



FLEXERA SOFTWARE®

## Software Vulnerability Manager

# Software Vulnerability Manager 2017 Release Notes

September 2017

<b>Introduction</b> .....	<b>2</b>
<b>New Features and Enhancements</b> .....	<b>2</b>
<b>System Requirements</b> .....	<b>3</b>
<b>Resolved Issues</b> .....	<b>4</b>
<b>Legal Information</b> .....	<b>5</b>

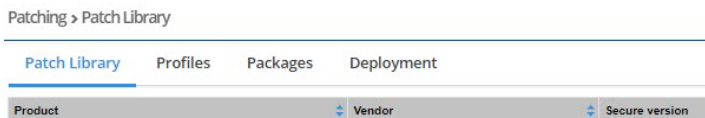
# Introduction

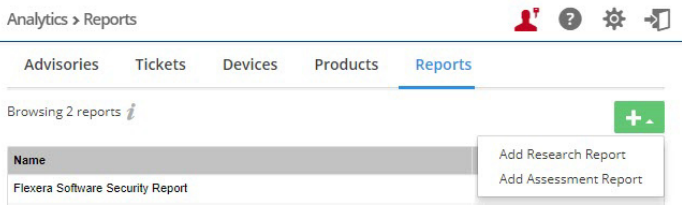
Software Vulnerability Manager reimagines how software is secured by closing the gap between IT Security and IT Operations by providing industry leading security research, risk assessment and remediation through Software Vulnerability Manager's key components:

- **Research:** Keep up with the latest software vulnerability research and advisories from Secunia Research
- **Patching:** Remediate software vulnerabilities in third-party applications
- **Assessment:** Discover where software vulnerabilities are installed across your organization

## New Features and Enhancements

The following table lists new features and enhancements for Software Vulnerability Manager 2017.

Reference Number	Feature or Enhancement Description
<b>SVM-57</b>	There is now an option to delete packages in the API.
<b>SVM-62</b>	Deleting a Daemon now removes all deployments (publishing) to that Daemon.
<b>SVM-63</b>	An account maintenance Celery task was created to clean up deleted frozen Daemons.
<b>SVM-72</b>	<p>The Vulnerable Software Discovery Tool for Mac <code>svmcan.macos</code> has been added to <b>Settings &gt; Assessment &gt; Downloads</b>.</p> <p>Information regarding the scanning option Agent-based Scan - Requirements (Mac OS X) has been added to the Assessment Scenarios section of the Software Vulnerability Manager User Guide and online help <a href="http://helpnet.flexerasoftware.com/svm/Default.htm#helplibrary/Assessment_Scenarios.htm">http://helpnet.flexerasoftware.com/svm/Default.htm#helplibrary/Assessment_Scenarios.htm</a>.</p>
<b>SVM-77</b>	<p>The Patch Library view in the Patching console now focuses on the Secure version of the patch rather than the product that needs to be patched.</p> 
<b>SVM-91</b>	The Ticket Comments field for a Ticket issued in the Vulnerability Manager console now allows spacing and formatting rather than one continuous line of text.
<b>SVM-97</b>	Updated all Software Vulnerability Manager product logos to the new Flexera logo.

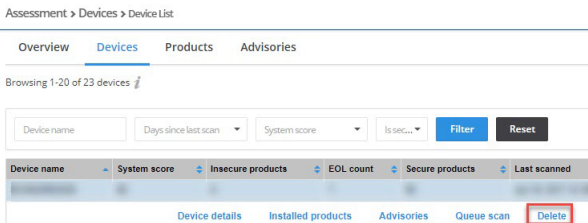
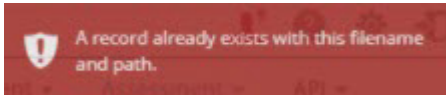
Reference Number	Feature or Enhancement Description
<b>SVM-111 and SVM-141</b>	In the Patching console, the Patch Library and Grouped Patch Library have been combined as the Patch Library.
<b>SVM-113</b>	Generic patch detection data can now be stored in the Daemon.
<b>SVM-116</b>	Under <b>Assessment &gt; Devices &gt; Device List</b> there is a column titled Inventory Source. The Inventory Source option for CSI Agent now includes the agent version.
<b>SVM-117</b>	Under <b>Analytics &gt; Reports</b> the reports that can be generated have been retitled as "Research Report" and "Assessment Report."
	
<b>SVM-120</b>	The new Flexera logo has been added to the email sent to new users to set up their Software Vulnerability Manager account.
<b>SVM-154</b>	In the Patching console, the default sorting for the Patch Library view includes sorting first by the Vendor column (A-Z) and then by the Product column (A-Z).
<b>SVM-163</b>	Software Vulnerability Manager's Help menu now includes the online help link: <a href="http://helpnet.flexerasoftware.com/svm/Default.htm">http://helpnet.flexerasoftware.com/svm/Default.htm</a>
<b>SVM-165</b>	Software Vulnerability Manager's Release Notes have been added to <a href="http://helpnet.flexerasoftware.com/">http://helpnet.flexerasoftware.com/</a>

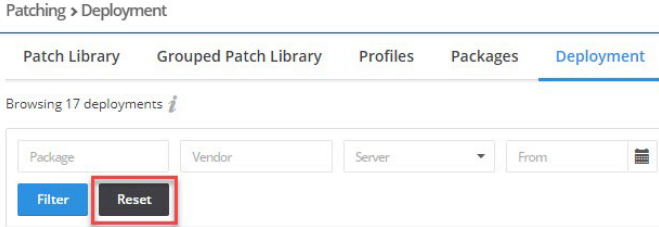
## System Requirements

The Software Vulnerability Manager 2017 User Interface will resize and adapt when being used on different devices. You can access the system from anywhere using any device, such as a smartphone or tablet, running Internet Explorer 11 or higher, Chrome, Opera, Firefox, Safari and mobile browsers with an Internet connection capable of connecting to <https://app.secunia.com/>.

# Resolved Issues

The following table lists resolved issues for Software Vulnerability Manager 2017.

Reference Number	Issue Summary
<b>SVM-4</b>	<p>Under <b>Assessment &gt; Devices &gt; Device List</b>, there is now a Delete option to delete a Device from the Devices panel.</p>  <p>The screenshot shows the 'Assessment &gt; Devices &gt; Device List' page. It has tabs for Overview, Devices, Products, and Advisories. Below the tabs, it says 'Browsing 1-20 of 23 devices'. There are search filters for Device name, Days since last scan, System score, and Insec... with Filter and Reset buttons. Below the filters is a table with columns: Device name, System score, Insecure products, EOL count, Secure products, and Last scanned. At the bottom of the table, there are links for Device details, Installed products, Advisories, Queue scan, and a 'Delete' button which is highlighted with a red box.</p>
<b>SVM-20</b>	<p>Users can now clean up old hosts and scan results.</p>
<b>SVM-32</b>	<p>In the Settings console, when users inadvertently create duplicate whitelist or blacklist Custom scan paths in <b>Settings &gt; Assessment &gt; Scan Configuration</b>, an error message will appear and the duplicate Custom scan path will not be saved.</p>  <p>The screenshot shows a red error message box with a shield icon and the text: 'A record already exists with this filename and path.'</p>
<b>SVM-33</b>	<p>The Status field in <b>Patching &gt; Deployment</b> has been resolved to show the correct build status for patch packages.</p>
<b>SVM-40</b>	<p>Apache Tomcat 8.x versions now appear in CPE for Secunia Advisory SA73849.</p>
<b>SVM-58</b>	<p>Corporate Software Inspector patch links have been resolved to create patch packages in Software Vulnerability Manager.</p>
<b>SVM-84</b>	<p>Patch packages can now be deployed to multiple servers in <b>Patching &gt; Development</b>.</p>
<b>SVM-92</b>	<p>APIs are disabled after an account expires.</p>
<b>SVM-93</b>	<p>In the Analytics console, reports are now generated per their custom schedule.</p>
<b>SVM-98</b>	<p>Under <b>Settings &gt; User Management &gt; User Group</b>, the new user role Device Database Reader was created to view information about devices, products installed and vulnerabilities.</p>

Reference Number	Issue Summary
<b>SVM-99</b>	Under <b>Settings &gt; User Management &gt; User Group</b> , the new user role Auditor was created to view audit logs of system usage.
<b>SVM-119</b>	The Reset button under <b>Patching &gt; Deployment</b> now works.  
<b>SVM-160</b>	The Software Vulnerability Manager User Guide module "Intelligence" has been renamed "Research".
<b>SVM-177</b>	After clicking <b>Available Patches</b> under <b>Assessment &gt; Devices &gt; Device Details</b> , the user is now directed to the appropriate patch under <b>Patching &gt; Patch Library</b> .

## Legal Information

### Copyright Notice

Copyright © 2017 Flexera. All Rights Reserved.

This publication contains proprietary and confidential information and creative works owned by Flexera and its licensors, if any. Any use, copying, publication, distribution, display, modification, or transmission of such publication in whole or in part in any form or by any means without the prior express written permission of Flexera is strictly prohibited. Except where expressly provided by Flexera in writing, possession of this publication shall not be construed to confer any license or rights under any Flexera intellectual property rights, whether by estoppel, implication, or otherwise.

All copies of the technology and related information, if allowed by Flexera, must display this notice of copyright and ownership in full.

### Intellectual Property

For a list of trademarks and patents that are owned by Flexera, see [www.flexerasoftware.com/intellectual-property](http://www.flexerasoftware.com/intellectual-property). All other brand and product names mentioned in Flexera products, product documentation, and marketing materials are the trademarks and registered trademarks of their respective owners.

### Restricted Rights Legend

The Software is commercial computer software. If the user or licensee of the Software is an agency, department, or other entity of the United States Government, the use, duplication, reproduction, release, modification, disclosure, or transfer of the Software, or any related documentation of any kind, including technical data and manuals, is restricted by a license agreement or by the terms of this Agreement in

accordance with Federal Acquisition Regulation 12.212 for civilian purposes and Defense Federal Acquisition Regulation Supplement 227.7202 for military purposes. The Software was developed fully at private expense. All other use is prohibited.

## Disclaimer

Information in this document is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. The provision of such information does not represent any commitment on the part of Flexera. Flexera makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Flexera shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

The software described in this document is furnished by Flexera under a license agreement. The software may be used only in accordance with the terms of that license agreement. It is against the law to copy or use the software, except as specifically allowed in the license agreement. No part of this document may be reproduced or retransmitted in any form or by any means, whether electronically or mechanically, including, but not limited to: photocopying, recording, or information recording and retrieval systems, for any purpose other than the purchaser's personal use, without the express, prior, written permission of Flexera.