HOW-TO GUIDE

Monitoring BitLocker in RMM

solarwinds msp

Last updated:
April 1, 2019

Table of Contents

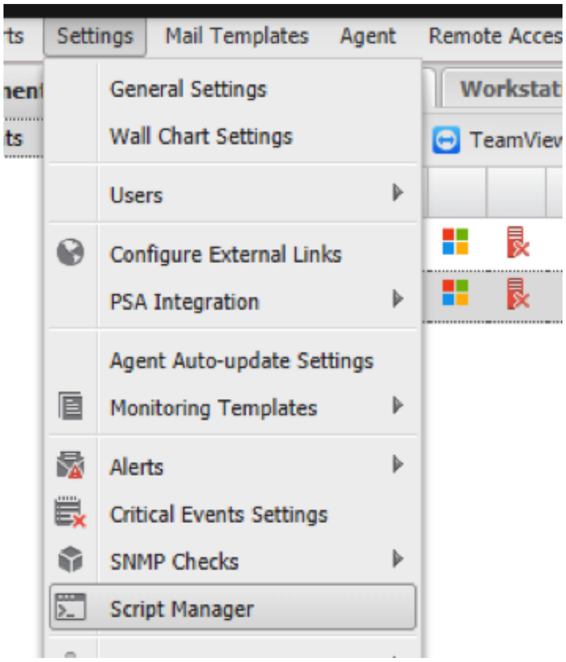
Overview

BitLocker is a feature available in all versions of Windows®, with the exception of Windows Home. This custom service looks at BitLocker overall and returns various information points.

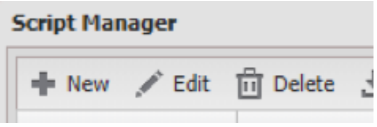
Uploading to RMM

To upload the check to your RMM server, follow this process:

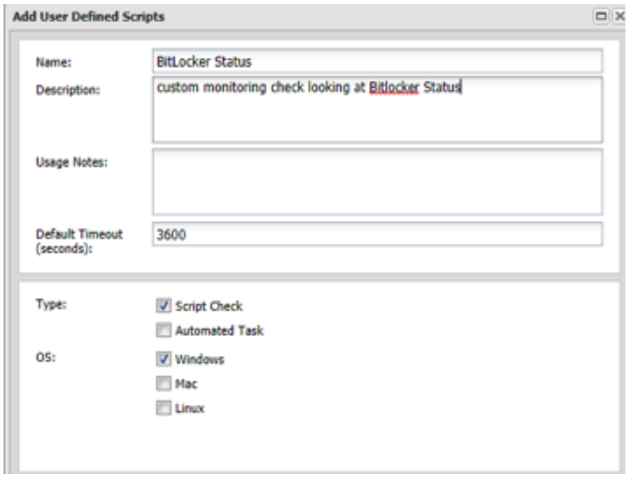
1. From the RMM main dashboard, click on Settings / Script Manager.



2. On this screen, we will need to click New to add a new script.



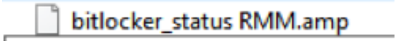
3. Put in the Name / Description, and select Script Check and Windows



Name: BitLocker Status
Description: custom monitoring check looking at Bitlocker Status
Usage Notes:
Default Timeout (seconds): 3600

Type: ☑ Script Check
☐ Automated Task
OS: ☑ Windows
☐ Mac
☐ Linux

4. Click on Browse to select the script, and select the BitLocker RMM AMP file attached with this document:

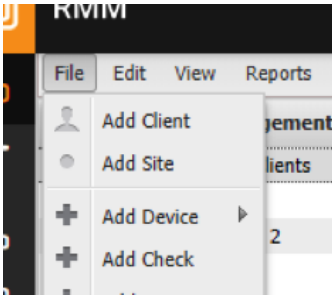

bitlocker_status RMM.amp

5. Click on Save to upload/save the script, and then Close to go back to the dashboard.

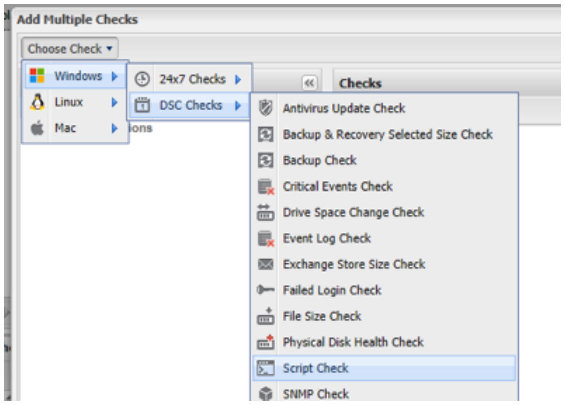
Adding the Check to Devices

To deploy the check to one or more devices, follow this process:

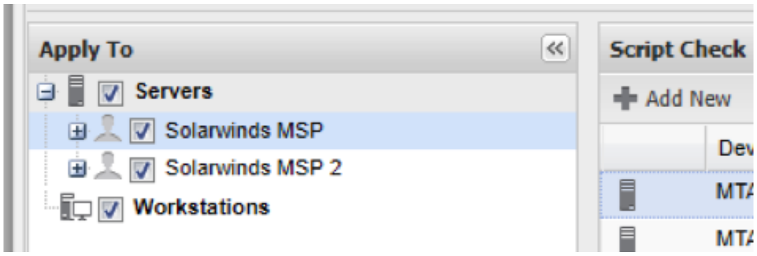
1. From the main dashboard, click on File / Add Check.



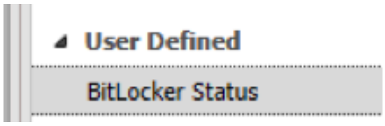
2. On this screen, click on Choose Check / Windows / DSC / Script Check.



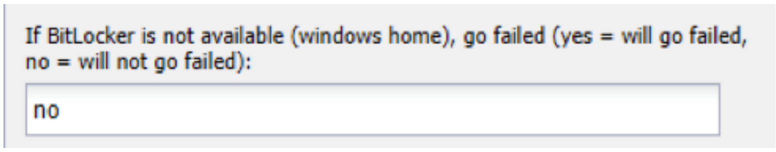
3. Select who to apply the service to in the list on the left, and click on Add New.



4. In the list, select BitLocker Status and click on Next.



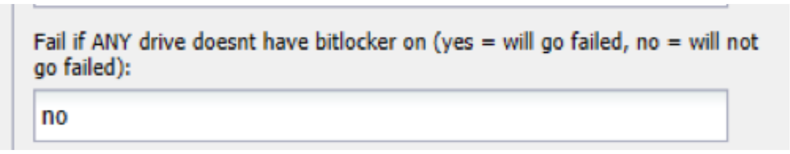
5. On this screen, you will select your input parameters. There are four fields available.
   A. The list of drives contains “C:” by default; you can add any other critical drive to the default list by adding a comma “,” in between drives, like so : “C:,D:,E:,”etc.
   B. The second field is an option so that if BitLocker is not available on that specific device (Windows Home), the check will have the option to “go failed.” By default, this is not the case. Change the value to “yes” to make it go failed if desired.



If BitLocker is not available (windows home), go failed (yes = will go failed, no = will not go failed):

no

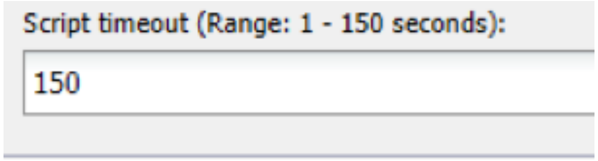
   C. The third field is an option where the service will fail if any drive on the device doesn’t have BitLocker, including drives not included in the list above. This may be more useful on servers. By default it is set to “no.” Change the value to “yes” if desired.



Fail if ANY drive doesnt have bitlocker on (yes = will go failed, no = will not go failed):

no

D. The last field is the timeout field. We recommend setting to 150 seconds as it is currently the maximum.

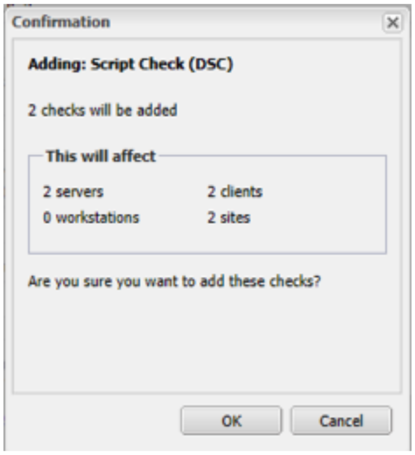


Script timeout (Range: 1 - 150 seconds):

150

E. Click on Finish to finish adding the service.

6. The system will ask you to confirm. Click OK to confirm.



Adding: Script Check (DSC)

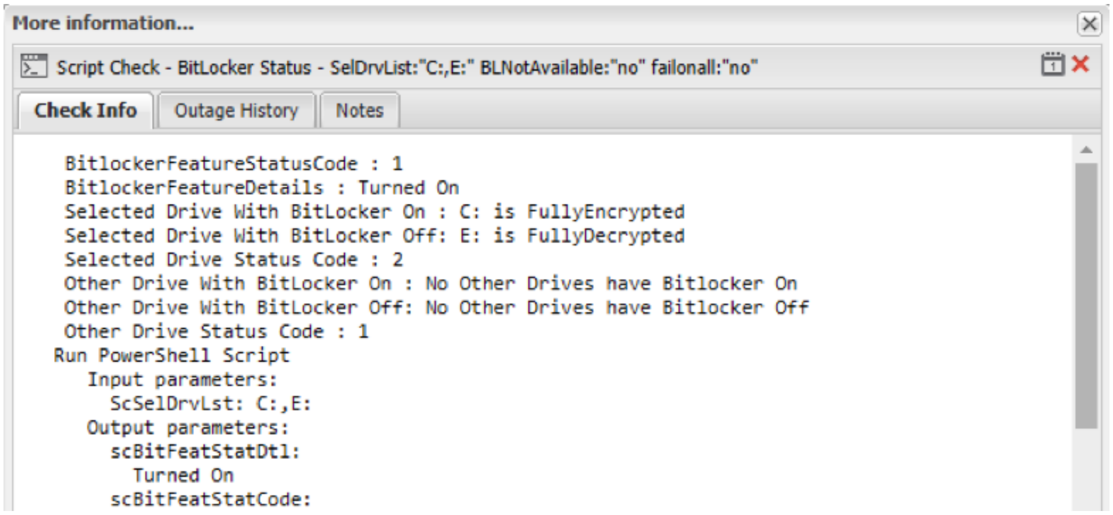
2 checks will be added

This will affect

2 servers
2 clients
0 workstations
2 sites

Are you sure you want to add these checks?

Sample


More information...
Script Check - BitLocker Status - SelDrvList:"C:,E:" BLNotAvailable:"no" failonall:"no"
Check Info
Outage History
Notes

```
    BitlockerFeatureStatusCode : 1
    BitlockerFeatureDetails : Turned On
    Selected Drive With BitLocker On : C: is FullyEncrypted
    Selected Drive With BitLocker Off: E: is FullyDecrypted
    Selected Drive Status Code : 2
    Other Drive With BitLocker On : No Other Drives have Bitlocker On
    Other Drive With BitLocker Off: No Other Drives have Bitlocker Off
    Other Drive Status Code : 1
   Run PowerShell Script
      Input parameters:
        ScSelDrvLst: C:,E:
      Output parameters:
        scBitFeatStatDtl:
          Turned On
        scBitFeatStatCode:
```