

AdminStudio 2018 R2

Release Notes

July 2018

Introduction	3
New Features in AdminStudio 2018 R2	4
Support for Microsoft MSIX Packages	4
Importing Microsoft MSIX Packages into the Application Catalog	4
Testing Windows Installer Packages for MSIX Conversion Compatibility	4
User Interface Modernization	4
New Features in AdminStudio 2018.....	5
Application Manager User Interface Redesign	5
Redesigned Ribbon Interface	5
Updated Deployment Type, Status, and Subnode Icons	7
New Pie Chart Display on Group View of Analyze Tab.....	8
New Supportability Risks and Security Risks Test Category Groups.....	10
Simplified Compatibility Test Results	10
Consolidation of Functionality in Application Manager	13
New App Risk Module (ARM) to Identify Security Vulnerabilities	14
Scanning Applications for Security Vulnerabilities	15
Viewing Security Vulnerability Test Results	16
Configuring App Risk Module Options	21
New Software Security Vulnerability Reports.....	22
New App Risk Module PowerShell Platform API Commands	23
Security Vulnerability Warning During Distribution	23
Legacy Add-On Packs Now Included with Professional and Enterprise Editions	23
InstallShield 2018.....	23
Specify Uninstallation Order of Packages in a Suite Project.....	24
Method to Run a Suite Installation with Minimum UI	25
Conditionally Set the Visibility of a Feature at Run Time	25
Perform Recursive or Non-Recursive IIS Registration	26
Set Forms Authentication on Web Applications.....	27
New Option to Control Whether to Load User Profile for an Application Pool Entity	27
Add Kill Process and PowerShell Custom Actions to a Transform Project.....	28
Save QuickPatch Projects in XML Format	28
Localize Product Name Property in Suite Projects.....	28

Include the Value of a Property in a Product Configuration's Setup File Name	29
New MSBuild Parameters to Set Summary Information Stream Comments and to Set Package File Name	29
Specify Line Break and Tab Characters in Text File Changes.....	30
Remove or Hide the Suite Loading Screen.....	31
Setting to Always Create Debug Logs for Suite Installers	31
New Out-of-the-Box Dialog to Set the IIS Certificate File for SSL Certificate at Runtime.....	32
Specify Absolute or Relative Path When Creating New Child Elements in an XML File	33
Setting the Default Keyboard Focus for Dialog Box Controls in Suite Projects	33
PowerShell Script Editor in Basic MSI Projects.....	34
New Option to Open Existing Transform File in InstallShield Transform Wizard	34
Additional Prerequisites Included	34
Important Information	35
Removal of Support for Symantec Workspace Virtual Packages	35
Removal of Support for Testing for Internet Explorer 9 and 10	35
Editions.....	36
System Requirements	43
Compatibility Summary	43
AdminStudio Machine	48
Distribution Systems	49
Application Catalog Database Server	50
AdminStudio Enterprise Server / Workflow Manager Server	51
Automated Application Converter	52
Virtual Machine Requirements	52
Virtual Technology Requirements.....	56
Downloading AdminStudio Installers.....	56
AdminStudio 2018 R2 Evaluation Restrictions	57
Resolved Issues.....	57
AdminStudio 2018 R2.....	57
AdminStudio 2018	58
Known Issues.....	59
Legal Information	59

Introduction

AdminStudio makes short work of application deployment chores such as updates, new releases, new applications, and Windows 10 migrations. More than a packaging tool, AdminStudio arms your IT team with a complete application readiness solution, enabling you to identify and mitigate issues before pulling the deployment trigger. No more surprises.

With AdminStudio, you can:

- Improve service quality and streamline service delivery
- Decrease risk and embrace new technologies faster
- Eliminate mobile application security and compatibility concerns
- Reliably prepare and deploy application virtualization formats
- Integrate seamlessly with leading software deployment systems
- Simplify and unify application management with standardized processes
- Boost efficiency with a central application repository
- Identify application packaging issues in minutes instead of days

AdminStudio 2018 introduces App Risk Module to keep you aware of application vulnerabilities from packaging to deployment. Don't let application vulnerabilities open the door to business risk. Add App Risk Module to your AdminStudio implementation to:

- Take a proactive approach to your cybersecurity defenses so your business doesn't fall victim to ransomware or the next big cybersecurity threat
- Make early vulnerability assessment and remediation integral to your Application Readiness process
- Stay on top of vulnerabilities with regularly scheduled, automatic scans against Flexera's extensive list of application titles
- Keep up on the fixes and patches available for known vulnerabilities so you can implement them early to minimize risk

New Features in AdminStudio 2018 R2

This section lists the new features that are included in AdminStudio 2018 R2:

- [Support for Microsoft MSIX Packages](#)
- [User Interface Modernization](#)

Support for Microsoft MSIX Packages

Microsoft has introduced a new installer technology, MSIX packages (.msix), to support platform independent installations. AdminStudio 2018 R2 supports this new MSIX deployment type.

MSIX is the next generation software deployment model for the Windows platform, bringing the best of MSI, AppX and App-V together in a single package. MSIX has the capability to run a traditional Win32 application in a native container, achieving application isolation, ease of deployment, fully clean uninstallation, and seamless software updates all at the same time. MSIX promises to be the alternative to MSI and become the gold standard of Windows deployments. You can choose to continue to use MSI, but the benefits of MSIX will greatly outweigh the need to maintain MSIs long-term, especially given that most enterprises and consumers are increasing their adoption of Windows 10.

Importing Microsoft MSIX Packages into the Application Catalog

AdminStudio 2018 R2 supports the import of Microsoft MSIX packages (.msix) into the Application Catalog.

To import an .msix package into the Application Catalog, select **Microsoft MSIX Package (.msix)** on the **Package Type Selection** panel of the Import Wizard.

Testing Windows Installer Packages for MSIX Conversion Compatibility

In AdminStudio 2018 R2, you can test the Windows Installer (.msi) packages in your Application Catalog for compatibility for conversion to MSIX package format.

When a Windows Installer package is tested during import or by clicking the **Execute Tests** button on the **Analyze** tab, the MSIX conversion compatibility tests are run. You can view an icon indicating the status of the test results in the **Supportability Risks** column of the **Analyze Application View** and **Analyze Group View**. Detailed test results can be viewed by clicking on the **MSIX Conversion Compatibility** status icon on the **Supportability Risks** tab of the **Analyze Deployment Type View**.

There is also a new **MSIX Conversion Compatibility** report on the **Reports** tab. This report identifies each application in the Application Catalog as either **Recommended** for conversion to the MSIX package format or **Not Recommended**.

User Interface Modernization

AdminStudio's splash screens and About dialog boxes have been updated to match the redesigned user interface.

New Features in AdminStudio 2018

This section lists the new features that are included in AdminStudio 2018:

- [Application Manager User Interface Redesign](#)
- [Consolidation of Functionality in Application Manager](#)
- [New App Risk Module \(ARM\) to Identify Security Vulnerabilities](#)
- [Legacy Add-On Packs Now Included with Professional and Enterprise Editions](#)
- [InstallShield 2018](#)

Application Manager User Interface Redesign

In AdminStudio 2018, the Application Manager user interface has been redesigned and updated to provide a clean, modern look that makes it easy to navigate through application readiness tasks.

- [Redesigned Ribbon Interface](#)
- [Updated Deployment Type, Status, and Subnode Icons](#)
- [New Pie Chart Display on Group View of Analyze Tab](#)
- [New Supportability Risks and Security Risks Test Category Groups](#)
- [Simplified Compatibility Test Results](#)

Redesigned Ribbon Interface

The look and feel of AdminStudio's ribbon interface has been updated with new icons, and the names of the tabs have been changed to more clearly reflect their purpose.

Home Tab

The ribbon on the Application Manager **Home** tab (previously named the **Catalog** tab) contains buttons that enable you to import packages into the Application Catalog, edit Windows Installer and virtual packages, and distribute applications. You can also launch other AdminStudio tools by clicking on the **AdminStudio Tools** button.

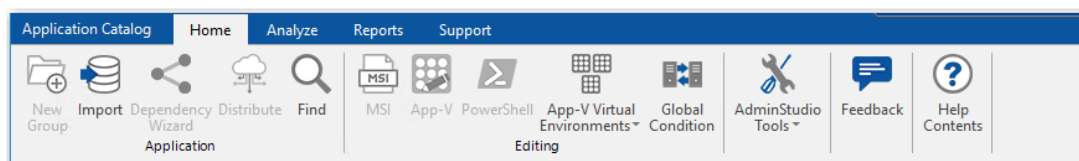


Figure 1: Home Tab Ribbon

New Feedback Button

The ribbon on the AdminStudio **Home** tab now includes a new **Feedback** button that you can use to provide feedback and ideas about AdminStudio tools. When you click the **Feedback** button, the Flexera Customer Community **Ideas** page opens, where you can post new ideas and browse ideas submitted by other users. If you like a posted idea, you can vote for it, and even add comments.

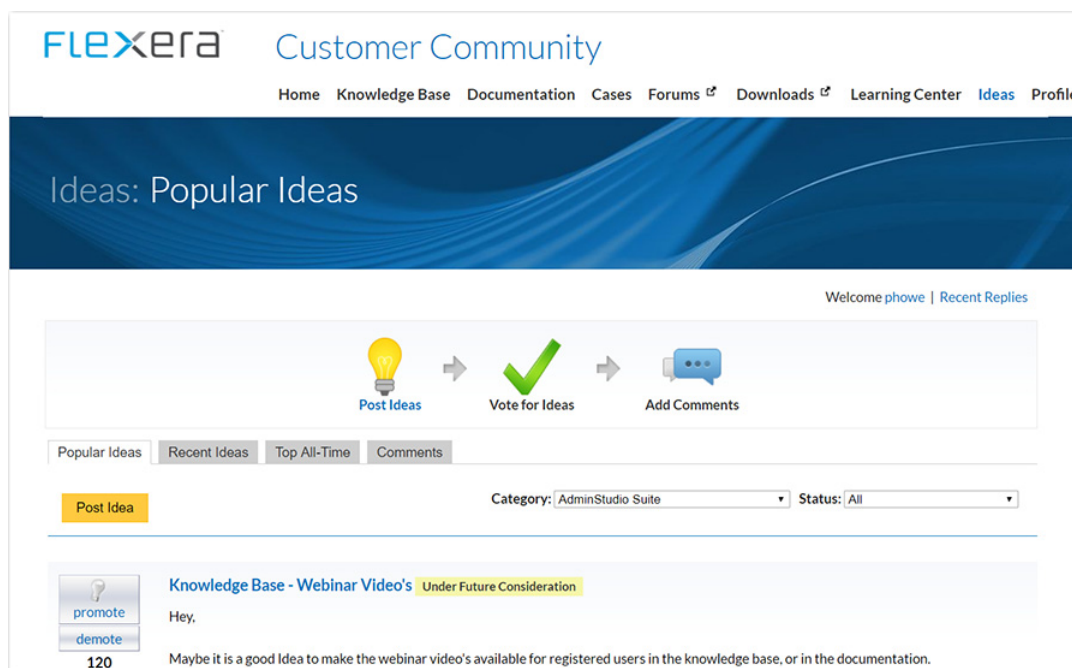


Figure 2: Flexera Customer Community Ideas Page

Analyze Tab

The ribbon on the Application Manager **Analyze** tab (previously named the **Test Center** tab) contains buttons that enable you perform all testing tasks. If you have AdminStudio Enterprise Edition with the App Risk Module (ARM), can perform security vulnerability testing of applications by clicking the **Check Vulnerabilities** button. For more information, see [New App Risk Module \(ARM\) to Identify Security Vulnerabilities](#)

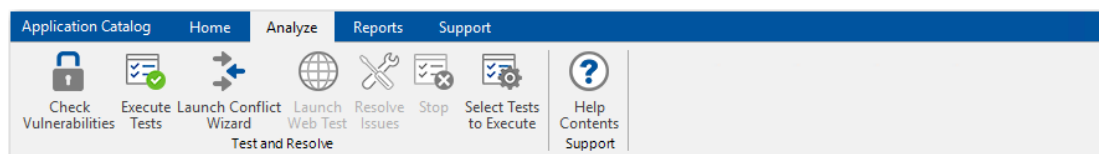


Figure 3: Analyze Tab Ribbon

Reports Tab

The ribbon on the Application Manager **Reports** tab (previously named the **Report Center** tab) contains buttons that enable you view all available reports, including the new **Software Security Vulnerability** reports.

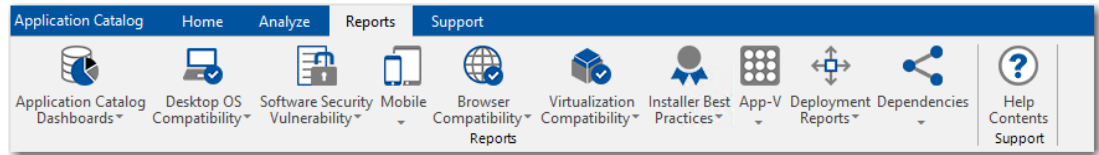


Figure 4: Reports Tab Ribbon

Support Tab

The ribbon on the Application Manager **Support** tab contains buttons that give you access to application information, the online help library, and the release notes. A new **Check for Updates** button has been added to make it easy to see if any updates are available for AdminStudio.



Figure 5: Support Tab Ribbon

Updated Deployment Type, Status, and Subnode Icons

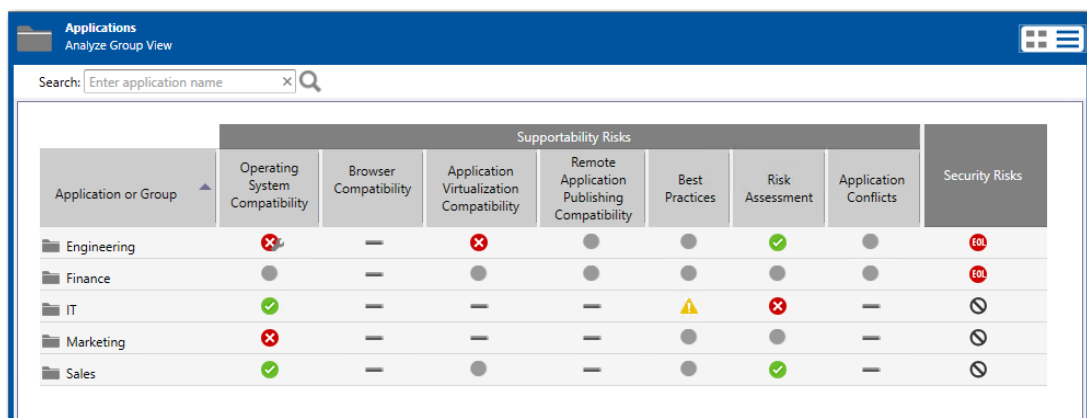
All deployment type, test status, and subnode icons have been updated to give Application Manager a refreshed look. For example, the following image displays a few deployment type icons that have been redesigned.



Figure 6: Redesigned Deployment Type Icons

New Pie Chart Display on Group View of Analyze Tab

In previous releases, the **Group View** of the **Analyze** tab (formerly **Test Center**) tab just listed summary icons of the test results for all applications in the group, similar to the following image.



The screenshot shows the 'Applications Analyze Group View' interface. It features a search bar at the top and a table with columns for 'Application or Group', 'Operating System Compatibility', 'Browser Compatibility', 'Application Virtualization Compatibility', 'Remote Application Publishing Compatibility', 'Best Practices', 'Risk Assessment', 'Application Conflicts', and 'Security Risks'. The table lists results for Engineering, Finance, IT, Marketing, and Sales departments, using icons like checkmarks, X's, and warning symbols to represent different test outcomes.

Application or Group	Supportability Risks							Security Risks
	Operating System Compatibility	Browser Compatibility	Application Virtualization Compatibility	Remote Application Publishing Compatibility	Best Practices	Risk Assessment	Application Conflicts	
Engineering	❌	—	❌	●	●	✅	●	❌
Finance	●	—	●	●	●	●	●	❌
IT	✅	—	—	—	⚠️	❌	—	⊘
Marketing	❌	—	—	—	●	●	—	⊘
Sales	✅	—	●	—	●	✅	—	⊘

Figure 7: Group View / List Format

In AdminStudio 2018, a new toggle button has been added to the top right side of this screen that enables you to switch to a graphical view of this same data.



Figure 8: Toggle Button

When you click the toggle button, you can switch between the standard list format and a new graphical, pie chart view.

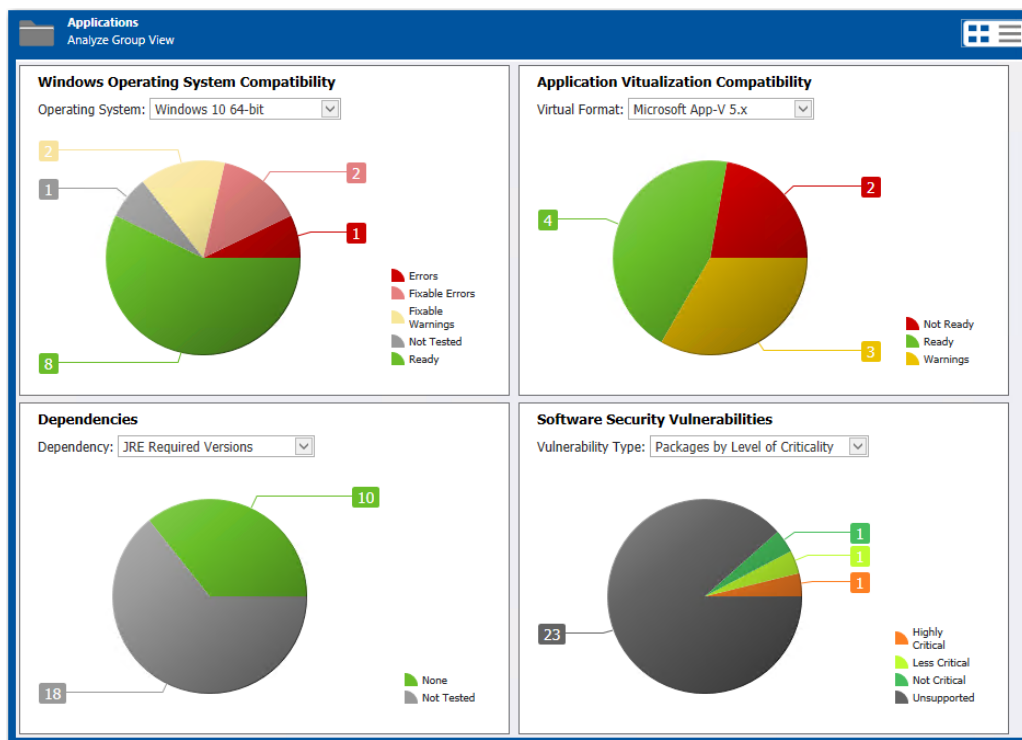


Figure 9: Group View / Chart Format

On the Chart view, you can make selections from the drop down lists to filter each pie chart by various criteria: operating systems, virtual format, dependencies, or vulnerability type.

New Supportability Risks and Security Risks Test Category Groups

On the **Analyze** tab, in order to separate standard compatibility, best practices, conflict test results from the new security vulnerability test results, all previously existing test categories have been grouped under the new **Supportability Risks** header. The new security vulnerability test results are displayed in the **Security Risks** column.

The screenshot shows the 'Applications Analyze Group View' interface. It features a search bar at the top and a table with columns for 'Application or Group', 'Operating System Compatibility', 'Browser Compatibility', 'Application Virtualization Compatibility', 'Remote Application Publishing Compatibility', 'Best Practices', 'Risk Assessment', 'Application Conflicts', and 'Security Risks'. The table lists results for Engineering, Finance, IT, Marketing, and Sales departments.

Application or Group	Operating System Compatibility	Browser Compatibility	Application Virtualization Compatibility	Remote Application Publishing Compatibility	Best Practices	Risk Assessment	Application Conflicts	Security Risks
Engineering	✗	—	✗	●	●	✓	●	✗
Finance	●	—	●	●	●	●	●	✗
IT	✓	—	—	—	⚠	✗	—	⊘
Marketing	✗	—	—	—	●	●	—	⊘
Sales	✓	—	●	—	●	✓	—	⊘

Figure 10: Supportability Risks and Security Risks Test Category Groups

Simplified Compatibility Test Results

In previous releases, when you viewed compatibility, best practices and risk assessment test results, a large list of numbers—identifying how many tests were executed, how many errors/warnings were generated, etc.—were displayed for each test. To view details of a particular test, you had to open a subtab, such as Operating System Compatibility, where test results for all of the tests in that category were listed.

The screenshot shows the 'Adobe Reader 8 Test Center Deployment Type View' interface. It displays a summary table with columns for 'Test Category', 'Executed', 'Errors', 'Warnings', 'Auto Fix Available', 'Issues Suppressed', and 'Overall Assessment'. The table lists results for 'Operating System Compatibility' across different Windows versions.

Test Category	Executed	Errors	Warnings	Auto Fix Available	Issues Suppressed	Overall Assessment
Operating System Compatibility	285	0	573	84	0	⚠
Windows 7 32-bit	42	0	94	14	0	⚠
Windows 7 64-bit	44	0	94	14	0	⚠
Windows Server 2008 R2	47	0	94	14	0	⚠
Windows 8 32-bit	49	0	97	14	0	⚠

Figure 11: Summary Deployment Type Test Results In Previous Releases

In AdminStudio 2018, a cleaner view of test results is displayed, with only a summary status icon displayed for each test. To see the detailed results for a specific test, you can now just click on that test to open the detailed view.

Test Category	Overall Assessment
Operating System Compatibility	
Windows 10 32-bit	
Windows 8.1 32-bit	
Windows 7 32-bit	
Windows 10 64-bit	
Windows 8.1 64-bit	
Windows 7 64-bit	
Windows Server 2016	
Windows Server 2012	
Windows Server 2008 R2	
Application Virtualization Compatibility	
Remote Application Publishing Compatibility	
Risk Assessment	
Windows Desktop Risk Assessment	
Best Practices	
Windows Installer Internal Consistency Evaluators	
Windows Installer Best Practices	

Figure 12: Summary Deployment Type Test Results In AdminStudio 2018

On the detailed test results view for an individual test, such as **Windows 10 64-bit** as shown in the following image, the test statistics are listed in color-coded boxes at the top of the view. To return to the Summary view, you just click on the back arrow to the left of the test name.

Windows 10 64-bit 53 Tests Executed 0 Errors 95 Warnings 0 Issues Suppressed 95 Total 14 Auto-Fix Available

Severity	Message	Count
Warning	2105 - Deferred Execution Custom Action Context: The Windows Installer database is scanned for the presence of any deferred execution custom actions that are not running in system context.	Count: 2
Warning	2120 - Standard User Changes (User Account Control): The Windows Installer database is scanned for the presence of .exe files (other than installers/updaters) that cause the User Account Control (UAC) prompt to be displayed.	Count: 5
Warning	2122 - Deprecated API Calls: The Windows Installer database is scanned for references to deprecated API calls. Scanned file extensions are: exe, dll, sys, src, drv, cpl, ocx.	Count: 49
Warning	2141 - Excluded .NET Framework Payload Files: The Windows Installer database is scanned for the presence of .NET assemblies compiled with Microsoft .NET Framework versions: 2.0, 3.0, 3.5.	Count: 3
Warning	2144 - Invalid Component Identifiers: The Windows Installer database is scanned for the presence of components with null, invalid or duplicated component identifiers.	Count: 1
Warning	2145 - Mixed Per-User and Per-Machine Data: The Windows Installer database is scanned for the presence of component containing mixed per-user and per-machine content.	Count: 6
Warning	2146 - Restart Manager Files In Use Dialog: The Windows Installer database is scanned for the absence of the Restart Manager Files In Use dialog and MSIRESTARTMANAGERCONTROL property value that disables Restart Manager.	Count: 1
Warning	2148 - Reboot Pending Launch Condition: The Windows Installer database is scanned for the absence of launch conditions that prevent the installation from continuing when a restart is pending.	Count: 1
Warning	2152 - Unsigned Executables: The Windows Installer database is scanned for the presence of unsigned executables. Scanned file extensions are: exe, dll, ocx, cab.	Count: 25

Figure 13: Detailed Deployment Type Test Results for an Individual Test

Consolidation of Functionality in Application Manager

In AdminStudio 2018, the focus has shifted to make Application Manager the central application in the entire AdminStudio toolkit. As demonstrated in the following diagram, all application readiness tasks can be either performed using Application Manager or launched from it.

AdminStudio® Application Manager

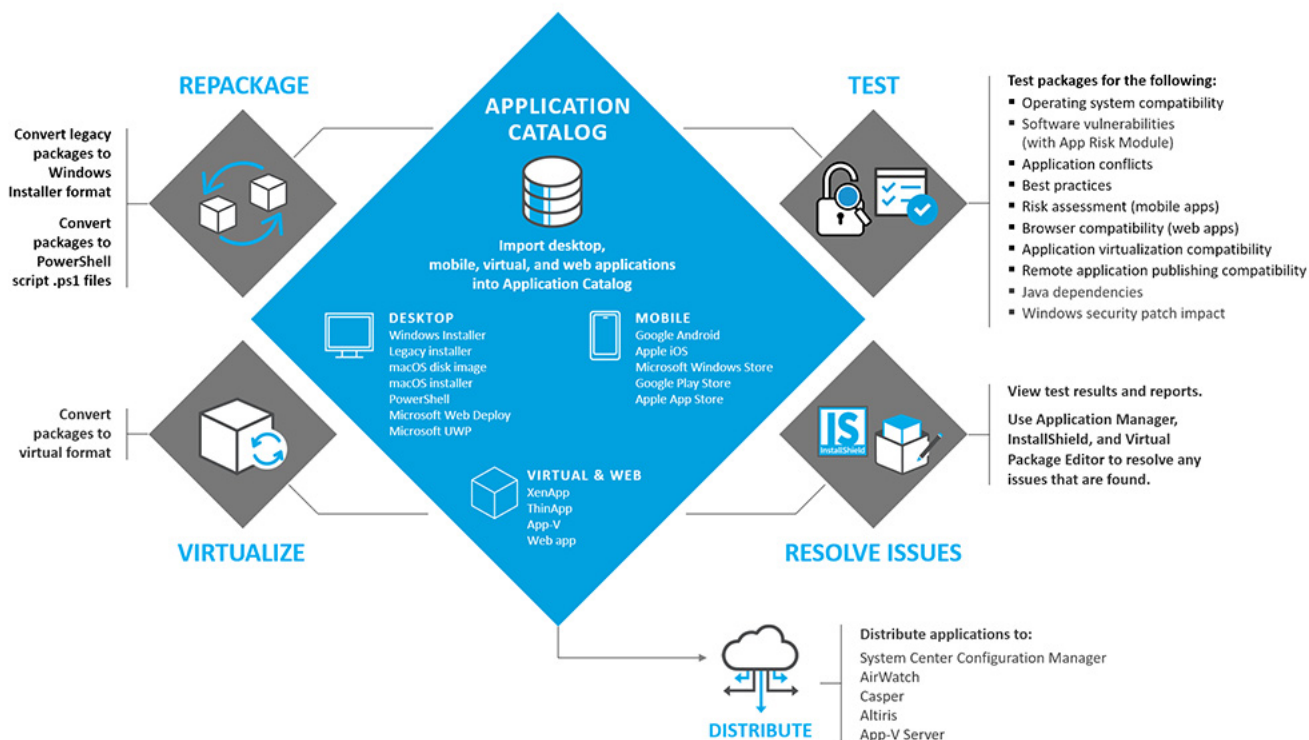


Figure 14: Application Manager Application Readiness Workflow

Ability to Launch AdminStudio Tools from Application Manager Home Tab

You can now launch other AdminStudio tools from the Application Manager **Home** tab by clicking the **AdminStudio Tools** button and making a selection from the menu.

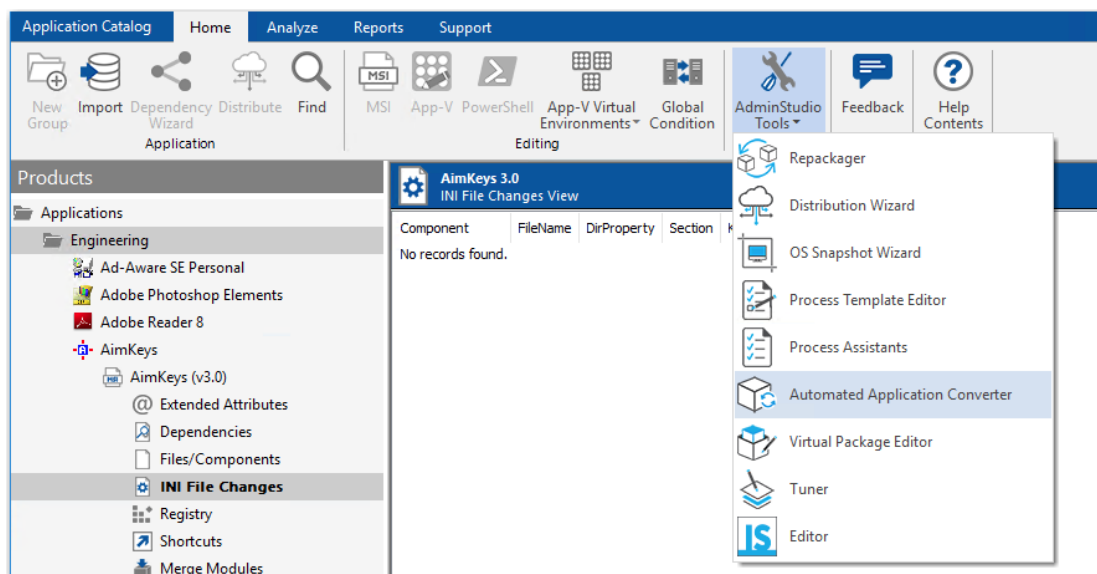


Figure 15: AdminStudio Tools Menu in Application Manager

New App Risk Module (ARM) to Identify Security Vulnerabilities

AdminStudio 2018 introduces the App Risk Module (ARM), which enables you to scan applications to identify those with security vulnerabilities. You will be able to view detailed reports of identified vulnerabilities for an application, and will be notified of any fixes or patches that are available.

App Risk Module is available as an optional subscription with AdminStudio 2018 Enterprise Edition.

App Risk Module is the right tool for guiding your IT folks to slash security risks by deploying reliable and secure apps. Flexera's deep knowledge of software vulnerabilities support the processes that make sure your employees have access to the apps they need when they need them. Safely.

With AdminStudio's App Risk Module, you will be able to:

- Reduce hidden threats and improve the security posture of your organization by scanning and assessing apps for vulnerabilities within your application portfolio.
- Make early vulnerability assessment and remediation integral to your Application Readiness process
- Stay on top of vulnerabilities with regularly scheduled, automatic scans against Flexera's list of more than 20,000 application titles
- Report on the criticality of the vulnerabilities to help prioritize remediation based on risk to your organization
- Keep up with the fixes and patches available for known vulnerabilities so you can implement them early to minimize risk.

Scanning Applications for Security Vulnerabilities

To scan applications for security vulnerabilities with App Risk Module, just open the **Analyze** tab, select an application or group containing Windows Installer (.msi) or installation packages (.exe) in the tree, and click **Check Vulnerabilities**.

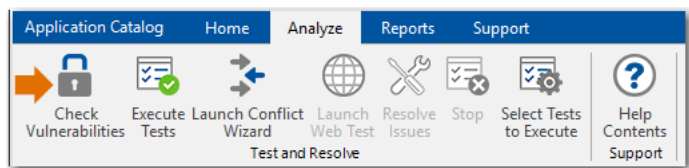






Figure 16: Check Vulnerabilities Button

Testing will begin and a message appears in the output window stating that the request is being processed in the background. You will be informed when the scan has been completed, and an icon will be displayed in the **Security Risks** column when that application is selected. One of the following status icons will be displayed:

Icon	Status	Description
	Insecure	A security vulnerability has been found for this application. When you click on this icon, an advisory report will be displayed, as described in Viewing Security Vulnerability Test Results
	Secure	The application is secure. A software vulnerability scan was run and no vulnerabilities were found.
	End-of-life	This application is no longer supported by its vendor. When you click on this icon, an advisory report will be displayed, as described in Viewing Security Vulnerability Test Results
	Unsupported	<p>There are multiple reasons why an application could be considered unsupported:</p> <ul style="list-style-type: none"> • Unsupported deployment type—This application is of an unsupported deployment type. AdminStudio only supports scanning Windows installer (.msi) and installation package (.exe) deployment types for software vulnerabilities. • Unable to extract Installation file—AdminStudio is unable to extract the .msi and/or .exe files required for analysis. To proceed you need to specify the location of this package's installation files. • Not found in App Risk Module database—There is no information on this application in the App Risk Module database. It is probable that this application has not yet reached our research team for vulnerability inspection. • Unknown—An error has occurred during testing.

Viewing Security Vulnerability Test Results

If security vulnerabilities have been found for an application, you can view test results in both a summary view and a detailed Advisory Report.

- [Summary View](#)
- [Advisory Report View](#)

Summary View

If a security vulnerability has been discovered for an application, when you select the deployment type in the tree and open the **Security Risks** tab, a list of related Advisory IDs are listed in a summary view.

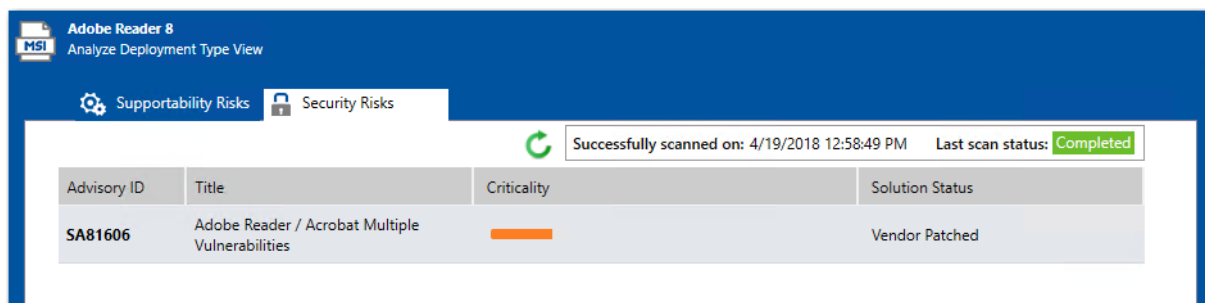

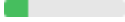


Figure 17: Security Risks Summary View

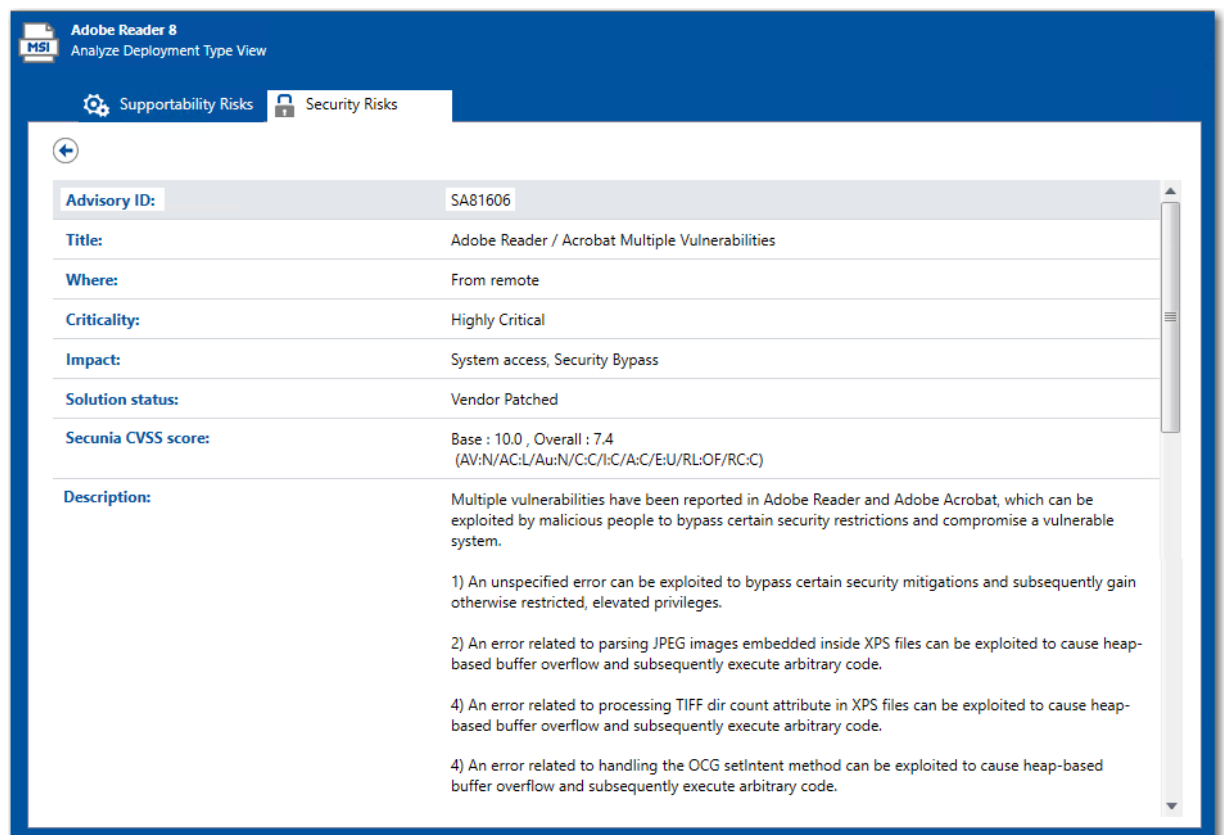
The icon in the **Criticality** column identifies the Advisory as one of the following degrees of criticality:

Icon	Criticality	Description
	Extremely critical	Remotely exploitable vulnerabilities that can lead to system compromise. Successful exploitation does not normally require any interaction and exploits are in the wild. These vulnerabilities can exist in services like FTP, HTTP, and SMTP or in certain client systems such as email programs or browsers.
	Highly critical	Remotely exploitable vulnerabilities that can lead to system compromise. Successful exploitation does not normally require any interaction, but there are no known exploits available at the time of disclosure. These vulnerabilities can exist in services like FTP, HTTP, and SMTP or in client systems, such as email programs or browsers.
	Moderately critical	Remotely exploitable Denial of Service vulnerabilities against services like FTP, HTTP, and SMTP, and for vulnerabilities that allow system compromises but require user interaction. This rating is also used for vulnerabilities allowing system compromise on LANs in services like SMB, RPC, NFS, LPD and similar services that are not intended for use over the Internet.

Icon	Criticality	Description
	Less critical	Cross-site scripting vulnerabilities and privilege escalation vulnerabilities. This rating is also used for vulnerabilities allowing exposure of sensitive data to local users.
	Not critical	Very limited privilege escalation vulnerabilities and locally exploitable Denial of Service vulnerabilities. This rating is also used for non-sensitive system information disclosure vulnerabilities (for example, remote disclosure of installation path of applications).

Advisory Report View

If you click on the ID in the **Advisory ID** column, a full **Advisory Report** is displayed.



The screenshot shows the 'Security Risks' tab in the Adobe Reader 8 interface. The advisory report for ID SA81606 is displayed, detailing the title, where the risk originates, its criticality, impact, solution status, and a detailed description of the vulnerabilities.

Advisory ID:	SA81606
Title:	Adobe Reader / Acrobat Multiple Vulnerabilities
Where:	From remote
Criticality:	Highly Critical
Impact:	System access, Security Bypass
Solution status:	Vendor Patched
Secunia CVSS score:	Base : 10.0 , Overall : 7.4 (AV:N/AC:L/Au:N/C:C/I:C/A:C/E:U/RL:OF/RC:C)
Description:	<p>Multiple vulnerabilities have been reported in Adobe Reader and Adobe Acrobat, which can be exploited by malicious people to bypass certain security restrictions and compromise a vulnerable system.</p> <p>1) An unspecified error can be exploited to bypass certain security mitigations and subsequently gain otherwise restricted, elevated privileges.</p> <p>2) An error related to parsing JPEG images embedded inside XPS files can be exploited to cause heap-based buffer overflow and subsequently execute arbitrary code.</p> <p>4) An error related to processing TIFF dir count attribute in XPS files can be exploited to cause heap-based buffer overflow and subsequently execute arbitrary code.</p> <p>4) An error related to handling the OCG setIntent method can be exploited to cause heap-based buffer overflow and subsequently execute arbitrary code.</p>

Figure 18: Advisory Report

The **Advisory Report** provides detailed information on the Advisory ID that has been detected for this application, and contains the following information.

Property	Description
Advisory ID	Identifies the security advisory.

Property	Description
Title	Title of the security advisory.
Where	<p>Identifies the Where (attack vector) value as one of the following:</p> <ul style="list-style-type: none"> ● Local System—Describes vulnerabilities where the attack vector requires that the attacker is a local user on the system. ● Local Network—Describes vulnerabilities where the attack vector requires that an attacker is situated on the same network as a vulnerable system (not necessarily a LAN). This category covers vulnerabilities in certain services (for example, DHCP, RPC, administrative services, and so on), which should not be accessible from the Internet, but only from a local network and optionally a restricted set of external systems. ● Remote—Describes vulnerabilities where the attack vector does not require access to the system nor a local network. This category covers services, which are acceptable to expose to the Internet (for example, HTTP, HTTPS, SMTP) as well as client applications used on the Internet and certain vulnerabilities, where it is reasonable to assume that a security conscious user can be tricked into performing certain actions.
Criticality	<p>Lists the advisory's criticality rating value as one of the following:</p> <ul style="list-style-type: none"> ● Extremely critical—Remotely exploitable vulnerabilities that can lead to system compromise. Successful exploitation does not normally require any interaction and exploits are in the wild. These vulnerabilities can exist in services like FTP, HTTP, and SMTP or in certain client systems such as email programs or browsers. ● Highly critical—Remotely exploitable vulnerabilities that can lead to system compromise. Successful exploitation does not normally require any interaction, but there are no known exploits available at the time of disclosure. These vulnerabilities can exist in services like FTP, HTTP, and SMTP or in client systems, such as email programs or browsers. ● Moderately critical—Remotely exploitable Denial of Service vulnerabilities against services like FTP, HTTP, and SMTP, and for vulnerabilities that allow system compromises but require user interaction. This rating is also used for vulnerabilities allowing system compromise on LANs in services like SMB, RPC, NFS, LPD and similar services that are not intended for use over the Internet. ● Less critical—Cross-site scripting vulnerabilities and privilege escalation vulnerabilities. This rating is also used for vulnerabilities allowing exposure of sensitive data to local users. ● Not critical—Very limited privilege escalation vulnerabilities and locally exploitable Denial of Service vulnerabilities. This rating is also used for non-sensitive system information disclosure vulnerabilities (for example, remote disclosure of installation path of applications).

Property	Description
Impact	<p>Categorizes the impact of this advisory as one of the following:</p> <ul style="list-style-type: none"> ● Brute Force—Used in cases where an application or an algorithm allows an attacker to guess passwords in an easy manner. ● Cross-Site Scripting—These vulnerabilities allow a third party to manipulate the content or behavior of a web application in a user's browser, without compromising the underlying system. Cross-Site Scripting vulnerabilities are often used against specific users of a website to steal their credentials or to conduct spoofing attacks. ● DoS (Denial of Service)—This includes vulnerabilities ranging from excessive resource consumption (for example, causing a system to use a lot of memory) to crashing an application or an entire system. ● Exposure of Sensitive Information—Vulnerabilities where documents or credentials are leaked or can be revealed either locally or remotely. ● Exposure of System Information—Vulnerabilities where excessive information about the system (for example, version numbers, running services, installation paths, and similar) are exposed and can be revealed from remote and, in some cases, locally. ● Hijacking—Covers vulnerabilities where a user session or a communication channel can be taken over by other users or remote attackers. ● Manipulation of Data—This includes vulnerabilities where a user or a remote attacker can manipulate local data on a system, but not necessarily be able to gain escalated privileges or system access. The most frequent type of vulnerabilities with this impact are SQL-injection vulnerabilities, where a malicious user or person can manipulate SQL queries. ● Privilege Escalation—Covers vulnerabilities where a user is able to conduct certain tasks with the privileges of other users or administrative users. This typically includes cases where a local user on a client or server system can gain access to the administrator or root account, thus taking full control of the system. ● Security Bypass—Covers vulnerabilities or security issues where malicious users or people can bypass certain security mechanisms of the application. The actual impact varies significantly depending on the design and purpose of the affected application. ● Spoofing—Covers various vulnerabilities where it is possible for malicious users or people to impersonate other users or systems. ● System Access—Covers vulnerabilities where malicious people are able to gain system access and execute arbitrary code with the privileges of a local user. ● Unknown—Covers various weaknesses, security issues, and vulnerabilities not covered by the other impact types, or where the impact is not known due to insufficient information from vendors and researchers.

Property	Description
Solution status	Identifies how this advisory can be resolved, such as Vendor Patched .
Secunia CVSS score	<p>The Common Vulnerability Scoring System (CVSS) consists of three groups:</p> <ul style="list-style-type: none"> ● Base—Represents the intrinsic qualities of a vulnerability. ● Temporal—Reflects the characteristics of a vulnerability that changes over time ● Environmental—Represents the characteristics of a vulnerability that are unique to any user's environment. <p>Each group produces a numeric score ranging from 0 to 10, and a vector: a compressed textual representation that reflects the values used to derive the score.</p> <p>For details on interpreting a CVSS vector, see the Common Vulnerability Scoring System v3.0: Specification Document.</p> <p>Secunia Advisories include a Secunia derived CVSS score and vector, as well as a link to an implementation of the NIST CVSS calculator so that a user can adjust temporal and environmental metrics for advisories that match your Watch Lists.</p> <p>The National Vulnerability Database (NVD) CVSS score/vector for each relevant CVE contained in an Advisory is also shown, and is similarly linked to the NIST CVSS calculator.</p>
Description	Description of the reported vulnerabilities found in this application, along with a list of the other products and versions that these vulnerabilities are found in.
Solution	Lists solutions to resolve these vulnerabilities, such as updating the application.
Provided and/or discovered by	Identifies the entities that reported these vulnerabilities, such as the vendor, research labs, individual testers, etc.
Release date	Release date of the advisory.
Last update	Date the advisory was last updated.
References	<p>Lists of references other related advisories on various websites such as the Zero Day Initiative website, such as:</p> <p>https://www.zerodayinitiative.com/advisories/ZDI-18-209/</p>
Changelog	List of changes made to this advisory, including the date.
Affected operating system and software	List of applications and operating systems affected by this advisory.
CVE references	ID numbers of related advisories from U.S. Department of Commerce's National Institute of Standards and Technology (NIST) National Vulnerability Database .

Configuring App Risk Module Options

When AdminStudio is installed and the App Risk Module is activated, an Access Token is automatically populated in the **Access Token** field of the **App Risk Module (ARM)** tab of the Application Manager **Options** dialog box.

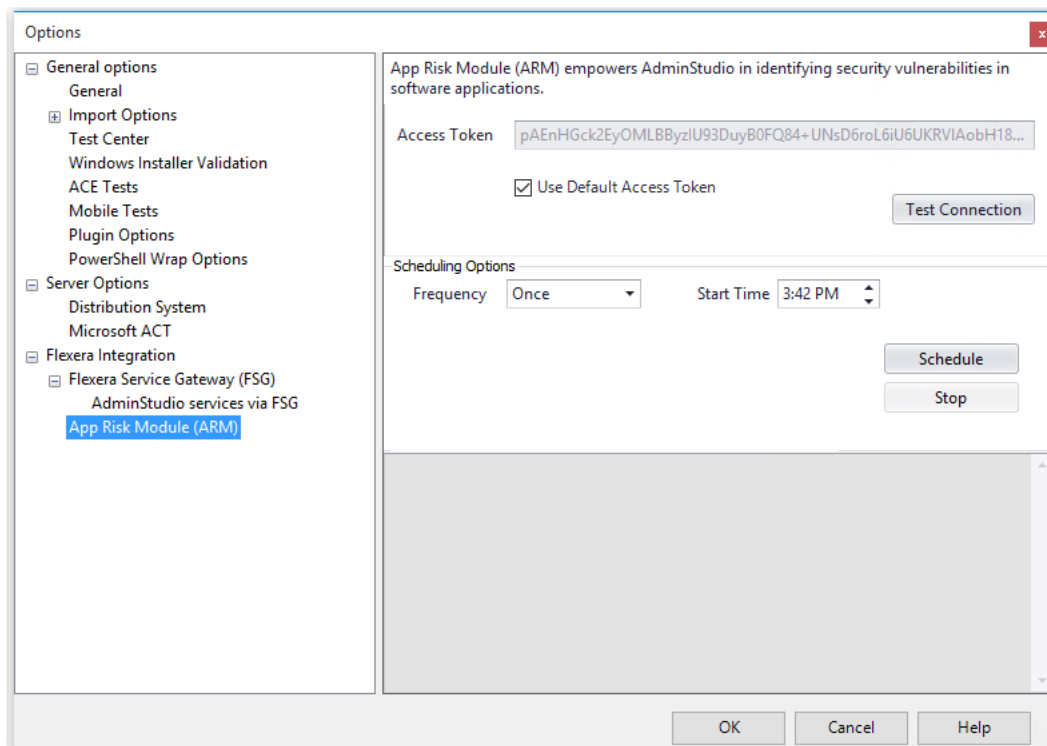


Figure 19: App Risk Module (ARM) Options on Application Manager Options Dialog Box

On the **App Risk Module (ARM)** tab, you can choose to enter a different access token, check your connection to the App Risk Module database, and schedule the frequency to perform security vulnerability scans.

The **App Risk Module (ARM)** tab of the Application Manager **Options** dialog box includes the following properties.

Property	Description
Access Token	Initially lists the Access Token provided when App Risk Module was installed. <div data-bbox="641 1549 675 1593" data-label="Image"></div> <p>Note • If you have also purchased Flexera Security Vulnerability Manager, you can clear the selection of the Use Default Access Token check box and enter a token specific to your instance of Security Vulnerability Manager.</p>
Test Connection	Click to test your connection to the App Risk Module database.

Property	Description
Scheduling Options	<p>Using the Frequency and Start Time fields, you can schedule the frequency and time of day when an automated security vulnerability scan will be performed on the applications in your Application Catalog.</p> <p>To modify the default schedule, select a Frequency (Once, Daily, Weekly, or Monthly) and a Start Time, and then click Schedule.</p> <p>Click Stop to stop an update in progress.</p>

New Software Security Vulnerability Reports

With the App Risk Module feature, you can also view new Software Security Vulnerability Reports on the **Reports** tab that summarize the security vulnerability status of applications in your Application Catalog.

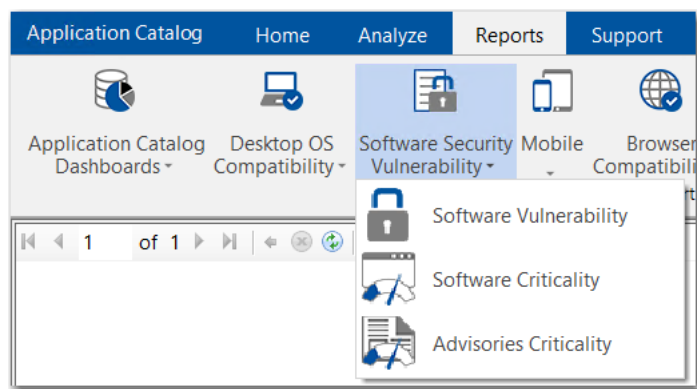


Figure 20: Security Vulnerability Reports

The following reports are available:

- Software Vulnerability**—Displays the vulnerability status of the applications in the Application Catalog, such as Secured, Insecure, End-of-Life, etc. Click on a segment of the pie to view a list of applications in that category. Click the **All Applications** button to see a list of the vulnerability and criticality status of all tested applications in the Application Catalog.
- Software Criticality**—Displays the level of criticality of applications in the Application Catalog, such as Highly Critical, Less Critical, etc. Click on a segment of the pie to view a list of applications in that category. Click the **All Applications** button to see a list of the vulnerability and criticality status of all tested applications in the Application Catalog.
- Advisories Criticality**—Displays the level of criticality of discovered advisories, such as Highly Critical, Less Critical, etc. Click on a segment of the pie to view a list of applications in that category.

New App Risk Module PowerShell Platform API Commands

As part of the App Risk Module feature, the following new PowerShell Platform API commands were added to AdminStudio:

- **Invoke-ASScanPackage**—Use to initiate a security vulnerability scan of a package.
- **Get-ASVulnerability**—Use to obtain the software vulnerabilities of a given package after a scan has been performed.

Security Vulnerability Warning During Distribution

When you are using Distribution Wizard to distribute an application to a distribution system, such as System Center Configuration Manager, if a security scan has already been performed for that application and a vulnerability has been found, a warning message will be displayed informing you of the vulnerability, and you will be prompted to confirm whether you want to proceed with distribution.

Legacy Add-On Packs Now Included with Professional and Enterprise Editions

Starting with AdminStudio 2018, AdminStudio Professional and Enterprise Editions now include all of the features that were previously only available in the Virtualization, Application Compatibility, and Mac and Mobile add-on packs.

Starting with AdminStudio 2018, all virtualization, application compatibility, and Apple / macOS features are now available in Professional and Enterprise Editions at no extra cost. For a detailed breakdown of the features in the various AdminStudio editions, see [Editions](#).



Note • AdminStudio 2018's new App Risk Module feature is available when you purchase AdminStudio Enterprise Edition with the App Risk Module (ARM) add-on module. For more information, see [New App Risk Module \(ARM\) to Identify Security Vulnerabilities](#)

InstallShield 2018



Note • For more information, see the [InstallShield 2018 Release Notes](#).

AdminStudio 2018 includes InstallShield 2018, which includes the following new features and enhancements:

- [Specify Uninstallation Order of Packages in a Suite Project](#)
- [Method to Run a Suite Installation with Minimum UI](#)
- [Conditionally Set the Visibility of a Feature at Run Time](#)
- [Perform Recursive or Non-Recursive IIS Registration](#)
- [Set Forms Authentication on Web Applications](#)

- New Option to Control Whether to Load User Profile for an Application Pool Entity
- Add Kill Process and PowerShell Custom Actions to a Transform Project
- Save QuickPatch Projects in XML Format
- Localize Product Name Property in Suite Projects
- Include the Value of a Property in a Product Configuration's Setup File Name
- New MSBuild Parameters to Set Summary Information Stream Comments and to Set Package File Name
- Specify Line Break and Tab Characters in Text File Changes
- Remove or Hide the Suite Loading Screen
- Setting to Always Create Debug Logs for Suite Installers
- New Out-of-the-Box Dialog to Set the IIS Certificate File for SSL Certificate at Runtime
- Specify Absolute or Relative Path When Creating New Child Elements in an XML File
- Setting the Default Keyboard Focus for Dialog Box Controls in Suite Projects
- PowerShell Script Editor in Basic MSI Projects
- New Option to Open Existing Transform File in InstallShield Transform Wizard
- Additional Prerequisites Included

Specify Uninstallation Order of Packages in a Suite Project



Project • This information applies to the following project types:

- *Advanced UI*
- *Suite/Advanced UI*

In InstallShield 2018, you can now specify the uninstallation order of packages in a suite project using the new **Uninstallation Order** property on the **Setup.exe** tab of the **Releases** view.

You can use this setting to specify the uninstallation order of the packages in a suite project by selecting one of the following options:

- **Same as Packages Order**—Uninstall the packages in the same order that packages were installed (as defined in the project).
- **Reverse of Packages Order**—Uninstall the packages in the reverse order that packages were installed (as defined in the project).

New UninstallOrder Method in Automation Interface

You can use the `UninstallOrder` method in the automation interface to set the **Uninstallation Order** property. Specify one of the following values:

- `euoForward(0)`—Uninstall the packages in the same order that packages were installed (as defined in the project).
- `euoReverse(1)`—Uninstall the packages in the reverse order that packages were installed (as defined in the project).

Method to Run a Suite Installation with Minimum UI



Project • This information applies to the following project types:

- *Advanced UI*
- *Suite/Advanced UI*

In InstallShield 2018, you can now use a new command line parameter to run a suite installation in minimum UI mode, only displaying a progress panel.

To run a suite installation in minimum UI mode, use the `/passive` parameter in the command line:

```
Setup.exe /passive
```

To uninstall using a minimum UI mode, use the following command:

```
Setup.exe /passive /remove
```

Conditionally Set the Visibility of a Feature at Run Time



Project • This information applies to the following project types:

- *Advanced UI*
- *Suite/Advanced UI*

In previous releases, you could set the **Visible** property of a feature in an Advanced UI or Suite/Advanced UI installation to **Yes** or **No** specify whether the feature should be visible on the **InstallationFeatures** wizard page of the installer.

In InstallShield 2018, you can conditionally show or hide a feature based upon a property at run time using the new **Condition** option under the **Visible** property on the **Features** view of the Installation Designer.

You can use the **Condition** setting to specify one or more conditions that the Advanced UI or Suite/Advanced UI installation should use to evaluate whether the feature should be visible for installation by default on the **InstallationFeatures** wizard page.

For example, if you want a particular feature to be visible by default on target systems that have a particular version of Windows, you can create a condition that specifies that version of Windows.

**Task****To conditionally display a feature in an Advanced UI or Suite/Advanced UI installation:**

1. On the **Features** view, click in the **Condition** row under the **Visible** property. A green plus sign, the **New Condition** button, appears at the end of the row.
2. Click the **New Condition** button. A new row is added under the **Condition** row.
3. Click the down arrow next to the **New Condition** button and select the appropriate option—**All**, **Any**, or **None
- 4. Then in the same row, click the **New Condition** button, and select the appropriate option to continue building the conditional statement.**

If one or more conditional statements are configured, the **Condition** property lists **(Condition)**. If none are configured, the **Condition** property lists **(Empty)**.

For more information, see [Building Conditional Statements in Advanced UI and Suite/Advanced UI Projects](#).

New Methods in Automation Interface to Support Conditional Visibility

The following new methods have been added to the automation interface to enable you to conditionally set the visibility of a feature at run time:

Method	Syntax
AddVisibleCondition	AddVisibleCondition() As ISWiSuiteCondition
DeleteVisibleCondition	DeleteVisibleCondition()
VisibleCondition	Read-only object property

Perform Recursive or Non-Recursive IIS Registration



Project • This information applies to the following project types:

- Basic MSI
- DIM
- InstallScript
- InstallScript MSI
- Merge Module

A new option named **ASP.NET Registration** has been added to the **Application** settings on the **Internet Information Services** view that enables you to perform recursive or non-recursive ASP.NET registration. Using this feature enables you to install both ASP.NET applications and ASP.NET Core applications to the same website.

To set the ASP.NET application registration option with Internet Information Services (IIS), set the **ASP.NET Registration** property to one of the following options:

- **Recursive**—Updates script maps and application-pool assignments for the specified application and for all sub-applications.
- **Non Recursive**—Updates script maps and application-pool assignments for only the specific application. No sub-applications are changed.

Set Forms Authentication on Web Applications



Project • This information applies to the following project types:

- *Basic MSI*
- *InstallScript MSI*

InstallShield 2018 includes a new option to set forms authentication on web applications. This new option, **Forms Authentication**, is displayed under the **Authenticated Access** section of the **Internet Information Services** view for a website.

Set the **Forms Authentication** option to **Yes** to enable forms authentication. ASP.NET forms-based authentication works well for sites or applications on public Web servers that receive many requests. This authentication mode lets you manage client registration and authentication at the application level, instead of relying on the authentication mechanisms provided by the operating system.



Important • Forms authentication sends the user name and password to the Web server as plain text. You should use Secure Sockets Layer (SSL) encryption for the Log On page and for all other pages in your application except the Home page.

New Option to Control Whether to Load User Profile for an Application Pool Entity



Project • This information applies to the following project types:

- *Basic MSI*
- *InstallScript MSI*

In InstallShield 2018, there is a new **Application Pool** settings property on the **Internet Information Services** view, named **Load User Profile**, that controls whether to load the user profile for an application pool entity.

Set the **Load User Profile** property to one of the following options:

- **Yes**—IIS will load the user profile for the application pool.
- **No**—IIS will not load the user profile for the application pool. This is the same behavior that occurred with IIS 6.0.

Add Kill Process and PowerShell Custom Actions to a Transform Project



Project • This information applies to the following project types:

- Basic MSI
- InstallScript MSI
- Transform

In previous releases, you were unable to add a Kill Process or PowerShell custom action to a Transform project. In InstallShield 2018, you can now add a **New Kill Process** or **New PowerShell** custom action to a Transform project in the **Custom Actions and Sequences** view.

Save QuickPatch Projects in XML Format



Project • This information applies to the following project types:

- Basic MSI
- QuickPatch

In InstallShield 2018, you can now save a QuickPatch project in XML format, and you can also create a QuickPatch project from projects saved in XML format. In previous releases, QuickPatch projects could only be saved in binary format.

Localize Product Name Property in Suite Projects



Project • This information applies to the following project types:

- Advanced UI
- Suite/Advanced UI

In InstallShield 2018, suite projects now support localizing the **Product Name** property.

To localize the Product Name property in a suite project, perform the following steps.



Task

To localize a property in a suite project:

1. Open a suite project and go to the **User Interface > String Editor** view.
2. Create a new string that contains the localized text for each of the languages supported by your suite project, such as ID_STRING2.
3. Open the **Installation Information > General Information** view.

4. Click the browse button next to the **Product Name** field to open the **Select String** dialog box.
5. Select the name of the string that you created that contains the localized text.

Include the Value of a Property in a Product Configuration's Setup File Name



Project • This information applies to the following project types:

- *Basic MSI*
- *InstallScript MSI*

In InstallShield 2018, you can now include the value of a property from the Property Table in product release configuration setup and package file names.

For example, you could enter any of the following properties in the **Setup File Name** or **MSI Package File Name** field on the **General** tab of the **Releases > Product Configuration** view:

```
setup[ProductVersion]
setup[CustomVersion]
setup[ProductCode]
setup[ProductCode][ProductVersion]
```

If you entered **setup[ProductVersion]** in the **Setup File Name** field, it would result in a setup named setup14.10.1234.exe, for example.

New MSBuild Parameters to Set Summary Information Stream Comments and to Set Package File Name

In InstallShield 2018, new MSBuild parameters were added to enable you to set add comments to an installer and to set the package file name of an installer.

- [New Parameter to Set Summary Information Stream Comments](#)
- [New Parameter to Set Package File Name](#)

New Parameter to Set Summary Information Stream Comments



Project • This information applies to the following project types:

- *Basic MSI*
- *InstallScript*
- *InstallScript MSI*
- *Merge Module*

You can add comments to an installer in the **Summary Information Stream Comments** field on the **General Information** view.

In InstallShield 2018, you also have the option of entering comments at build time. A new parameter has been added to the MSBuild.exe task, named **SummaryInfoComments**, to set the **Summary Information Stream** comments at build time, such as including the build number, as shown in the following example:

```
MSBuild.exe c:\installers\Setup.sln /Property:SummaryInfoComments="Insert Comments Here"
```

The comments that are added using the SummaryInfoComments property can be viewed on the **Properties** dialog box of the built installer.

New Parameter to Set Package File Name



Project • This information applies to the following project types:

- Basic MSI
- InstallScript MSI

You can specify the package file name of an installer in the **MSI Package File Name** field on the **General** tab for a **Product Configuration** field on the **Releases** view.

In InstallShield 2018, you also have the option of setting the package file name at build time. A new parameter has been added to the MSBuild.exe task, named **MSIPackageFileName**, to set the package file name of the built installer at build time, as shown in the following example:

```
MSBuild.exe c:\installers\Setup.isproj /Property:MSIPackageFileName="MySetup"
```

When entering the value for the MSIPackageFileName parameter, you need to enter the file name—without the period or the file extension—that InstallShield should use for the .msi file.

Specify Line Break and Tab Characters in Text File Changes



Project • This information applies to the following project types:

- Basic MSI
- DIM
- InstallScript MSI
- Merge Module
- MSI Database
- Transform

In your installer, you can configure search-and-replace behavior for content in text files that you want to modify at run time on the target system. To do this, you open the **System Configuration > Text File Changes** view and add a text **Change Set** that identifies the text files that will be searched at runtime, and also specifies the text to search for (**Find What**) and the text to replace it with (**Replace With**).

In InstallShield 2018, when adding a text Change Set, you can now enter escape sequence characters in the **Replace What** field to specify a line break or a tab.

Character	Escape Sequence
Line break	\r\n
Tab	\t



Note • For the Windows operating system, you must enter both `\r\n` to insert a line break.

When the search-and-replace action is taken at runtime, a line break will be inserted where `\r\n` was entered in the **Replace With** field, and a tab will be entered where `\t` was entered.

For these characters to be recognized as escape sequences, you also have to set the **Parse Escape Sequences** option to **Yes**.

Remove or Hide the Suite Loading Screen



Project • This information applies to the following project types:

- Advanced UI
- Suite/Advanced UI

In InstallShield 2018, you now have the ability to control whether or not the Suite Loading Screen is displayed during installation.

To control whether this screen is displayed, a new property has been added to the **Setup.exe** tab of the **Releases** view named **Show Suite Loading Screen**. If you want to hide the Suite Loading Screen for your Advanced UI or Suite/Advanced UI setup launcher, set this property to **No**.

New ShowSuiteLoadingScreen Method in Automation Interface

You can use the ShowSuiteLoadingScreen method in the automation interface to set the **Show Suite Loading Screen** setting on the **Setup.exe** tab of the **Releases** view. The default value is True.

Setting to Always Create Debug Logs for Suite Installers



Project • This information applies to the following project types:

- Advanced UI
- Suite/Advanced UI

In InstallShield 2018, you can now select an option to turn on logging for a suite project without passing debuglog through the command line.

A new option, **Always Create Debug Log**, has been added to the **Setup.exe** tab of the **Releases** view for Advanced UI and Suite/Advanced UI projects.

If you want to always create debug logs for your Advanced UI or Suite/Advanced UI setup launcher, set the **Always Create Debug Log** option to **Yes**.

New CreateDebugLog Method in Automation Interface

You can use the CreateDebugLog method in the automation interface to set the **Always Create Debug Log** setting on the **Setup.exe** tab in the **Releases** view. The default value is `False`.

New Out-of-the-Box Dialog to Set the IIS Certificate File for SSL Certificate at Runtime



Project • This information applies to the following project types:

- *Basic MSI*

InstallShield 2018 includes a new out-of-the-box dialog (IISBrowseSSLCertificate) for the installer that enables the end user to browse to a IIS certificate file that they provide for the SSL Certificate and enter a password at installation runtime.

To add a **Configure SSL for IIS** dialog to your installer, perform the following steps:



Task

To add a “Configure SSL for IIS” dialog to your installer:

1. In the **View List** under **Server Configuration**, click **Internet Information Services**.
2. Right-click the **Web Sites** explorer and click **Add Web Site**. InstallShield adds a new Web site.
3. Select the new web site and locate the **SSL Certificate** and **SSL Certificate Password** properties under **Security > Secure Communication**.
4. Set the **SSL Certificate** and **SSL Certificate Password** properties to the following values:

Property	Value
SSL Certificate	[IS_IIS_WEBCERTPATH]
SSL Certificate Password	[IS_IIS_WEBCERTPASSWORD]

5. Open the **User Interface > Dialogs** view and add the **IISBrowseSSLCertificate** dialog to the dialog sequences.

The property name for the SSL Certificate and password configured by the user is required to update in the **IISBrowseSSLCertificate** dialog for the **Edit** boxes (**IISWebCertPassword** and **IISWebCertPath**) and the push button (**BrowseCertificate**) events.

Specify Absolute or Relative Path When Creating New Child Elements in an XML File



Project • This information applies to the following project types:

- Basic MSI
- DIM
- InstallScript
- InstallScript MSI
- Merge Module
- MSI Database
- Transform

In previous releases, when using the **System Configuration > XML File Changes** view to add a new child element to an XML file that has the same name as a child element in an existing parent element, the XML file change would fail.

The path of a node in an XML document can be either absolute or relative. Absolute paths start at the root. When adding a new child element to an XML file that has the same name as a child element in an existing parent element, it is necessary to use the absolute path.

In InstallShield 2018, a new setting has been added to the **XML File Changes** view named **Use Absolute XPath** to enable you to specify that you want to use an absolute path when creating child elements.

The behavior used when creating a child element depends upon the **Use Absolute XPath** option setting:

- **Selected**—If this option is selected, Absolute XPath will be used when adding a child element.
- **Not selected**—If this option is not selected, Generic XPath will be used when adding a child element. By default, the **Use Absolute XPath** option is not selected.

Setting the Default Keyboard Focus for Dialog Box Controls in Suite Projects



Project • This information applies to the following project types:

- Advanced UI
- Suite/Advanced UI

In InstallShield 2018, when defining the wizard pages for a Suite project, you can now specify which control on a wizard page will have the default keyboard focus.

On the **Wizard Interface** view, there is a new property under **Appearance** named **Default Focus**, which lists all of the controls defined on that wizard page. Select a control to set the default keyboard focus to that control.

PowerShell Script Editor in Basic MSI Projects



Project • This information applies to the following project types:

- *Basic MSI*
- *InstallScript MSI*

In InstallShield 2018, the PowerShell script editor is available on the **Custom Actions and Sequences > Custom Actions** view for Basic MSI projects, on the new **Script** tab. In previous releases, the PowerShell Script Editor was only available for Suite/Advanced UI projects.

New Option to Open Existing Transform File in InstallShield Transform Wizard



Project • This information applies to the following project types:

- *Transform*

In InstallShield 2018, you can now open an existing transform file in the InstallShield Transform Wizard (as if it were being opened in the Transform Wizard for the first time), where you will be prompted to select a base MSI package for the transform file. This enables you to use the same generic transform file for multiple MSI packages.

To open an existing transform file in the InstallShield Transform Wizard, right-click on the transform file in Windows Explorer and select **Open in InstallShield Transform Wizard** from the context menu.

Additional Prerequisites Included

InstallShield 2018 includes the following additional prerequisites:

- [Visual C++ 2017 x86 and x64 Prerequisites](#)
- [Microsoft SQL Server 2014 SP1 and SP2 Prerequisites](#)
- [Microsoft .NET Framework 4.7 Prerequisite](#)

Visual C++ 2017 x86 and x64 Prerequisites

Because Microsoft Visual Studio 2017 has been released, InstallShield now includes the prerequisites for Visual C++ 2017 x86 and x64.

Microsoft SQL Server 2014 SP1 and SP2 Prerequisites

Because Microsoft SQL Server 2014 has had 2 Service Packs released, InstallShield now includes the prerequisites for both Microsoft SQL Server 2014 SP1 and SP2.

Microsoft .NET Framework 4.7 Prerequisite

InstallShield now includes a prerequisite for Microsoft .NET Framework 4.7.

Important Information

This section lists important information regarding AdminStudio 2018:

- [Removal of Support for Symantec Workspace Virtual Packages](#)
- [Removal of Support for Testing for Internet Explorer 9 and 10](#)

Removal of Support for Symantec Workspace Virtual Packages

In AdminStudio 2018, converting packages to Symantec Workspace virtual packages is no longer supported. Also, you can no longer import Symantec Workspace virtual packages into the Application Catalog.

Removal of Support for Testing for Internet Explorer 9 and 10

Application Manager no longer includes browser compatibility tests for Internet Explorer 9 or 10.



Note • *Even though browser compatibility testing for Internet Explorer 9 and 10 has been removed in AdminStudio 2018, if you are using an Application Catalog that was upgraded from a previous version of AdminStudio, test results for Internet Explorer 9 and 10 will still be displayed.*

Editions

AdminStudio 2018 R2 is available in Standard, Professional, and Enterprise Editions. With Enterprise Edition, you can also purchase an additional App Risk Module (ARM) add-on to perform security vulnerability testing.

- [Feature Breakdown by Edition](#)
- [App Risk Module \(ARM\) Add-On](#)

Feature Breakdown by Edition

The following table lists the tools and features available in each of AdminStudio's three editions: Standard, Professional, and Enterprise.

Edition	Feature Type	Tools	Functionality
STANDARD	General	Repackager	Repackage applications into Windows Installer format Perform basic ISO tagging, including creation of tag files
		Package Distribution Wizard	Prepare packages for distribution
		InstallShield 2018 (Professional Edition)	Customize Windows Installer packages by either directly editing them or by creating transforms
		Tuner	Customize Windows Installer packages by creating transforms
		Application Isolation Wizard	Resolve component versioning conflicts
	Application Virtualization	Automated Application Converter (Single Application Version)	Convert a package to a virtual application in the following formats: <ul style="list-style-type: none"> • Microsoft App-V (4.x and 5.1) • Citrix XenApp • VMware ThinApp (4.x and 5.x) Convert one package at a time
		Conversion Wizard (Single Application Version)	
		Virtual Package Editor	Edit App-V packages
		Microsoft App-V Assistant ThinApp Assistant Citrix Assistant	Create a customized virtual package from an InstallShield project

Edition	Feature Type	Tools	Functionality
PROFESSIONAL	Same as Standard Edition , plus:		
	General	Application Manager / Home Tab	<p>Manage applications in an Application Manager database</p> <p>Manage a package's System Center Configuration Manager (2012 or Current Branch) and Symantec Altiris Client Management Suite deployment data</p> <p>View an application's System Center Configuration Manager (2012 or Current Branch) deployment status</p> <p>Perform advanced ISO tag file creation, editing, and storage</p>
		Application Manager / Analyze Tab	<p>Perform tests in the following categories:</p> <ul style="list-style-type: none"> Windows Installer Internal Consistency Evaluators Windows Installer Best Practices Application Conflicts <p>Test and fix one package at a time</p>
		Distribution Wizard	<p>Publish applications to System Center Configuration Manager (2012 or Current Branch) and Symantec Altiris Management Server.</p>
		OS Snapshot Wizard	<p>Capture basic operating system configuration in an OS Snapshot, which can be imported into the Application Manager to check for potential OS conflicts</p>
		QualityMonitor	<p>Perform Windows Installer testing, including testing in a locked down environment</p>
		Automated Application Converter	<p>Automatically repackage a legacy package (.exe) into a Windows Installer package (.msi)</p>
		(Single Application Version)	<p>Repackage one package at a time</p>
		Conversion Wizard	
		(Single Application Version)	
		Test on Virtual Machine Wizard	<p>Automatically launch a specified virtual machine and install a selected Windows Installer (.msi), App-V package (.appv), or installation executable (.exe) package for testing.</p>

Edition	Feature Type	Tools	Functionality
PROFESSIONAL (Continued)	Application Virtualization	Enhancements to Application Manager / Home Tab	<p>Import virtual packages into Application Manager</p> <p>View virtual package data in Application Manager</p> <p>Manage System Center Configuration Manager (2012 or Current Branch) deployment data for App-V 4.x and 5.1 packages</p> <p>Manage Citrix XenApp Server deployment data for Citrix XenApp profiles and App-V 4.x packages</p> <p>Manage Symantec Altiris Client Management Suite deployment data for Symantec Workspace and VMware ThinApp packages</p> <p>Manage App-V Server deployment data for App-V 4.x and 5.1 packages</p>
		Enhancements to Application Manager / Analyze Tab	<p>Test packages for compatibility to be virtualized to App-V, ThinApp, and XenApp formats</p> <p>Test App-V packages for best practices</p> <p>Test App-V packages for conflicts with other packages</p>
		Enhancements to Distribution Wizard	<p>Publish applications containing App-V 4.x and 5.1 packages to Microsoft App-V Server</p> <p>Publish applications containing App-V packages to System Center Configuration Manager (2012 or Current Branch) and Citrix XenApp Server</p> <p>Publish applications containing Citrix XenApp profiles and App-V 4.x packages to Citrix XenApp Server</p> <p>Publish applications containing Symantec Workspace and VMware ThinApp packages to Symantec Altiris Client Management Suite Server</p>

Edition	Feature Type	Tools	Functionality
PROFESSIONAL (Continued)	Application Compatibility Testing	Enhancements to Application Manager / Analyze Tab	<p>Test packages for compatibility with the following operating systems:</p> <ul style="list-style-type: none"> • Windows 7 (32-bit and 64-bit) • Windows 8 (32-bit and 64-bit) • Windows 10 (32-bit and 64-bit) • Windows Server 2008 R2 • Windows Server 2012 and 2012 R2 • Windows Server 2016 <p>On the Operating System Compatibility tab of the Analyze Deployment Type View, you can see detailed data for only the last package tested; for all other packages in the Application Manager, this tab is blank (even if the package has been previously tested)</p> <p>Ability to display Microsoft Application Compatibility Toolkit (ACT) database test results on ACT Summary tab of the Analyze Deployment Type View</p>
	Mobile App and macOS Support	Enhancements to Application Manager / Home Tab	<ul style="list-style-type: none"> • Import of the following macOS desktop applications into the Application Manager: <ul style="list-style-type: none"> • Apple installer package (.pkg file) • Apple disk image (.dmg file) • Mac App Store app (public store link) • Import of the following mobile app formats into the Application Manager: <ul style="list-style-type: none"> • Apple iOS mobile apps (local and public store link) • Google Android mobile apps (local and public store link) • Microsoft Windows Store mobile apps (local and public store link) • Ability to import iOS Enterprise Policy Configuration files, view their settings, and determine the policy compatibility of iOS mobile apps. • Ability to view iOS and Android mobile app reporting on feature use, device compatibility, and OS compatibility.

Edition	Feature Type	Tools	Functionality
PROFESSIONAL (Continued)	Mobile App and macOS Support (Continued)	Enhancements to Application Manager / Home Tab (Continued)	<ul style="list-style-type: none"> ● Ability to customize Apple Installer Package PKG installer settings ● Ability to view deployment data for Windows Store mobile apps, including detection methods and framework customizations ● Ability to manage AirWatch Server deployment data for both Apple iOS and Google Android mobile apps (local and public store link) ● Ability to view and modify Casper deployment settings for macOS desktop applications
		Enhancements to Application Manager / Analyze Tab	<ul style="list-style-type: none"> ● Test Apple iOS mobile apps for best practices ● Test Apple iOS, Microsoft Windows, and Google Android mobile apps for risk assessment ● Test Apple iOS, Microsoft Windows, and Google Android mobile apps for operating system compatibility ● Test macOS desktop applications (.pkg, .dmg, and Mac App Store apps) for operating system compatibility and best practices
		Enhancements to Distribution Wizard	<p>Ability to publish applications containing the following mobile app formats to System Center Configuration Manager (2012 R2 or Current Branch) and AirWatch Server:</p> <ul style="list-style-type: none"> ● Apple iOS mobile apps (local and public store link) ● Google Android mobile apps (local and public store link) <p>Ability to publish applications containing the following mobile app format to System Center Configuration Manager (2012 R2 or Current Branch):</p> <ul style="list-style-type: none"> ● Windows Store (local and public store link) ● Microsoft UWP app packages (.appx) <p>Ability to publish applications containing the following package formats to JAMF Casper Suite:</p> <ul style="list-style-type: none"> ● Apple installer package (.pkg file) ● Apple disk image (.dmg file) ● Mac App Store app (public store link)

Edition	Feature Type	Tools	Functionality
ENTERPRISE	Same as Professional Edition , plus:		
	General	InstallShield 2018 (Premier Edition instead of Professional Edition)	Advanced customization of Windows Installer packages by either directly editing them or by creating transforms
		Application Manager / Reports Tab	Advanced reports including detailed summary and dashboard reports on Analyze test results, package data, and deployment information
		Platform API	Use to integrate your existing .NET applications or scripting environments like Microsoft PowerShell with AdminStudio
		Software Repository	Secure storage system for AdminStudio package data, including version management
		Reports (Web Tool)	Generate reports on packages stored in the Application Manager, including reports using custom SQL queries
		Security Console (Web Tool)	Manage AdminStudio user accounts and directory services Manage AdminStudio roles and permissions
		Automated Application Converter (Multiple Application Version) Conversion Wizard (Multiple Application Version)	Automatically repackage legacy packages (.exe) into Windows Installer packages (.msi) Ability to perform automated repackaging of multiple packages at a time
	Application Virtualization	Automated Application Converter (Multiple Application Version) Conversion Wizard (Multiple Application Version)	Ability to perform automated conversion of multiple packages at a time
		Enhancements to Application Manager / Reports	Includes the Application Virtualization Compatibility Dashboard report The Application Readiness Dashboard includes an Application Virtualization Compatibility summary chart and App-V Best Practices and App-V Conflicts test results summary charts.

Edition	Feature Type	Tools	Functionality
ENTERPRISE (Continued)	Application Compatibility Testing	Enhancements to Application Manager / Analyze Tab	<p>Ability to test and fix multiple packages or groups of packages simultaneously</p> <p>Ability to view package-level test details for Operating System Compatibility and Browser Compatibility tests for all packages in the Application Manager, not just the last one tested</p> <p>Import of web applications and web deploy packages into the Application Manager</p> <p>Test web applications for compatibility with the following browsers:</p> <ul style="list-style-type: none">● Internet Explorer 11● Microsoft Edge <p>Test web deploy packages for compatibility with the following platforms:</p> <ul style="list-style-type: none">● Windows Server 2012 R2● Windows Server 2016● Microsoft Azure Application Services <p>Test web deploy packages for best practices.</p> <p>Test web deploy packages for browser compatibility.</p>
		Enhancements to Application Manager / Reports	Display of Microsoft ACT database test results on the Reports tab
		Enhancements to Platform API	Ability to use the Test-ASPackage and Resolve-ASPackage Platform API commands to perform batch package testing and issue resolution.

App Risk Module (ARM) Add-On

If you purchase the App Risk Module (ARM) add-on, AdminStudio can scan applications to identify those with security vulnerabilities. You will be able to view detailed reports of identified vulnerabilities for an application, and will be notified of any fixes or patches that are available. For more information, see [New App Risk Module \(ARM\) to Identify Security Vulnerabilities](#).

System Requirements

This section lists the requirements for the AdminStudio machine, Application Catalog database server, Web server, and virtual machines.

- [Compatibility Summary](#)
- [AdminStudio Machine](#)
- [Distribution Systems](#)
- [Application Catalog Database Server](#)
- [AdminStudio Enterprise Server / Workflow Manager Server](#)
- [Software Repository](#)
- [Automated Application Converter](#)

Compatibility Summary

AdminStudio 2018 R2 supports the following versions of the listed software.

Category	Item	Supported Versions
Operating System for: <ul style="list-style-type: none"> • AdminStudio • Standalone Repackager • Standalone Tuner 	Microsoft Windows	<ul style="list-style-type: none"> • Windows 7 • Windows 8 and 8.1 • Windows 10 • Windows Server 2008 R2 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016
AdminStudio Web Server Operating System (AdminStudio Enterprise Server, AdminStudio Inventory and Rationalization, Workflow Manager)	Microsoft Windows Server	<ul style="list-style-type: none"> • Windows Server 2008 R2 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016
Application Catalog Database	Microsoft SQL Server	<ul style="list-style-type: none"> • 2008 R2 • 2012 • 2016 • 2017

Category	Item	Supported Versions
Flexera Software Product Integration	FlexNet Manager Platform / FlexNet Manager Suite (On Premises)	9.2 SP1 or later
	FlexNet Manager Suite (Cloud)	2014 or later
	App Portal	7.5.3 or later
	Workflow Manager	2015 or later
	Flexera Service Gateway	1.0 or later
Virtual Machines for Virtualization	VMware Workstation	6.5 or later
	VMware ESXi	VMware ESX/ESXi Server, Version 3.5 Update 3 or later
	VMware vSphere	5.5
	Microsoft Hyper-V Server	2008 R2 or later
Virtual Formats	App-V	App-V 4.5 through 5.1
	VMware ThinApp	4.x and 5x
Microsoft App-V Sequencer	App-V Sequencer	5.1
Desktop Distribution (Applications)	System Center Configuration Manager	2007, 2012 R2, 2012 R2 SP1, Current Branch
	Microsoft App-V Server	5.1
	Symantec Altiris Client Management Suite	7.5
	Citrix XenApp Server	6.5





Category	Item	Supported Versions
Desktop Distribution (Packages)	Novell ZENworks Configuration Management	10 and 11
	LANDESK Management Suite	9
	System Center Configuration Manager	2007, 2012 R2, 2012 R2 SP1, Current Branch
	Altiris Notification Server	6.5
	Marimba NCP	4.7.2
Mobile Distribution	AirWatch Server	6.5
	Microsoft App-V Server	5.1
	Microsoft System Center Configuration Manager	2012 R2, 2012 R2 SP1
Desktop Operating Systems Supported for compatibility testing	Windows	<ul style="list-style-type: none"> 7 (32-bit and 64-bit) 8.1 (32-bit and 64-bit) 10 (32-bit and 64-bit)
	Windows Server	<ul style="list-style-type: none"> 2008 R2 2012 2016
	Mac OS	<ul style="list-style-type: none"> 10.11 (El Capitan) 10.12 (Sierra)

Category	Item	Supported Versions
Mobile Operating Systems Supported for compatibility testing	Apple iOS	<ul style="list-style-type: none"> • 6 (32-bit) • 7 (32-bit and 64-bit) • 8 (32-bit and 64-bit) • 9 (32-bit and 64-bit) • 10 (32-bit and 64-bit)
	Google Android	<ul style="list-style-type: none"> • 4.1 Jelly Bean • 4.2 Jelly Bean • 4.3 Jelly Bean • 4.4 KitKat • 5.0 Lollipop • 6.0 Marshmallow • 7.0 Nougat
	Windows Phone	<ul style="list-style-type: none"> • 8.1 • 10
Internet Browsers Supported for browser compatibility testing	Microsoft Internet Explorer	11
	Microsoft Edge	Current version
Internet Browsers For viewing AdminStudio Enterprise Server, AdminStudio Inventory and Rationalization, and Workflow Manager	Mozilla Firefox	Firefox for Windows 25.0 or later
	Google Chrome	Chrome for Windows 33.0 or later
	Microsoft Internet Explorer	Microsoft Internet Explorer 9.0 or later
	Microsoft Edge	Current version
	Apple Safari	Safari for Mac OS X and iOS

Category	Item	Supported Versions
Mobile Devices	Apple iOS Devices	<ul style="list-style-type: none"> ● iPad WiFi ● iPad 2 3G and iPad 2 WiFi ● iPad Third Gen and iPad Third Gen 4G ● iPad Fourth Gen and iPad Fourth Gen 4G ● iPad Fifth Gen and iPad Fifth Gen 4G ● iPad Sixth Gen and iPad Sixth Gen LTE ● iPad Pro 9.7, 9.7 LTE ● iPad Pro 12.9, 12.9 LTE ● iPad Mini ● iPad Mini 3 and iPad Mini 3LTE ● iPad Mini 4G ● iPad Mini 4 and 4LTE ● iPad Mini Retina and iPad Mini Retina 4G ● iPhone 4S ● iPhone 5, iPhone 5c, and iPhone 5s ● iPhone 6 and iPhone 6 Plus ● iPhone 6s and iPhone 6s Plus ● iPhone SE
	Google Android Devices	<ul style="list-style-type: none"> ● Samsung Galaxy Grand 2 ● Google Nexus 5, 5X, 6, 6P, 9 ● Samsung Galaxy Note 2, 3, 4, 5, 6, 7 ● Samsung Galaxy Note Pro ● Samsung Galaxy S4, S5, S7 ● Samsung Galaxy Tab S2, 3
	Windows Phone Devices	<ul style="list-style-type: none"> ● Microsoft Lumia535 ● Microsoft Lumia 930 ● Microsoft SurfacePro 3
API	PowerShell	4.x
Application Compatibility	Microsoft Application Compatibility Toolkit (ACT)	5.6

AdminStudio Machine

The following table lists the recommended system configuration for a machine running AdminStudio.


Item	Description
Processor	32-bit or 64-bit processor at 2 GHz or greater  Note • All of the AdminStudio tools run on 64-bit Windows operating systems. To repackage 64-bit applications or create 64-bit App-V packages, install AdminStudio on a 64-bit Windows operating system.
RAM	4 GB
Hard Disk	4 GB of free space
Display	Designed for XGA at 1024 x 768 resolution or higher  Note • For the best user experience, a monitor resolution of 1920 x 1080 or greater is recommended.
MSXML	MSXML 6.0  Note • MSXML is installed by the AdminStudio installer.
Operating Systems	<ul style="list-style-type: none"> • Windows 7 • Windows 8 and Windows 8.1 • Windows 10 • Windows Server 2008 R2 • Windows Server 2012, Windows Server 2012 R2, Windows Server 2016  Note • Support for Windows Vista was removed due to a modification made by Microsoft. For more information, see the following articles: <ul style="list-style-type: none"> • An ADO application does not run on down-level operating systems after you recompile it on a computer that is running Windows 7 SP 1 or Windows Server 2008 R2 SP 1 or that has KB983246 installed [Microsoft Article 2517589] • A Better Solution for the Windows 7 SP1 ADO GUID Changes
Browser	Microsoft Internet Explorer 7.0 or later
Privileges	Administrative privileges on the system

Distribution Systems

AdminStudio supports distribution of both applications and packages.

Application Distribution

AdminStudio supports the following distribution systems for the distribution of applications.

Distribution System	Support Version(s)
System Center Configuration Manager	2007, 2012 R2, 2012 R2 SP1, Current Branch
Symantec Altiris Client Management Suite	7.5
JAMF Casper Suite Server	9.9
Citrix XenApp Server	6.5
AirWatch Server	6.5 [Mobile applications only]
Microsoft App-V Server	5.1
	 <p>Note • In order for you to distribute packages to a Microsoft App-V Server, the WinRM service must be running, and the App-V Server must be in the list of trusted hosts. Both of these can be accomplished from PowerShell by running the following command:</p> <pre>set-item wsman:\localhost\Client\TrustedHosts -value <Machine Name></pre>

Package Distribution

AdminStudio supports the following distribution systems for the distribution of packages using the Legacy Distribution Wizard.

Distribution System	Supported Versions
Altiris Notification Server	Version 6.5
LANDESK Management Suite	Version 9
Novell ZENworks Configuration Management	Versions 10 and 11
Microsoft System Center Configuration Manager	2007, 2012 R2, 2012 R2 SP1, Current Branch

Application Catalog Database Server

The following table lists the recommended system configuration for a database server to store AdminStudio Application Catalog databases.



Note • While minimum requirements are listed below, the recommended system configuration for a database server is dependent upon the number of users and the number of packages that will be imported into the Application Catalog database.

Item	Description
Processor	32-bit or 64-bit processor at 2 GHz or greater
RAM	4 GB or greater (8 GB preferred)
Hard Disk Space	80 GB or greater
Operating System	Windows Server 2008 R2 or later (Windows Server 2012 or later preferred)
Database Software	<p>SQL Server 2008 R2 or later databases, including SQL Server 2012, SQL Server 2014, SQL Server 2016, and SQL Server 2017.</p> <ul style="list-style-type: none"> Dictionary sort order—SQL Server must be installed with case-insensitive dictionary sort order 52 on Code Page 1252 for non-Unicode data. For more information, use the <code>sp_helpsort</code> T-SQL command, which returns the following: Latin1-General, case-insensitive, accent-sensitive, kanatype-insensitive, width-insensitive for Unicode Data, SQL Server Sort Order 52 on Code Page 1252 for non-Unicode data Collation setting—SQL_Latin1_General_CP1_CI_AS is the required collation setting for AdminStudio database server. It is the only supported collation.



Note • Before attempting to connect to an existing Microsoft SQL Server, open SQL Server Configuration Manager and make sure that the following three protocols are enabled:



- Shared Memory
- Named Pipes
- TCP/IP

AdminStudio Enterprise Server / Workflow Manager Server

The following table lists the system requirements for the Web server that hosts the Workflow Manager Data Web service and the actual Workflow Manager Web site and/or AdminStudio Enterprise Server.



Note • While minimum requirements are listed below, the recommended system configuration for this web server is dependent upon the number of users.

Item	Description
Processor	32-bit or 64-bit processor at 2 GHz or greater  Note • AdminStudio Enterprise Server / Workflow Manager runs in 32-bit mode on a 64-bit OS.
RAM	4 GB or greater (8 GB preferred)
Hard Disk Space	100 GB or greater
Operating System	Windows Server 2008 R2 or later / English base language (Windows Server 2012 or later preferred)
IIS	IIS 7.0 or later
.NET	.NET Framework 4.0
MSXML	MSXML 6.0  Note • MSXML is installed by the AdminStudio Enterprise Server / Workflow Manager installer.

Automated Application Converter

This section lists the requirements for the virtual machines used by Automated Application Converter to perform repackaging. Also, the software requirements for specific virtual technologies are listed.

- [Virtual Machine Requirements](#)
- [Virtual Technology Requirements](#)

Virtual Machine Requirements



Edition • *Automated Application Converter is included with AdminStudio Application Virtualization.*

Automated Application Converter performs automated repackaging on virtual machines. This section lists the virtual machine platform and virtual machine image system requirements.

- [Supported Virtual Machine Platforms](#)
- [VMware Requirements](#)
- [Microsoft Hyper-V Server Requirements](#)
- [Virtual Machine Image Requirements](#)

Supported Virtual Machine Platforms

The Automated Application Converter supports automated repackaging on virtual machines from the following platforms:

- VMware ESX/ESXi Server, Version 3.5 Update 3 or later
- VMware Workstation 6.5 or later
- VMware vSphere 5.5
- Microsoft Hyper-V Server 2008 R2 or later

VMware Requirements

As described above, Automated Application Converter supports automated repackaging on VMware ESX/ESXi Server and VMware Workstation.

- [VMware VIX API Requirement](#)
- [VMware ESX/ESXi Server Permission Requirements](#)
- [vSphere 5.5 Account Requirements](#)

VMware VIX API Requirement

In order for Automated Application Converter to perform automated repackaging, it needs to communicate with the virtualization technology that you are using. If you are using VMware virtualization technology (VMware ESX or ESXi Server or a local VMware Workstation), the VMware VIX API needs to be installed on the same machine as the Automated Application Converter. You can do this by either installing VMware Workstation on that machine or by downloading and installing the VMware VIX API from the following location:

<http://www.vmware.com/support/developer/vix-api>



Note • When using VMware Workstation, it is recommended that you install VMware Workstation on the same machine as Automated Application Converter so that Automated Application Converter will use the version of the VIX API that was designed for that specific version of VMware Workstation. Although it is likely that newer versions of the VIX API will also work, it seems that the best approach is for Automated Application Converter to use the version of the VIX API that was bundled with your version of VMware Workstation.

VMware ESX/ESXi Server Permission Requirements

If you plan to use a VMware ESX/ESXi Server in conjunction with Automated Application Converter, make sure that the account that you use to log in to this server has the permissions/roles needed to automatically open a VM using VMware VIX API. The account needs to either have an administrator role assigned or, at least, have the following three roles assigned:

- All Privileges/Virtual Machine/State/Create Snapshot
- All Privileges/Virtual Machine/State/Delete Snapshot
- All Privileges/Virtual Machine/Interaction/Console Interaction

If the login account does not have these permissions/roles, Automated Application Converter will be unable to automatically boot up a virtual machine on that server.

vSphere 5.5 Account Requirements

In order to make Automated Application Converter (AAC) work with VMware virtual machines residing under vSphere 5.5, there are certain minimum permissions required for the vSphere user account. To assign these permissions to a vSphere user account, perform the following steps:

**Task**

To configure a vSphere 5.5 account to be used with Automated Application Converter:

1. In vSphere 5.5, open the **Assign Permissions** dialog box and assign a user the **Virtual machine power user (sample)** role, which consists of the following permissions:

Category	Permission	
Datastore	<ul style="list-style-type: none"> ● Browse datastore 	
Global	<ul style="list-style-type: none"> ● Cancel task 	
Scheduled task	<ul style="list-style-type: none"> ● Create task ● Remove task ● Modify task ● Run task 	
Virtual machine > Configuration	<ul style="list-style-type: none"> ● Add existing disk ● Modify device settings ● Add new disk ● Remove disk ● Add or remove device ● Rename ● Advanced ● Reset guest information ● Change CPU count ● Settings ● Change resource ● Upgrade virtual machine compatibility ● Disk lease ● Memory 	
Virtual machine > Interaction	<ul style="list-style-type: none"> ● Answer question ● Power off ● Configure CD media ● Power on ● Configure floppy media ● Reset ● Console interaction ● Suspend ● Device connection ● VMware Tools install ● Guest operating system management by VIX API 	
Virtual machine > Snapshot management	<ul style="list-style-type: none"> ● Create snapshot ● Rename snapshot ● Remove snapshot ● Revert to snapshot 	

2. Also give the user account read-only access to the rest of the server.

Microsoft Hyper-V Server Requirements

As described above, Automated Application Converter supports automated repackaging on Microsoft Hyper-V Server. When preparing a Hyper-V Server for use with Automated Application Converter, make sure that the following conditions are met:

- **Configuration tools**—Verify that the Hyper-V configuration tools are installed on the Hyper-V server machine. These tools can be installed using the Microsoft Hyper-V Management Console.
- **Connection**—Verify that you can successfully connect to the Hyper-V Server from the machine where AdminStudio Automated Application Converter is installed.
- **Permissions**—Make sure that the Hyper-V Server user has the following permissions to perform operations on the Hyper-V machines:
 - Permission to create/restore/delete VM snapshots
 - Permission to start and stop virtual machines
 - Permission to access console sessions
- **Configuration settings**—Connecting to a WMI namespace on a remote computer running Windows Vista or Windows Server 2008 may require changes to configuration settings. Check the following configuration settings on the AdminStudio machine as well as on the Hyper-V Server machine:
 - Windows Firewall Settings
 - User Account Control (UAC) Settings
 - DCOM Settings
 - Common Information Model Object Manager (CIMOM) Settings

For detailed information, see [Connecting to WMI Remotely](#) at:

[http://msdn.microsoft.com/en-us/library/aa822854\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/aa822854(VS.85).aspx)

Virtual Machine Image Requirements

Automated Application Converter uses virtual machines to perform automated repackaging. These virtual machines have the following requirements:

Virtual Machine System Requirements

When creating a virtual machine image that will be hosted on one of the virtual machine platforms listed above, the recommended minimum requirements should meet those required by the applications you are trying to repackage. Since you repackage on the target deployment platform, the virtual machine image should closely resemble the target deployment environment.

Preparing Your Virtual Machines for Use With the Automated Application Converter

You need to prepare each virtual machine that you are going to use with the Automated Application Converter to perform automated repackaging by running the Virtual Machine Preparation setup and by creating a snapshot. For instructions, see [Preparing Your Virtual Machines for Use With the Automated Application Converter](#).

Virtual Technology Requirements

In order to convert to some virtual formats, there are some software requirements:

Virtual Format	Requirement
App-V 5.1	<ul style="list-style-type: none"> ● Conversion—To convert a package to App-V 5.1 format using Automated Application Converter's App-V 5.x with Sequencer method, the Microsoft Application Virtualization 5.1 Sequencer must be installed on the virtual machine where the conversion will take place. ● Upgrade—To upgrade an imported App-V 4.x package to App-V 5.1 format directly from Application Manager using the App-V Upgrade Wizard, the Microsoft Application Virtualization 5.1 Sequencer must be installed on the same machine as AdminStudio. ● Testing—To test an App-V package using Automated Application Converter, the Microsoft Application Virtualization 5.1 Client must be installed on the same machine as AdminStudio.
VMware ThinApp	To convert a package to VMware ThinApp format, VMware ThinApp must be installed on the same machine as AdminStudio, and all license agreements must have been accepted.

Downloading AdminStudio Installers

You can download the installers for AdminStudio, AdminStudio Service Packs, Standalone Repackager, Standalone Quality Monitor, and the FlexNet Licensing Server from the **Flexera Software Product and License Center**:

<https://flexerasoftware.flexnetoperations.com>

For information on using the Flexera Software Product and License Center, see the **Download and License Overview for AdminStudio**:

<http://www.flexerasoftware.com/downloads/instructions/productlicensing/en/adminstudio.htm>

AdminStudio 2018 R2 Evaluation Restrictions

When you run AdminStudio in trial/evaluation mode, all of the features in the AdminStudio Enterprise Edition tools are fully available, with the following restrictions:

- **Can create only one Application Catalog**—You are permitted to create only one Application Catalog, and it must be named AdminStudio Evaluation Catalog.
- **Ten package import limit**—Only 10 total packages (of one or more deployment types) can be imported into the Application Catalog.
- **Package deletion not permitted**—After you import a package into the Application Catalog, you are not permitted to delete it.
- **AdminStudio Platform API support is disabled**—All platform support is disabled.

Resolved Issues

This section lists the customer issues that were resolved in the following versions of AdminStudio:

- [AdminStudio 2018 R2](#)
- [AdminStudio 2018](#)

AdminStudio 2018 R2

The following table lists the customer issues that were resolved in AdminStudio 2018 R2.

Issue	Description
IOJ-1825352	With the Software Repository enabled, if you import an MSI package and right click the package and choose Open file location , an error will be generated stating that the path is inaccessible. Application Manager is looking in the incorrect folder for the package.
IOJ-1842009	When logging into an SQL Server Application Catalog database using server authentication, Application Manager crashes if the login password contains an equal sign (=) character, even though clicking the Test button returns “Test connection succeeded!”.
IOJ-1849682	Sample code for PowerShell.exe.config copied from AdminStudio User Guide PDF generates errors due to formatting issue.
IOJ-1873175	Request to add a Package Version column to operating system compatibility reports.
IOJ-1873482	The msxml4.dll file, distributed with AdminStudio 2016 SP2, needs to be updated to a more current version (6.0 or the latest), as it is end of life and could pose a security risk.
IOJ-1876278	The Get-ASProperty Platform API generates errors upon invocation and adds them to the \$Error object in PowerShell. The Get-ASProperty cmdlet should not generate errors unless it actually fails.

AdminStudio 2018

The following table lists the customer issues that were resolved in AdminStudio 2018.

Issue	Description
IOA-000084704 IOJ-1719381 IOJ-1781861	After a package has been imported into the Application Catalog, user is requesting the ability to update the package path location from within the Application Manager user interface.
IOJ-1722082	When an EXE package is imported into the Application Catalog, AdminStudio does not automatically create a detection method for that package. Then later, when you try to publish that application to SCCM 2012, the publication fails because the package(s) in the application have no detection methods.
IOJ-1729105	Request to add a new, or enhance an existing PowerShell command (such as Set-ASProperty) to allow customer to add requirements for their deployments using the PowerShell interface.
IOJ-1802627	When a package is reimported after fixing errors, AdminStudio generates a software tag for that package even though the option to generate software tags is disabled.
IOJ-1831806	If you have deployed an application that has custom requirements defined, and later try to delete the distribution system connection from the Options dialog box, you will receive an unhandled exception.
IOJ-1831940	Request that when distributing to SCCM, the Distribution Wizard should create a folder named after the application, not a folder named after the GUID.
IOJ-1834039	If you have a database from a previous version of AdminStudio (2015 or earlier), and you used the Package Auto Import feature, the database will not be properly upgraded. This will cause an unhandled exception when accessing the Package Auto Import options in Application Manager.
IOJ-1835906	When attempting to distribute to an AirWatch Server, distribution is unsuccessful because the URL was hard coded to a specific instance instead of being able to distribute to the customer's AirWatch instance URL.
IOJ-1847809	Visual C++ 2012 Update 4 x64 is included as a prerequisite of the Standalone Repackager install but is not included in the actual package. This causes the install to fail on machines without Internet access.

Known Issues

For a complete list of known issues that pertain to the AdminStudio 2018 R2 release, see the AdminStudio Support Knowledge Base article at:

https://flexeracommunity.force.com/customer/articles/en_US/INFO/AdminStudio-2018-Known-Issues

Legal Information

Copyright Notice

Copyright © 2018 Flexera

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 <https://www.flexera.com/producer/company/about/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.