

Kelverion Automation Automated Patching Solution Solution

User's Guide

Version 1.4

Table of Contents

1. Overview	3
1.1. Runbook and Service Desk Overview	4
1.1.1. Keverion Automation Portal	4
1.1.2. ServiceNow	4
1.1.3. Runbooks	4
1.2. Automated Patching Solution Operation	4
2. Pre-Installation Information	6
2.1. Keverion Automated Patching Solution Package Contents	6
2.2. Integration Packs Required	6
2.3. Persistent Data Store	6
3. PDS Creation	8
3.1. PDS Creation Steps	8
4. Automation Portal Installation Steps	9
4.1. Runbook Solution Installation	9
4.2. Automation Portal Service Installation	9
4.3. Configuring the Patch Schedules	9
5. ServiceNow Solution Installation Steps	11
5.1. Runbook Solution Installation	11
5.2. ServiceNow Update Set Installation	11
5.3. ServiceNow Configuration	12
5.3.1. Keverion Auto Patching Solution Patch Schedules	12
5.3.2. Keverion Auto Patching Solution Software Update Groups	13
6. Orchestrator Solution Configuration	14
6.1. System Center Orchestrator Configuration	14
6.1.1. Integration Packs	14
6.1.2. Selecting your Service Desk Application	15
6.1.3. Variables	16
6.2. System Center Configuration Manager Dependencies	17
7. Installing Temporary License of Keverion Integration Packs	18
8. Upgrade Warning	19
9. Notes	20

1. Overview

This System Center Orchestrator driven solution delivers an automated patching solution that is designed to initiate from an approved weekly change control. Approved and pre-tested patches that are collated into SCCM software update groups can be delivered to pre-defined schedules via a change control process. Device owners will be able to select which schedule their device is allocated too. The SCCM patch deployment jobs are only enabled between defined patch windows, to provide additional control over the process and prevent unscheduled reboots of devices outside of the change control process.

The Kolverion Automated Patching Solution leverages the Persistent Data Store design philosophy and the Kolverion Orchestrator Integration Packs to provide a scalable and robust solution.

This solution is available for both the Kolverion Automation Portal and ServiceNow. Both configurations are included in a self-installation package. The solution is recommended for customers proficient with System Center.

For customers who are less familiar with System Center, Kolverion or our partners can provide as a complete installation and configuration solution where we work with you to customise the solution for your environment.

This document provides the guidance on how to setup and configure these Runbooks and Management Packs in your environment. It is aimed at an experienced System Center users. Users should also reference Microsoft supplied documentation for the System Center tools and Kolverion Integration Pack User Guides.

1.1. Runbook and Service Desk Overview

The solution is written for both Kolverion Automation Portal and ServiceNow.

1.1.1. Kolverion Automation Portal

The Kolverion Automation Portal comes with a Services import file with a set of Service Offerings for the required portal requests. The required CI data is pulled directly from SCCM for devices and stored in the PDS for the Patch schedules.

1.1.2. ServiceNow

The ServiceNow solution is provided as an Update Set that creates a custom application. This can be added to the ServiceNow catalog. The included pre-built request offerings can be launched from the catalog.

1.1.3. Runbooks

The Runbooks use monitors depending on the chosen request offering selected. The monitors in-turn set a relevant sequence of Runbooks in motion pending the dependent service request or change request that is raised. The two available options to select are:

- Create Automatic Patching Deployment Change Request
- Define or Change Device Patching Schedule

1.2. Automated Patching Solution Operation

The Runbooks utilise a common Persistent Data Store (PDS). From a very high level, the Runbooks operate as follows:

Populated the service desk CI with Software Update Groups:

1. Daily check SCCM for new Software Update Groups. Record details in the PDS (SUPGroups).
2. Monitor the PDS (SUPGroups) for changes. Check PDS entries and remove or add the corresponding software update groups from Configuration Item (Software Update Groups).

Device Patching Schedule Service Request:

3. Monitor the service desk for any service request offerings to change a devices patch schedule. Record the required changes in the PDS (DeviceSchedules).
4. Monitor the PDS (DeviceSchedules) for changes. Remove the chosen device from all patch schedule AD Groups listed in the Patch Schedules CI. Update the PDS (DeviceSchedules).
5. Monitor the PDS (DeviceSchedules) for changes. Add the corresponding device(s) to the required AD Group.

Patch deployment Change Request:

6. Monitor the service desk for any approved change request raised from the request offering for deploying patches. Record the details in the PDS (PatchCR).
7. Monitor the PDS (PatchCR) for changes. Create the Enable, Start and End days to a date and record into the PDS (PatchCR).
8. Monitor the PDS (PatchCR) for changes. Create the required patch deployment jobs in SCCM. Disable these jobs in the corresponding collections. Update the PDS (PatchCR).
9. Monitor the View (v_Deployment_Ready_To_Enable) for entries. Enable all deployments in the collection. Update the PDS (PatchCR).
10. Monitor the View (v_Deployment_Ready_To_Disable) for entries. Disable all deployments in the collection. Update the PDS (PatchCR).

All of the Runbooks are based around our experience of building these types of solutions for many customers. The Runbook sets are designed as solution which provides the foundations out of the box and allows extension and modification to tailor the solution to exact customer requirements.

By using the Persistent Data Store approach any complex decision logic can be handled using the database and Orchestrator Runbooks. You can extend the Runbooks yourself or we can provide consultancy to help you with the design update and Runbook modifications.

2. Pre-Installation Information

2.1. Keverion Automated Patching Solution Package Contents

The Automated Patching Solution Package contains the following elements:

- Keverion Persistent Data Store creation script (Microsoft SQL Server)
- Automated Patching Solution Runbook Set
- Keverion Automated Patching Solution Users Guide
- ServiceNow 'Keverion Auto Patch Solution' Update Set (xml)
- Keverion Automation Portal import file (export)
- Keverion Data Manipulation file (xml)

2.2. Integration Packs Required

The solution requires the following Integration Packs:

Microsoft

- Active Directory Integration Pack
- System Center Configuration Manager Integration Pack

Keverion

- | | |
|-------------------------------|---|
| • Data Manipulation | - Used with the Automation Portal version |
| • SQL Server Integration Pack | - Used with all versions |
| • ServiceNow Integration Pack | - Used with the ServiceNow version |
| • Text Manipulation | - Used with the ServiceNow version |

Before importing any Runbooks please ensure these Integration Packs are installed in Orchestrator. If you do not already have Keverion Integration Packs they can be downloaded for evaluation from our website.

2.3. Persistent Data Store

The Persistent Data Store or PDS is a SQL Server database that is used by this Solution to allow all of the actions that the Runbooks take to be carried out in a robust way. The use of the database at each “step” allows us to design the Runbooks such that each Runbook is simple and can be considered a discrete unit. In programming terms, it allows the Runbooks to be modular.

In your environment there may be a number of constraints that control the creation of a new database. For example, the location of the log and data files, the recovery options that should be used, and the collation of the server. These requirements are

typically specified by the DBA responsible for your database server. These options do not affect the Runbooks so please use the appropriate options for your environment.

Location

Typically, the PDS is created on the same database instance as is used for the Orchestrator database. There is no specific requirement that this must be the case. In environments where there is very high load you may find that creating the PDS on a different database instance advantageous.

Database version

The Runbooks provided, have been tested against SQL2019 with the latest patches / updates applied. You may need to modify the SQL Script to get it to operate in your environment or to install it on older versions of SQL Server.

Collation

The Runbooks have all been developed on systems using **Case Insensitive** collations as per the Microsoft System Center Orchestrator implementation guidelines, the specific collation setting used for your environment must be case insensitive other than that though the setting can be chosen as appropriate for your environment.

Sizing

The minimum recommended size of the PDS is 1GB.

The amount of space required will depend on the two following factors:

- Number of requests processed
- Housekeeping frequency as defined by your DBAs

3. PDS Creation

Each Kolverion Runbook Solution uses a set of common tables within the PDS Database and a set of tables specific to itself.

As part of each solution package you are provided with a SQL script which will generate the PDS database tables required for the solution. When the SQL scripts are executed they check for the existence of each table they required in the PDS database. If this is a new installation they will create both the Common Tables and their Solution Specific database tables. If you are already using a Kolverion Runbook Solution then the script will detect that some of the tables this solution requires already exist and the script skips these table creation steps and creates only the tables which do not exist in your installation.

This means you can easily deploy one or more Kolverion Runbook Solution to an existing PDS database without damaging and tables which already exist. This also means when installing multiple Runbook Solutions in a new installation of the PDS you can run each Solution PDS creation script in any order you like and know that when done you will have all the tables you need for all your Runbook Solutions to operate.

3.1. PDS Creation Steps

1. Create a New Database on your SQL Server called PDS_LIVE or connect to your existing PDS_LIVE database
2. Then execute the SQL Script provided within the PDS_LIVE database you created.
3. Once the PDS_LIVE database is created you must ensure the Orchestrator Runbook Server Service Account has as a minimum Read and Write Access permissions to the PDS_LIVE database.

4. Automation Portal Installation Steps

The installation steps below assume that the Kolverion Automation Portal application is installed. These steps should be followed by an experienced user.

4.1. Runbook Solution Installation

The Runbook Solution installation steps are as follows:

1. Install the required Kolverion and Microsoft System Center Integration Packs into Orchestrator.
2. Import the Automated Patching Solution Runbook Set.

4.2. Automation Portal Service Installation

The installation steps are as follows:

1. 'Import' the Services file into the Automation Portal
2. Go to the Queries section and edit the following imported queries, so that they point at your PDS and SCCM databases:
 - a. PatchingSchedules
 - b. PatchingDevices
 - c. PatchingSUPGroup
3. Check the Service Offerings are set to the appropriate access groups (AD Security Groups)

4.3. Configuring the Patch Schedules

The patch schedules are defined in the PDS under the table (PatchSchedules).

Column	Type	Mandatory Field
_created	datetime	
_owner	nvarchar	
_state	nvarchar	
AD_Group	nvarchar	
Enable_Day	nvarchar	TRUE
Enable_Time	nvarchar	TRUE
End_Day	nvarchar	TRUE
End_Time	nvarchar	TRUE
Start_Day	nvarchar	TRUE
Start_Time	nvarchar	TRUE
Reboot	nvarchar	TRUE
SCCM Collection	nvarchar	TRUE
Schedule Name	nvarchar	TRUE

You must create at least one instance in this table

Example Data

```
_created          :
_owner            : Admin
_state            : New
AD_Group          : AUTO_Patch_Sunday1600Reboot
Enable_Day        : Sunday
Enable_Time       : 10:00
End_Day           : Monday
End_Time          : 04:00
Start_Day         : Sunday
Start_Time        : 16:00
Reboot            : Allow Reboot
SCCM_Collection   : AUTO_Patch_Sunday1600Reboot
Schedule Name     : Sunday 16:00 Reboot

_created          :
_owner            : Admin
_state            : New
AD_Group          : AUTO_Patch_Saturday1800NoReboot
Enable_Day        : Saturday
Enable_Time       : 12:00
End_Day           : Sunday
End_Time          : 06:00
Start_Day         : Sunday
Start_Time        : 18:00
Reboot            : Suppress Reboot
SCCM_Collection   : AUTO_Patch_Saturday1800NoReboot
Schedule Name     : Saturday 18:00 No Reboot
```

4.3.1.1. *Data Entry Notes*

The SCCM Administrator should ensure that any patching schedule created falls inside any previously created maintenance windows. The automated patching solution does not alter any maintenance windows.

The 'Day' will always be the following day after the change request has been approved.

Enable = When the deployment job is enabled, and the patch content is made available for clients to download.

Start = Deployment deadline for starting patch installations

End = Sets when the deployment job is disabled

5. ServiceNow Solution Installation Steps

The installation steps below assume that the System Center Configuration Manager application is installed and there is an available ServiceNow instance. These steps should be followed by an experienced user.

5.1. Runbook Solution Installation

The Automation Solution installation steps are as follows:

1. Install the required Kerverion and Microsoft System Center Integration Packs into Orchestrator.
2. Import the Automated Patching Solution Runbook Set.

5.2. ServiceNow Update Set Installation

The installation steps are as follows:

1. From System Applications > Applications, ensure that any previous version of the 'Kerverion Automated Patching Solution' application is removed from ServiceNow.
2. From System Update Sets > Retrieved Update Sets, ensure that any previous version of the 'Kerverion Automated Patching Solution' update set is removed from ServiceNow.
3. From the System Update Sets > Retrieved Update Sets, select 'Import Update Set from XML'.
4. Select the provided XML file
sys_remote_update_set_a0f964094f39ee0064042d118110c764.xml and click on Upload.
5. Select the 'Kerverion Automated Patching Solution' update set and choose 'Preview Update Set'.
6. From Service Catalog > Catalogs, select the + for 'Add Content'
7. Select the 'Kerverion Automated Patching Solution' and choose the location of where you wish to place the widget with the appropriate 'Add here'.

5.3. ServiceNow Configuration

The execution of the solution and the choices available in the Service Offering, are controlled by the available data within tables in the custom application.

The solution defines 2 new tables which are described below.

5.3.1. Kolverion Auto Patching Solution Patch Schedules

The Kolverion Auto Patching Solution Patch Schedules table contains.

Property	Type	Mandatory Field
Deployment AD Group	String	TRUE
Deployment Enable Day	List	TRUE
Deployment Enable Time	String	TRUE
Deployment End Day	List	TRUE
Deployment End Time	String	TRUE
Deployment Start Day	List	TRUE
Deployment Start Time	String	TRUE
Device Schedule Name	String	TRUE
Reboot	List	TRUE
SCCM Collection	String	TRUE
Schedule Name	String	TRUE

You must create at least one instance in this table before you use the solution.

Example Data

```

Schedule Name      : Sunday 16:00 Reboot
Reboot             : Allow Reboot
Deployment Enable Day : Sunday
Deployment Enable Time : 10:00
Deployment End Day   : Monday
Deployment End Time   : 04:00
Deployment Start Day  : Sunday
Deployment Start Time : 16:00
SCCM Collection     : AUTO_Patch_Sunday1600Reboot

```

```

Schedule Name      : Saturday 18:00 No Reboot
Reboot             : Suppress Reboot
Deployment Enable Day : Saturday
Deployment Enable Time : 12:00
Deployment End Day   : Sunday
Deployment End Time   : 06:00
Deployment Start Day  : Saturday
Deployment Start Time : 18:00
SCCM Collection     : AUTO_Patch_Saturday1800NoReboot

```

5.3.1.1. *Data Entry Notes*

The SCCM Administrator should ensure that any patching schedule created falls inside any previously created maintenance windows. The automated patching solution does not alter any maintenance windows.

The 'Day' will always be the following day after the change request has been approved.

Enable = When the deployment job is enabled and the patch content is made available for clients to download.

Start = Deployment deadline for starting patch installations

End = Sets when the deployment job is disabled

5.3.2. *Kolverion Auto Patching Solution Software Update Groups*

The Kolverion Auto Patching Solution Software Update Groups table will be used for each of the software update groups detected in the SCCM environment.

Property	Type	Mandatory Field
Created By	String	FALSE
Date Created	Date Time	FALSE
Software Update Group Name	String	FALSE

The configuration items in this class are populated by the runbook solution.

Example Data

```

Software Update Group Name      : January 2016
Created By                      : Domain\SCCMAdmin
Date Created                    : 01/14/2016 3:05:22 PM

Software Update Group Name      : December 2015
Created By                      : Domain\SCCMAdmin
Date Created                    : 12/10/2015 3:16:05 PM

```

6. Orchestrator Solution Configuration

6.1. System Center Orchestrator Configuration

To use the solution, you must do a series of simple configuration steps to make the runbooks operate in your environment.

6.1.1. Integration Packs

Kerverion Data Manipulation IP:

In the Options Menu of Runbook Designer find the Kerverion Data Manipulation settings. Create a new configuration called 'AutoPatch'. Set the Type to 'XML Specification'.

Point the file at the AutoPatch.xml file. This can be a UNC path on your Orchestrator Runbook server.

Kerverion SQL Server IP:

In the Options Menu of Runbook Designer find the Kerverion SQL Server settings. In here you will see a default database connection (PDS_LIVE), which is required for the IP operation against the PDS.

Leaving the default Database Name (PDS_LIVE), modify the default database connection by changing the 'Server Name' and authentication details to values appropriate to your environment.

In the Authentication scheme field, select how the connection request will be authenticated.

If you selected *SQL Server Authentication*, type the SQL user credentials into the User name and User password fields.

Kerverion ServiceNow IP:

In the Options Menu of Runbook Designer, find the Kerverion ServiceNow setting. Configure the properties of the 'ServiceNow' configuration with the name of **ServiceNow** and appropriate settings for your environment.

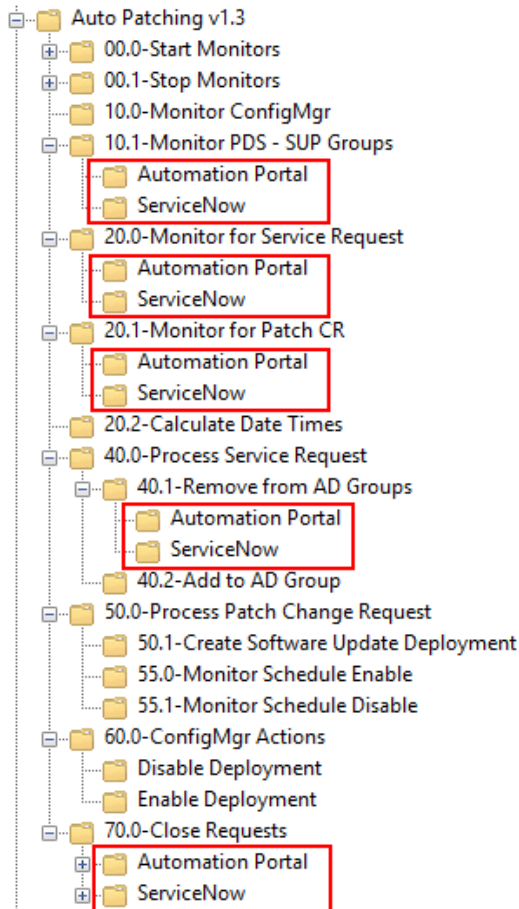
Microsoft System Center Configuration Manager IP:

In the Options Menu of Runbook Designer, find the SC Configuration Manager setting. Configure the properties of the 'SCCM' configuration appropriate for your environment.

6.1.2. Selecting your Service Desk Application

As the solution comes with both Kelverion Automation Portal and ServiceNow runbooks, you can choose to either ignore or delete the runbooks that you do not require.

Each folder that has a runbook for these applications will have two child folders called Automation Portal and ServiceNow. You just simply need to delete the unwanted folders in each case, as shown below.



6.1.3. Variables

The runbook solution has several variables that will require configuration.

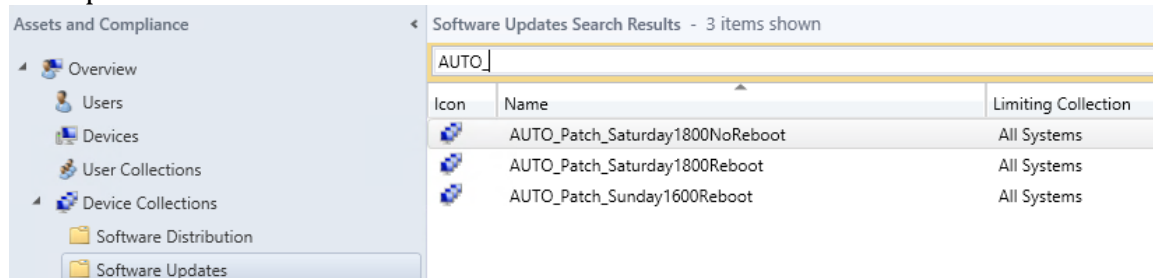
Variable	Description	Allowed Value
Runbooks root path	Solution root folder	\Auto Patching v1.3
SCCM	NETBIOS name of the SCCM server that has the SCCM console and PowerShell cmdlets installed.	Server Name
SCCM Sitecode	3 Digit SCCM Site Code	XXX
SCCM_PowerShellPath	Path to PowerShell module on the SCCM site server. e.g. C:\Program Files (x86)\Microsoft Configuration Manager\AdminConsole\bin	C:\InstallDirectory\
SCCM_ServiceAccount	Domain and account name of the service account that has rights to the SCCM console. N.B: Ensure you test this first by opening the console with the account.	Domain\AccountName
SCCM_ServiceAccount_Password	Password for the service account. N.B: Select the encrypted check box after typing the password.	
SCOM_InstallFails	True: SCOM is notified of deployment failures of the patch deployments False: SCOM is not notified of any patch deployment failures	True \ False

6.2. System Center Configuration Manager Dependencies

For the Automated Patching Solution to operate successfully, it is assumed that SCCM has the required collections and linked Active Directory groups created. Each patching schedule will require its own SCCM device collection and corresponding active group to populate it.

SCCM will need 'Active Directory Group Discovery' enabled on the OU that you have your AD groups located.

Example SCCM Device Collections:



Icon	Name	Limiting Collection
	AUTO_Patch_Saturday1800NoReboot	All Systems
	AUTO_Patch_Saturday1800Reboot	All Systems
	AUTO_Patch_Sunday1600Reboot	All Systems

Example AD Groups:

Name	Type	Description
AutoPatch-Sat-1800-NoReboot	Security Group...	AutoPatch Solution
AutoPatch-Sat-1800-Reboot	Security Group...	AutoPatch Solution
AutoPatch-Sun-1600-Reboot	Security Group...	AutoPatch Solution

SCCM Query to link the AD groups:

```
select
SMS_R_SYSTEM.ResourceID,SMS_R_SYSTEM.ResourceType,SMS_R_SYSTEM.Name,SMS_
R_SYSTEM.SMSUniqueIdentifier,SMS_R_SYSTEM.ResourceDomainORWorkgroup,SMS_
R_SYSTEM.Client from SMS_R_System where SMS_R_System.SecurityGroupName =
"Domain\ADGroupName"
```

7. Installing Temporary License of Kelverion Integration Packs

To run the solution, you will need a full or evaluation licence key for Kelverion Integration Packs.

The licence files need to be copied into a folder called C:\Program Files\Kelverion Automation\Licenses. If this folder does not already exist on your system please first create the folder

C:\Program Files\Kelverion Automation\Licenses
and then copy the attached files into it.

The license key is regularly updated as it includes a specific license end date after which the product will no longer work. If you have a license or date format error on trying to run this product please contact info@kelverion.com detailing date of download and error details.

To purchase a license please contact your Kelverion representative, reseller or email info@kelverion.com

8. Upgrade Warning

The Runbooks provided in this Automated Patching solution are provided for installation in a clean Orchestrator environment. If you have deployed any previous versions of this Runbook Solution, then installing this version will overwrite any changes you have made to the currently deployed Runbooks.

You can either delete you existing Runbook deployment and then install this new Runbook Solution set or manually upgrade your existing deployment.

9. Notes

Kelverion Automation Ltd
1 Lea Business Park
Lower Luton Road
Harpenden
AL5 5EQ
United Kingdom
Email: info@kelverion.com
Web: www.kelverion.com