HOW-TO GUIDE

Monitoring Bitlocker in N-central

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.

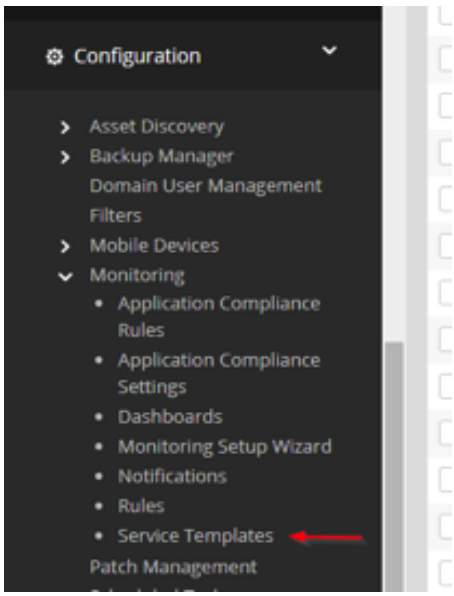
Note that this is packaged as a zip file that contains the script, custom service and three service templates to work on laptops, workstations, and servers.

Supported Versions

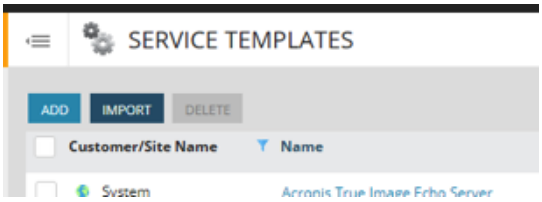
This custom service will run on N-central® 12.0.0.285 and newer.

Deployment

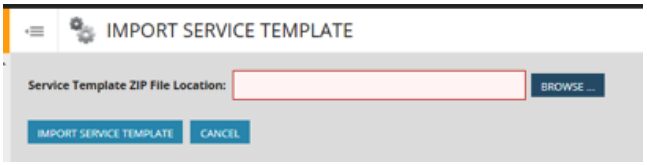
1. Go to the SO level, under Configuration / Monitoring / Service Templates.



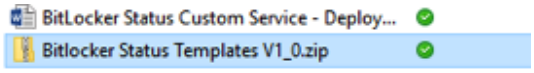
2. On this page, click on the IMPORT button at the top.

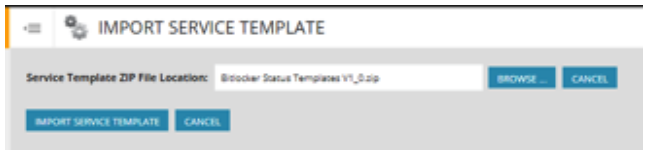


3. Click on BROWSE to open the file browser.

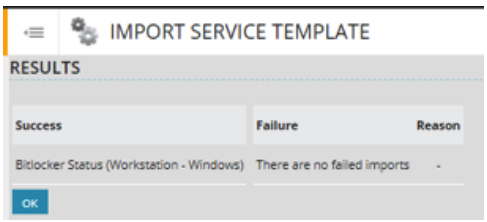


4. Select the zip file included with this guide and click on OPEN.

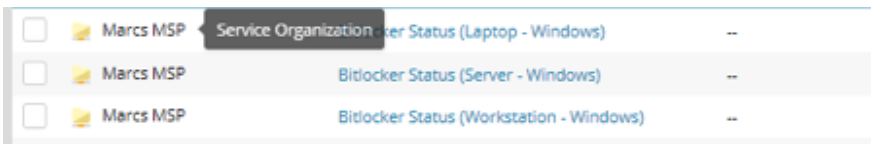




5. Click on IMPORT SERVICE TEMPLATE to import the template. The screen will show that the Workstation template has been created and that there is no failure. Click on OK.



6. If you browse the list, you will see three new service templates.



7. The templates and custom service are now ready to be used. Note that you can customize the threshold, monitored drives, and add self-healing if desired. To do so, go in the service template and modify the service.

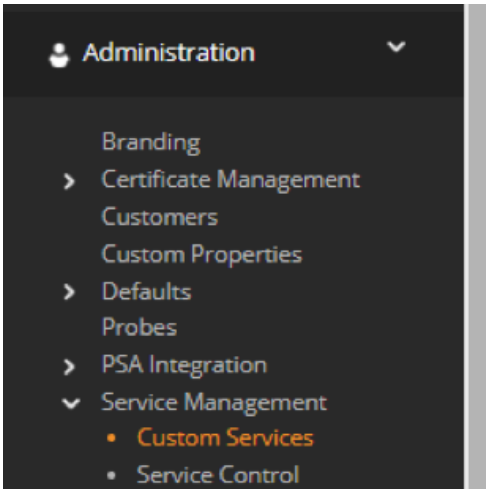
Configuring Input Parameters

This service monitors drives in two main categories: “selected” drives and “other” drives. This allows you to monitor and threshold on C: and/or any other critical drive, and report on noncritical drives like USB thumb drives.

To configure this, you can do this either in the service or in the template.

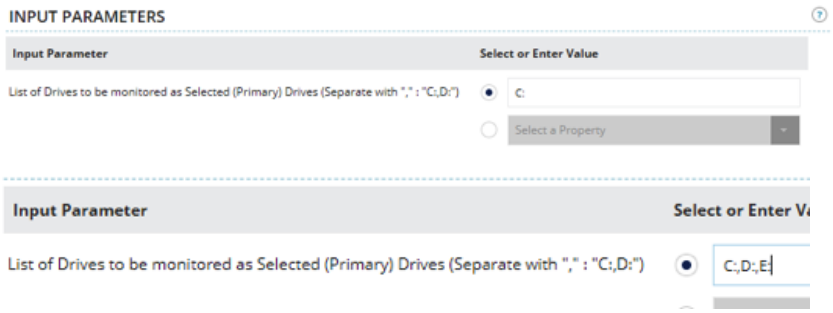
TO CONFIGURE IT IN THE SERVICE:

1. At the SO level, go to Administration / Service Management / Custom Service.



2. In that list, you will see your BitLocker Status service. Click on it.

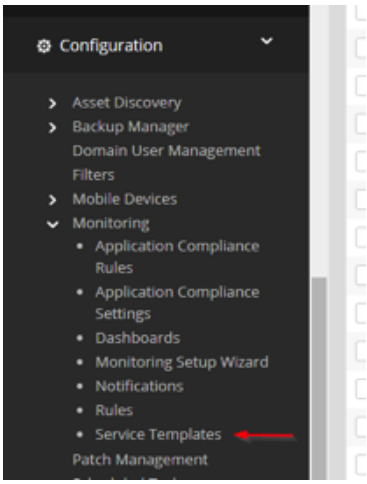
3. On this screen, you will see the Input Parameters section. The list of drives contains “C:” by default; you can add any other critical drive to the default list by adding a comma “,” in between drives, like so : “C:,D:,E:,”etc. Note that you could also link it to a device property if desired.



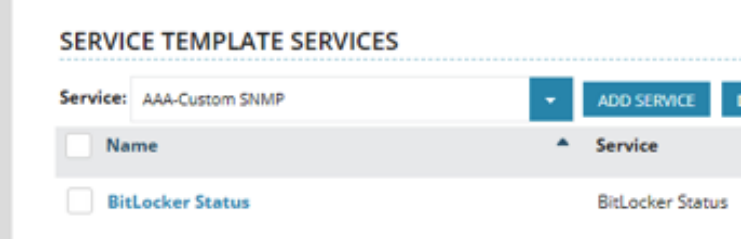
4. Click on Save to save it. Note that this will not affect existing devices and templates. This will change the service default only.

TO CONFIGURE IT AT THE TEMPLATE LEVEL:

1. Go to Configuration / Monitoring / Service Templates.



2. Click on any template containing the service (or one of the default templates).



3. Click on the BitLocker Status service. On this screen, you will see the Input Parameters section. 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. Note that you could also link it to a device property if desired.

   A. Note that to modify it, you will need to uncheck “Use Default Values” first.

4. Click on Save to save the service, and Save again to save the template. Repeat this process for any other template that may require modification.

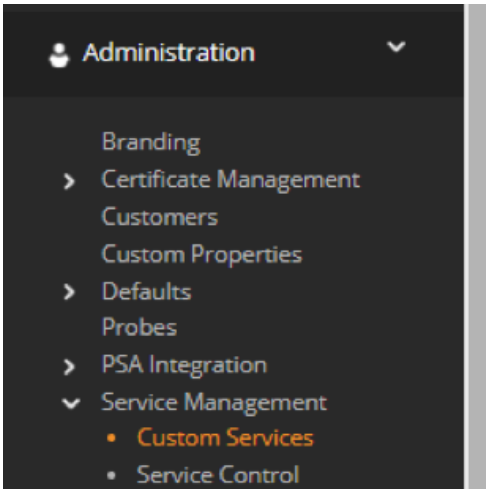
Configuring Thresholds

This service contains a total of eight output items that can all have configured thresholds. We only recommend putting a threshold on the three status codes as there is logic based on whether BitLocker is available on the device or not.

To configure this, you can do this either in the service or in the template.

TO CONFIGURE IT IN THE SERVICE:

1. At the SO level, go to Administration / Service Management / Custom Service.



2. In that list, you will see your BitLocker Status service. Click on it.

3. In BitLocker Status, click on the Thresholds Tab.

4. The threshold tab allows you to modify the individual items. Note that the various string fields are set to not threshold on anything, as the intent was to use the code fields to threshold when needed. We recommend looking at those three fields only.

   A. BitLocker Status Feature code: This is the overall status of BitLocker—whether it is installed on the computer or not, and whether it is available. The status is split up as follows:

      i. Code 1 - OK: BitLocker is installed

      ii. Code 2 - Fail: BitLocker is supported but not installed

      iii. Code 3 - Warning: BitLocker is not supported (Windows Home)

   B. Selected Drive Status Code: The drives entered in the details tab will be included in that list. By default, if any of those drives do not have BitLocker on, the service will fail. The mapping by default is as follows:

      i. Code 1 - OK: BitLocker is enabled on all “selected” drives

      ii. Code 2 - Fail: BitLocker is not enabled on at least one of the “selected” drives

      iii. Code 3 - Warning: BitLocker is not supported (Windows Home)

   C. Other Drive Status Code: All drives that are not entered in the “selected” drives will go in “other.” By default, the service will behave the same way as “selected” drives, but it is possible to disable the Threshold by selecting Off in that field.

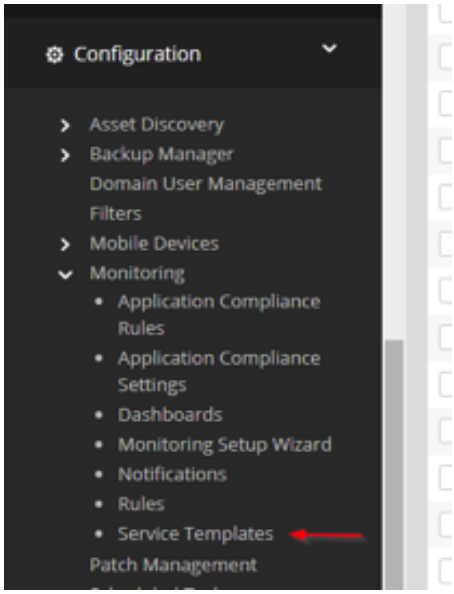
      i. Code 1 - OK: BitLocker is enabled on all “other” drives

      ii. Code 2 - Fail: BitLocker is not enabled on at least one of the “other” drives

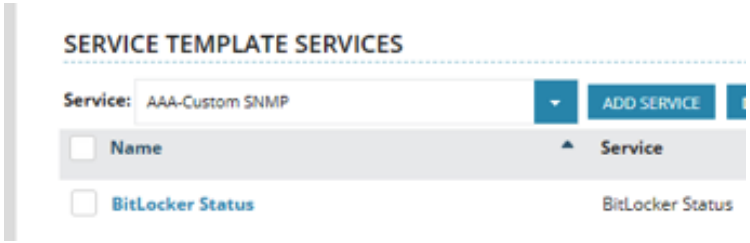
      iii. Code 3 - Warning: BitLocker is not supported (Windows Home)

TO CONFIGURE IT AT THE TEMPLATE LEVEL:

1. Go to Configuration / Monitoring / Service Templates.



2. Click on any template containing the service, or one of the default templates.



3. In here, click on the Thresholds tab

4. The Threshold tab allows you to modify the individual items. Note that the various string fields are set to not threshold on anything, as the intent was to use the code fields to threshold when needed. We recommend looking at those three fields only.

   A. BitLocker Status Feature code: This is the overall status of BitLocker—whether it is installed on the computer or not, and whether it is available. The status is split up as follows:

      i. Code 1 - OK: BitLocker is installed

      ii. Code 2 - Fail: BitLocker is supported but not installed

      iii. Code 3 - Warning: BitLocker is not supported (Windows Home)

   B. Selected Drive Status Code: The drives entered in the details tab will be included in that list. By default, if any of those drives do not have BitLocker on, the service will fail. The mapping by default is as follows:

      i. Code 1 - OK: BitLocker is enabled on all “selected” drives

      ii. Code 2 - Fail: BitLocker is not enabled on at least one of the “selected” drives

      iii. Code 3 - Warning: BitLocker is not supported (Windows Home)

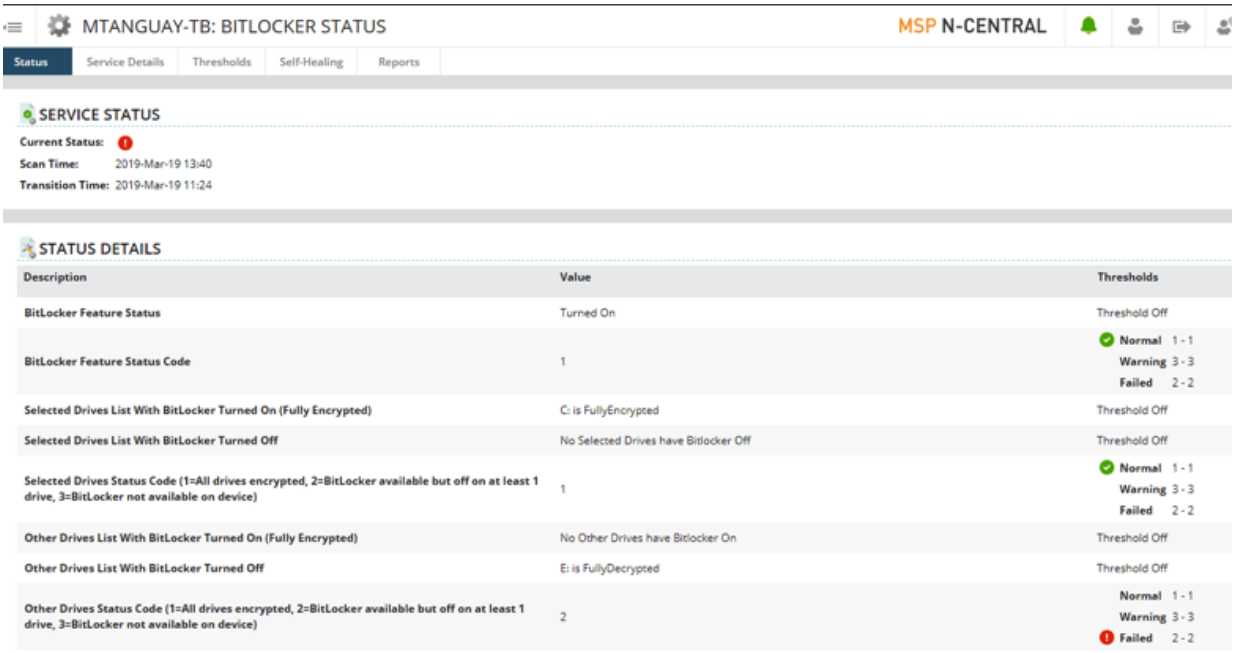
   C. Other Drive Status Code: All drives that are not entered in the “selected” drives will go in “other.” By default, the service will behave the same way as selected drives, but it is possible to disable the Threshold by selecting Off in that field.

      i. Code 1 - OK: BitLocker is enabled on all “other” drives

      ii. Code 2 - Fail: BitLocker is not enabled on at least one of the “other” drives

      iii. Code 3 - Warning: BitLocker is not supported (Windows Home)

Sample



MTANGUAY-TB: BITLOCKER STATUS

MSP N-CENTRAL

Status | Service Details | Thresholds | Self-Healing | Reports

SERVICE STATUS

Current Status:
Scan Time: 2019-Mar-19 13:40
Transition Time: 2019-Mar-19 11:24

STATUS DETAILS

Description	Value	Thresholds
BitLocker Feature Status	Turned On	Threshold Off
BitLocker Feature Status Code	1	Normal 1 - 1 Warning 3 - 3 Failed 2 - 2
Selected Drives List With BitLocker Turned On (Fully Encrypted)	C: is FullyEncrypted	Threshold Off
Selected Drives List With BitLocker Turned Off	No Selected Drives have Bitlocker Off	Threshold Off
Selected Drives Status Code (1=All drives encrypted, 2=BitLocker available but off on at least 1 drive, 3=BitLocker not available on device)	1	Normal 1 - 1 Warning 3 - 3 Failed 2 - 2
Other Drives List With BitLocker Turned On (Fully Encrypted)	No Other Drives have Bitlocker On	Threshold Off
Other Drives List With BitLocker Turned Off	E: is FullyDecrypted	Threshold Off
Other Drives Status Code (1=All drives encrypted, 2=BitLocker available but off on at least 1 drive, 3=BitLocker not available on device)	2	Normal 1 - 1 Warning 3 - 3 Failed 2 - 2