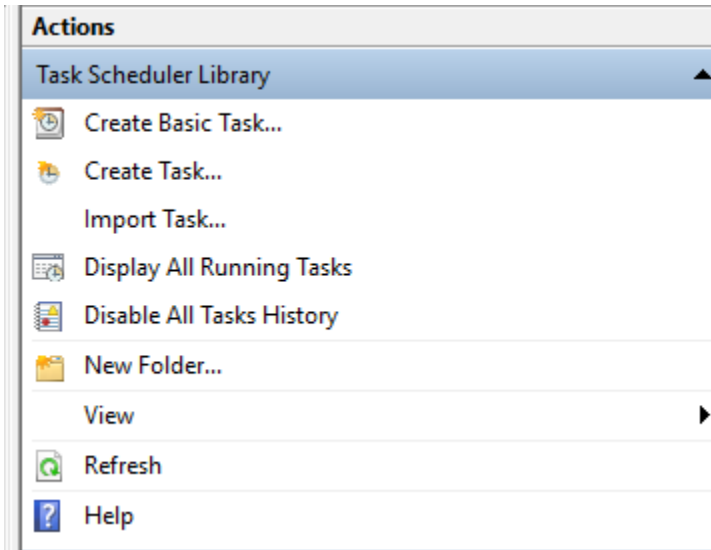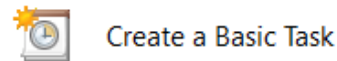# Windows Defender Definition Update – Daily

If you want Windows Defender to install definition update daily, it can be achieved through task schedule as detailed below.

Open Task Scheduler

Create Basic Task Wizard

Task Trigger

Create a Basic Task

Trigger
Action
Finish

When do you want the task to start?

- (•) Daily
- ( ) Weekly
- ( ) Monthly
- ( ) One time
- ( ) When the computer starts
- ( ) When I log on
- ( ) When a specific event is logged

< Back   Next >   Cancel

Create Basic Task Wizard

Daily

Create a Basic Task
Trigger
Daily
Action
Finish

Start: 01- Dec -2018   4:00:00 AM   ☐ Synchronize across time zones

Recur every: 1   days

< Back   Next >   Cancel

Create Basic Task Wizard

Action

Create a Basic Task
Trigger
   Daily
Action
Finish

What action do you want the task to perform?

◉ Start a program
○ Send an e-mail (deprecated)
○ Display a message (deprecated)

< Back | Next > | Cancel

"C:\Program Files\Windows Defender\MpCmdRun.exe"
-SignatureUpdate

Create Basic Task Wizard

Start a Program

Create a Basic Task
Trigger
   Daily
Action
   Start a Program
Finish

Program/script:

"C:\Program Files\Windows Defender\MpCmdRun.exe" | Browse...

Add arguments (optional): | -SignatureUpdate

Start in (optional):

< Back | Next > | Cancel

Task Scheduler ✕

❓ It appears as though arguments have been included in the Program text
box. Do you want to run the following program:
"C:\Program

With the following arguments:
Files\Windows Defender\MpCmdRun.exe" -SignatureUpdate

| Yes | No | Cancel |

Create Basic Task Wizard ✕

🗓️ Summary

Create a Basic Task
Trigger
  Daily
Action
  Start a Program
Finish

Name: | Defender Definition Update |

Description: | This task will update definition daily at 4AM to all workstations running Windows Defender. |

Trigger: | Daily; At 4:00 AM every day |

Action: | Start a program; "C:\Program Files\Windows Defender\MpCmdRun.exe" -Sig |

☐ Open the Properties dialog for this task when I click Finish

When you click Finish, the new task will be created and added to your Windows schedule.
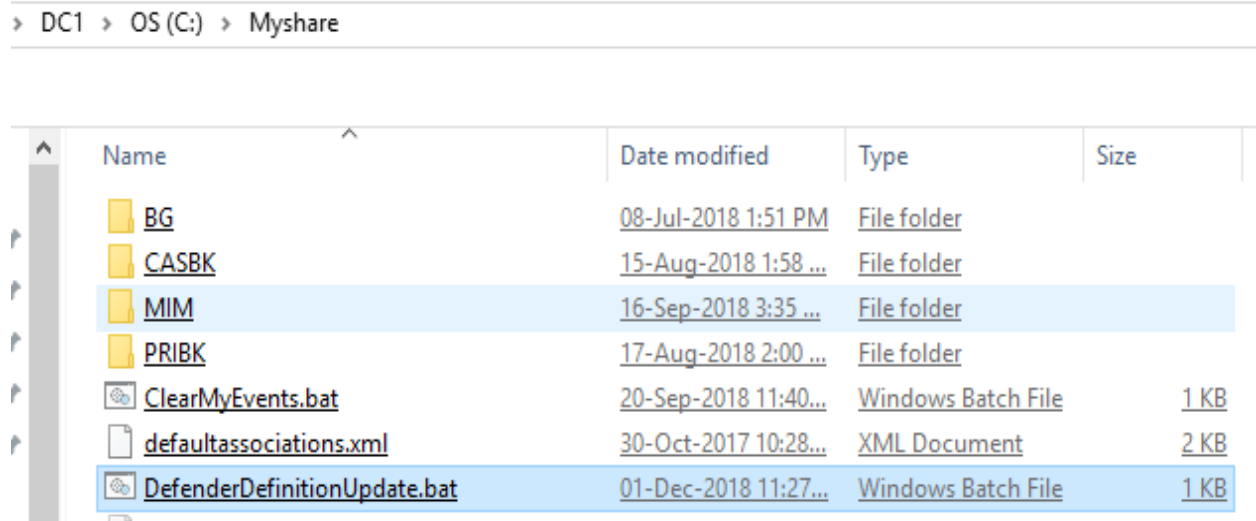
| < Back | Finish | Cancel |

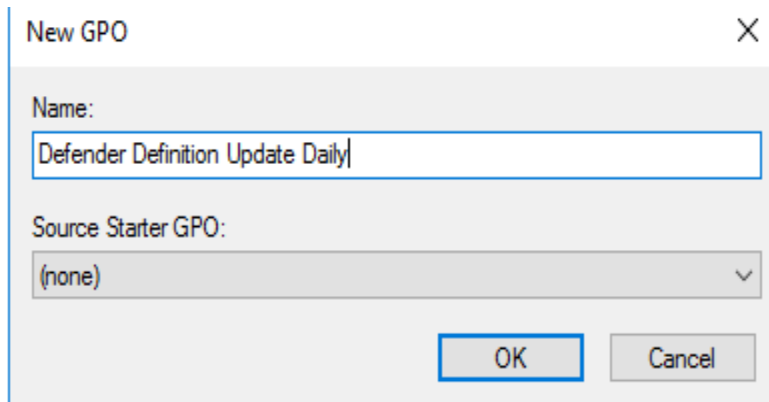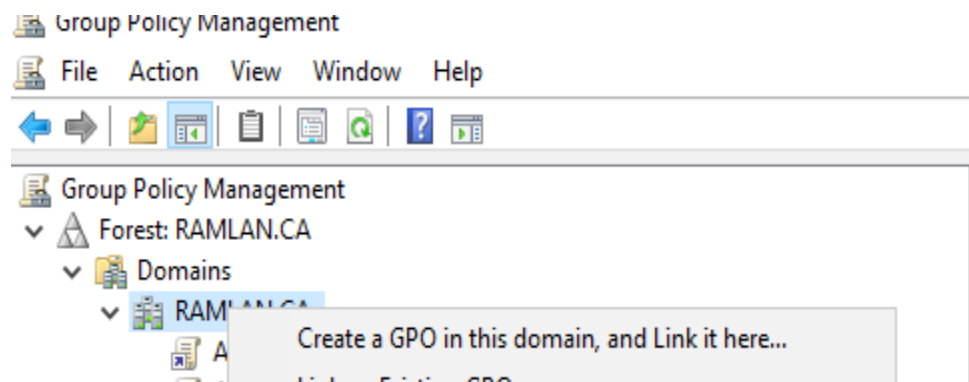Above task will run daily as set out above.

If you want to deploy to multiple workstations then a batch file is the way to go. Here are the steps for that.

First copy the batch file to a network share. In my case the file is copied to Myshare on the Domain Controller.

> DC1 > OS (C:) > Myshare

Name	Date modified	Type	Size
BG	08-Jul-2018 1:51 PM	File folder	
CASBK	15-Aug-2018 1:58 ...	File folder	
MIM	16-Sep-2018 3:35 ...	File folder	
PRIBK	17-Aug-2018 2:00 ...	File folder	
ClearMyEvents.bat	20-Sep-2018 11:40...	Windows Batch File	1 KB
defaultassociations.xml	30-Oct-2017 10:28...	XML Document	2 KB
DefenderDefinitionUpdate.bat	01-Dec-2018 11:27...	Windows Batch File	1 KB

Now we can create a GPO that will copy the batch file to every workstation to C:\Temp folder.

Open GPMC

Group Policy Management

File   Action   View   Window   Help

Group Policy Management
Forest: RAMLAN.CA
  Domains
    RAMLAN.CA
      A   Create a GPO in this domain, and Link it here...

New GPO   ✕

Name:

Defender Definition Update Daily

Source Starter GPO:

(none)

            OK   Cancel

Edit the GPO
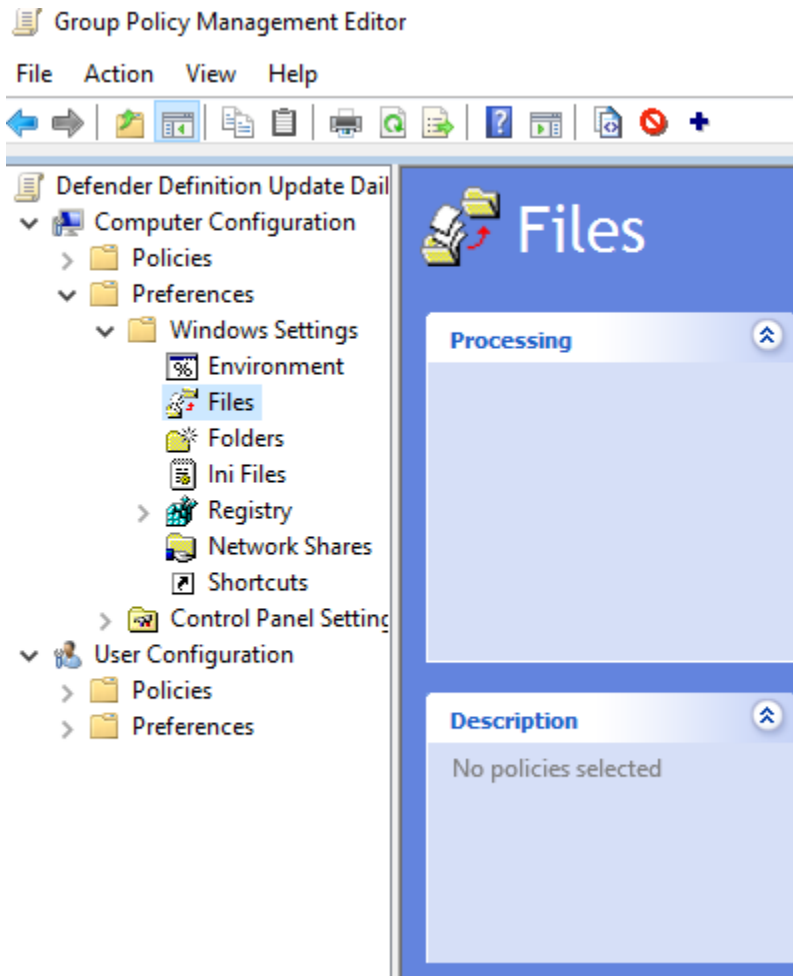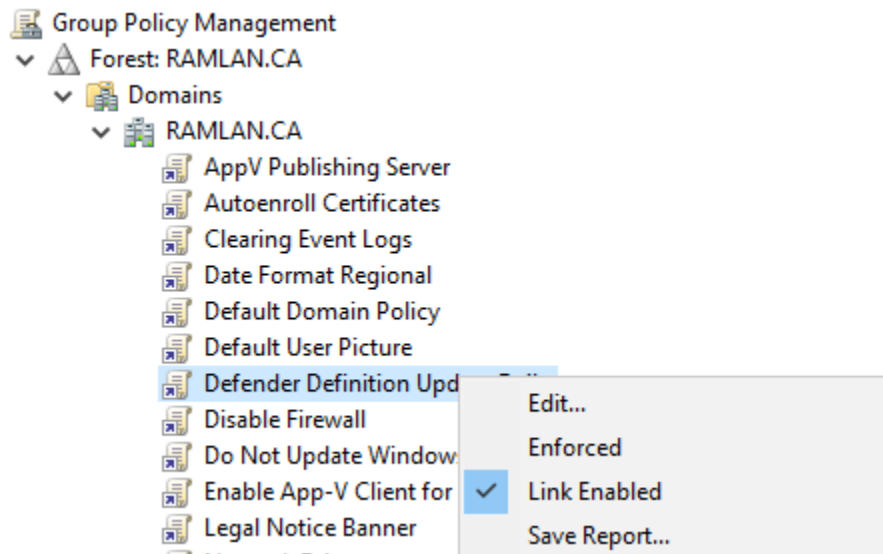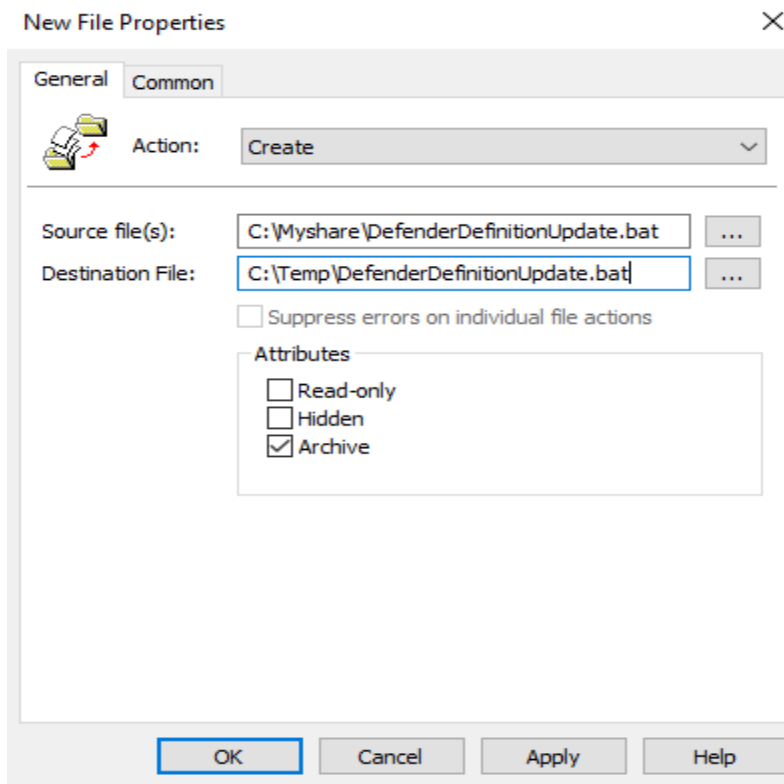
Above will copy the batch file from network share to local system C:\Temp folder

Now we will create a scheduled task using GPO

New Task (At least Windows 7) Properties   ✕

| General | Triggers | Actions | Conditions | Settings | Common |

Action: Update ▼

Name: Defender Definition   [...]

Author: RAMLAN\Administrator

Description:

[   ]

Security options

When running the task, use the following user account:

NT AUTHORITY\System   [Change User or Group...]
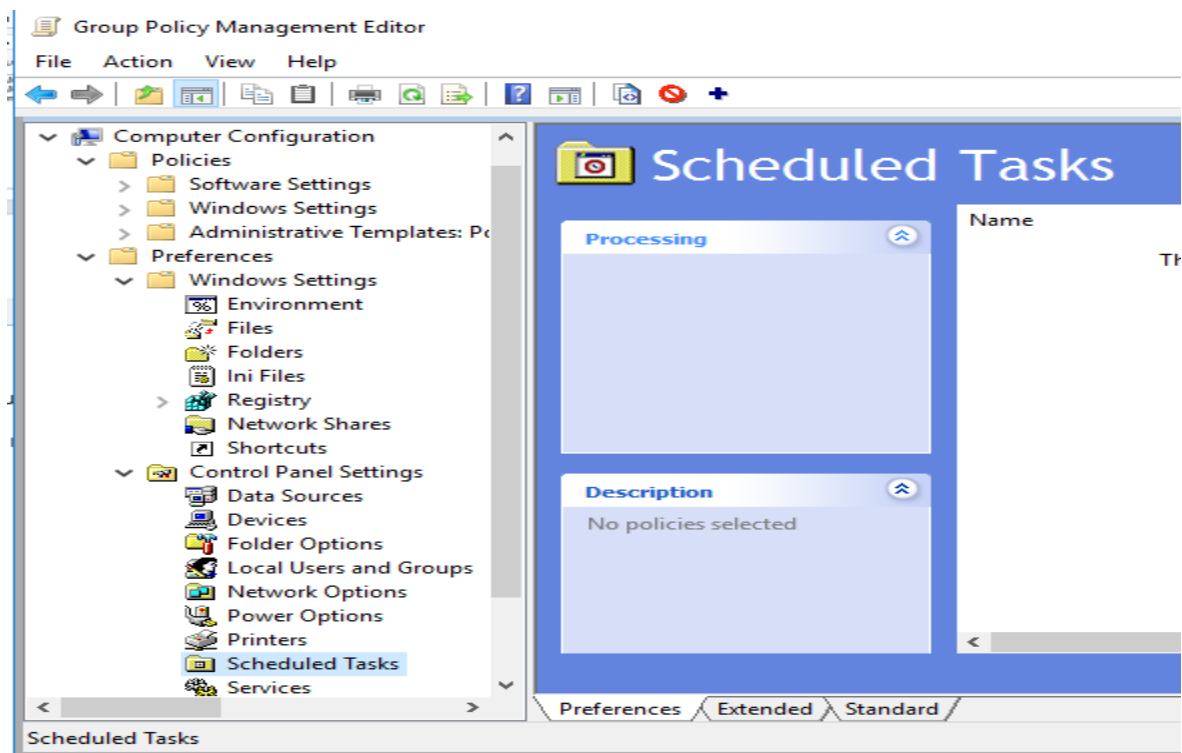
◯ Run only when user is logged on

◉ Run whether user is logged on or not

☑ Do not store password. The task will only have access to local resources.

☐ Run with highest privileges

☐ Hidden   Configure for: Windows® 7, Windows Server™ 2008R2 ▼

[OK]   [Cancel]   [Apply]   [Help]

New Trigger   ✕

Begin the task: On a schedule ▼

Settings

◯ One time   Start: 09-Dec-2018 ▼   8:54:57 AM ⏷   ☐ Synchronize across time zones

◉ Daily

◯ Weekly   Recur every: [1]   days

◯ Monthly

Advanced Settings

☑ Delay task for up to (random delay):   8 hours ▼

☐ Repeat task every: 1 hour ▼   for a duration of: 1 day ▼

☐ Stop all running tasks at end of repetition duration

☐ Stop task if it runs longer than: 3 days ▼

☐ Expire: 09-Dec-2018 ▼   8:54:57 AM ⏷   ☐ Synchronize across time zones

☑ Enabled

[OK]   [Cancel]

New Action

You must specify what action this task will perform.

Action: Start a program

Settings

Program/script:

\\dc1\myshare\DefenderDefinitionUpdate.bat

Browse...

Add arguments(optional):

Start in(optional):

OK   Cancel

New Task (At least Windows 7) Properties

General | Triggers | Actions | Conditions | Settings | Common

Specify the conditions that, along with the trigger, determine whether the task should run. The task will not run if any condition specified here is not true.

Idle

☐ Start the task only if the computer is idle for: 5 minutes

  Wait for idle for: 1 hour

  ☐ Stop if the computer ceases to be idle

    ☐ Restart if the idle state resumes

Power

☐ Start the task only if the computer is on AC power

  ☐ Stop if the computer switches to battery power

☑ Wake the computer to run this task

Network

☐ Start only if the following network connection is available:

Any connection

OK   Cancel   Apply   Help

Defender Definition Properties

General | Triggers | Actions | Conditions | Settings | Common

Special additional settings that affect the behavior of the task.

☑ Allow task to be run on demand

☐ Run task as soon as possible after a scheduled start is missed

☐ If the task fails, restart every: 1 minute ▾

    Attempt to restart up to: 3   times

☐ Stop the task if it runs longer than: 3 days ▾

☐ If the running task does not end when requested, force it to stop

☐ If the task is not scheduled to run again, delete it after: 30 days ▾

If the task is already running, then the following rule applies:

Do not start a new instance ▾

| OK | Cancel | Apply | Help |

New Task (At least Windows 7) Properties

General | Triggers | Actions | Conditions | Settings | Common

Options common to all items
☐ Stop processing items in this extension if an error occurs.
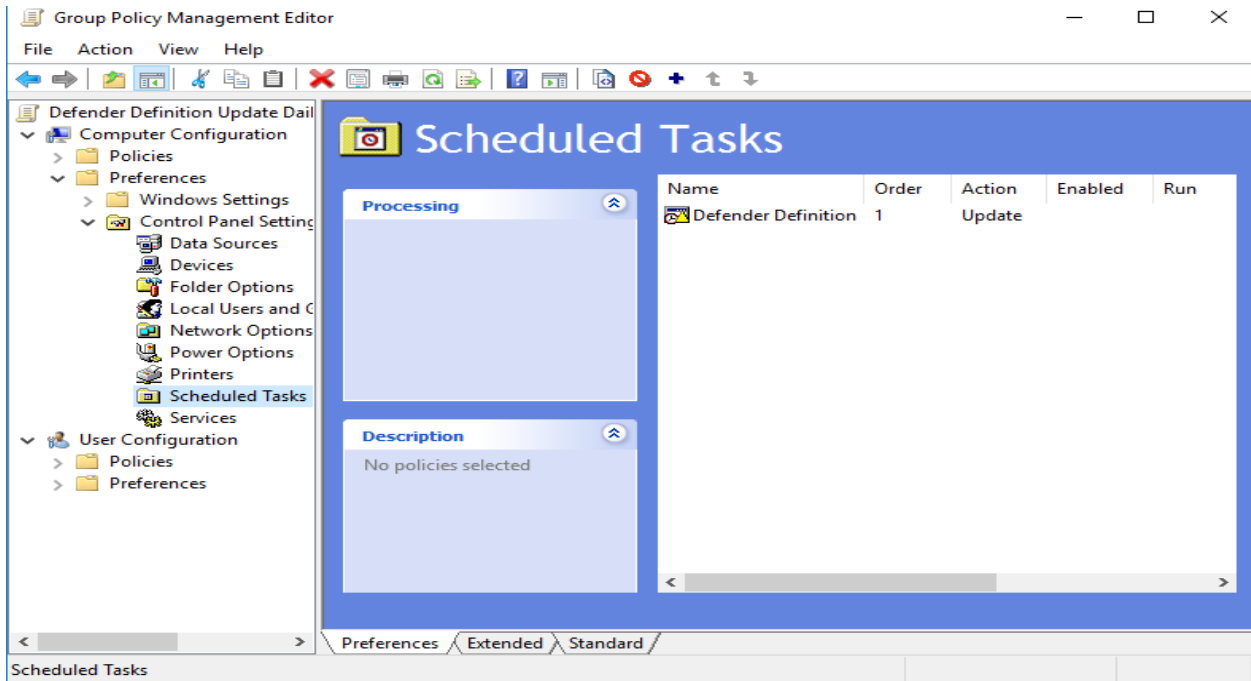☐ Run in logged-on user's security context (user policy option).
☐ Remove this item when it is no longer applied.
☐ Apply once and do not reapply.
☐ Item-level targeting.   Targeting...

Description

| OK | Cancel | Apply | Help |

Group Policy Management Editor

File   Action   View   Help

Defender Definition Update Dail
- Computer Configuration
  - Policies
  - Preferences
    - Windows Settings
    - Control Panel Setting
      - Data Sources
      - Devices
      - Folder Options
      - Local Users and C
      - Network Options
      - Power Options
      - Printers
      - Scheduled Tasks
      - Services
- User Configuration
  - Policies
  - Preferences

Scheduled Tasks

Processing

Description

No policies selected

Name	Order	Action	Enabled	Run
Defender Definition	1	Update		

Preferences \ Extended \ Standard

Scheduled Tasks

Computer Configuration (Enabled)

Preferences

Windows Settings

Files

File (Target Path: C:\Temp\DefenderDefinitionUpdate.bat)

DefenderDefinitionUpdate.bat (Order: 1)

General

Action	Create
Properties	
Source file(s)	C:\Myshare\DefenderDefinitionUpdate.bat
Destination file	C:\Temp\DefenderDefinitionUpdate.bat
Attributes	
Read-only	Disabled
Hidden	Disabled
Archive	Enabled

Control Panel Settings

Scheduled Tasks

Scheduled Task (At least Windows 7) (Name: Defender Definition)

Defender Definition (Order: 1)

General

Action		Update	
Task			
	Name	Defender Definition	
	Author	RAMLAN\Administrator	
	Description		
	Run only when user is logged on	S4U	
	UserId	NT AUTHORITY\System	
	Run with highest privileges	LeastPrivilege	
	Hidden	No	
	Configure for	1.2	
	Enabled	Yes	
Triggers			
1. Daily			
	Delay task for up to (random delay)	1 hour	
	Activate	09-Dec-2018 8:57:59 AM	Synchronize across time zones	No
	Enabled	Yes	
	Recur every 1 days		
Actions			
1. Start a program			
	Program/script	\\dc1\myshare\DefenderDefinitionUpdate.bat	

I performed gpupdate /force on a workstation to check, if the task completed successfully. Here is the screen shot.
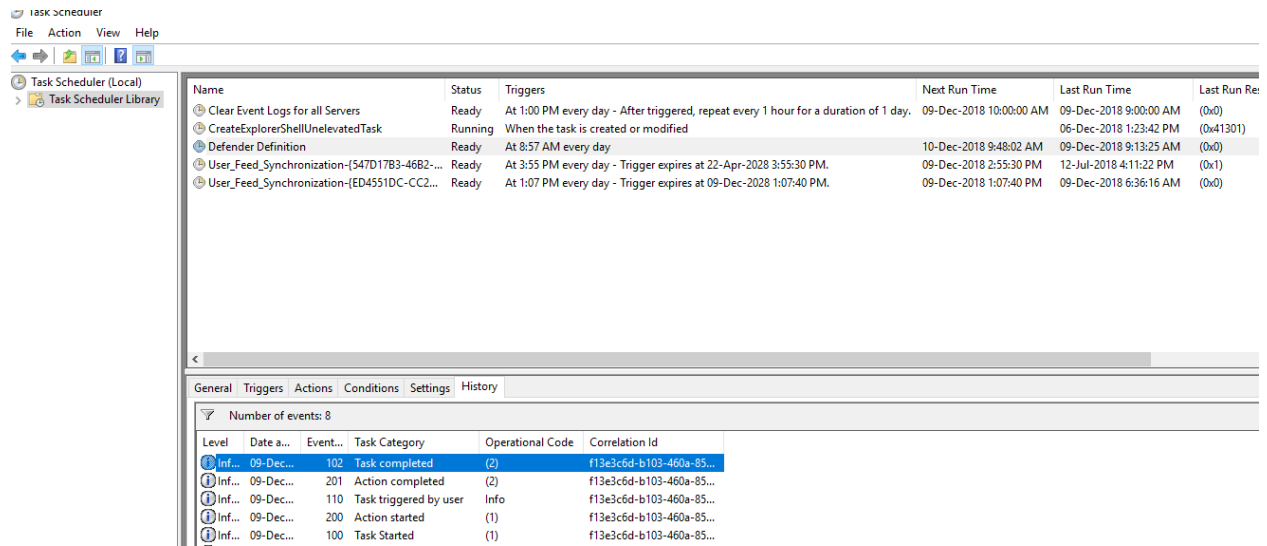
Now the GPO scheduled task will run every 8 hours and update Windows Defender Definition daily without any user input.

Thanks

Ram Lan
9th Dec 2018