provide for the **Destination** folder here. So I'm going to highlight that, paste that in and we're going to change the end folder to a new name calling it Clear for where my clear data will land after the UXP folder, or excuse me, file is authenticated and the data is extracted. The one thing that is different here actually there are two. We don't need to provide a **Machine ID** here in this **Script Parameters** because it is an **Auto-Unprotect** process. The thing we need to worry about is whether or not we need to delete the **UXP** files once they've been authenticated and the data is extracted. The default is true, meaning that they will delete. If you prefer them to keep them for whatever reason, you're certainly welcome to do so, but I want to keep it at true. So we've completed all the parameters that we need to set up our **Tasks**. So let's go back through and look at basic options and see if we've covered everything to make sure it's all in place as it needs to be. We see scrolling through and looking at everything. **Executable** is the really important one. That's the correct script. **File Processing**. We do have our folder identified. Our **Include Filter** looks good. And our **Script Parameters**. We've provided our folder here. We wanted to delete our files. We've got our folder checks... checked here, so we're looking good. And now we can click OK.

[00:05:08] So let's go out into the **series one** folder and make sure those folders were created.

[00:05:16] And they have been. So Clear and Unprotect are now provided so we close that down. So what you see shift in our **Data Protector** main window is that **Auto Unprotect** is now populating under **Tasks**. And both **Tasks** are sitting at idle and the configuration is inactive. So how you activate a configuration is a very simple process. It's literally just turning it on. But what you need to know about **Active** and **Inactive** status is that only one configuration at a time can be activated. So if you've got the Default active that means series one cannot be active. So instead of focusing on how to shut this one off, we're

going to actually just go up here right click and activate it. And **Data Protector** switches it around for us automatically. So it activates our series one configuration and it puts our **Tasks** in a **Waiting State**. So what **Waiting State** is is that the **Task** is ready to execute. provided a change occurs, but that change won't occur until 30 minutes down the road because we have that **Scan Interval** set at 30 minutes and the **Enabled** box with checked. And that's why they are ready to go, but not necessarily doing anything. So in 30 minutes, they will scan. The **Data Protector** will scan those **Source** folders to look for file change. If nothing has occurred, it'll stay in that **Waiting State**. In the event that there is a file change, the **Task** will execute. Date and time and number will populate. Hopefully we remain at zero in our errors with no comments and also the logs will land in our logs folder here under this configuration. The one thing that is interesting about a configuration is that you can have more than two **Tasks** activated at one time. You can have multiple **Tasks**, but only one under one configuration and one configuration is active. So just keep that in mind as you're building your **Task**. You can actually have multiple **Tasks** occurring at the same time. So that pretty much completes what you need to know about creating your **Auto-Unprotect Task** and activating your configuration.