

Creating an Automatic Deployment Rule.

- The purpose of this lecture is to demonstrate how to automate the collection of new updates and deliver them to clients.
- From the workspace if we click **software library** then in the navigation pane we click **all software Updates**. What we see here is a synchronization of windows defender updates from Microsoft online.
- Notice that some file definitions have an icon with an x.
What this means is that these x's represent out dated definitions. So, what we will want to do is filter out the irrelevant definitions and create a current list of updates for windows defender that we will send out to our Endpoint Protection clients.

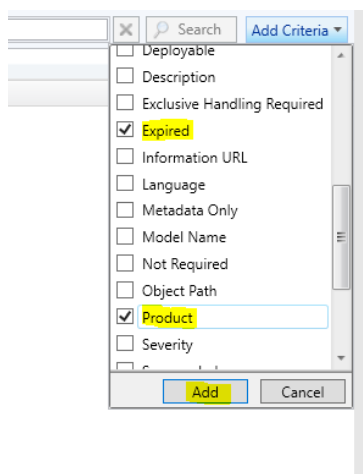
All Software Updates 19 items

Search

Icon	Title	Bulletin ID	Required	Installed	Percent Compliant
	Definition Update for Windows Defender - KB2267602 (Definition 1.249.466.0)		0	0	100
	Definition Update for Windows Defender - KB2267602 (Definition 1.249.474.0)		0	0	100
	Definition Update for Windows Defender - KB2267602 (Definition 1.249.476.0)		0	0	100
	Definition Update for Windows Defender - KB2267602 (Definition 1.249.477.0)		0	0	100
	Definition Update for Windows Defender - KB2267602 (Definition 1.249.480.0)		0	0	100
	Definition Update for Windows Defender - KB2267602 (Definition 1.249.483.0)		0	2	100
	Definition Update for Windows Defender - KB2267602 (Definition 1.249.983.0)		1	0	0
	Definition Update for Windows Defender - KB2267602 (Definition 1.249.984.0)		1	0	0
	Definition Update for Windows Defender - KB2267602 (Definition 1.249.985.0)		1	0	0
	Definition Update for Windows Defender - KB2267602 (Definition 1.249.986.0)		1	0	0
	Definition Update for Windows Defender - KB2267602 (Definition 1.249.987.0)		1	0	0
	Definition Update for Windows Defender - KB2267602 (Definition 1.249.988.0)		0	1	50

To accomplish this, we need to configure a Search

- From the search bar, click the **Add criteria** button, Scroll down and click **expired**, scroll down then check **product**, click **add**.



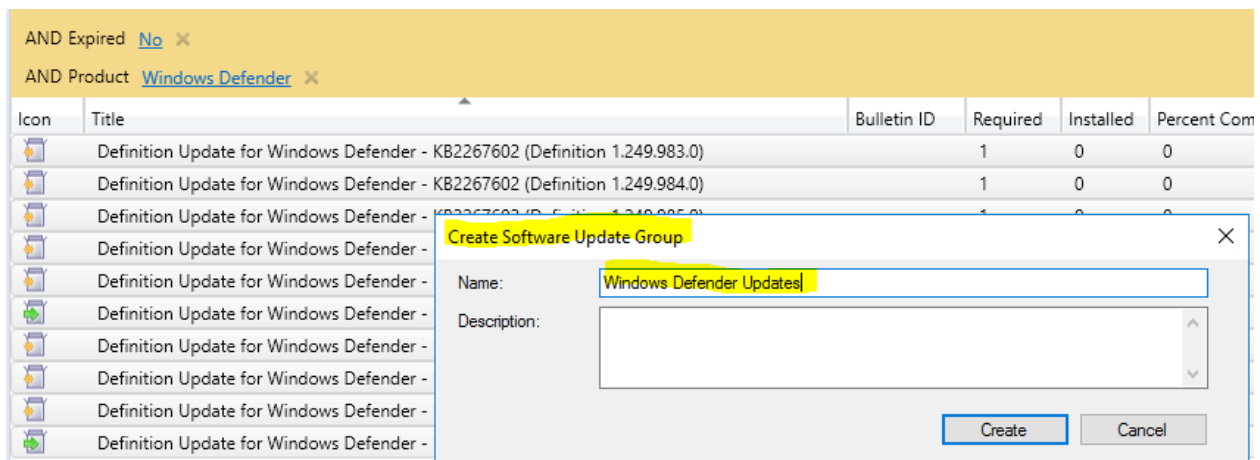
- On the left side, right under the search bar, by AND expired click **Yes**, then change this setting to **NO**
- To the right of **And Product**, click the **underlined selection**, Scroll down and click **Windows Defender**.
- From the search bar, click the **search button**, now you have a filtered list of unexpired windows 10 defender updates.

Icon	Title	Bulletin ID	Required	Installed	Percent Compliant	Downloaded	Deployed
	Definition Update for Windows Defender - KB2267602 (Definition 1.249.983.0)		1	0	0	Yes	Yes
	Definition Update for Windows Defender - KB2267602 (Definition 1.249.984.0)		1	0	0	Yes	Yes
	Definition Update for Windows Defender - KB2267602 (Definition 1.249.985.0)		1	0	0	Yes	Yes
	Definition Update for Windows Defender - KB2267602 (Definition 1.249.986.0)		1	0	0	Yes	Yes
	Definition Update for Windows Defender - KB2267602 (Definition 1.249.987.0)		1	0	0	Yes	Yes
	Definition Update for Windows Defender - KB2267602 (Definition 1.249.988.0)		0	1	50	Yes	Yes
	Definition Update for Windows Defender - KB915597 (Definition 1.249.480.0)		0	0	100	Yes	Yes
	Definition Update for Windows Defender - KB915597 (Definition 1.249.641.0)		0	0	0	Yes	Yes
	Definition Update for Windows Defender - KB915597 (Definition 1.249.764.0)		0	0	0	Yes	Yes
	Definition Update for Windows Defender - KB915597 (Definition 1.249.918.0)		0	0	0	Yes	Yes

- So you might ask, **How does this work with the Automatic Deployment Rule?**

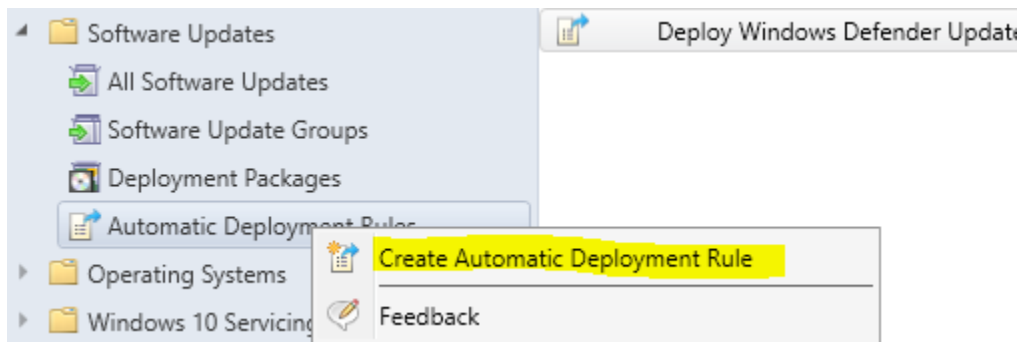
Create a Software Update Group

- What we are going to do is select all the updates, by pressing (Ctrl – a)
- Right click and select **create software update group**.
This group represents like the name implies this a group of updates.
We will use this group with our automatic defender rule.
- **Name, type Windows Defender Updates, click create.**

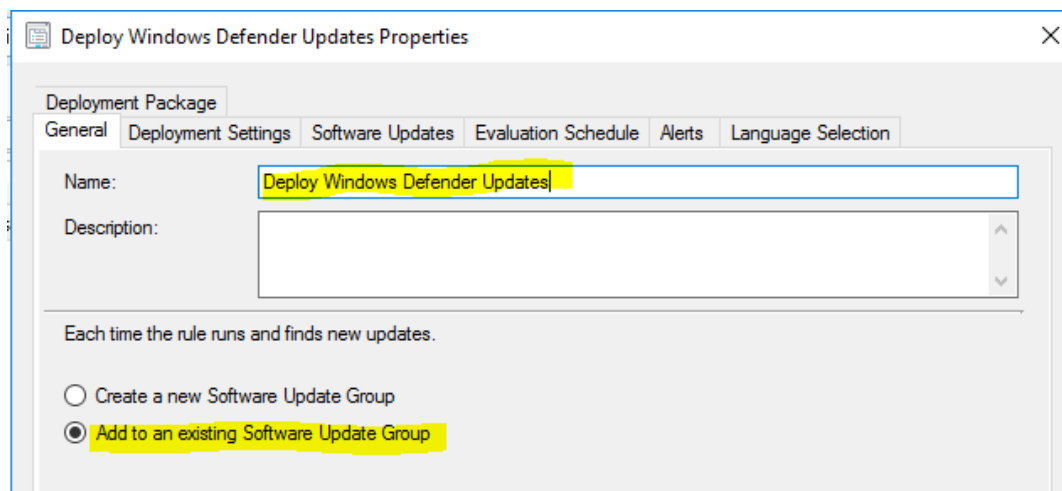


On the left, click **software update group**, on the right you can see the software Updates Group of updates called **Windows Defender Updates**, has been created.

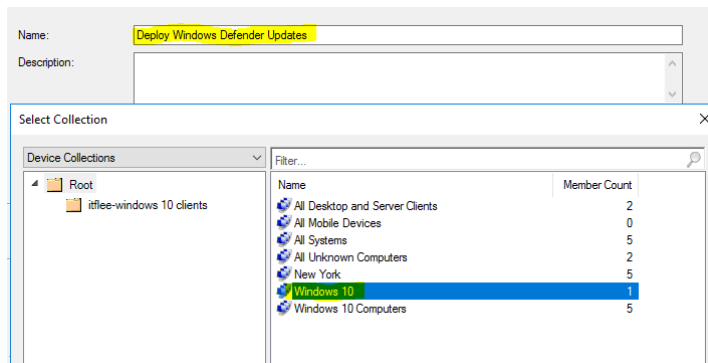
- That is important because when you create an automatic deployment rule, on a scheduled basis the ADR will look for new updates and put them into an **existing software update group**, in this case, the **Windows Defender Updates group**, and then deploy them out to clients.
- From the Navigation Pane, right click **Automatic Deployment Rule**, click create Automatic Deployment Rule.



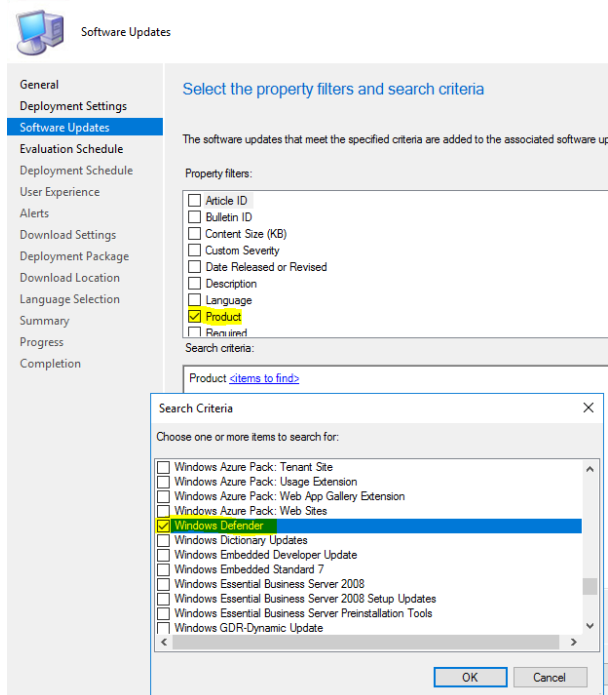
- Type a Name – **Deploy Windows Defender Updates**,



- Specify a **device collection** – Click Browse, in this case I choose **windows 10**,



- Click add to an **existing update group**, here you will be **adding new updates to an existing update group**, called Windows Defender Updates group, click **next**.
- From **deployment settings**, click **next**.
- From Software Updates, click **Product**, click **next**.
- Beside product click **items to find** and scroll down and check **windows defender**, click ok, then click **next**.



- From **Evaluation Schedule**, click **run the rule after any update synchronization**. This setting is going to be looking at new updates after SCCM synchronizes its update, click next.
- From **Deployment Schedule** – Select **as soon as possible** for both settings then click **next**.

Deployment Schedule

User Experience

Alerts

Download Settings

Deployment Package

Download Location

Language Selection

Summary

Progress

Completion

Time based on: Client local time

Software available time

Specify when software updates are available. After this rule is run, software updates are distributed. Software updates are available to install as soon as possible or scheduled to install at a configured time.

Note: You must enable this deployment before software updates are available to install.

☒ **As soon as possible**

☐ Specific time: 7 Days

Available time:

Installation deadline

Specify a deadline for required software updates. The deadline is determined by adding the specified time to the time the deployment is available. When the deadline is reached, required software updates are installed on the device and the device is ready for the next update.

☒ **As soon as possible**

☐ Specific time: 7 Days

Deadline time (from deployment available time):

- From **User experience**, User notifications, click the down arrow and select **Display in software center** and **show all notifications**, click **next**.
- From **Alerts**, check **generate an alert when this rule fails**, click **next**.
- From **Download settings**, accept the defaults, click **next**.
- From **Deployment Package**, we need to **create a new deployment package** which is used to download the updates. You might ask, aren't the updates downloaded? What did we see in Configuration Manager? What we saw was the meta-data, stored in the configuration manager database and not the actual binary files.
- From **Name**, type **Defender Deploy Package**. This needs a location to store the actual binaries on the network.
- From **Package Source**. Specify a UNC path to a **shared folder** that has already been created. In this case I type [\\ITFSCCM01\EPUpdates](#), Click **next**.

Create a new deployment package

Name:

Description:

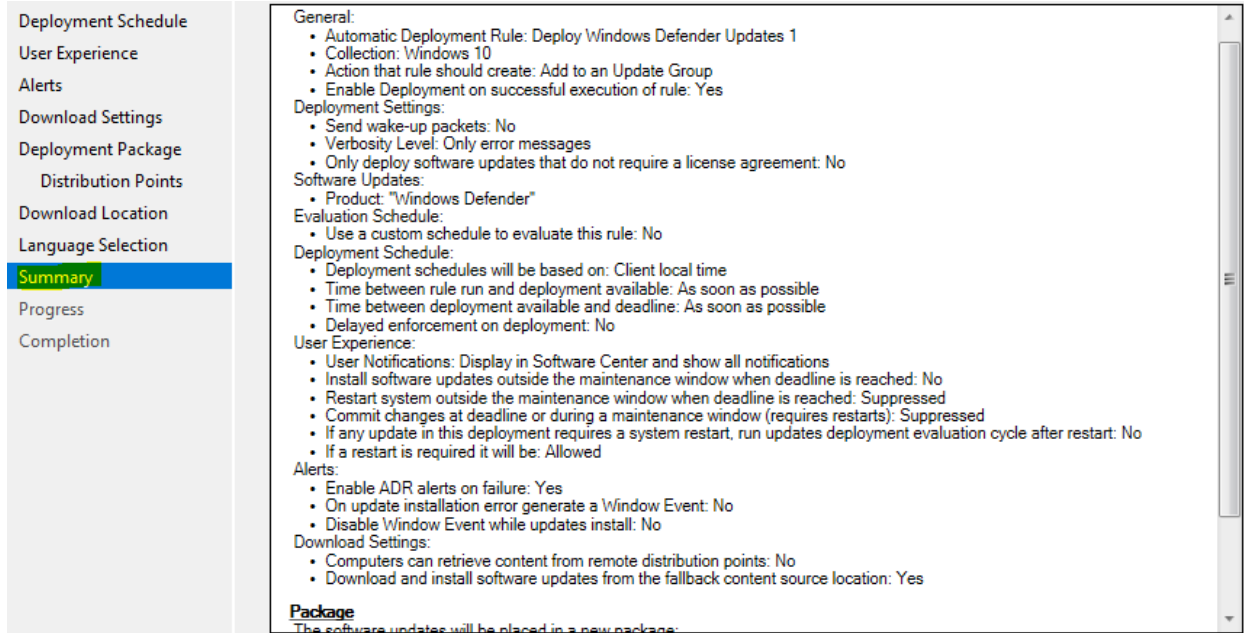
Package source (Example): \\<server>\<folder path>

- From **distribution point**, click **add**. This is the actual server that holds the updates. click **distribution point**. Select the server, in this case I **click** the ITFSCCM01 server, click **ok**, then click **next**.

Filter...	Name	Type	Description
	<input checked="" type="checkbox"/> ITFSCCM01.ITFLEE.COM	On-premises	

- From **Download Location** – Click **download software updates from the internet**. This downloads the actual binaries from the internet and stores those files in the EPUUpdates shared folder. Click **next**
- From **language**, if appropriate uncheck all but English, click **next**,

- Verify the Summary, then click **next**.



For a summary of steps:

We have created a new Deployment Rule called **Deploy Windows Defender Updates** that automatically looks at new Windows Defender Updates after SCCM get those updates from the internet. Now these updates are ready to be automatically deployed to our Windows 10 clients.

Congratulations you have completed this lecture, thanks for watching, and we will see you in the next lecture.