# AdminStudio 2018

Evaluation Guide

# Legal Information

| | |
|---|---|
| **Book Name:** | AdminStudio 2018 Evaluation Guide |
| **Part Number:** | ADS-2018-EG00 |
| **Product Release Date:** | 26 April 2018 |

## Copyright Notice

## 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.

# Contents

# AdminStudio 2018 Evaluation Guide

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

You can use this Evaluation Guide to quickly learn how to use AdminStudio to prepare Windows Installer, virtual applications, web applications, macOS desktop applications, and mobile applications for deployment. This Evaluation Guide is organized into the following sections:

**Table 1** • AdminStudio 2018 Evaluation Guide

| Section | Description |
|---|---|
| **Getting Started** | Explains what is included in this Evaluation Guide and how to get started. |
| **New Features in AdminStudio 2018** | Provides an overview of the new features in AdminStudio 2018. |
| **Setting Up AdminStudio Infrastructure** | Explains how to perform the one-time set-up tasks that you need to complete prior to using AdminStudio including creating an Application Catalog, configuring a virtual machine, configuring e-mail settings, and specifying server connection settings. |
| **Migrating to Windows Installer** | Explains how to convert a sample setup to a Windows Installer package, import it into the Application Catalog, test it for operating system compatibility, best practices, and conflicts, and then prepare it for distribution. |
| **Migrating to Application Virtualization** | Explains how to use the Automated Application Converter to convert Windows Installer packages to virtual packages, and then test and distribute the virtual packages. |
| **Testing for Application Compatibility** | Explains how to use Application Manager to test packages for compatibility with the latest versions of Microsoft Windows, Windows Server, macOS, Apple iOS, Google Android, and Windows Phone operating systems, as well as to test web applications for compatibility with Internet Explorer 11 and Microsoft Edge. |

# Getting Started

This section explains what is included in this Evaluation Guide and how to get started:

- About Evaluating AdminStudio
- Purpose of Evaluation Guide
- Organization of Evaluation Guide
- Evaluation Guide Data Files

## About Evaluating AdminStudio

You can choose to evaluate AdminStudio for 21 days. By clicking **Continue to Evaluate AdminStudio** dialog box that opens when you launch AdminStudio, you can begin evaluating the AdminStudio Enterprise Edition client tools.

Information about evaluating the AdminStudio client tools includes the following topics:

- AdminStudio Client Tools Evaluation Restrictions
- Evaluating AdminStudio’s Microsoft App-V Support
- Evaluating the Automated Application Converter “Multiple Application” Option

### AdminStudio Client Tools Evaluation Restrictions

When you run AdminStudio in trial/evaluation mode, all of its features 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.

### Evaluating AdminStudio’s Microsoft App-V Support

While evaluating the AdminStudio Enterprise Edition client tools, you will be able to convert a Windows Installer package to an App-V application using the Automated Application Converter, Conversion Wizard, Repackager, and the InstallShield App-V Assistant. However, an App-V application built using an evaluation version of AdminStudio will display the following message every time it is launched:

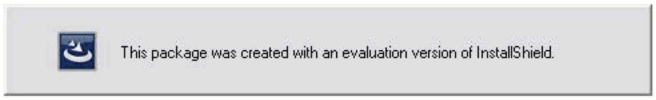

This package was created with an evaluation version of InstallShield.

**Figure 1:** Evaluation Version Message

After activating AdminStudio, you will be able to remove this message by rebuilding the App-V application.

### Evaluating the Automated Application Converter “Multiple Application” Option

The Multiple Application option of Automated Application Converter is only available when you purchase AdminStudio Enterprise Edition.

***Note** • With AdminStudio Standard or Professional Editions, you will only be able to convert one package at a time, using one virtual machine.*

When using an evaluation version of AdminStudio, you will be able to use Automated Application Converter to convert a directory full of Windows Installer packages into individual virtual packages, but the conversion will be limited to three packages per run, using only one virtual machine. Therefore, only the first three packages that Automated Application Converter encounters will be converted to virtual applications.

## Purpose of Evaluation Guide

The purpose of this Evaluation Guide is to help system administrators and other reviewers learn how to quickly get started using AdminStudio to prepare Windows Installer and virtual applications for deployment. By performing the exercises in this Evaluation Guide using the provided data files, you will learn how to:

- Create an Application Catalog
- Repackage a sample package
- Import packages into the Application Catalog
- Test Windows Installer packages, App-V packages, and web applications
- Configure a virtual machine for use in automated repackaging
- Convert Windows Installer packages to virtual applications
- Distribute Windows Installer and App-V packages
- Perform operating system compatibility and browser compatibility testing

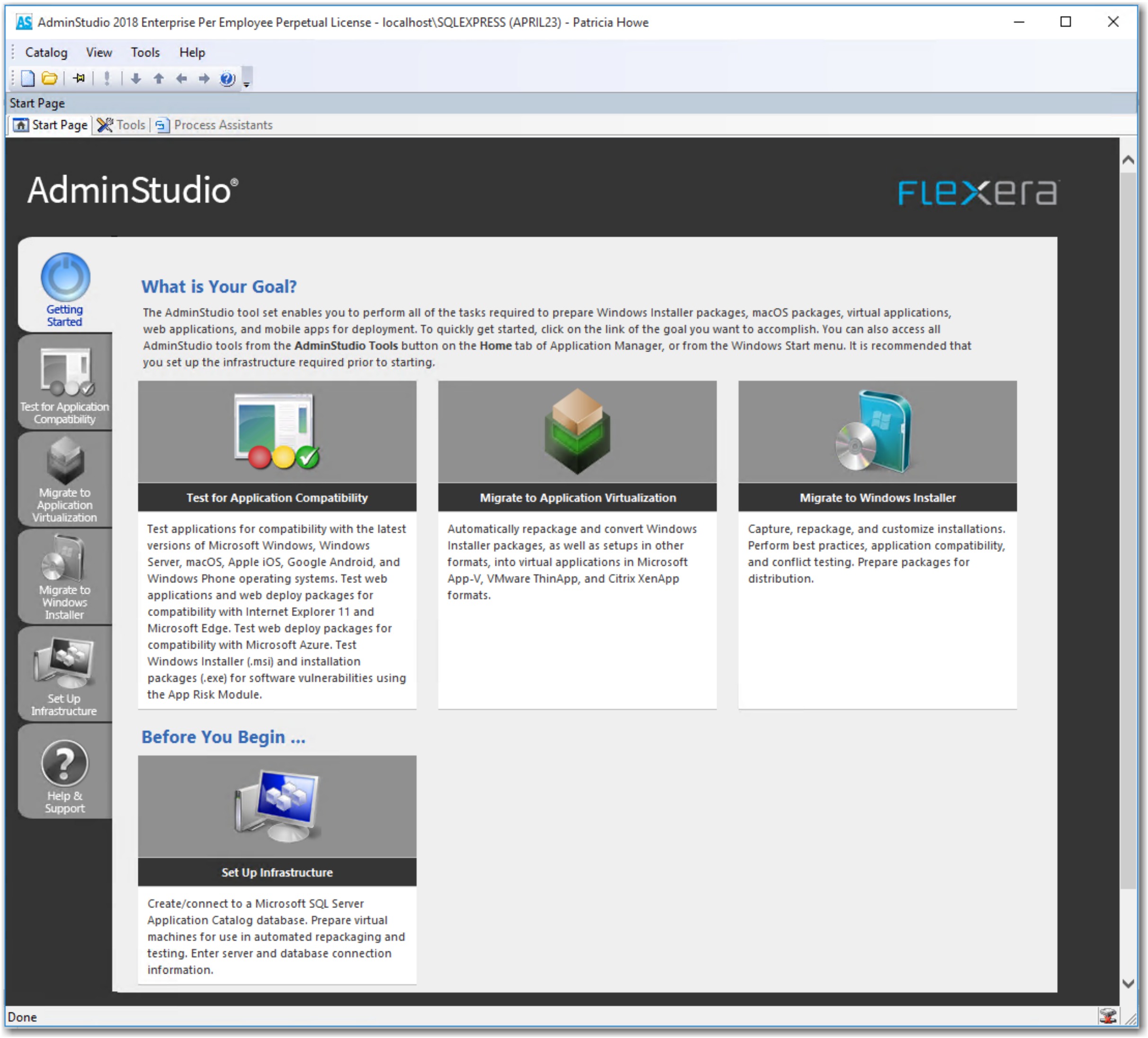
# Organization of Evaluation Guide

This Evaluation Guide provides exercises that guide you through performing the following key procedures:

**Table 2 •** Evaluation Exercises

| Procedure | Procedure |
|---|---|
| **Setting Up AdminStudio Infrastructure** | In these set of exercises, you will perform the one-time setup tasks that are necessary to get started using AdminStudio:<br>● Creating an Application Catalog<br>● Configuring a Virtual Machine<br>● Setting E-Mail Notification Settings<br>● Entering Server/Database Connection Settings |
| **Migrating to Windows Installer** | In this set of exercises, you will migrate a sample setup (such as an `.exe` file) to a deployable Windows Installer package (`.msi`):<br>● Repackaging a Sample Package<br>● Importing Packages into the Application Catalog<br>● Testing a Repackaged Application and Resolving Issues<br>● Distributing a Repackaged Application |
| **Migrating to Application Virtualization** | In this set of exercises, you will migrate a set of applications into virtual applications that are ready for deployment:<br>● Identifying Packages to Virtualize<br>● Converting to Virtual Formats<br>● Testing and Distributing Converted Packages |
| **Testing for Application Compatibility** | In this set of exercises, you will test Windows Installer packages for application readiness on the latest versions of Microsoft Windows and Windows Server. You will also test web applications for compatibility with Internet Explorer 11 and Microsoft Edge.<br>● Importing Packages, Web Applications, and Mobile Apps<br>● Selecting Tests to Run and Setting Default Fix Option<br>● Performing Testing and Viewing Results |

These four main procedures are also featured on AdminStudio’s Start Page.


AdminStudio 2018 Enterprise Per Employee Perpetual License - localhost\SQLEXPRESS (APRIL23) - Patricia Howe
Catalog
View
Tools
Help
Start Page
Start Page
Tools
Process Assistants
AdminStudio®
FLEXERA
Getting Started
Test for Application Compatibility
Migrate to Application Virtualization
Migrate to Windows Installer
Set Up Infrastructure
Help & Support
Done

### What is Your Goal?

The AdminStudio tool set enables you to perform all of the tasks required to prepare Windows Installer packages, macOS packages, virtual applications, web applications, and mobile apps for deployment. To quickly get started, click on the link of the goal you want to accomplish. You can also access all AdminStudio tools from the **AdminStudio Tools** button on the **Home** tab of Application Manager, or from the Windows Start menu. It is recommended that you set up the infrastructure required prior to starting.

**Test for Application Compatibility**

Test applications for compatibility with the latest versions of Microsoft Windows, Windows Server, macOS, Apple iOS, Google Android, and Windows Phone operating systems. Test web applications and web deploy packages for compatibility with Internet Explorer 11 and Microsoft Edge. Test web deploy packages for compatibility with Microsoft Azure. Test Windows Installer (.msi) and installation packages (.exe) for software vulnerabilities using the App Risk Module.

**Migrate to Application Virtualization**

Automatically repackage and convert Windows Installer packages, as well as setups in other formats, into virtual applications in Microsoft App-V, VMware ThinApp, and Citrix XenApp formats.

**Migrate to Windows Installer**

Capture, repackage, and customize installations. Perform best practices, application compatibility, and conflict testing. Prepare packages for distribution.

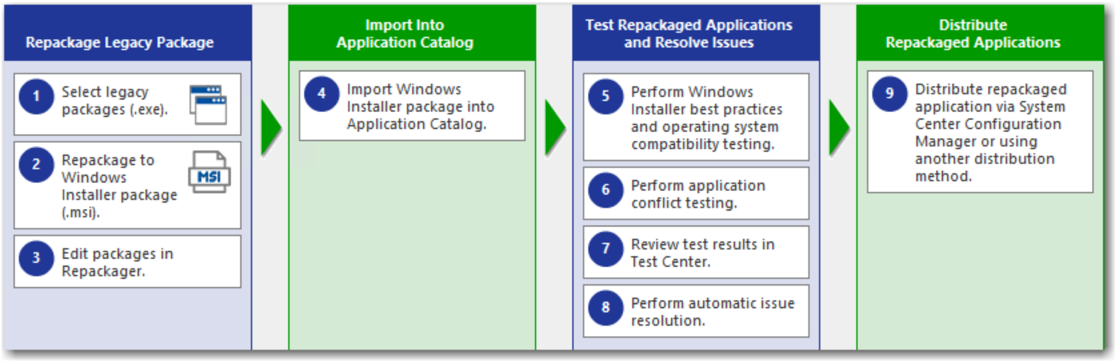
### Before You Begin ...

**Set Up Infrastructure**

Create/connect to a Microsoft SQL Server Application Catalog database. Prepare virtual machines for use in automated repackaging and testing. Enter server and database connection information.

**Figure 2:** AdminStudio Start Page

Each subtab of the Start Page includes a flowchart that lists the steps in each procedure. For example, the following flowchart is displayed on the **Migrate to Windows Installer** tab:



Repackage Legacy Package

1 Select legacy packages (.exe).

2 Repackage to Windows Installer package (.msi).

3 Edit packages in Repackager.

Import Into Application Catalog

4 Import Windows Installer package into Application Catalog.

Test Repackaged Applications and Resolve Issues

5 Perform Windows Installer best practices and operating system compatibility testing.

6 Perform application conflict testing.

7 Review test results in Test Center.

8 Perform automatic issue resolution.

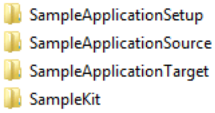
Distribute Repackaged Applications

9 Distribute repackaged application via System Center Configuration Manager or using another distribution method.

**Figure 3:** Migrate to Windows Installer Tab of AdminStudio Start Page

# Evaluation Guide Data Files

To perform the exercises in the AdminStudio Evaluation Guide, you will be using the sample data that is provided in the `AS2018EvalGuideDataFiles.zip` file. These data files are organized into the following directories:



SampleApplicationSetup
SampleApplicationSource
SampleApplicationTarget
SampleKit

**Figure 4:** Directory Structure of AdminStudio Evaluation Guide Data Files

These data files demonstrate the recommended organizational structure that you should use when you want to import a directory of packages into the Application Catalog:

- **One root directory**—Organize the packages you want to import in one root directory (`AS2018EvalGuideDataFiles` in this example).
- **Each application in a subdirectory**—Each application should be stored in its own first level subdirectory (such as `SampleKit` or `SampleApplicationTarget`).
- **Each deployment type in a sub-subdirectory**—Each deployment type should be stored in its own sub-subdirectory (`AppV`, `MSI`, etc.) of the application directory.

Unzip this data file and place its contents in a location accessible to your installation of AdminStudio, such as:

```
C:\AS2018EvalGuideDataFiles
```

# 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.

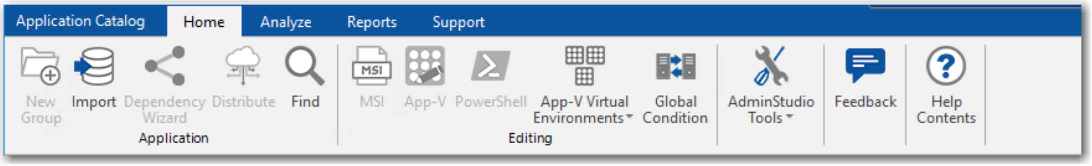
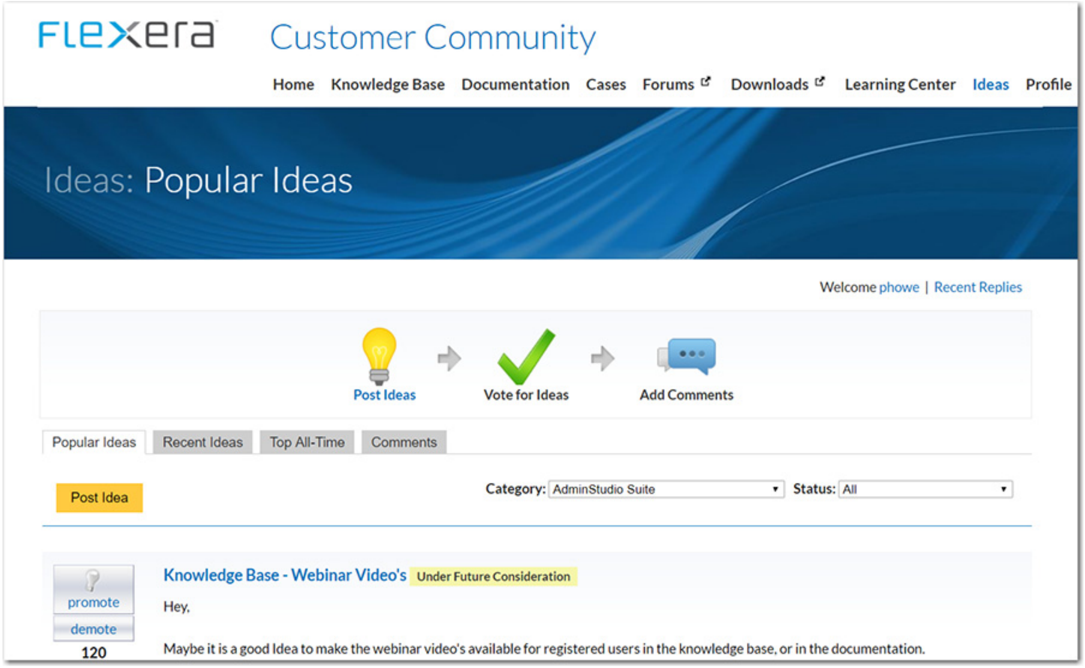


**Figure 5:** Home Tab Ribbon

### 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.



Hey,

Maybe it is a good Idea to make the webinar video's available for registered users in the knowledge base, or in the documentation.

**Figure 6:** 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

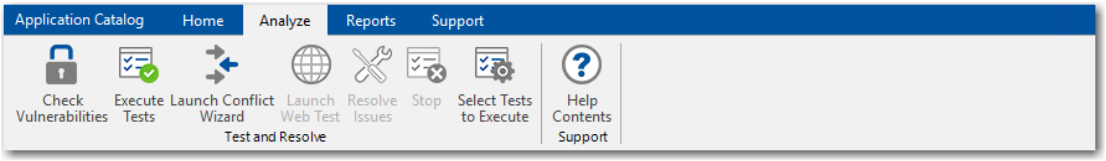


**Figure 7:** Analyze Tab Ribbon

## 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.

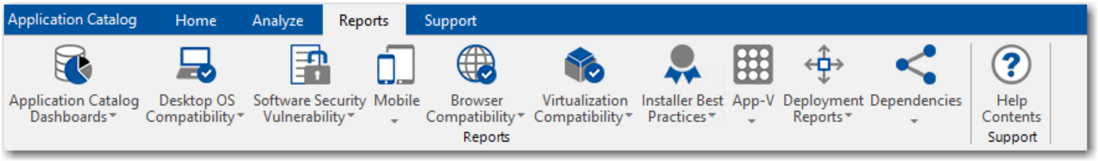


**Figure 8:** Reports Tab Ribbon

## 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.

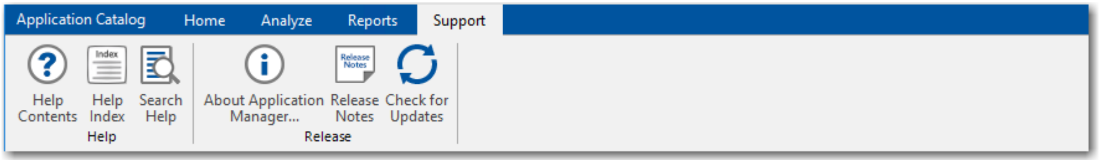


**Figure 9:** Support Tab Ribbon

# 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.

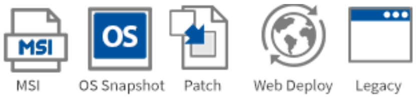
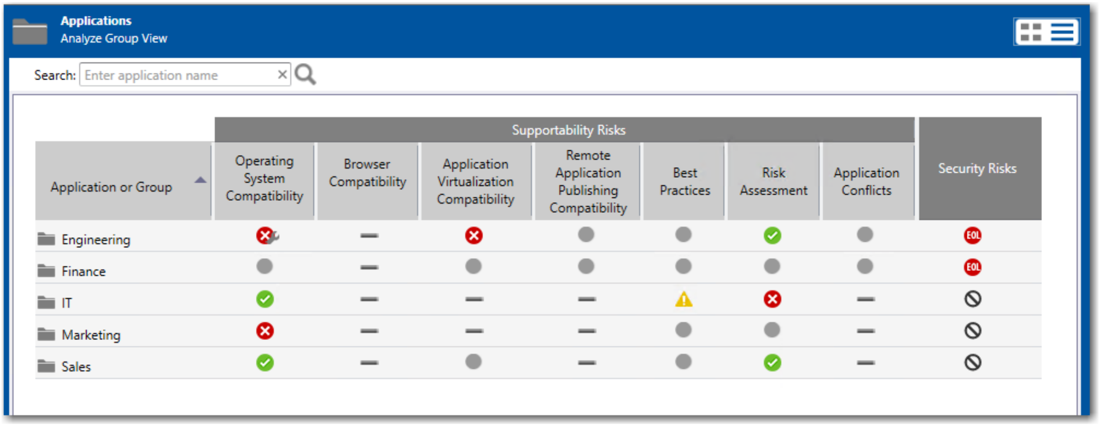


**Figure 10:** Redesigned Deployment Type Icons

# 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.



Applications
Analyze Group View

Search: Enter application name

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

**Figure 11:** 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.

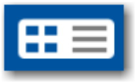
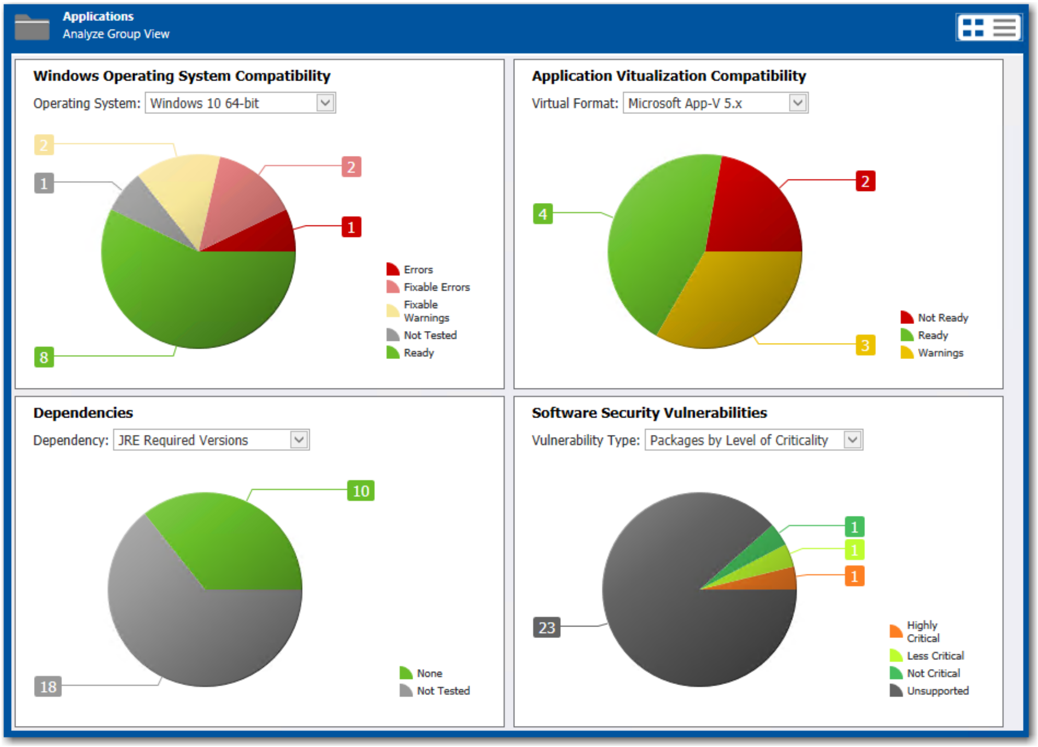


**Figure 12:** Toggle Button

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



Applications
Analyze Group View

**Windows Operating System Compatibility**
Operating System: Windows 10 64-bit

**Application Vitualization Compatibility**
Virtual Format: Microsoft App-V 5.x

**Dependencies**
Dependency: JRE Required Versions

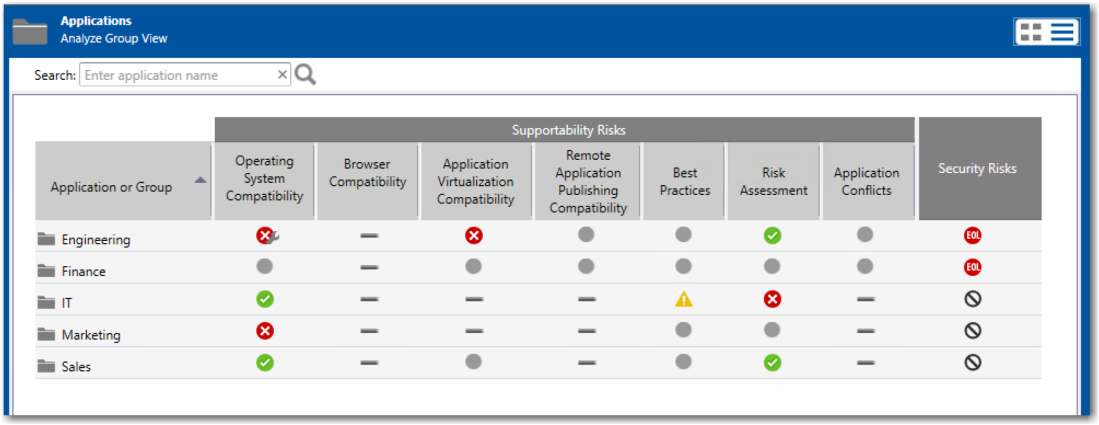
**Software Security Vulnerabilities**
Vulnerability Type: Packages by Level of Criticality

**Figure 13:** 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.



Applications
Analyze Group View

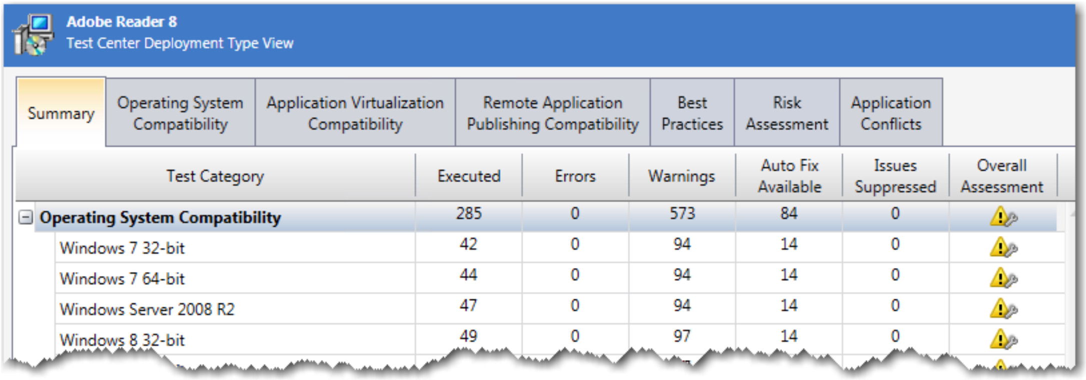
Search: Enter application name

| | Supportability Risks | | | | | | | Security Risks |
|---|---|---|---|---|---|---|---|---|
| Application or Group | Operating System Compatibility | Browser Compatibility | Application Virtualization Compatibility | Remote Application Publishing Compatibility | Best Practices | Risk Assessment | Application Conflicts | |
| Engineering | ✖ | — | ✖ | ● | ● | ✓ | ● | EOL |
| Finance | ● | — | ● | ● | ● | ● | ● | EOL |
| IT | ✓ | — | — | — | ⚠ | ✖ | — | ⃠ |
| Marketing | ✖ | — | — | — | ● | ● | — | ⃠ |
| Sales | ✓ | — | ● | — | ● | ✓ | — | ⃠ |

**Figure 14:** Supportability Risks and Security Risks Test Category Groups

# Simplified Compatibility Test Results

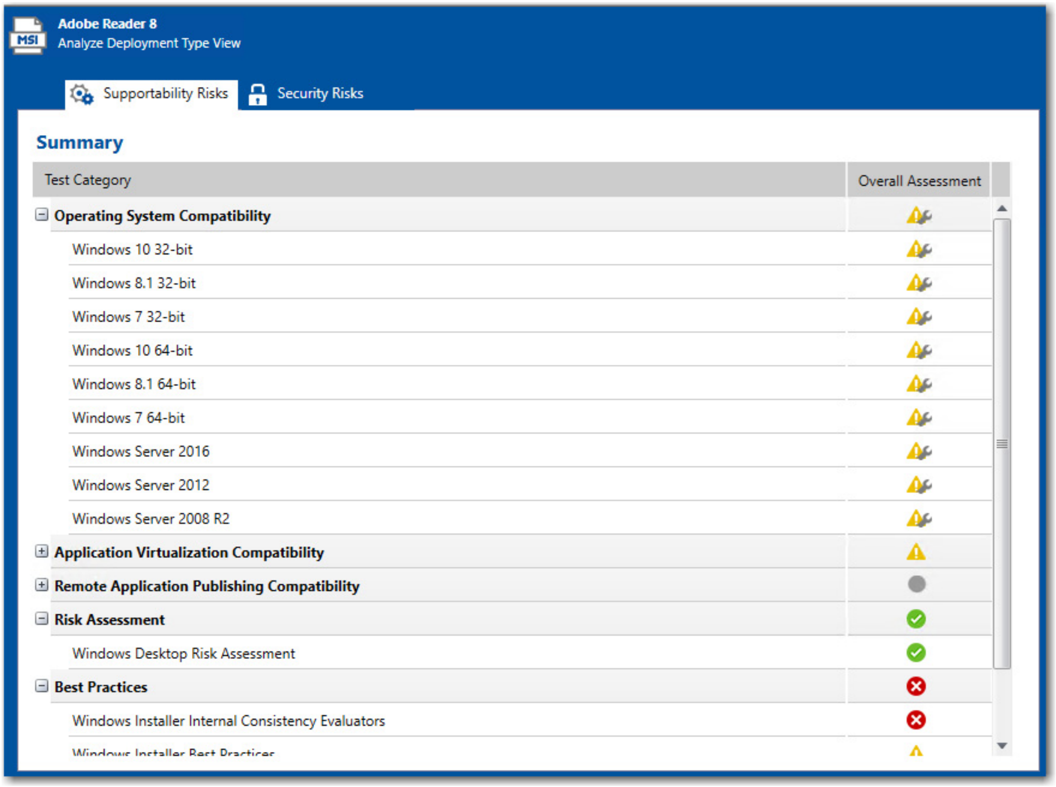
In previous releases, when you viewed compatibility, best practices and risk assessment test results, a large list of numbers—identifying how many tests were executed, how many errors/warnings were generated, etc.—were displayed for each test. To view details of a particular test, you had to open a subtab,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


Adobe Reader 8
Test Center Deployment Type View
Summary
Operating System Compatibility
Application Virtualization Compatibility
Remote Application Publishing Compatibility
Best Practices
Risk Assessment
Application Conflicts

| 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 15:** Summary Deployment Type Test Results In Previous Releases

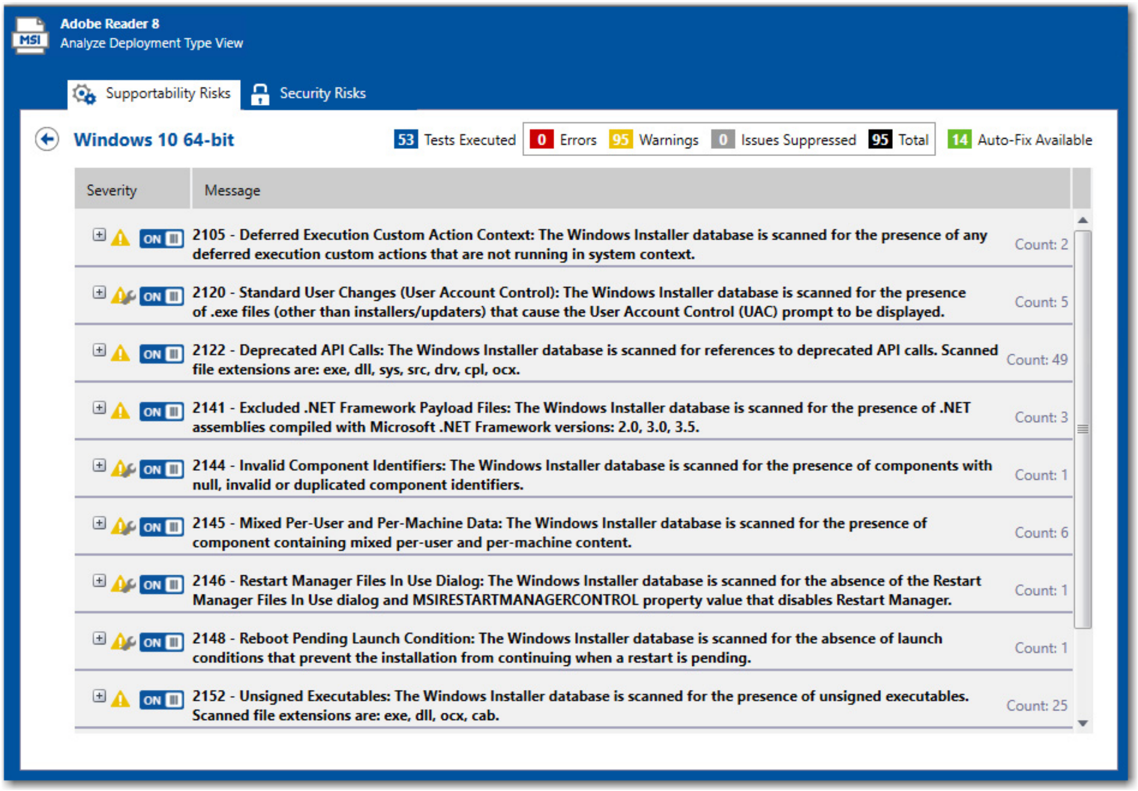
In AdminStudio 2018, a cleaner view of test results is displayed, with only a summary status icon displayed for each test. To see the detailed results for a specific test, you can now just click on that test to open the detailed view.



| 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 16:** 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.



Adobe Reader 8
Analyze Deployment Type View

Windows 10 64-bit

53 Tests Executed | 0 Errors | 95 Warnings | 0 Issues Suppressed | 95 Total | 14 Auto-Fix Available

| Severity | Message | |
|---|---|---|
| ⊞ ⚠ ON | 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 |
| ⊞ ⚠ ON | 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 |
| ⊞ ⚠ ON | 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 |
| ⊞ ⚠ ON | 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 |
| ⊞ ⚠ ON | 2144 - Invalid Component Identifiers: The Windows Installer database is scanned for the presence of components with null, invalid or duplicated component identifiers. | Count: 1 |
| ⊞ ⚠ ON | 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 |
| ⊞ ⚠ ON | 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 |
| ⊞ ⚠ ON | 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 |
| ⊞ ⚠ ON | 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 17:** 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.

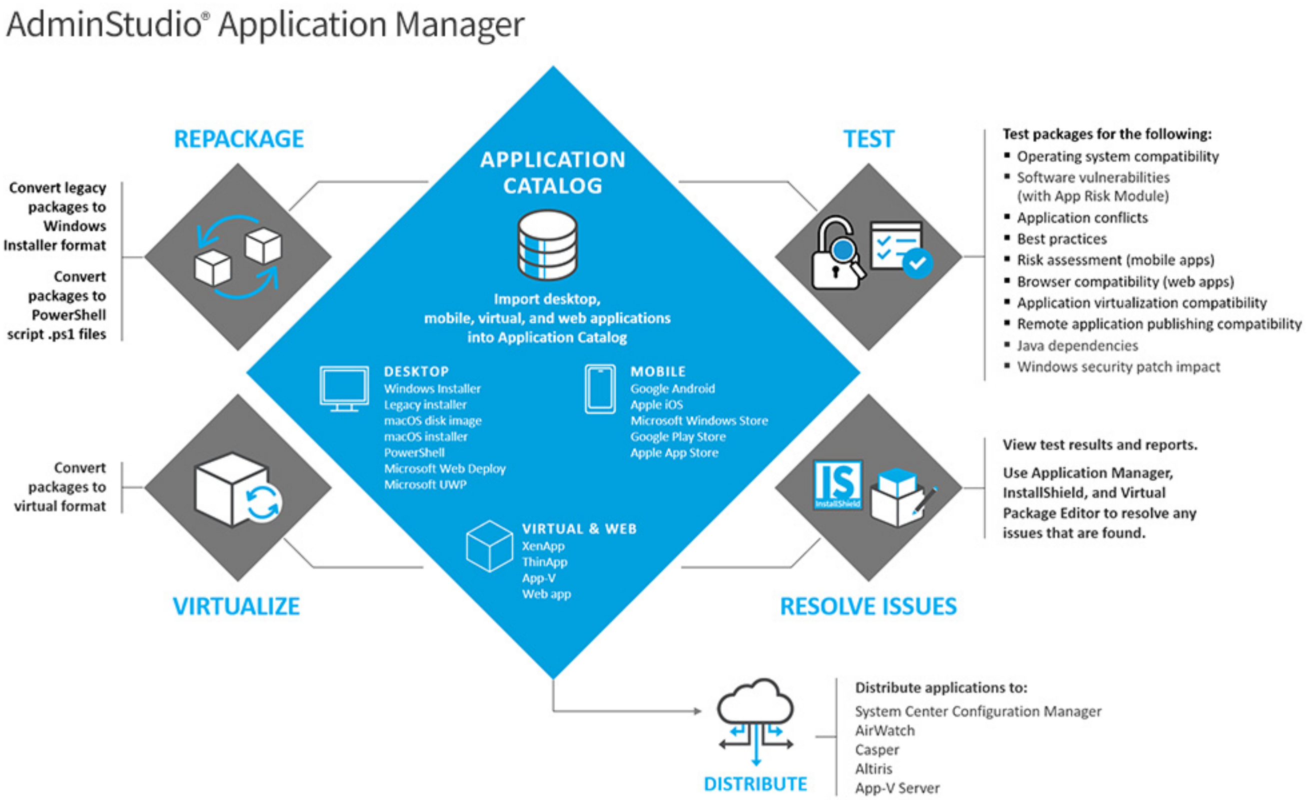
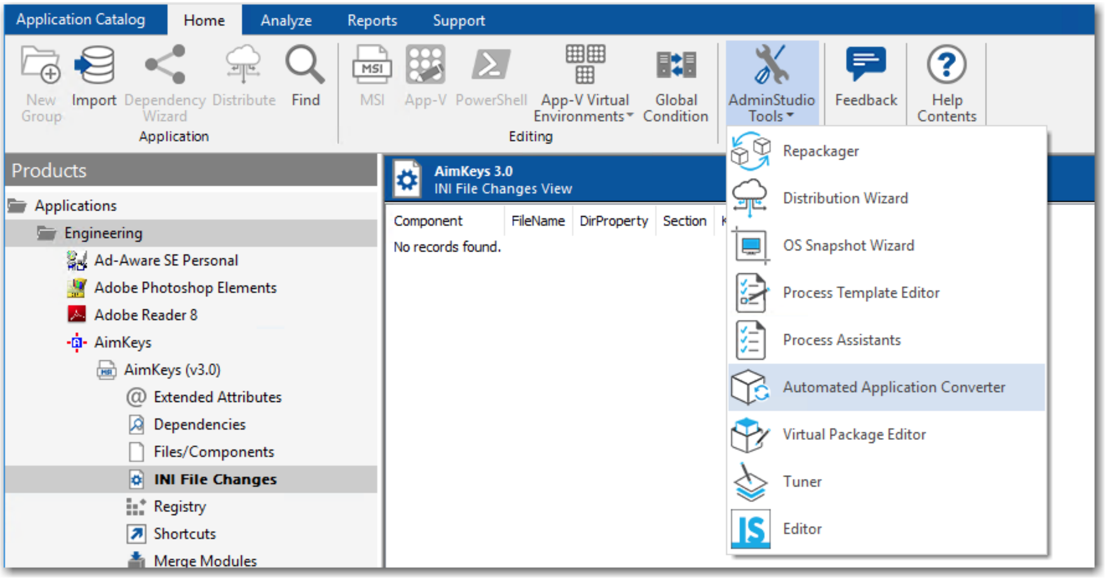

AdminStudio® Application Manager
REPACKAGE
Convert legacy packages to Windows Installer format
Convert packages to PowerShell script .ps1 files
APPLICATION CATALOG
Import desktop, mobile, virtual, and web applications into Application Catalog
DESKTOP
Windows Installer
Legacy installer
macOS disk image
macOS installer
PowerShell
Microsoft Web Deploy
Microsoft UWP
MOBILE
Google Android
Apple iOS
Microsoft Windows Store
Google Play Store
Apple App Store
VIRTUAL & WEB
XenApp
ThinApp
App-V
Web app
TEST
Test packages for the following:
Operating system compatibility
Software vulnerabilities (with App Risk Module)
Application conflicts
Best practices
Risk assessment (mobile apps)
Browser compatibility (web apps)
Application virtualization compatibility
Remote application publishing compatibility
Java dependencies
Windows security patch impact
Convert packages to virtual format
VIRTUALIZE
IS InstallShield
View test results and reports.
Use Application Manager, InstallShield, and Virtual Package Editor to resolve any issues that are found.
RESOLVE ISSUES
DISTRIBUTE
Distribute applications to:
System Center Configuration Manager
AirWatch
Casper
Altiris
App-V Server

**Figure 18:** 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.



No records found.

**Figure 19:** 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**.

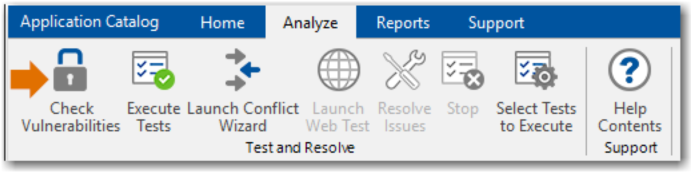


**Figure 20:** Check Vulnerabilities Button

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. |
| EOL | **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** | There are multiple reasons why an application could be considered unsupported:<br>● **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.<br>● **Unable to extract Installation file**—AdminStudio in 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.<br>● **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.<br>● **Unknown**—An error has occurred during testing. |

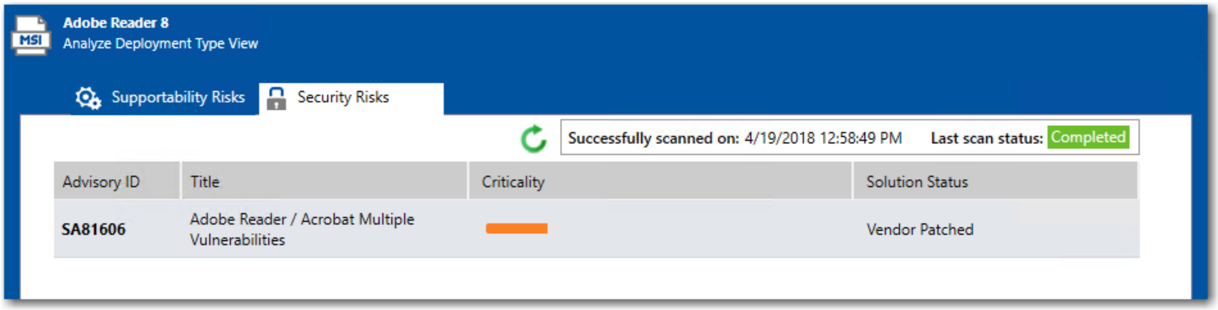
# Viewing Security Vulnerability Test Results

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.



Adobe Reader 8
Analyze Deployment Type View

**Successfully scanned on:** 4/19/2018 12:58:49 PM **Last scan status:** Completed

| Advisory ID | Title | Criticality | Solution Status |
|---|---|---|---|
| **SA81606** | Adobe Reader / Acrobat Multiple Vulnerabilities | 🟧 | Vendor Patched |

**Figure 21:** Security Risks Summary View

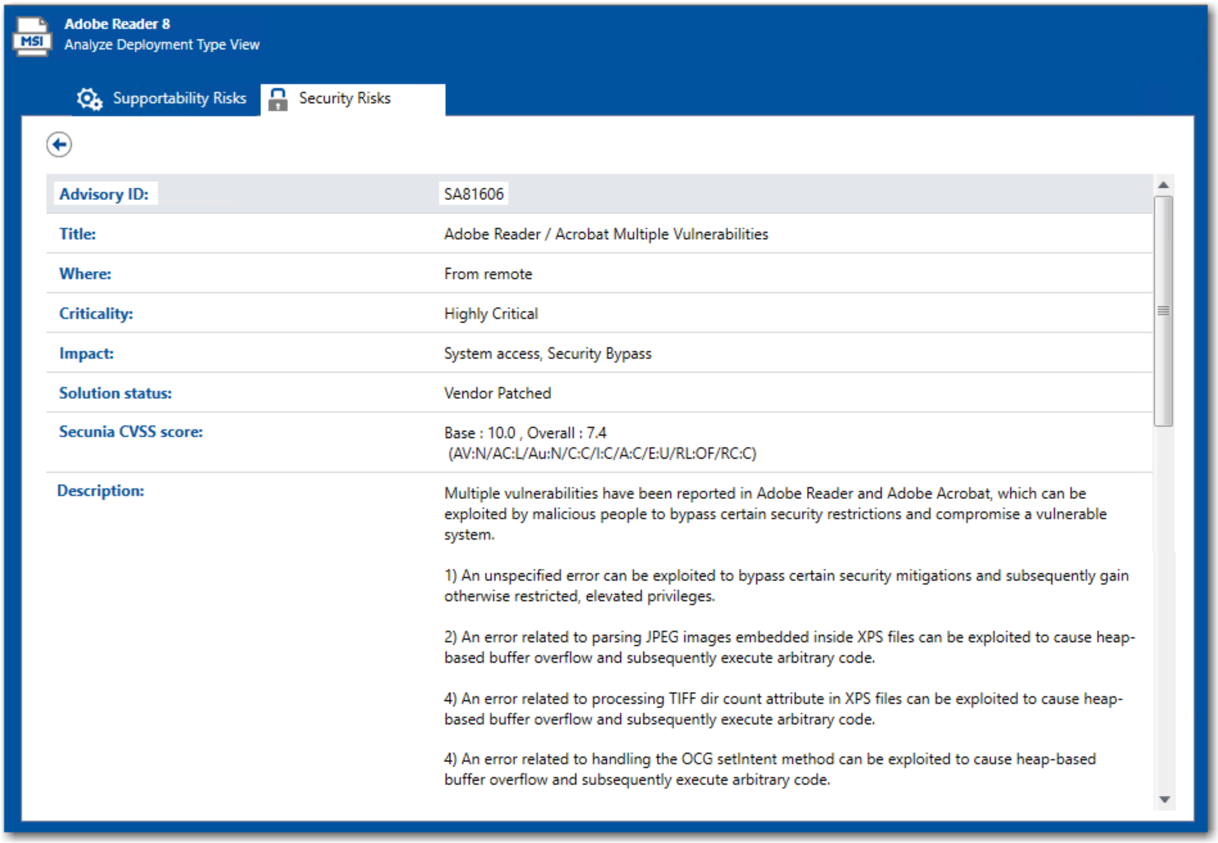
The icon in the **Criticality** column identifies the Advisory as one of the following degrees of criticality:

| 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.



| | |
|---|---|
| **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<br>(AV:N/AC:L/Au:N/C:C/I:C/A:C/E:U/RL:OF/RC:C) |
| **Description:** | 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.<br>1) An unspecified error can be exploited to bypass certain security mitigations and subsequently gain otherwise restricted, elevated privileges.<br>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.<br>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.<br>4) An error related to handling the OCG setIntent method can be exploited to cause heap-based buffer overflow and subsequently execute arbitrary code. |

**Figure 22:** Advisory Report

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

**Table 3 •** Advisory Report

| Property | Description |
|---|---|
| **Advisory ID** | Identifies the security advisory. |
| **Title** | Title of the security advisory. |
| **Where** | Identifies the **Where** (attack vector) value as one of the following:<br>● **Local System**—Describes vulnerabilities where the attack vector requires that the attacker is a local user on the system.<br>● **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.<br>● **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. |

**Table 3 •** Advisory Report

| Property | Description |
|---|---|
| **Criticality** | Lists the advisory’s criticality rating value as one of the following:<br>● **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.<br>● **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.<br>● **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.<br>● **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.<br>● **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). |

**Table 3 •** Advisory Report

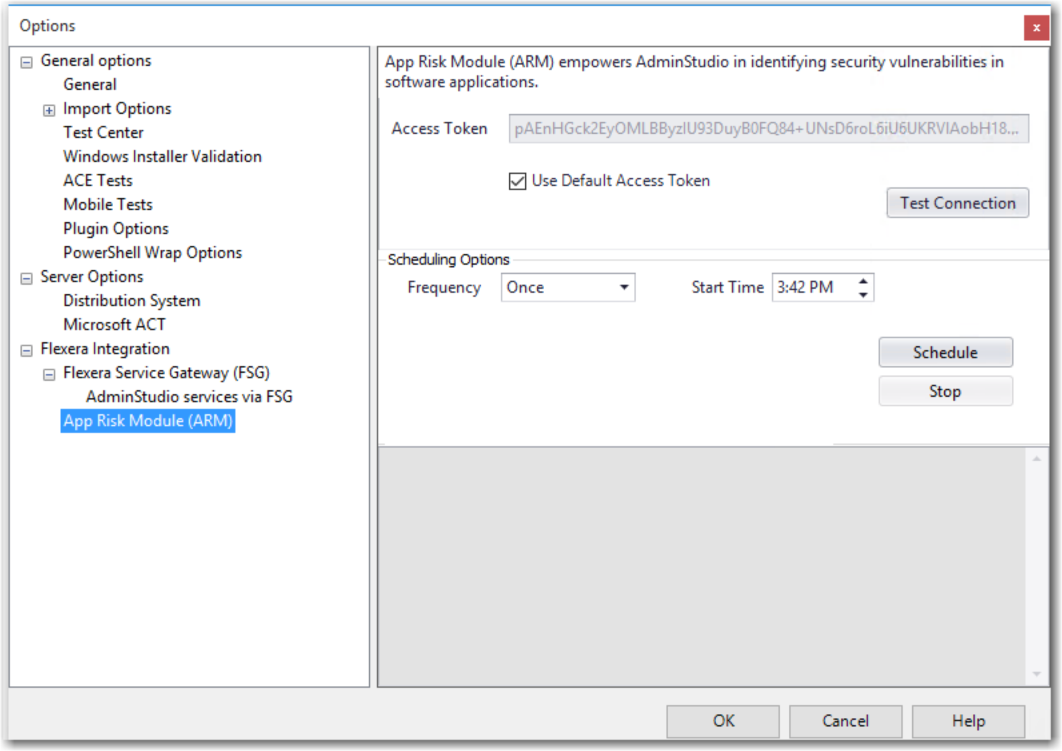
| Property | Description |
|---|---|
| **Impact** | Categorizes the impact of this advisory as one of the following:<br>● **Brute Force**—Used in cases where an application or an algorithm allows an attacker to guess passwords in an easy manner.<br>● **Cross-Site Scripting**—These vulnerabilities allow 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.<br>● **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.<br>● **Exposure of Sensitive Information**—Vulnerabilities where documents or credentials are leaked or can be revealed either locally or remotely.<br>● **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.<br>● **Hijacking**—Covers vulnerabilities where a user session or a communication channel can be taken over by other users or remote attackers.<br>● **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.<br>● **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.<br>● **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.<br>● **Spoofing**—Covers various vulnerabilities where it is possible for malicious users or people to impersonate other users or systems.<br>● **System Access**—Covers vulnerabilities where malicious people are able to gain system access and execute arbitrary code with the privileges of a local user.<br>● **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. |
| **Solution status** | Identifies how this advisory can be resolved, such as **Vendor Patched**. |

**Table 3 •** Advisory Report

| Property | Description |
|---|---|
| **Secunia CVSS score** | The Common Vulnerability Scoring System (CVSS) consists of three groups:<br>● **Base**—Represents the intrinsic qualities of a vulnerability.<br>● **Temporal**—Reflects the characteristics of a vulnerability that changes over time<br>● **Environmental**—Represents the characteristics of a vulnerability that are unique to any user's environment.<br>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.<br>For details on interpreting a CVSS vector, see the Common Vulnerability Scoring System v3.0: Specification Document.<br>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.<br>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. |
| **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** | Lists of references other related related advisories on various websites such as the Zero Day Initiative website, such as:<br>https://www.zerodayinitiative.com/advisories/ZDI-18-209/ |
| **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.



App Risk Module (ARM) empowers AdminStudio in identifying security vulnerabilities in software applications.

Access Token: pAEnHGck2EyOMLBByzIU93DuyB0FQ84+UNsD6roL6iU6UKRVIAobH18...

☑ Use Default Access Token

Frequency: Once

Start Time: 3:42 PM

**Figure 23:** 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.

**Table 4 •** App Risk Module (ARM) Tab of Options Dialog Box

| Property | Description |
|---|---|
| **Access Token** | Initially lists the Access Token provided when App Risk Module was installed.<br>***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.* |
| **Test Connection** | Click to test your connection to the App Risk Module database. |

**Table 4 •** App Risk Module (ARM) Tab of Options Dialog Box

| Property | Description |
|---|---|
| **Scheduling Options** | 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.<br>To modify the default schedule, select a **Frequency** (Once, Daily, Weekly, or Monthly) and a **Start Time**, and then click **Schedule**.<br>Click **Stop** to stop an update in progress. |

## 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.

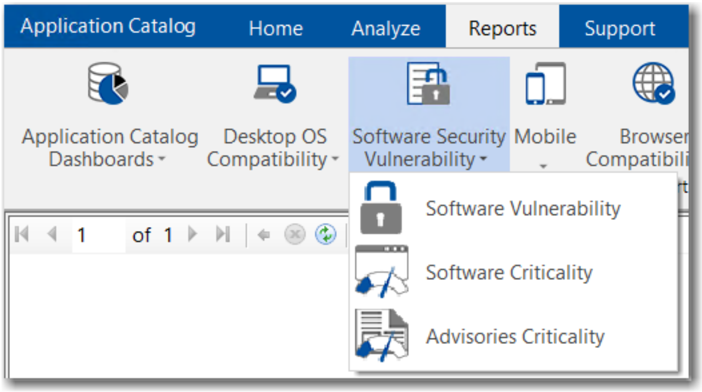


**Figure 24:** Security Vulnerability Reports

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 the AdminStudio 2018 Release Notes.

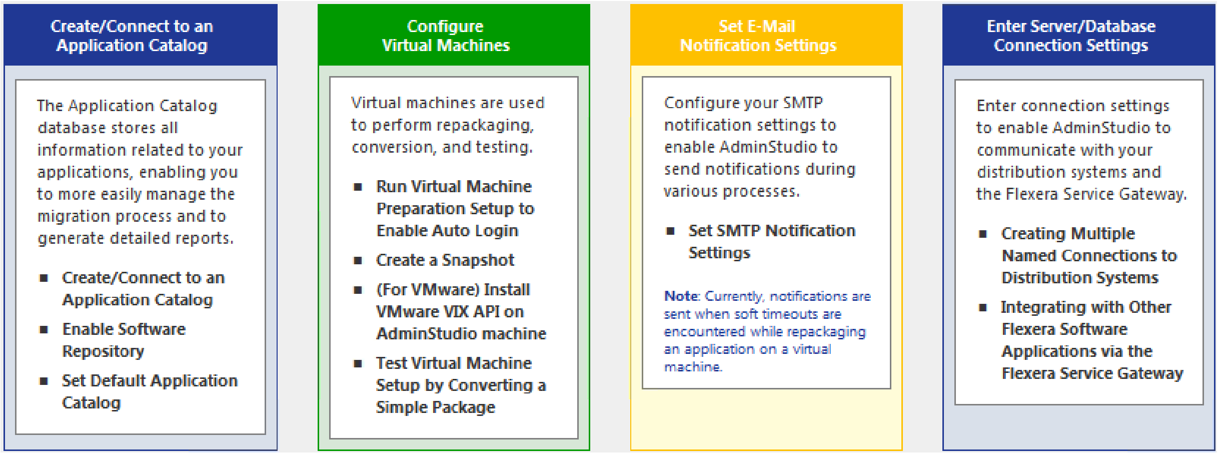
***Note** • AdminStudio 2018's new App Risk Module feature is available when you purchase AdminStudio Enterprise Edition with the App Risk Module (ARM) add-on module. For more information, see New App Risk Module (ARM) to Identify Security Vulnerabilities*

# InstallShield 2018

AdminStudio 2018 includes InstallShield 2018. For a complete list of new features in InstallShield 2018, see the InstallShield 2018 Release Notes.

# Setting Up AdminStudio Infrastructure

The flowchart on the **Set Up Infrastructure** tab of the AdminStudio Start page lists the steps you need to perform before you can get started using AdminStudio.



**Create/Connect to an Application Catalog**

The Application Catalog database stores all information related to your applications, enabling you to more easily manage the migration process and to generate detailed reports.

- Create/Connect to an Application Catalog
- Enable Software Repository
- Set Default Application Catalog

**Configure Virtual Machines**

Virtual machines are used to perform repackaging, conversion, and testing.

- Run Virtual Machine Preparation Setup to Enable Auto Login
- Create a Snapshot
- (For VMware) Install VMware VIX API on AdminStudio machine
- Test Virtual Machine Setup by Converting a Simple Package

**Set E-Mail Notification Settings**

Configure your SMTP notification settings to enable AdminStudio to send notifications during various processes.

- Set SMTP Notification Settings

**Note**: Currently, notifications are sent when soft timeouts are encountered while repackaging an application on a virtual machine.

**Enter Server/Database Connection Settings**

Enter connection settings to enable AdminStudio to communicate with your distribution systems and the Flexera Service Gateway.

- Creating Multiple Named Connections to Distribution Systems
- Integrating with Other Flexera Software Applications via the Flexera Service Gateway

**Figure 25:** Set Up Infrastructure Tab of AdminStudio Start Page

These are specific one-time set-up tasks that you need to perform prior to using AdminStudio. To set up AdminStudio infrastructure, perform the following exercises:

- Creating an Application Catalog
- Configuring a Virtual Machine
- Setting E-Mail Notification Settings
- Entering Server/Database Connection Settings

# Creating an Application Catalog

With AdminStudio, you manage your applications and their deployment types in an Application Catalog database, which stores all package information, including test results. This enables you to perform enterprise level data checking. You can share your Application Catalog between multiple AdminStudio users.

AdminStudio and many of its tools (such as Application Manager) require you to be connected to an Application Catalog, while others give you the option of working with packages on a local or network directory or from Microsoft System Center Configuration Manager Server.

In this exercise, you will create a new AdminStudio Application Catalog and set it as the default.

**Table 5 •** Create/Connect to an Application Catalog

| # | Step | Instructions | Result |
|---|---|---|---|
| **1.** | **Create an Application Catalog** | Open AdminStudio and create a new SQL Server Application Catalog database named `AdminStudio Evaluation Catalog`, as described in Creating New Application Catalogs Using the AdminStudio Interface.<br>***Note** • On the **Select Software Repository Location** panel of the **Application Catalog Wizard**, do NOT select the **Enable Software Repository** option.* | AdminStudio is open and connected to a new Application Catalog named `AdminStudio Evaluation Catalog`. |

# Configuring a Virtual Machine

Virtual machines are used by Automated Application Converter during automated repackaging (performed during conversion to virtual applications) and when testing applications.

You need to prepare each virtual machine that you are going to use with the Automated Application Converter to perform automated repackaging or testing by doing the following:

- **Run Virtual Machine Preparation setup**—On each virtual machine you are going to use with the Automated Application Converter, run the Virtual Machine Preparation setup, an application that will enable automatic login. You need to run this application one time on all of the virtual machines that you are going to use with the Automated Application Converter.
- **Create a snapshot**—After you have run the Virtual Machine Preparation setup on a virtual machine, you need to shut it down and create a snapshot named `AutoRepack_Base`. This enables the Automated Application Converter to revert the virtual image to a clean state after each repackaging run.
- **Install VMware VIX API (VMware only)**—In order for the 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 6.5 or later), you need to have the VMware VIX API installed on the same machine as the Automated Application Converter.

In this exercise, you will configure a virtual machine for use with Automated Application Converter.

**Table 6 •** Configure Virtual Machines

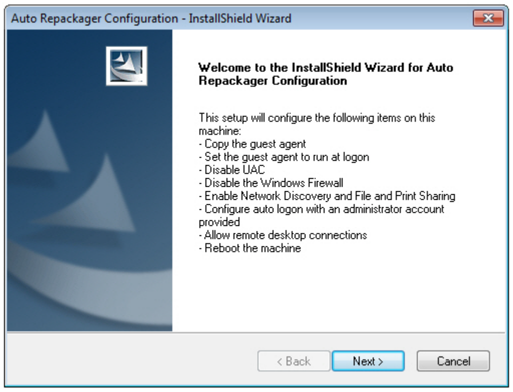
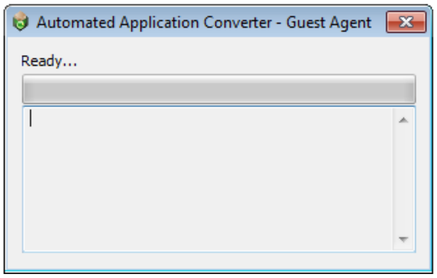
| # | Step | Instructions | Result |
|---|---|---|---|
| **1.** | **Run Virtual Machine Preparation setup to enable auto login** | On a Microsoft Hyper-V Server image, VMware ESX/ESXi Server image, or VMware Workstation (6.5+) image, run the virtual machine preparation setup.<br><br> <br>**Welcome to the InstallShield Wizard for Auto Repackager Configuration**<br>This setup will configure the following items on this machine:<br>- Copy the guest agent<br>- Set the guest agent to run at logon<br>- Disable UAC<br>- Disable the Windows Firewall<br>- Enable Network Discovery and File and Print Sharing<br>- Configure auto logon with an administrator account provided<br>- Allow remote desktop connections<br>- Reboot the machine<br> <br>***Note*** • *For instructions, see Preparing Your Virtual Machines for Use With the Automated Application Converter.* | When you restart the virtual machine image, you are automatically logged in and `GuestAgent.exe` is launched.<br><br> <br>Ready... |
| **2.** | **Create a snapshot for repackaging** | On the prepared virtual image, create a clean snapshot named `AutoRepack_Base`.<br>***Note*** • *For instructions, see* ***Taking a Snapshot*** *in Preparing Your Virtual Machines for Use With the Automated Application Converter.* | A clean snapshot named `AutoRepack_Base` exists on the virtual machine. |

**Table 6 •** Configure Virtual Machines

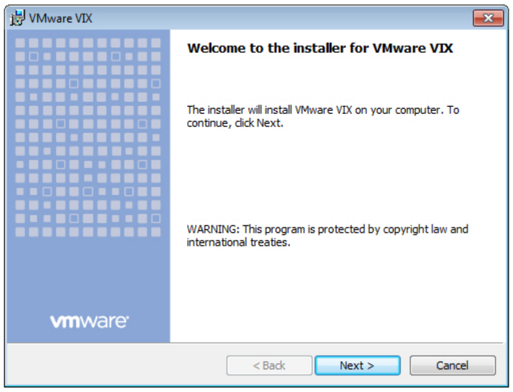
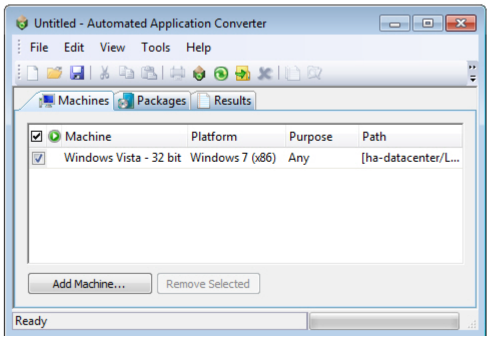
| # | Step | Instructions | Result |
|---|---|---|---|
| **3.** | **Install VMware VIX** | If you are using a VMware ESX/ESXi Server or VMware Workstation image, you need to install the VMware VIX API on the AdminStudio machine.<br><br> <br>**Welcome to the installer for VMware VIX**<br>The installer will install VMware VIX on your computer. To continue, click Next.<br>WARNING: This program is protected by copyright law and international treaties.<br>To install the VMware VIX API on the AdminStudio machine, do one of the following:<br>● Install VMware Workstation on the AdminStudio machine.<br>● Download and install the VMware VIX API on the AdminStudio machine. You can download the VMware VIX API from the following location:<br>http://www.vmware.com/support/developer/vix-api<br>***Note** • For instructions, see VMware VIX API Requirement.* | The VMware VIX API is installed successfully. |

**Table 6 •** Configure Virtual Machines

| # | Step | Instructions | Result |
|---|---|---|---|
| **4.** | **Add a virtual machine to Automated Application Converter** | Open Automated Application Converter by clicking **Add Virtual Machines** on the **Set Up Infrastructure** tab of the AdminStudio Start page. The **Application Conversion Project Wizard** opens.<br>Cancel the wizard. Then open the **Machines** tab and follow the instructions in Adding Virtual Machines Using the Virtual Machine Import Wizard to add the prepared virtual machine to the **Machines** tab.<br>***Note*** *• When prompted, save the Automated Application Converter project file to the following directory:*<br>`C:\Users\YOURNAME\Documents\MyProject.aacx`<br>*All of the connection information for the virtual machine that you have set up is stored in the project file, so remember the name and location of your Automated Application Converter project file.* | A virtual machine is listed on the **Machines** tab of Automated Application Converter.<br><br>Untitled - Automated Application Converter<br>Machine \| Platform \| Purpose \| Path<br>Windows Vista - 32 bit \| Windows 7 (x86) \| Any \| [ha-datacenter/L...<br>Ready<br> File Edit View Tools Help<br>Machines<br>Packages<br>Results<br>Add Machine...<br>Remove Selected |

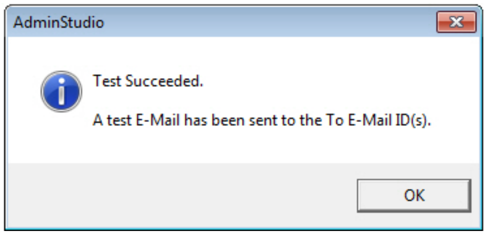
# Setting E-Mail Notification Settings

To enable AdminStudio to send you e-mail notifications during various processes, you need to configure your SMTP notification settings.

Currently, e-mail notifications are sent when soft time-outs are encountered while using Automated Application Converter to repackage an application on a virtual machine.

In this exercise, you will enter the SMTP settings for e-mail notifications. This enables AdminStudio to send notifications when a soft time out is encountered during repackaging on a virtual machine by Automated Application Converter.

**Table 7 •** Set E-Mail Notification Settings

| # | Step | Instructions | Result |
|---|---|---|---|
| **1.** | **Set SMTP Notification Settings** | On the **Notification Settings** tab of the AdminStudio **Options** dialog box, enter your SMTP settings for e-mail notifications.<br>***Note*** *• For instructions, see Setting E-Mail Notification Settings.* | When you click **Test** on the **Notifications Settings** tab, a successful message opens.<br><br>AdminStudio<br>Test Succeeded.<br>A test E-Mail has been sent to the To E-Mail ID(s).<br> |

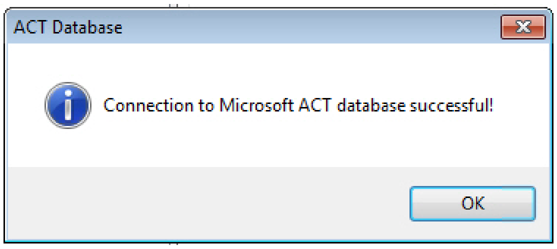
# Entering Server/Database Connection Settings

In AdminStudio 2018, you can define multiple named connections to System Center Configuration Manager, Citrix XenApp, Symantec Altiris Client Management Suite, Microsoft Server App-V, JAMF Casper Suite, and AirWatch distribution systems. This enables you to both have multiple connections easily available during import and distribution, and to refer to those connection settings by name in Platform API commands.

You need to specify at least one named connection to a distribution system in order for Application Manager to import packages, distribute applications, or report on application deployment status.

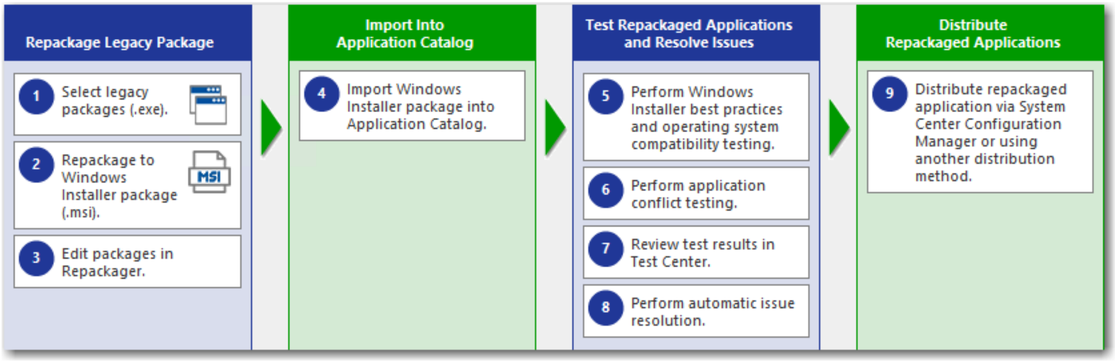
To enable AdminStudio to display data from your Microsoft ACT (Application Compatibility Toolkit) database in views and reports, you need to enter connection information for your Microsoft ACT database.

**Table 8 •** Enter Server Connection Settings

| # | Step | Instructions | Result |
|---|---|---|---|
| **1.** | **Enter System Center Configuration Manager connection settings** | Open the Application Manager **Options** dialog box, and on the **Distribution System** tab, create a named connection to System Center 2012 Configuration Manager.<br>***Note*** *• For instructions, see Creating a New Distribution System Connection Setting* | When you click **Test** on the **Distribution System** tab, the following message is displayed:<br>`Connection to ServerName Succeeded` |
| **2.** | **Entering Microsoft ACT database connection settings** | Open the Application Manager **Options** dialog box, and on the **Microsoft ACT** tab, enter Microsoft ACT database connection information.<br>***Note*** *• For instructions, see Entering Microsoft ACT Database Connection Settings*<br>***Note*** *• This is an optional step that you can perform if your organization has a Microsoft ACT database and you want to display that data in Application Manager.* | When you click **Test** on the **Microsoft ACT** tab, a successful message opens:<br><br>ACT Database<br>Connection to Microsoft ACT database successful!<br> |

# Migrating to Windows Installer

The flowchart on the **Migrate to Windows Installer** tab of the AdminStudio Start page lists the steps you need to perform to migrate a sample setup (such as an `.exe` file) to a deployable Windows Installer package.



Repackage Legacy Package

1 Select legacy packages (.exe).

2 Repackage to Windows Installer package (.msi).

3 Edit packages in Repackager.

Import Into Application Catalog

4 Import Windows Installer package into Application Catalog.

Test Repackaged Applications and Resolve Issues

5 Perform Windows Installer best practices and operating system compatibility testing.

6 Perform application conflict testing.

7 Review test results in Test Center.

8 Perform automatic issue resolution.

Distribute Repackaged Applications

9 Distribute repackaged application via System Center Configuration Manager or using another distribution method.

**Figure 26:** Migrate to Windows Installer Tab of AdminStudio Start Page

In this section, you will convert a sample setup named `SampleApplicationSetup.exe` to a Windows Installer Package, import it into the Application Catalog, test it for best practices, operating system compatibility, and application conflicts, and then prepare it for distribution using Distribution Wizard.

***Important*** • *It is preferable to repackage 32-bit applications on 32-bit operating systems. In this exercise, we will be repackaging a 32-bit application.*

To migrate a sample application to a Windows Installer package, perform the following steps:

- Repackaging a Sample Package
- Importing Packages into the Application Catalog
- Testing a Repackaged Application and Resolving Issues

# Repackaging a Sample Package

In this procedure, you will repackage a sample setup, perform some minor edits in Repackager, and then build a Windows Installer package.

**Table 9** • Repackage a Sample Package

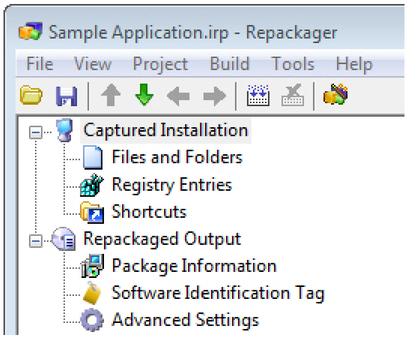
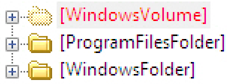
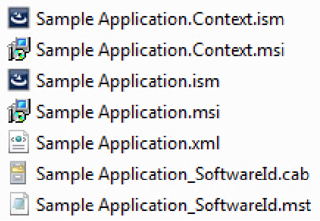
| # | Step | Instructions | Result |
|---|---|---|---|
| **1.**<br>**2.** | **Select and repackage a sample package (.exe) to a Windows Installer Package (.msi)** | Use Repackaging Wizard (**Installation Monitoring** method) to repackage the following sample setup:<br>`C:\AS2018EvalGuideDataFiles\`<br>`SampleApplicationSetup\`<br>`SampleApplicationSetup.exe`<br>***Important*** • *It is recommended that you repackage this sample package on a clean machine.*<br>Save the captured data in the following directory:<br>`C:\Packages`<br>***Note*** • *For instructions, see Repackaging Using the Installation Monitoring Method.* | The captured data was converted into a Repackager project file (`SampleApplication.irp`) and opened in the Repackager interface.<br> Sample Application.irp - Repackager<br>File View Project Build Tools Help<br>Captured Installation<br>Files and Folders<br>Registry Entries<br>Shortcuts<br>Repackaged Output<br>Package Information<br>Software Identification Tag<br>Advanced Settings |

**Table 9 •** Repackage a Sample Package

| # | Step | Instructions | Result |
|---|---|---|---|
| **3.** | **Edit package in Repackager and build Windows Installer package** | To exclude files that are not part of the package, open the **Files and Folders** view, right-click on the **[WindowsVolume]** folder and select **Exclude All** from the context menu. Click **Save**.<br>***Note** • For instructions, see Excluding All Files in a Directory.* | The **[WindowsVolume]** folder is displayed in red to indicate that it is excluded:<br><br>[WindowsVolume]<br>[ProgramFilesFolder]<br>[WindowsFolder] |
| | | Open the **Repackaged Output** view and click **Build** to build a Windows Installer package.<br>***Note** • For instructions, see Building a Windows Installer Package.* | The Repackager project file has been converted to a Windows Installer package, located in the following directory:<br>`C:\Packages\MSI_Package\SampleApplication.msi` |
| | | Copy all of the files in the `C:\Packages\MSI_Package` directory (including the `SampleApplication.msi` file) to the following directory on the machine where AdminStudio is installed:<br>`C:\AS2018EvalGuideDataFiles\SampleApplicationSetup\` | New Windows Installer package (and other associated files) are now in the same main directory as the other evaluation data files.<br><br>Sample Application.Context.ism<br>Sample Application.Context.msi<br>Sample Application.ism<br>Sample Application.msi<br>Sample Application.xml<br>Sample Application_SoftwareId.cab<br>Sample Application_SoftwareId.mst |

# Importing Packages into the Application Catalog

In this procedure, you will import Windows Installer packages into the Application Catalog, including the one you created in Repackaging a Sample Package:

**Table 10 •** Import Into Application Catalog

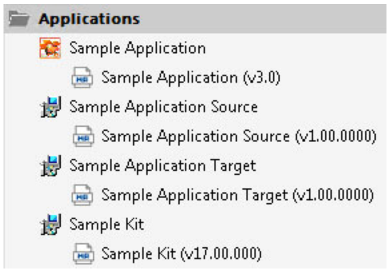
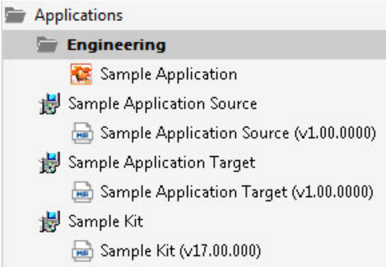
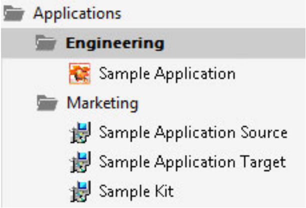
| # | Step | Instructions | Result |
|---|---|---|---|
| **4.** | **Import Windows Installer package into Application Catalog** | Before beginning import, open the Application Manager **Options** dialog box and clear the selection of the **Automatically Execute Tests After Import** option.<br>Next, use the Import Wizard to import all of the packages in the `AS2018EvalGuideDataFiles` directory.<br>● On the **Source** panel, select **Folder of multiple applications**.<br>● On the **Package Type Selection** panel, select the **Microsoft Windows Installer package (.msi)** option<br>● On the **Package Folder Selection** panel, select the `C:\AS2018EvalGuideDataFiles` directory.<br>● On the **Select Applications** panel, leave all of the applications selected.<br>● On the **Destination Group** panel, select the **Applications** folder in the tree. Do not select the **Create subgroups based on source folder structure** option.<br>***Note** • For instructions on how to import a directory of packages into the Application Catalog, see Importing a Folder of Multiple Packages.* | The packages are now listed in the Application Manager tree, each under its own Application node:<br><br>**Applications**<br>Sample Application<br>Sample Application (v3.0)<br>Sample Application Source<br>Sample Application Source (v1.00.0000)<br>Sample Application Target<br>Sample Application Target (v1.00.0000)<br>Sample Kit<br>Sample Kit (v17.00.000) |

**Table 10** • Import Into Application Catalog

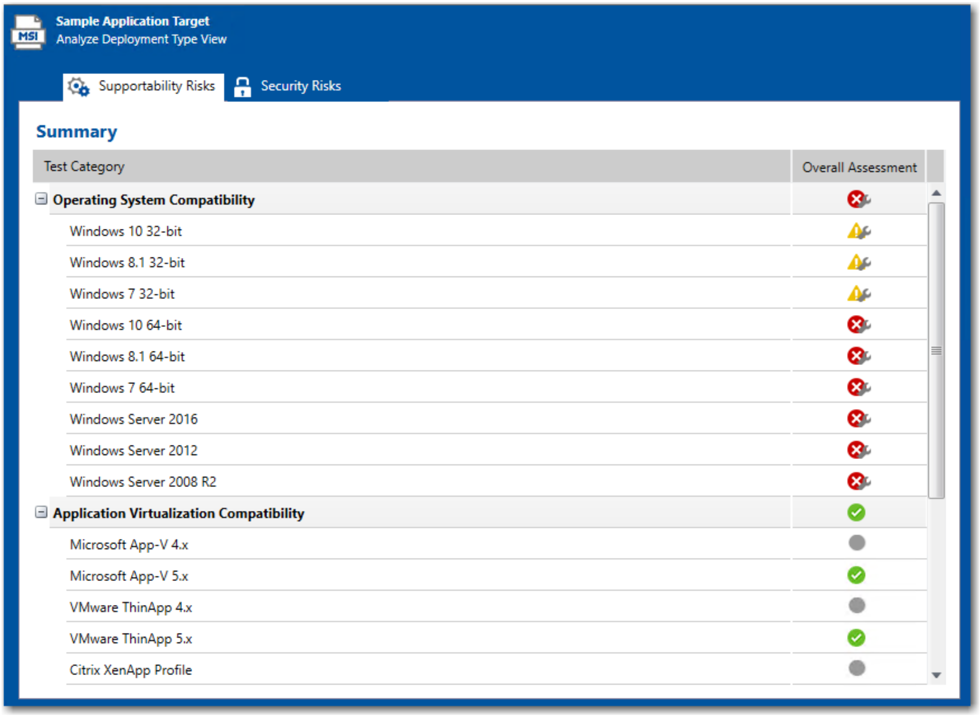
| # | Step | Instructions | Result |
|---|---|---|---|
| **4.** | **Import Windows Installer package into Application Catalog**<br>**(Continued)** | Create a new group in the Application Manager tree named `Engineering` and move the **Sample Application** into that new group.<br>***Note*** • *For instructions, see Adding Groups and Organizing Applications in Application Manager.* | The Application Manager tree should now be organized as follows:<br><br>Applications<br>**Engineering**<br>Sample Application<br>Sample Application Source<br>Sample Application Source (v1.00.0000)<br>Sample Application Target<br>Sample Application Target (v1.00.0000)<br>Sample Kit<br>Sample Kit (v17.00.000) |
| | | Create another new group in the Application Manager tree named `Marketing`, and move the other three applications into that group. | The Application Manager tree should now be organized as follows:<br><br>Applications<br>**Engineering**<br>Sample Application<br>Marketing<br>Sample Application Source<br>Sample Application Target<br>Sample Kit |

# Testing a Repackaged Application and Resolving Issues

In this procedure, you will test the Windows Installer packages you imported into the Application Catalog, and then distribute a package to a network location.

**Table 11 •** Test and Distribute Repackaged Applications

| # | Step | Instructions | Results |
|---|---|---|---|
| **5.** | **Perform Windows Installer best practices and OS compatibility testing** | To perform Windows Installer best practices and operating system compatibility testing on all of the packages in the Application Catalog, first select the **Analyze** tab in the Application Manager ribbon. Then, select the **Applications** group in the Application Manager tree, and click **Execute Tests**.<br>***Note •*** *For more information, see Performing Compatibility and Best Practices Testing.*<br>When testing is finished, view the test results by selecting a Windows Installer package in the tree to open the **Summary** view on the **Supportability Risks** tab of the **Analyze Deployment Type View**, as shown below: | |



Sample Application Target
Analyze Deployment Type View

Summary

| 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** | ✓ |
| Microsoft App-V 4.x | ● |
| Microsoft App-V 5.x | ✓ |
| VMware ThinApp 4.x | ● |
| VMware ThinApp 5.x | ✓ |
| Citrix XenApp Profile | ● |

| | | | |
|---|---|---|---|
| | | On **Analyze** tab views, groups, applications, and packages are assigned a test status in each test group using status icons. For packages, the status icon identifies that package's test status (as described in About Status Icons). For groups and applications, Application Manager considers all of the packages in that group or application, and displays the status icon for the package that has the status at the highest hierarchical level, as described in the **Hierarchical Level of Status Icons** section of the About Status Icons help topic.<br>***Note •*** *For more information, see Viewing Summary Test Results.* | |

**Table 11 •** Test and Distribute Repackaged Applications

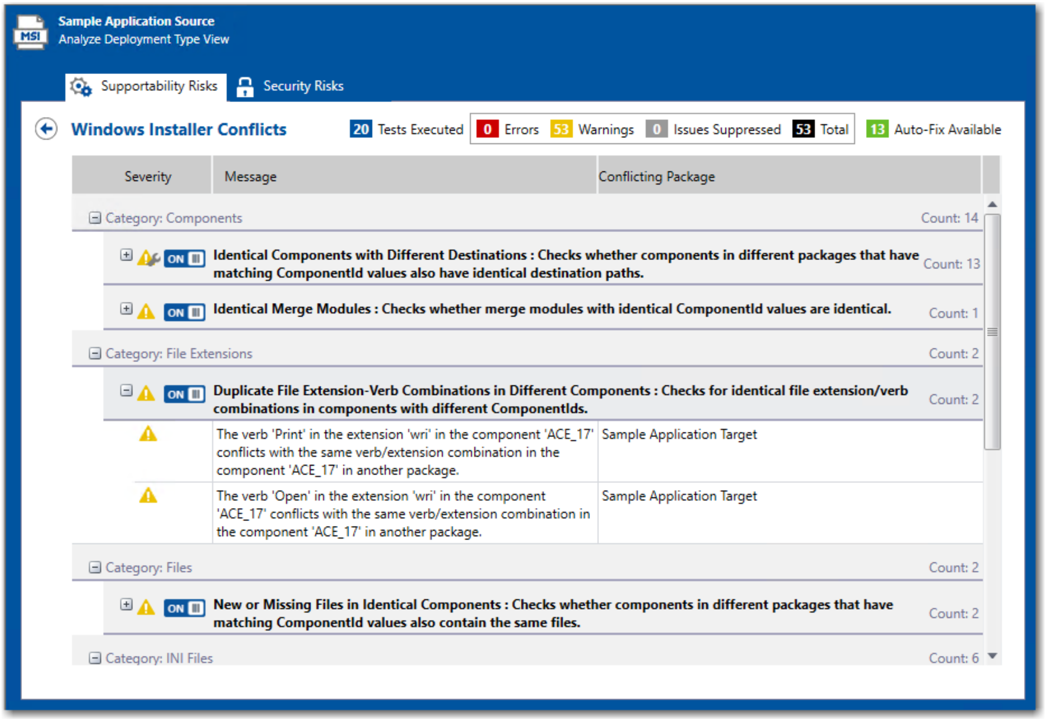
<table>
<tr><th>#</th><th>Step</th><th>Instructions</th><th>Results</th></tr>
<tr><td>6.</td><td>**Perform application conflict testing**</td><td colspan="2">Use the Conflict Wizard to detect conflicts between the following two packages:<br>- **Source**: Sample Application Source<br>- **Target**: Sample Application Target<br>***Note •*** *For instructions, see Testing for Conflicts Between Packages.*</td></tr>
<tr><td>7.</td><td>**Review test results**</td><td colspan="2">When application conflict testing is finished, view the test results by selecting the Sample Application Source MSI package in the tree, and then clicking on **Windows Installer Conflicts** under **Application Conflicts** on the **Supportability Risks** tab of the **Analyze Deployment Type View**. Errors and warnings are listed. Click the plus sign next to a test name to view individual error/warning messages for that package:<br><br>Sample Application Source<br>Analyze Deployment Type View<br> <br>Windows Installer Conflicts<br>20 Tests Executed | 0 Errors | 53 Warnings | 0 Issues Suppressed | 53 Total | 13 Auto-Fix Available
<table>
<tr><th>Severity</th><th>Message</th><th>Conflicting Package</th></tr>
<tr><td>⊟ Category: Components</td><td></td><td>Count: 14</td></tr>
<tr><td>⊞ ⚠ ON</td><td>Identical Components with Different Destinations : Checks whether components in different packages that have matching ComponentId values also have identical destination paths.</td><td>Count: 13</td></tr>
<tr><td>⊞ ⚠ ON</td><td>Identical Merge Modules : Checks whether merge modules with identical ComponentId values are identical.</td><td>Count: 1</td></tr>
<tr><td>⊟ Category: File Extensions</td><td></td><td>Count: 2</td></tr>
<tr><td>⊟ ⚠ ON</td><td>Duplicate File Extension-Verb Combinations in Different Components : Checks for identical file extension/verb combinations in components with different ComponentIds.</td><td>Count: 2</td></tr>
<tr><td>⚠</td><td>The verb 'Print' in the extension 'wri' in the component 'ACE_17' conflicts with the same verb/extension combination in the component 'ACE_17' in another package.</td><td>Sample Application Target</td></tr>
<tr><td>⚠</td><td>The verb 'Open' in the extension 'wri' in the component 'ACE_17' conflicts with the same verb/extension combination in the component 'ACE_17' in another package.</td><td>Sample Application Target</td></tr>
<tr><td>⊟ Category: Files</td><td></td><td>Count: 2</td></tr>
<tr><td>⊞ ⚠ ON</td><td>New or Missing Files in Identical Components : Checks whether components in different packages that have matching ComponentId values also contain the same files.</td><td>Count: 2</td></tr>
<tr><td>⊟ Category: INI Files</td><td></td><td>Count: 6</td></tr>
</table>
Next, click the suppress (ON/OFF) button next to the **Identical Merge Modules** error to suppress that test from test totals and from automatic resolution. The button toggles to the OFF position and the error icon turns to gray.<br>***Note •*** *For more information, see the following topics:*<br>- *Viewing Detailed Package Test Results*<br>- *Viewing Application Conflicts Test Results*<br>- *Filtering Test Results by Suppressing Errors/Warnings*</td></tr>
</table>

**Table 11 •** Test and Distribute Repackaged Applications

| # | Step | Instructions | Results |
|---|---|---|---|
| **8.** | **Perform automatic issue resolution** | Issues for which automatic fixes are available are identified by the Error With Fix or Warning With Fix icon:<br>❌ ⚠<br>To automatically resolve all issues for which automatic fixes are available, select the **Applications** group node in the tree and click **Resolve Issues** on the **Analyze** tab of the ribbon.<br>***Note*** *• For more information, see Performing Automatic Issue Resolution.* | Issue resolution begins, progress messages appear in the Output window, and Application Manager performs the following tasks:<br>● **Reruns tests**—Application Manager reruns all of the selected tests to ensure that the issues that it is going to resolve still exist in the current version of the package and its associated transforms.<br>● **Creates transform files**—To resolve issues, Application Manager generates fix transform files.<br>● **Reimports packages**—Application Manager then automatically reimports each package and its fix transform files into the Application Catalog.<br>When issue resolution and reimporting is complete, look at the **Analyze Group View**, **Application View**, or **Deployment Type View** of the package, application, or group that you tested. You will see that the Error With Fix and Warning With Fix icons have been replaced with the status icon with the next highest level (as described in the **Hierarchical Level of Status Icons** section of the About Status Icons help topic) in that test category. |

# Distributing a Repackaged Application

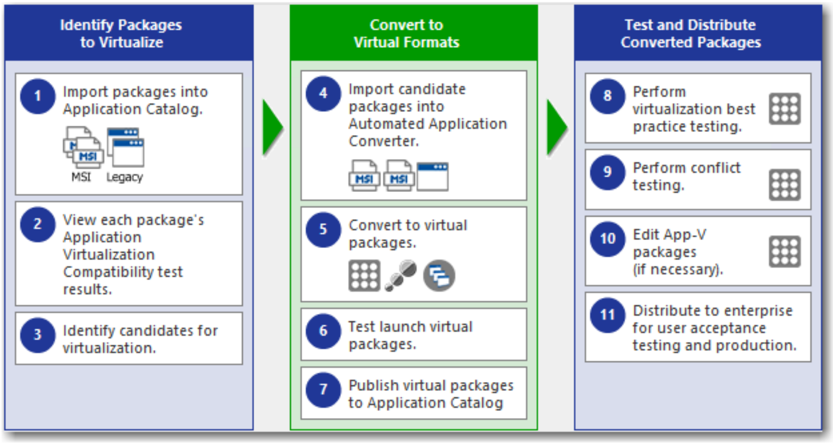
In this procedure, you will distribute a Windows Installer package to a network location.

**Table 12 •** Distribute a Repackaged Application

| # | Step | Instructions | Results |
|---|---|---|---|
| **9.** | **Distribute repackaged application** | Use the Legacy Distribution Wizard to distribute the **Sample Application** Windows Installer package to a **Network** location. You open the Legacy Distribution Wizard by opening the **Home** tab of the ribbon, selecting the Windows Installer package node and then selecting **Distribute Package** from the context menu.<br>For instructions on how to distribute a package to a network location, see Distributing Packages to Network Locations.<br>***Note •*** *To distribute an **application** to a System Center 2012 Configuration Manager, Citrix XenApp, Symantec Altiris, JAMF Casper Suite, or AirWatch, select the application node in the tree and then click the **Distribute** button in the ribbon. You must have already set up a named connection to that distribution system on the **Options** dialog box.*<br>***Note •*** *You can publish applications containing App-V 4.x packages and Citrix XenApp profiles to Citrix XenApp server, and can publish applications containing Windows Installer, Symantec Workspace, VMware ThinApp, or legacy installers to Symantec Altiris server.*<br>*If an application contains a package of an unsupported deployment type, that package will be ignored.* | `SampleApplication.msi` is copied to the specified network location, making it available to your enterprise. |

# Migrating to Application Virtualization

The flowchart on the **Migrate to Application Virtualization** tab of the AdminStudio Start page lists the steps you need to perform to migrate your application portfolio into virtual applications that are ready for deployment within the enterprise.



**Identify Packages to Virtualize**

1 Import packages into Application Catalog.

2 View each package's Application Virtualization Compatibility test results.

3 Identify candidates for virtualization.

**Convert to Virtual Formats**

4 Import candidate packages into Automated Application Converter.

5 Convert to virtual packages.

6 Test launch virtual packages.

7 Publish virtual packages to Application Catalog

**Test and Distribute Converted Packages**

8 Perform virtualization best practice testing.

9 Perform conflict testing.

10 Edit App-V packages (if necessary).

11 Distribute to enterprise for user acceptance testing and production.

**Figure 27:** Migrate to Application Virtualization Tab of AdminStudio Start Page

In this section, you will use the Automated Application Converter to convert Windows Installer packages to virtual packages, and then test and distribute the virtual packages.

To migrate your application portfolio into virtual applications, perform the following steps:

- Identifying Packages to Virtualize
- Converting to Virtual Formats
- Testing and Distributing Converted Packages

# Identifying Packages to Virtualize

In this procedure, you will import packages into the Application Catalog and identify the packages you want to virtualize.

**Table 13 •** Identify Packages to Virtualize

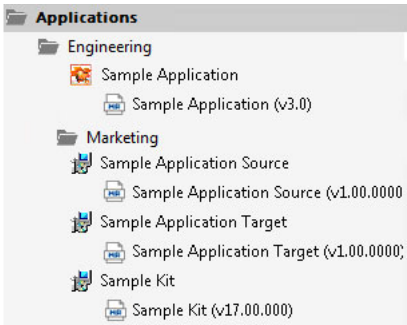
| # | Step | Instructions | Results |
|---|---|---|---|
| 1. | **Import packages into Application Catalog.** | Open Application Manager and locate the packages that you imported in Importing Packages into the Application Catalog. | The four Windows Installer packages are listed in the Application Manager tree:<br><br>Applications<br>Engineering<br>Sample Application<br>Sample Application (v3.0)<br>Marketing<br>Sample Application Source<br>Sample Application Source (v1.00.0000<br>Sample Application Target<br>Sample Application Target (v1.00.0000)<br>Sample Kit<br>Sample Kit (v17.00.000) |

**Table 13 •** Identify Packages to Virtualize

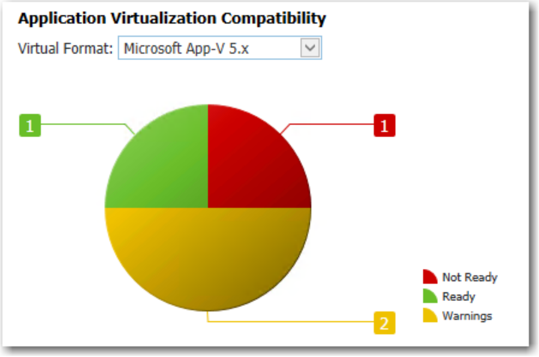
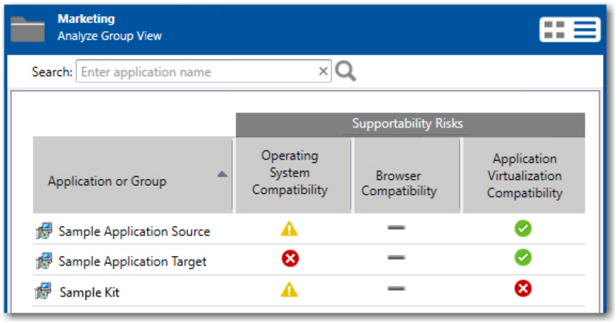
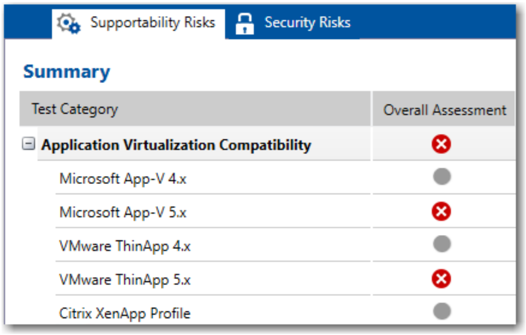
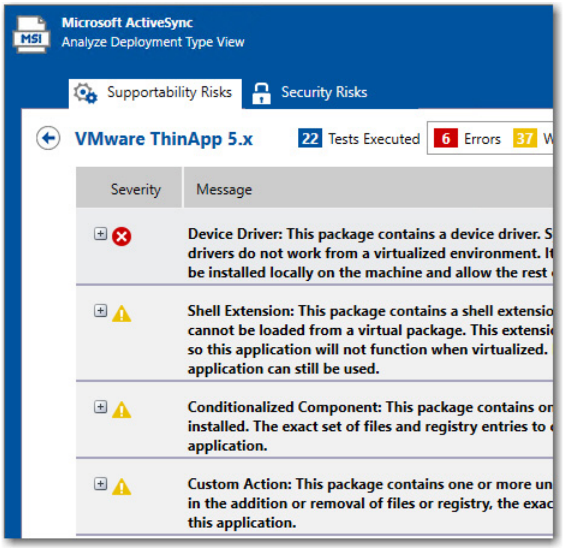
| # | Step | Instructions | Results |
|---|---|---|---|
| **2.** | **View package's Application Virtualization Compatibility test results.** | To view application virtualization compatibility test results, open the **Analyze** tab, and then select a group in the tree to open the **Analyze Group View**. | The packages' application virtualization compatibility test results are listed in both chart and list view. The following is the chart view:<br><br>Application Virtualization Compatibility<br>Virtual Format: Microsoft App-V 5.x<br> <br>Test results are also shown in the **Application Virtualization Compatibility** column under **Supportability Risks** on the **Analyze Group View**.<br><br>Marketing<br>Analyze Group View<br>Search: Enter application name<br>Application or Group \| Supportability Risks: Operating System Compatibility \| Browser Compatibility \| Application Virtualization Compatibility<br>Sample Application Source \| ⚠ \| — \| ✓<br>Sample Application Target \| ✗ \| — \| ✓<br>Sample Kit \| ⚠ \| — \| ✗<br>You can switch between chart and list view of clicking the toggle button in the top right corner of the view. |

**Table 13 •** Identify Packages to Virtualize

<table>
<tr><th>#</th><th>Step</th><th>Instructions</th><th>Results</th></tr>
<tr>
<td>3.</td>
<td><b>Identify candidates for virtualization.</b></td>
<td>You will notice that in the <b>Application Virtualization Compatibility</b> column, two of the packages have a Ready status (Sample Application Source and Sample Application Target), while the other has an Error status (Sample Kit).<br>Therefore, for the package with the error status, select the deployment type icon in the tree to open the Summary view, and then click on the error status icon under <b>Application Virtualization Compatibility</b> next to the unsupported virtualization type.</td>
<td>This <b>Summary</b> view lists the virtualization formats that generated the error:


Summary
<table>
<tr><th>Test Category</th><th>Overall Assessment</th></tr>
<tr><td>⊟ Application Virtualization Compatibility</td><td>☒</td></tr>
<tr><td>Microsoft App-V 4.x</td><td>●</td></tr>
<tr><td>Microsoft App-V 5.x</td><td>☒</td></tr>
<tr><td>VMware ThinApp 4.x</td><td>●</td></tr>
<tr><td>VMware ThinApp 5.x</td><td>☒</td></tr>
<tr><td>Citrix XenApp Profile</td><td>●</td></tr>
</table>
If you click on the error icon in the <b>Overall Assessment</b> column, you will see the details of the error:


Microsoft ActiveSync<br>Analyze Deployment Type View<br>VMware ThinApp 5.x<br>22 Tests Executed 6 Errors 37 W
<table>
<tr><th>Severity</th><th>Message</th></tr>
<tr><td>⊞ ☒</td><td>Device Driver: This package contains a device driver. S drivers do not work from a virtualized environment. It be installed locally on the machine and allow the rest</td></tr>
<tr><td>⊞ ⚠</td><td>Shell Extension: This package contains a shell extensio cannot be loaded from a virtual package. This extensi so this application will not function when virtualized. application can still be used.</td></tr>
<tr><td>⊞ ⚠</td><td>Conditionalized Component: This package contains or installed. The exact set of files and registry entries to application.</td></tr>
<tr><td>⊞ ⚠</td><td>Custom Action: This package contains one or more un in the addition or removal of files or registry, the exac this application.</td></tr>
</table>
</td>
</tr>
</table>

# Converting to Virtual Formats

In this procedure, you will use Automated Application Converter to convert Windows Installer packages to App-V packages.

**Table 14 •** Convert to Virtual Formats

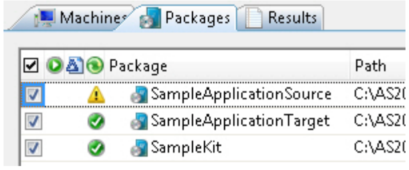
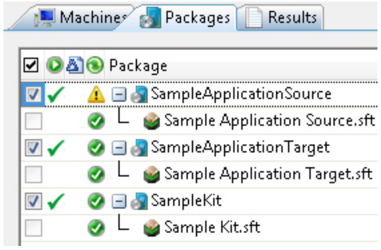
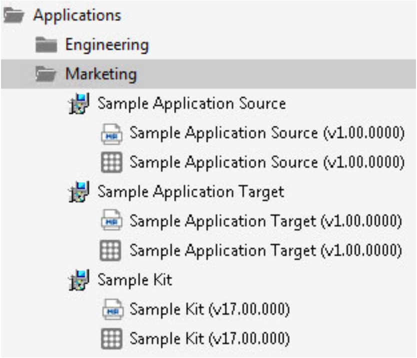
| # | Step | Instructions | Results |
|---|---|---|---|
| **4.** | **Import candidate packages into Automated Application Converter.** | Open Automated Application Converter, open the existing project you created in Configuring a Virtual Machine, and use the **Package Import Wizard** to add the packages that you identified in Identifying Packages to Virtualize.<br>***Note*** • *For instructions, see Selecting Packages from an AdminStudio Application Catalog.* | Packages are listed on the **Packages** tab.<br><br> <br>☑ Package — Path<br>☑ SampleApplicationSource — C:\AS2<br>☑ SampleApplicationTarget — C:\AS2<br>☑ SampleKit — C:\AS2 |
| **5.** | **Convert to virtual packages.** | First. open the **Project Options** dialog box and make sure that the **Package Creation** property is set to **App-V 4.6 with AdminStudio**.<br>Then, use the Application Conversion Wizard to convert the packages to App-V 4.x applications.<br>***Note*** • *For instructions, see Performing a Conversion Using the Application Conversion Wizard.*<br>***Important*** • *Make sure that you have already performed the steps in Configuring a Virtual Machine before beginning this step.* | When conversion is complete, each virtual package is listed in a tree structure under its original package on the **Packages** tab.<br><br> <br>☑ Package<br>☑ ✓ SampleApplicationSource<br>□ └ Sample Application Source.sft<br>☑ ✓ SampleApplicationTarget<br>□ └ Sample Application Target.sft<br>☑ ✓ SampleKit<br>□ └ Sample Kit.sft |
| **6.** | **Test launch virtual packages.** | Test the virtual packages by launching them on a virtual machine.<br>***Note*** • *For instructions, see Performing Automated Testing of App-V Packages.* | Virtual packages launch successfully. |

**Table 14** • Convert to Virtual Formats

| # | Step | Instructions | Results |
|---|---|---|---|
| **7.** | **Publish virtual packages to Application Catalog.** | Import the new virtual packages into the Application Catalog.<br>***Note*** • *For instructions, see Importing a Single Package File.* | The virtual packages are listed in the Application Manager tree under their associated Application.<br><br>Applications<br>Engineering<br>Marketing<br>Sample Application Source<br>Sample Application Source (v1.00.0000)<br>Sample Application Source (v1.00.0000)<br>Sample Application Target<br>Sample Application Target (v1.00.0000)<br>Sample Application Target (v1.00.0000)<br>Sample Kit<br>Sample Kit (v17.00.000)<br>Sample Kit (v17.00.000)<br>***Note*** • *You may need to click Ctrl + R to refresh the Application Catalog tree.* |

# Testing and Distributing Converted Packages

In this procedure, you will validate the converted packages, perform conflict analysis against other packages, resolve any issues found, and distribute the packages.

**Table 15** • Test and Distribute Converted Packages

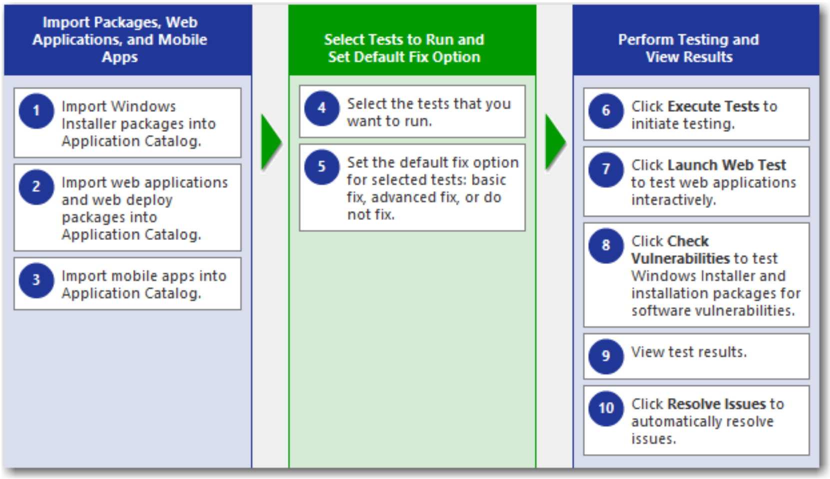
| # | Step | Instructions | Results |
|---|---|---|---|
| **8.** | **Perform virtualization best practices testing.** | By default, App-V best practices testing is performed during import (as described in Import Options). To perform this testing manually, first select the **Analyze** tab in the Application Manager ribbon. Then, select one of the App-V packages in the Application Manager tree, and click **Execute Tests**.<br>Messages appear in the Output Window.<br>***Note*** • *For more information, see Performing Compatibility, Best Practices, and Risk Assessment Testing.* | When testing is complete, results are displayed on the **Summary** tab of the **Analyze Deployment Type View**. |

**Table 15 •** Test and Distribute Converted Packages

| # | Step | Instructions | Results |
|---|---|---|---|
| **9.** | **Perform conflict testing.** | In Application Manager, perform conflict testing of the **Sample Application Source** App-V package against the **Sample Application Target** App-V package.<br>***Note •*** *For instructions, see Testing for Conflicts Between Packages.* | Conflict analysis results are listed in the **Output** window and in the **Conflicts** view. An error is detected:<br>`Package ‘Sample Application Source’ has a conflicting root Directory ‘SampleAp.100’ with package ‘Sample Application Target’.` |
| **10.** | **Edit App-V packages (if necessary).** | To resolve the error that was found during testing on **Sample Application Source** App-V package, select it on the **Home** tab of the Application Manager tree and select **Edit with Virtual Package Editor**.<br>In the Virtual Package Editor’s **General Information** view, change the **Root Folder Name** property to **`SampleAp.200`** and click **Save**.<br>***Note •*** *For instructions, see Using the Virtual Package Editor.*<br>Return to Application Manager and reimport the edited package. | The edited App-V package is imported into the Application Catalog.<br>***Note •*** *When you rerun the conflict testing that you ran in the previous step, no error will be generated.* |
| **11.** | **Distribute to enterprise for user acceptance testing and production.** | Distribute this tested App-V package to a **Network** location.<br>***Note •*** *For instructions on how to distribute a package, see Distributing Packages to Network Locations.*<br>***Tip •*** *Distribution Wizard also supports deploying applications to System Center Configuration Manager (Current Branch), System Center 2012 Configuration Manager, System Center 2007 Configuration Manager, Citrix XenApp Server, JAMF Casper Suite, AirWatch Server, Microsoft App-V Server, and Symantec Altiris distribution systems. For more information, see Distributing Applications.* | The selected App-V package is copied to the specified network location, making it available to your enterprise. |

# Testing for Application Compatibility

The flowchart on the **Test for Application Compatibility** tab of the AdminStudio Start page outlines how to use Application Manager to test packages for compatibility with the latest versions of Windows and Windows Server operating systems, as well as to test web applications for compatibility with Internet Explorer 11 and Microsoft Edge.



**Import Packages, Web Applications, and Mobile Apps**

1 Import Windows Installer packages into Application Catalog.

2 Import web applications and web deploy packages into Application Catalog.

3 Import mobile apps into Application Catalog.

**Select Tests to Run and Set Default Fix Option**

4 Select the tests that you want to run.

5 Set the default fix option for selected tests: basic fix, advanced fix, or do not fix.

**Perform Testing and View Results**

6 Click **Execute Tests** to initiate testing.

7 Click **Launch Web Test** to test web applications interactively.

8 Click **Check Vulnerabilities** to test Windows Installer and installation packages for software vulnerabilities.

9 View test results.

10 Click **Resolve Issues** to automatically resolve issues.

**Figure 28:** Test for Application Compatibility Tab of AdminStudio Start Page

In this section, you will test some packages for operating system compatibility fix issues that were found. You will also test web applications, both statically and dynamically.

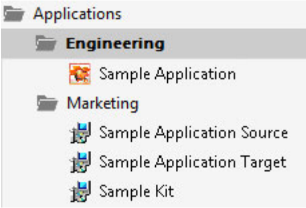
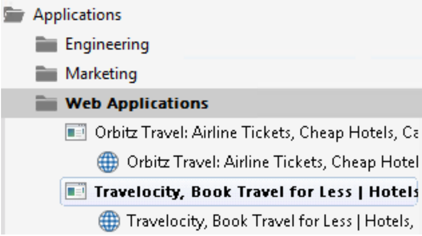
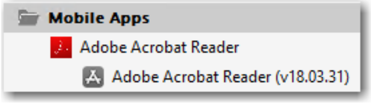
To perform application compatibility testing, perform the following steps:

- Importing Packages, Web Applications, and Mobile Apps
- Selecting Tests to Run and Setting Default Fix Option
- Performing Testing and Viewing Results

# Importing Packages, Web Applications, and Mobile Apps

In this procedure, you will load the packages to test and select the reports to run.

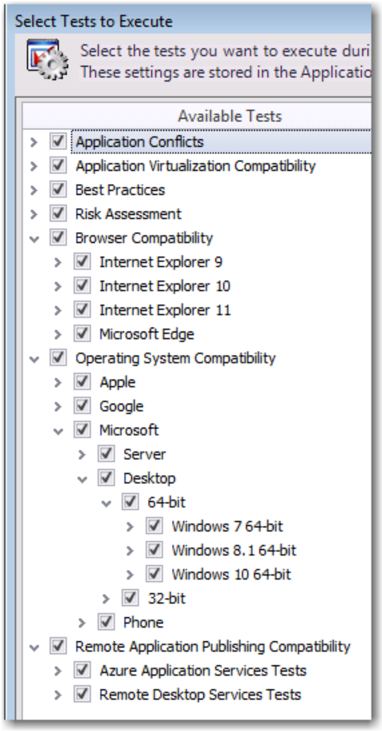
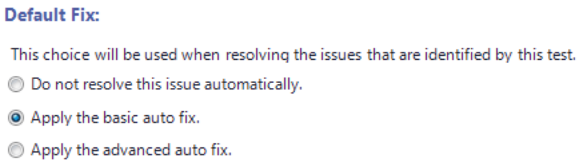
**Table 16 •** Importing Packages and Web Applications

| # | Step | Instructions | Result |
|---|---|---|---|
| **1.** | **Import Windows Installer packages into Application Catalog.** | For this exercise, we will test Windows Installer packages that were imported into the Application Catalog earlier in this guide in Importing Packages into the Application Catalog.<br>***Note •*** *For instructions on how to import a directory of packages into the Application Catalog, see Importing a Folder of Multiple Packages.* | The Application Manager tree should now be organized as follows:<br><br>Applications<br>**Engineering**<br>Sample Application<br>Marketing<br>Sample Application Source<br>Sample Application Target<br>Sample Kit |
| **2.** | **Import web applications into Application Catalog.** | First, open the **Import Options > General** tab of the Application Manager **Options** dialog box, and clear the selection of the **Automatically Execute Tests After Import** option.<br>Next, create a new group in the Application Manager tree named **Web Applications**.<br>Then import the following web applications into the **Web Applications** folder, as described in Importing a Deployed Web Applications.<br>● **Orbitz** at: http://www.orbitz.com<br>● **Travelocity** at: http://www.travelocity.com<br>Because these web applications do not require a login to access, leave the **User name** and **Password** fields on the **Web Site Details** panel blank. | The web applications are listed in the Application Manager tree:<br><br>Applications<br>Engineering<br>Marketing<br>**Web Applications**<br>Orbitz Travel: Airline Tickets, Cheap Hotels, Ca<br>Orbitz Travel: Airline Tickets, Cheap Hotel<br>**Travelocity, Book Travel for Less \| Hotels**<br>Travelocity, Book Travel for Less \| Hotels, |
| **3.** | **Import a mobile app into the Application Catalog** | Create a new group in the Application Manager tree named **Mobile Apps**.<br>Then, import an Apple iOS mobile app from the Apple App Store, as described in Importing Public Store Mobile Apps. | The iOS public store mobile app is listed in the Application Manager tree.<br><br>**Mobile Apps**<br>Adobe Acrobat Reader<br>Adobe Acrobat Reader (v18.03.31) |

# Selecting Tests to Run and Setting Default Fix Option

In this procedure, you will select the Operating System Compatibility and Browser Compatibility tests to run and set default fix options.

**Table 17 •** Selecting Tests to Run and Setting Default Fix Option

| # | Step | Instructions | Result |
|---|---|---|---|
| **4.** | **Select the operating system and browser compatibility tests that you want to run.** | Select the **Operating System Compatibility** and **Browser Compatibility** tests that you want to run, as described in Selecting Tests to Execute.<br>***Tip*** *• To speed up testing, it is recommended that you select just the operating systems and browser versions that are being used in your organization.* | The **Operating System Compatibility** and **Browser Compatibility** tests that you want to run are selected on the **Select Tests to Execute** dialog box.<br><br>Select Tests to Execute<br>Select the tests you want to execute duri<br>These settings are stored in the Applicatio<br>Available Tests<br>☑ Application Conflicts<br>☑ Application Virtualization Compatibility<br>☑ Best Practices<br>☑ Risk Assessment<br>☑ Browser Compatibility<br>☑ Internet Explorer 9<br>☑ Internet Explorer 10<br>☑ Internet Explorer 11<br>☑ Microsoft Edge<br>☑ Operating System Compatibility<br>☑ Apple<br>☑ Google<br>☑ Microsoft<br>☑ Server<br>☑ Desktop<br>☑ 64-bit<br>☑ Windows 7 64-bit<br>☑ Windows 8.1 64-bit<br>☑ Windows 10 64-bit<br>☑ 32-bit<br>☑ Phone<br>☑ Remote Application Publishing Compatibility<br>☑ Azure Application Services Tests<br>☑ Remote Desktop Services Tests |
| **5.** | **Set the default fix option for selected tests: basic fix, advanced fix, or do not fix.** | Some of the tests in the **Operating System Compatibility** and **Browser Compatibility** test group let you specify whether to perform a basic or advanced fix when you automatically resolve issues, as described in Setting Automatic Fix Preferences for Operating System Compatibility and Browser Compatibility Tests.<br>On the **Select Tests to Execute** dialog box, review the **Default Fix** section of several of your selected tests. For this exercise, it is not necessary to make any changes to the **Default Fix** settings. | A **Default Fix** selection is made for all **Operating System Compatibility** and **Browser Compatibility** tests.<br><br>**Default Fix:**<br>This choice will be used when resolving the issues that are identified by this test.<br>○ Do not resolve this issue automatically.<br>● Apply the basic auto fix.<br>○ Apply the advanced auto fix. |

# Performing Testing and Viewing Results

In this procedure, you will test packages and web applications for operating system and browser compatibility, view test results, and automatically fix issues.

**Table 18 •** Performing Testing and Viewing Results

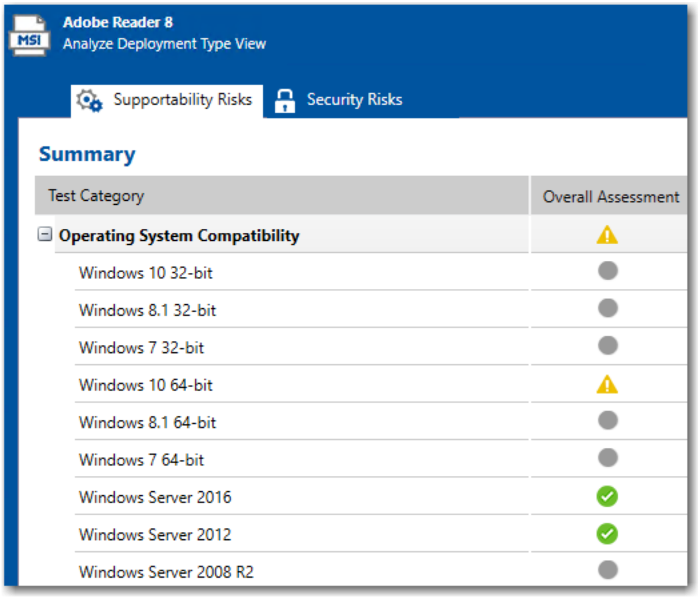
| # | Step | Instructions | Result |
|---|---|---|---|
| **6.** | **Click Execute Tests to test Windows Installer packages, mobile apps, and web applications (statically).** | First select the **Analyze** tab in the Application Manager ribbon<br>Then, select the **Applications** group in the Application Manager tree, and click **Execute Tests**.<br>***Note •*** *For more information, see Performing Compatibility, Best Practices, and Risk Assessment Testing.* | Messages are listed in the Output Window. When testing is complete, the following message is displayed:<br>`Testing finished at: Monday, April 23, 2018 - 13:47:04`<br>`Tested 6 packages of 6.` |

**Table 18** • Performing Testing and Viewing Results

| # | Step | Instructions | Result |
|---|---|---|---|
| 7. | **Click Launch Web Test to test web applications interactively.** | To interactively, dynamically test a web application, select a web application node in the tree and click **Launch Web Test**.<br>***Note*** • *For more information, see Performing Dynamic Testing of Web Applications.*<br>Application Manager launches the web application in your browser. Then, as you perform tasks and navigate around the web application, Application Manager records any warnings or errors that are encountered while using that version of the browser.<br>When you have finished testing, close the browser window.<br>***Tip*** • *You should always use dynamic testing when a web application requires a login to access.*<br>***Tip*** • *As each page loads, Application Manager begins testing. Links on each page do not become active until testing is complete on that page, so you may have to wait several seconds before proceeding.* | Messages are listed in the Output Window. When testing is complete, the following message is displayed:<br>`Testing finished at: Monday, April 23, 2018 - 13:58:08`<br>`Completed testing package(s).` |

**Table 18 •** Performing Testing and Viewing Results

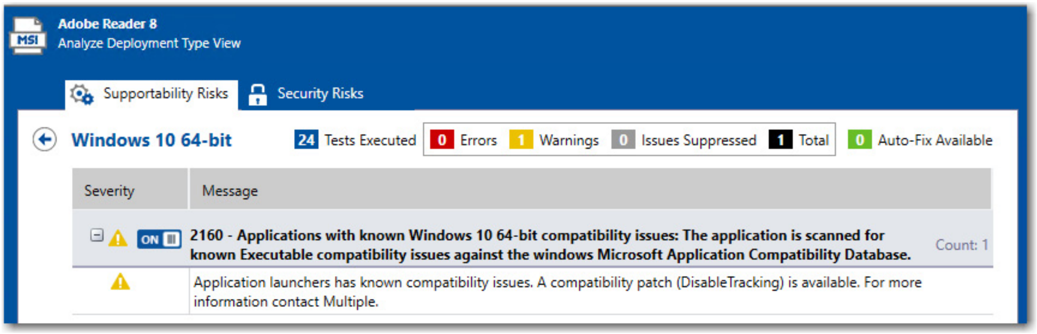
| # | Step | Instructions | Result |
|---|---|---|---|
| **8.** | **View test results.** | When testing is finished, view the test results by selecting a Windows Installer package or web application in the tree to open the **Summary** view of the **Supportability Risks** of the **Analyze Deployment Type View**. | |



**Summary**

| 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 | ● |

Click an icon in the Overall Assessment column to view detailed test results :



**Windows 10 64-bit** 24 Tests Executed 0 Errors 1 Warnings 0 Issues Suppressed 1 Total 0 Auto-Fix Available

| Severity | Message | |
|---|---|---|
| ⊟ ⚠ ON | **2160 - Applications with known Windows 10 64-bit compatibility issues: The application is scanned for known Executable compatibility issues against the windows Microsoft Application Compatibility Database.** | Count: 1 |
| ⚠ | Application launchers has known compatibility issues. A compatibility patch (DisableTracking) is available. For more information contact Multiple. | |

Click the Suppress (ON/OFF) button to suppress any issues that are not important to your organization.

***Note •*** *For more information, see Viewing Operating System Compatibility Test Results and Viewing Browser Compatibility Test Results.*

**Table 18 •** Performing Testing and Viewing Results

| # | Step | Instructions | Result |
|---|---|---|---|
| **9.** | **Click Resolve Issues to automatically resolve issues.** | Issues for which automatic fixes are available are identified by the Error With Fix or Warning With Fix icon:<br>✖ ⚠<br>To automatically resolve all issues for which automatic fixes are available, select the **Applications** group node in the tree and click **Resolve Issues** in the **Analyze** tab of the ribbon.<br>***Note •*** *For more information, see Performing Automatic Issue Resolution.* | Issue resolution begins, progress messages appear in the Output window, and Application Manager performs the following tasks:<br>● **Reruns tests**—Application Manager reruns all of the selected tests to ensure that the issues that it is going to resolve still exist in the current version of the package and its associated transforms.<br>● **Creates transform files**—To resolve issues, Application Manager generates fix transform files.<br>● **Reimports packages**—Application Manager then automatically reimports each package and its fix transform files into the Application Catalog.<br>When issue resolution and reimporting is complete, look at the **Analyze Group View**, **Application View**, or **Deployment Type View** of the package, application, or group that you tested. You will see that the Error With Fix and Warning With Fix icons have been replaced with the status icon with the next highest level (as described in the **Hierarchical Level of Status Icons** section of the About Status Icons help topic) in that test category. |