RAYQC®ad

Collision and Compatibility Management

User Guide RayQC
Advanced 6.5

RayQC Ad is part of RaySuite.

•rayNET

Contents

Introduction

RayQC Advanced is a rule-based tool to create and execute proof-criteria in one or more checklists. It offers various modules to check the quality of applications and software packages all along the Application Lifecycle Management process and also allows you to integrate your own test criteria. The execution of the various test phases is typically done via a combination of manual (i.e. are there available and sufficient licenses for the application?) and automated tasks (i.e. are the MSI properties set according to the packaging guidelines?).

More than the ease-of-use of the checklist viewers in RayQC Advanced, the rule-based interpretation of the individual test results takes quality control to a new level. It is for example possible that the overall quality control phase does not fail, even when one or more test criteria are set as "not achieved", thanks to predefined interpretation rules. All the control steps are also summarized in a final quality report which is intended to be handed over to the next packaging process phase.

RayQC Advanced therefore meets the requirements for an enterprise level software packaging quality control tool. With RayQC Advanced from Raynet, you can rapidly see a reduction in errors, and in the long-term secure the quality of business processes, which in turn drastically relieves IT and Helpdesk alike. Not to mention the significant positive influence on the incurring expenses for Application Lifecycle TCO in general.

Tip:
Various online references are used throughout this document. Although an online connection is not required for this help file, further reading and reference material is available if you do have an internet connection for any of the external links present in this document.

RayQC Advanced is a part of RaySuite

"Best-practice workflow" for Enterprise Application Lifecycle Management

RaySuite offers product solutions for the creation, operation and control of individually customized Enterprise Application Lifecycle Management projects in automatically administered environments.

Designed as part of the RaySuite, Raynet's product suite for Enterprise Application Lifecycle Management, RayQC Advanced is a packaging process related quality assurance tool. However, due to its flexible design RayQC Advanced actually is a multi-purpose application for any kind of checklist-based validation procedure. It may be used either way - standalone or as integrated part of RaySuite.

When RayQC Advanced is used as part of the RaySuite, it is connected to RayFlow, the workflow management component of the RaySuite. In this case there are some additional features, such as directly exporting checklist results to RayFlow, which will not be available in a standalone instance of RayQC Advanced. Please refer to the RaySuite website for further information regarding the benefits this product family offers for your daily business tasks.

Development Roadmap

Upcoming releases will introduce additional new components and features, resulting in boosted productivity, time and resource savings and improvements regarding the product experience. As the development of RayQC Advanced is customer oriented, please let us know if you have any ideas or suggestions of how you see your ideal quality assurance and checklist execution tool. Our sales team will be happy to help you, also make sure to check our website http://raynet.de to never miss our next releases, announcements, special offers and product trainings.

Additional Resources

Further information regarding RayQC Advanced can be found in several resources.

- The *RayPack Studio Release Notes* provide an overview about the changes and new features that are part of this version of RayQC Advanced.

- The *RayQC Advanced 6.5 Operations Supplement* provides information about third-party software packages and libraries redistributed with RayQC Advanced.

- The *RayQC Advanced 6.5 Get Started Guide* provides all information that are necessary to start working with RayQC Advanced.

- The product website www.rayqc.de provides information about the product, news, and support.

- Raynet and its partners offer a range of training courses that can also be customized to meet your requirements. For more information on these courses, speak with your Raynet consultant or contact the Raynet Sales department via sales@raynet.de.

System Requirements

The given requirements name prerequisites for devices running the RayQC Advanced application.

Hardware Requirements

Minimal

- CPU: Intel Core i5
- Screen resolution: 1024 x 768 pixels
- RAM: 4GB
- Disk space: 10GB

Recommended

- CPU: Intel Core i7
- Screen resolution: 1280 x 1024 pixels
- RAM: 16GB or higher
- Disk space: 100GB or more

Note:
The installation of the RayQC Advanced framework itself requires about 200MB of disk space. The amount of additional space required depends on the amount of packaging material and the location of your data store.

Supported OS

The following represents the list of supported operating systems at the time of release.

- Windows Vista SP2
- Windows 7 SP1
- Windows 8
- Windows 8.1
- Windows 10
- Windows Server 2008 R2
- Windows Server 2008 SP1
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

Prerequisite Software

General

- .NET 4.5 Client & Full for Windows Vista up to Windows 8 systems (both 32-bit and 64-bit)
- Microsoft SQL Server Express 2012 or higher. The server can either be hosted locally or on a remote machine.

RayFlow

In order to use RayFlow functionality directly from RayQC Advanced, a running RayFlow server has to be accessible.

Hyper-V integration

- RayQC Advanced requires that RayPack 6.5 is installed on the same machine in order to use Hyper-V functions..
- Both host and guest machine must have PowerShell 3.0 or newer installed.
- Windows Remote Management
- RayPack Studio Tools for Hyper-V need to be installed on the guest machine.

The tools can be installed from a Windows Installer package that is present in the RayQC Advanced subfolder `Tools\HyperVTools\Packaging Suite Tools for Hyper-V.msi`.
The installation of the tools is required, so that the user can see interactive prompts and windows on Hyper-V machines. It is recommended to install the tools as a part of the base snapshot.

VMware Workstation / ESXi5.5 - 6.0

RayQC Advanced requires that RayPack 6.5 is installed on the same machine in order to use ESXi/ Workstation functions. RayQC Advanced supports the following products:

- VMware vSphere 5.5-6.0
- VMware Workstation 10 and newer
- VMware Workstation 7, 8, 9 and for VMware vSphere 4.x, 5 and 5.1 are underlined experimentally supported.

To use any of VMware Workstation / ESX machines, one of the following must be installed in an appropriate version:

- VMware Workstation
- VMware VIX API (https://my.vmware.com/web/vmware/details?productId=26&downloadGroup=VIX-API-162)
- vSphere

The required VIX API version depends on the systems that it needs to connect to. The below table presents the supported versions of VMware products depending on the installed VIX API version.

VIX API Version	VMware Platform Products	Library Location
1.11	vSphere 5, Workstation 8 or earlier	Workstation-8.0.0-and-vSphere-5.0.0

VIX API Version	VMware Platform Products	Library Location
1.12	vSphere 5.1, Workstation 9 or earlier	Workstation-9.0.0-and-vSphere-5.1.0
1.13	vSphere 5.5, Workstation 10 or earlier	Workstation-10.0.0-and-vSphere-5.5.0
1.14	Workstation 11 or earlier	Workstation-11.0.0
1.15.0	Workstation 12 or earlier	Workstation-12.0.0

ESXi 6.5 and newer

RayQC Advanced requires that RayPack 6.5 is installed on the same machine in order to use ESXi/ Workstation functions..

To make use of ESXi 6.5+ servers, the following prerequisites must be met:

- PowerShell 3.0
- PowerShell Execution Policy set to Unrestricted or RemoteSigned
- PowerCLI installer (https://www.powershellgallery.com/packages/ VMware.PowerCLI/11.2.0.12483598)
- VMware Tools installed on the VM
- **Guest operations** and **System** permissions granted to the user executing the product.

Combination of supported versions is presented in the following table:

	VMware PowerCLI															
	12.0.0	11.5.0	11.4.0	11.3.0	11.2.0	11.1.0	11.0.0	10.2.0	10.1.1	10.1.0	10.0.0	6.5.4	6.5.3	6.5.2	6.5.1	6.5.0
⌄ VMware vSphere Hypervisor (ESXi)																
7.0	✅	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
6.7 U3	✅	✅	✅	✅	—	—	—	—	—	—	—	—	—	—	—	—
6.7 U2	✅	✅	✅	✅	✅	—	—	—	—	—	—	—	—	—	—	—
6.7 U1	✅	✅	✅	✅	✅	✅	✅	—	—	—	—	—	—	—	—	—
6.7.0	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	—	—	—	—	—	—
6.5 U3	✅	✅	✅	✅	—	—	—	—	—	—	—	—	—	—	—	—
6.5 U2	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	—	—	—	—	—	—
6.5 U1	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	—	—
6.5.0	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅
6.0 U3	—	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅
6.0.0 U2	—	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅
6.0.0 U1	—	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅
6.0.0	—	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅
5.5 U3	—	—	—	—	—	—	—	✅	✅	✅	✅	✅	✅	✅	✅	✅
5.5 U2	—	—	—	—	—	—	—	✅	✅	✅	✅	✅	✅	✅	✅	✅
5.5 U1	—	—	—	—	—	—	—	✅	✅	✅	✅	✅	✅	✅	✅	✅
5.5	—	—	—	—	—	—	—	✅	✅	✅	✅	✅	✅	✅	✅	✅

More information about PowerCLI:

- https://pubs.vmware.com/vsphere-51/index.jsp?topic=%2Fcom.vmware.powercli.cmdletref.doc%2FGet-VMGuest.html
- https://pubs.vmware.com/vsphere-51/topic/com.vmware.powercli.cmdletref.doc/Invoke-VMScript.html
- https://pubs.vmware.com/vsphere-50/index.jsp?topic=%2Fcom.vmware.wssdk.pg.doc_50%2FPG_ChD_Privileges_Reference.22.3.html

Migration

Upgrading the RayQC Advanced Application

General Upgrade Preparations

RayQC Advanced 6.5 is delivered as an MSI software package. In order to install it safely:

1. Download the MSI package for RayQC Advanced 6.5 from the Raynet resource repositories. (If you have not already received credentials, please contact the Raynet support team via our Support Panel).

2. Copy all files that need to be kept for later reuse or look-up (such as resources of global external plug-ins, log, settings and config files, the `*.rsl` file, etc.) to a temporary transfer directory outside the RayQC Advanced application directory (where they usually reside).

3. Make a backup of your SQL Server database which is used by RayQC Advanced.

4. Execute the RayQC Advanced 6.5 MSI package and work yourself through the setup routine. The installation of RayQC Advanced 6.5 is described in the *RayQC Advanced 6.5 Installation Guide*.

> **Note:**
> If upgrading RayQC Advanced, ensure that a **running** SQL server is available before starting the migration/installation.

Adjusting the Newly Installed RayQC Advanced Instance

1. Launch RayQC Advanced.

2. Define config files and settings according to the old system state.

3. Test the new settings and configurations by creating and evaluating checklists, communicating with RayFlow, reviewing log files, etc.

4. If there are issues regarding broken or missing functionality, please feel free to contact the Raynet support team via our Support Panel.

RayUpdater

During the migration, if database changes are necessary, these will be done automatically. While executing the setup routine, RayUpdater, the tool used for a safe migration of the data, will be launched automatically and perform all necessary steps without the necessity of any user input.

Installing RayQC Advanced

The RayQC Advanced installation resources come along as a MSI file with additional documents, such as the current *Release Notes* and a *User Guide*. Usually, these documents are delivered via FTP server as provided by our support which you can contact via our Support Panel.

Before the application is installed on a device some preparations are needed:

1. Please make sure, that you have your order number or license file at hand. Either one will be provided by your Raynet sales representative or our support team which you can contact via our Support Panel.
2. The target system needs to meet the system requirements described within the *System Requirements* chapter.

3. A Windows User with sufficient rights for installations has to be logged in

4. Close all dispensable applications during the setup routine execution.

5. Make sure that a **running** SQL server is available for connection and for the setup of the RayQC Advanced database, before installing RayQC Advanced.

> **Be aware:**
> No SQL server is installed during the setup! Therefore ensure, that a running SQL server is available if installing RayQC Advanced.

Installing RayQC Advanced

Launch the RayQC Advanced setup with a double-click on the MSI file and wait for the **Welcome Screen** to be prepared.

Click on the **Next >** button to proceed with the installation.
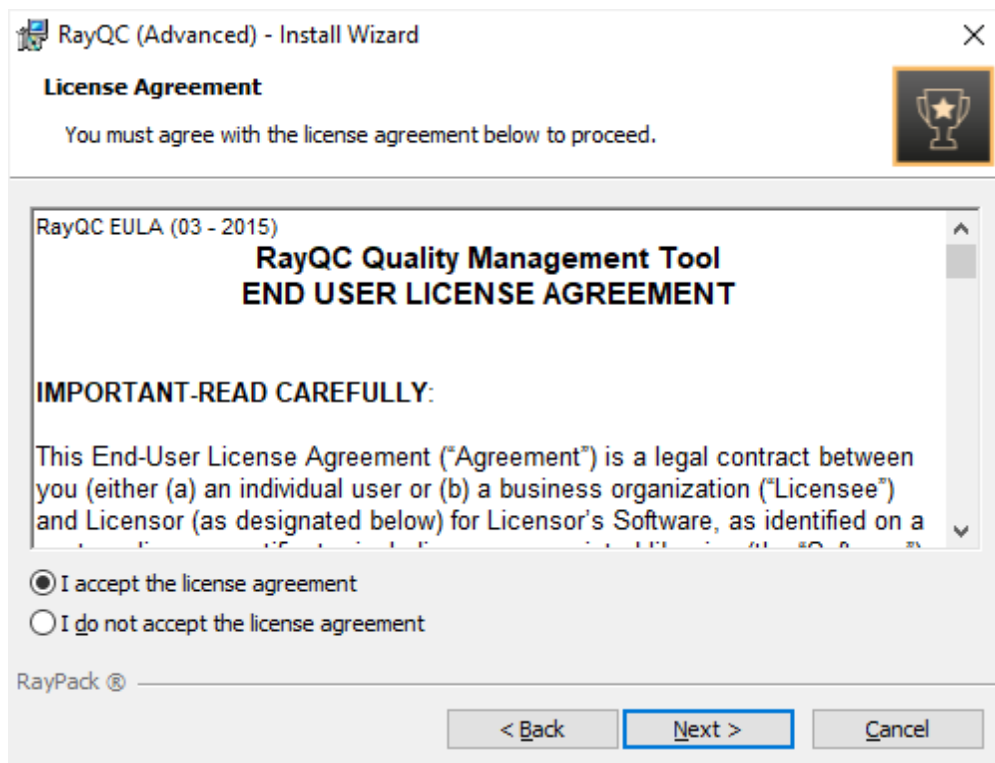
The **End User License Agr**eement dialog appears. In order to install RayQC Advanced, the End

User License Agreement has to be accepted. To proceed, read the End User License Agreement, select the **I accept the license agreement** option, and click on the **Next >** button.
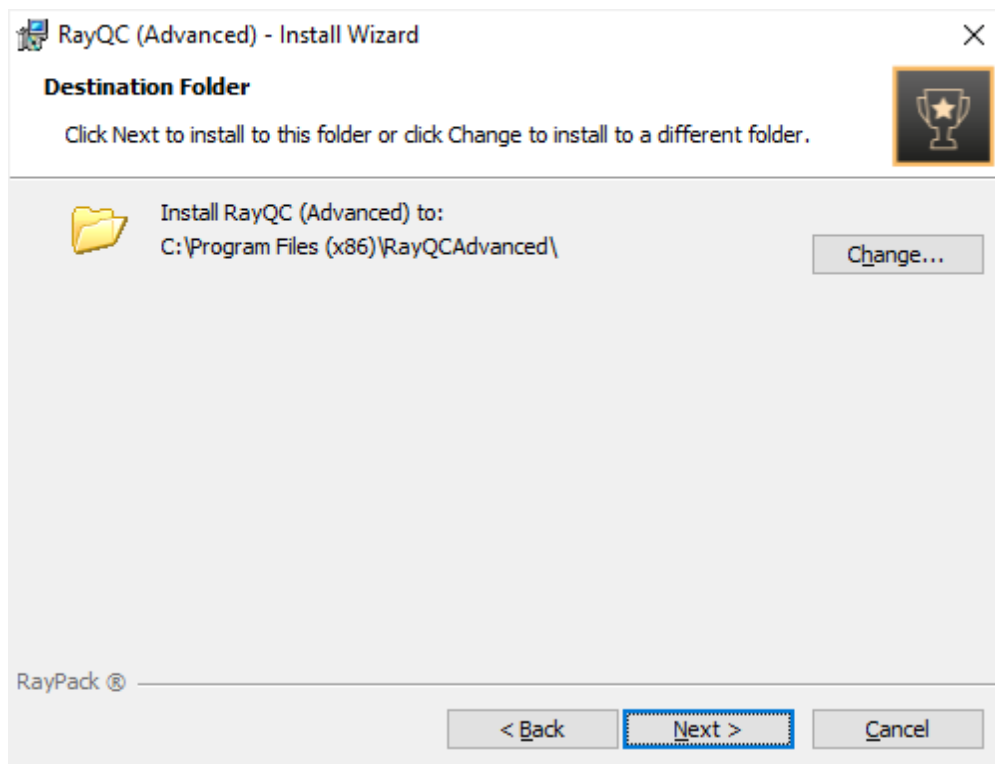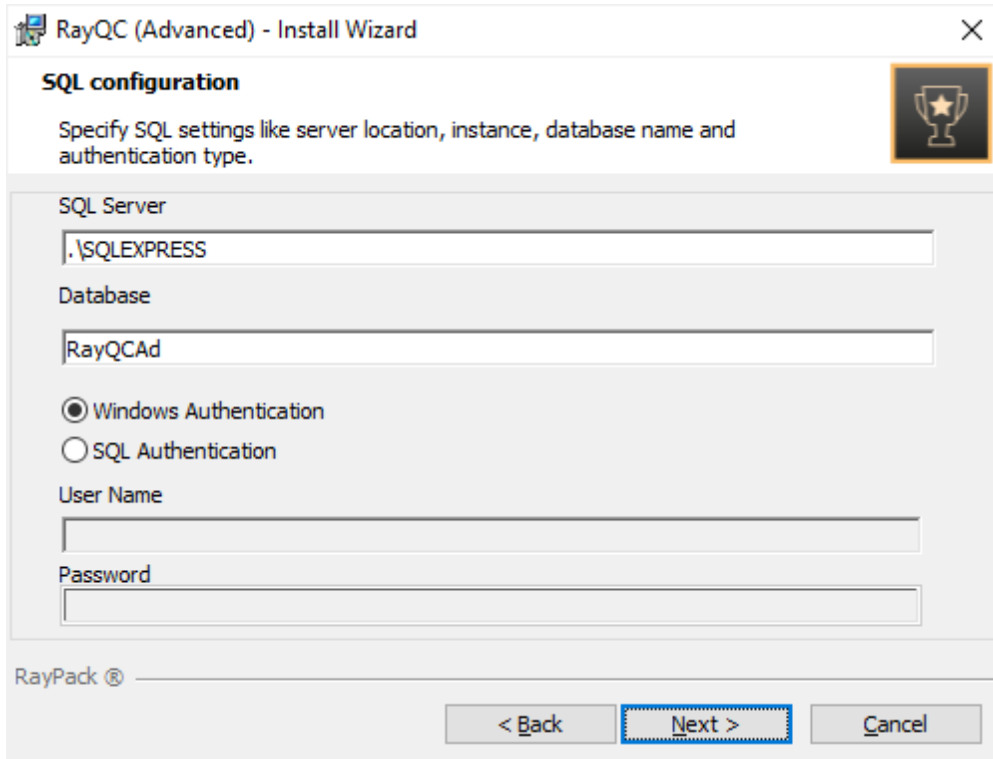
Choose the destination folder by either keeping the suggested default or by clicking on the **Change...** button to select another target directory.
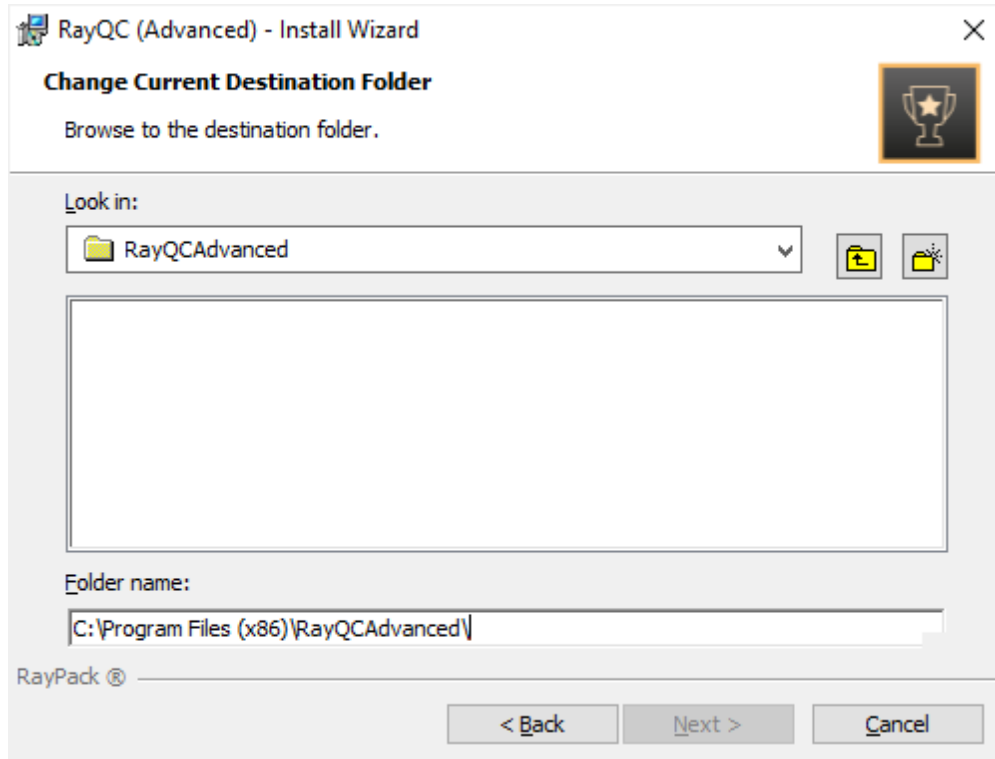
If a custom destination folder has to be defined, use the icons in the dialog above to navigate to the desired installation directory or to create a new one. After this, click on the **OK** button to return to the **Destination Folder** dialog. The path will be updated to display the custom destination recently selected. Click the **Next >** button in the **Destination Folder** dialog to proceed.

In the **SQL configuration** dialog the SQL server connection credentials will be set up.

SQL Server: The SQL server needs to be defined. Please specify the server together with the instance (if an instance is required). The server can be specified either by its name or by its IP address. The server must exist and must have a user which can create a database and has read and write access to the newly created database.

Database: Define a database which will be used by RayQC Advanced.

Authentication: Choose between Windows Authentication or SQL Authentication. If SQL Authentication is chosen enter the user name and password of a user which can create a database and will have read and write access to the newly created database.

Click on the **Next >** button in the SQL Configuration dialog to proceed. After clicking the **Next** > button the installer will check if the database exists. If the database does not exist a new database will be created by the installer.

> **Be aware:**
> When using Windows Authentication, if the installing user differs from the executing user check database permissions:
> The user executing the installed instance of RayQC Advanced will need read and write access to the database created during the installation, though he does not need permissions to create new databases.
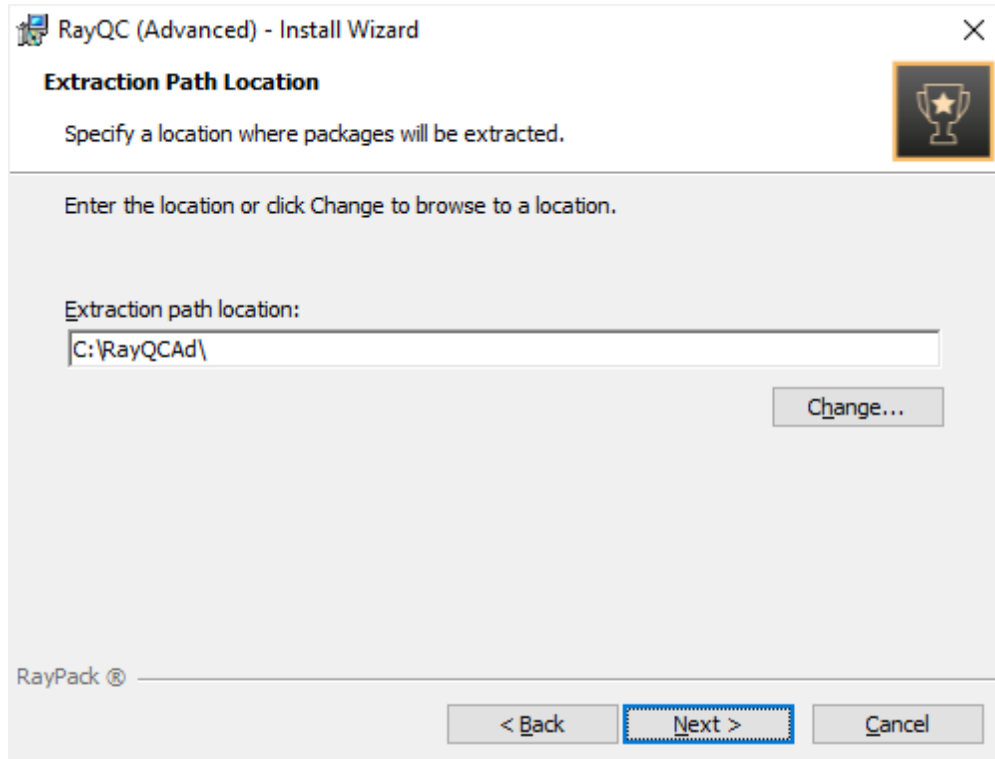
Choose a folder. RayQC Advanced will use this folder to store files and packages extracted during the import into the RayQC Advanced library.
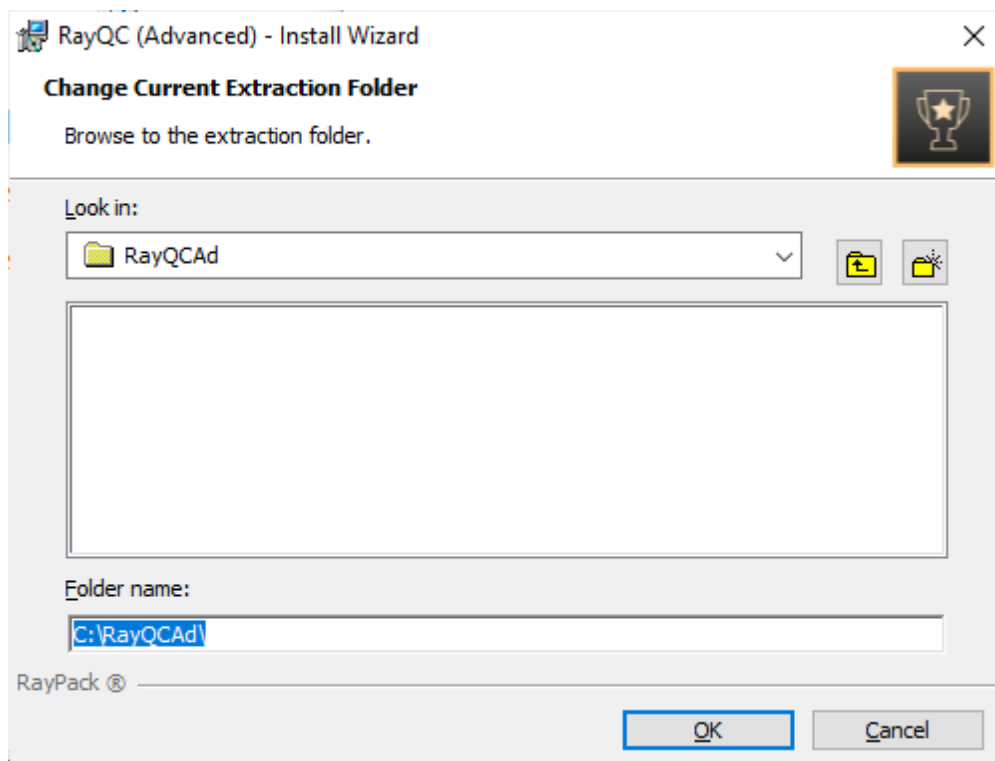
If a custom extraction folder has to be defined, use the icons in the dialog above to navigate to the desired installation directory or to create a new one. After this, click on the **OK** button to return to the **Extraction Path Location** dialog. The path will be updated to display the custom destination recently selected. Click the **Next >** button in the **Extraction Path Location** dialog to proceed.
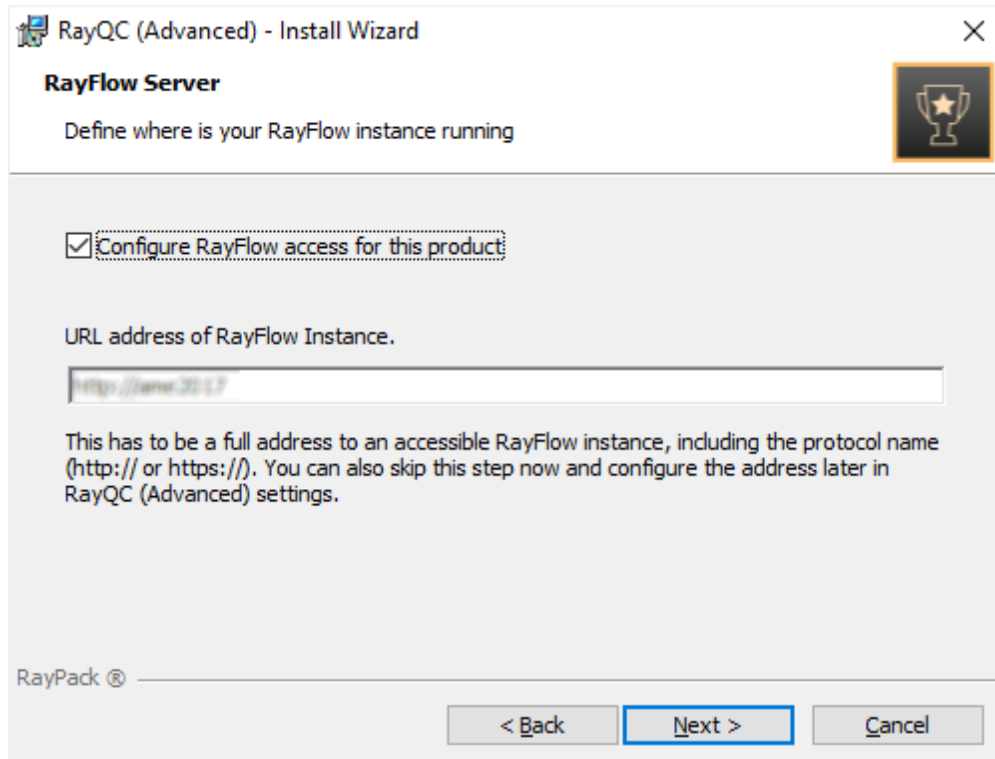
The RayFlow access for this product needs to be configured. If the **Configure RayFlow access for this product** checkbox is checked, the RayFlow server can be configured. The full address of the RayFlow instance that is about to be used for RayQC Advanced needs to be entered in the text field. If the **Configure RayFlow access for this product checkbox** is left unchecked, RayFlow access can still be configured in the **Settings** page of RayQC Advanced after the installation has been successfully completed.

Click the **Next >** button in the **RayFlow Server** dialog to proceed.
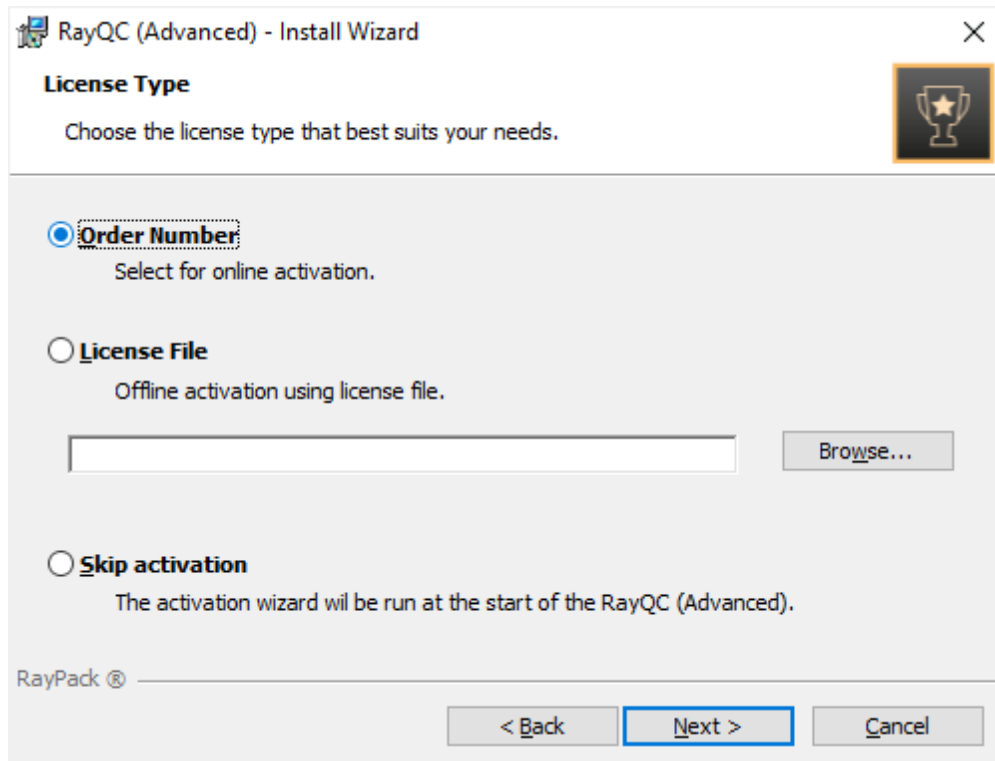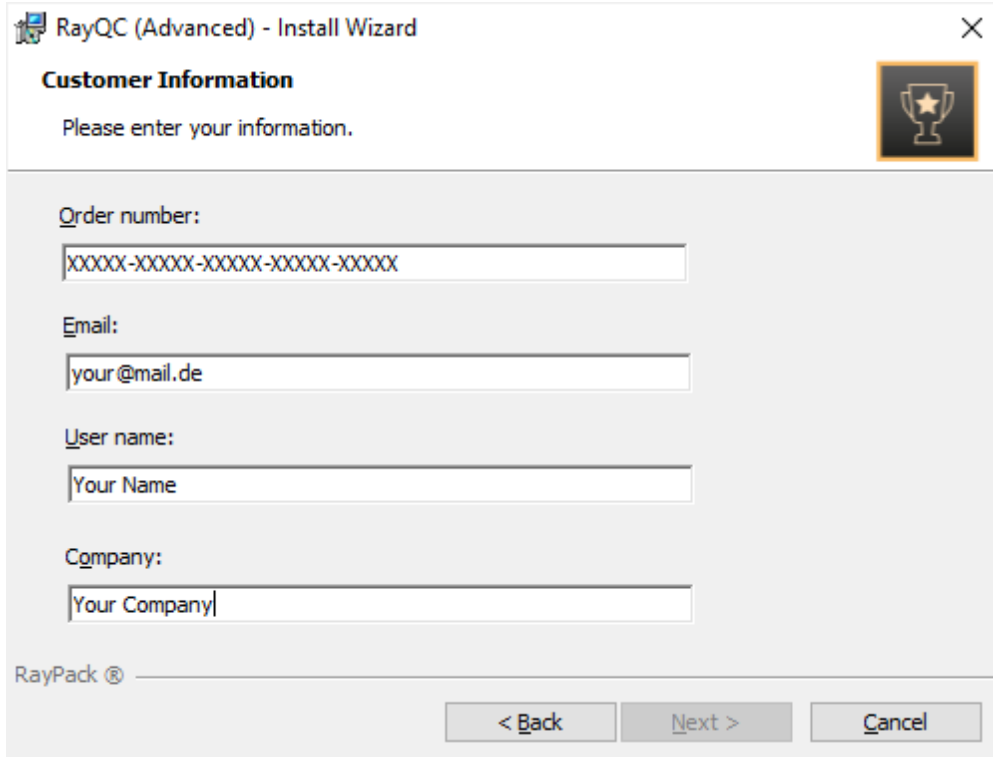
The **License Type** screen provides options to either activate the RayQC Advanced instance via order number and online activation service, by using an already prepared file (`*.license`), or to skip activation for now. If the activation is skipped, it will need to be performed later when RayQC Advanced is launched. For more information on product activation at the first launch of RayQC Advanced read this *section*.

To use an already existing license file, which most likely has been provided by the Raynet support team, the **Browse...** button has to be clicked. Use the controls of the system browser dialog to navigate to the `*.license` file and select it with a click on the **Open** button.

Click the **Next >** button to proceed.

If activation by order number has been selected during the previous step, the **Customer Information** dialog is displayed:

Please enter your individual RayQC Advanced Order number and provide user information, such as Email, user name, and company name. The information will be used to verify the order number during the upcoming execution procedure.

Click the **Next >** button to proceed.
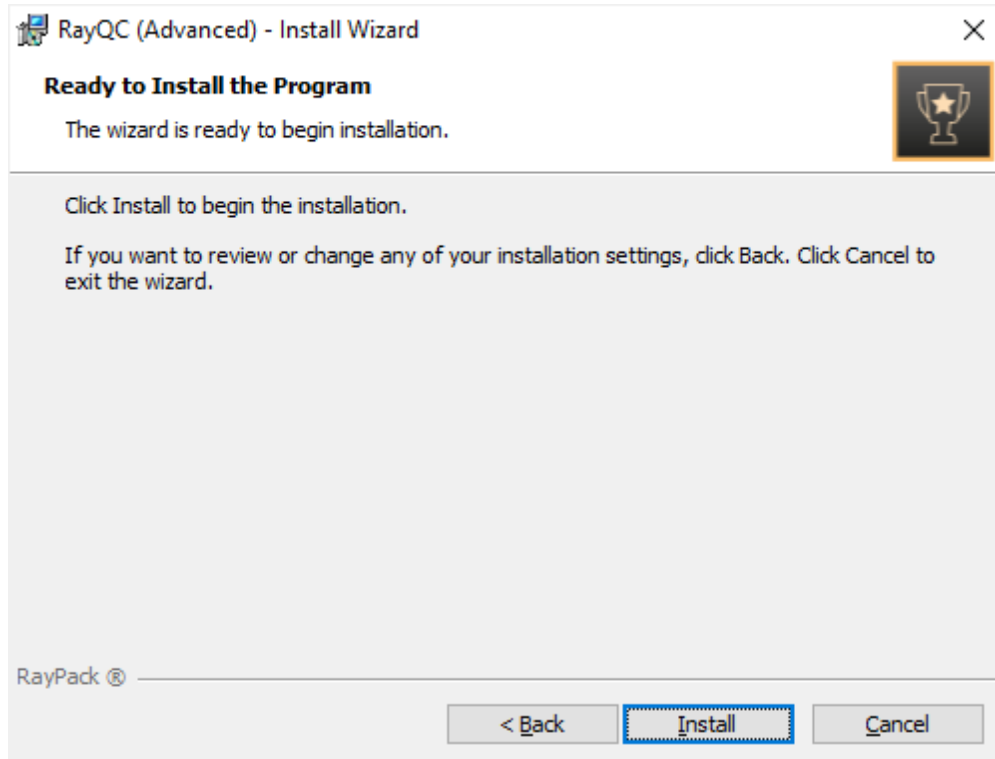
All required settings and properties are now defined and RayQC Advanced is ready to be installed. Click on the **Install** button to start the process.

A progress indication dialog is displayed as long as the installation steps are executed.
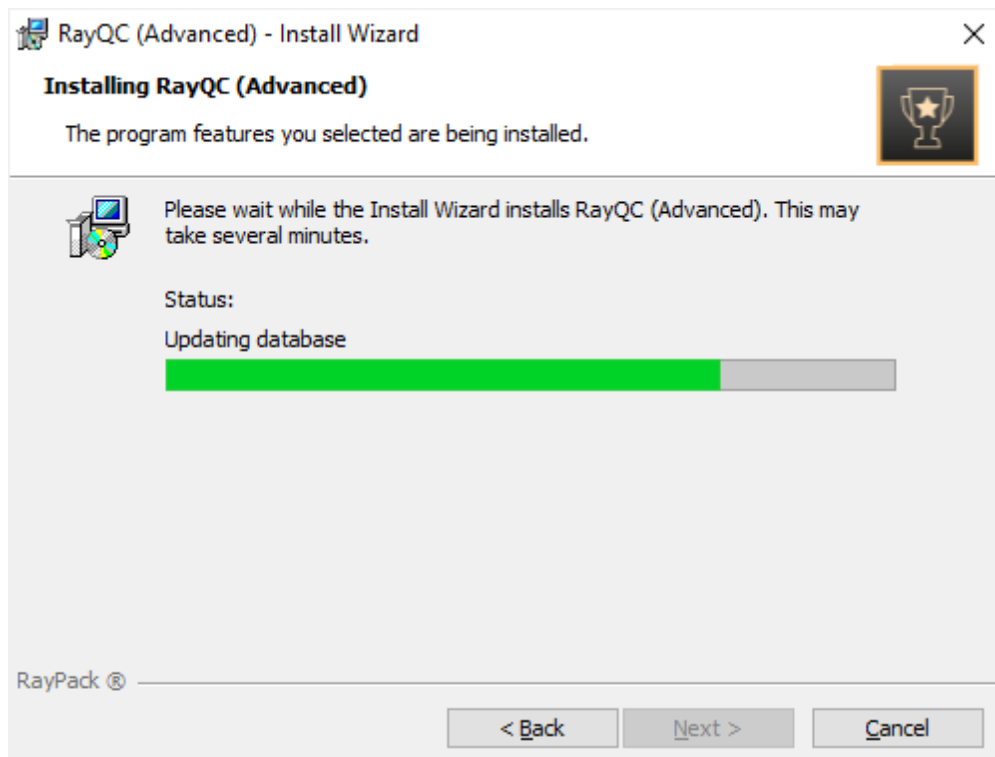
As soon as all required measures are done, the **Install Completed** dialog is presented.
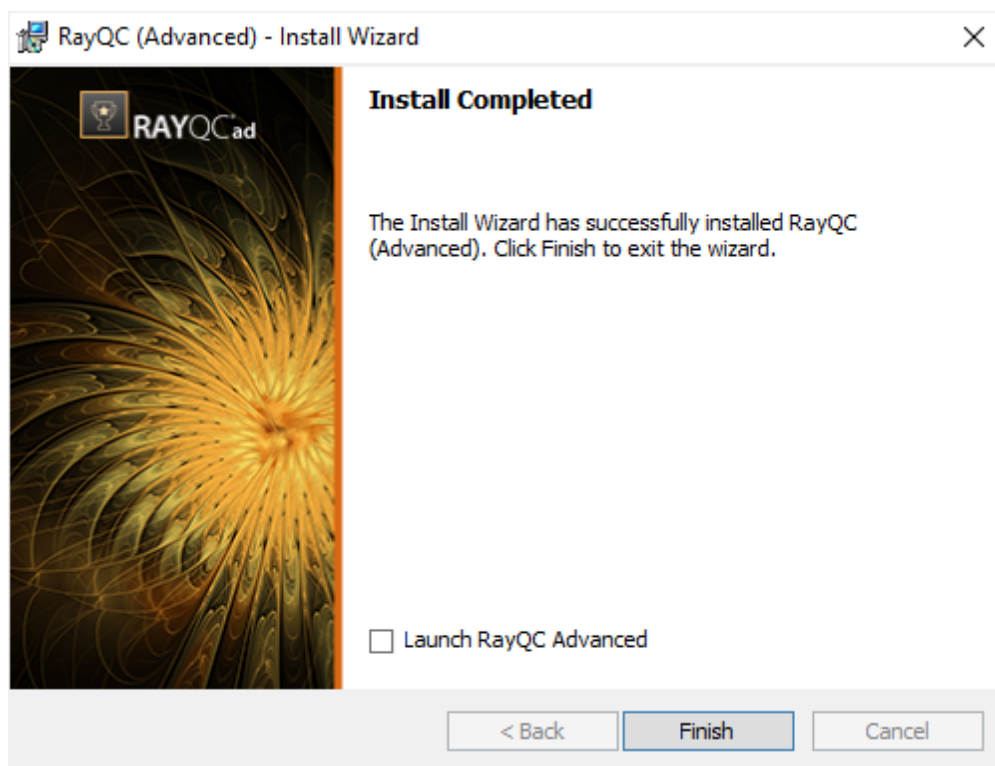
Check the **Launch RayQC Advanced** checkbox to launch the RayQC Advanced application after the setup has been finished. If the **Open Release Notes Checkbox** is checked, the *Release Notes* will be opened after the setup has been finished.

Click the **Finish** button to exit the setup.

Product Activation

The product can be activated using one of the following methods:

- Directly within the installation
  - By supplying the order number
  - By supplying an already generated license file (`.rsl` format)
- When the product is started for the first time.

If RayQC Advanced detects that no valid license is present on start-up, the license activation wizard will be shown after starting the main executable. The tool can be also started manually, by executing `Raynet.LicenseActivation.exe` from the main installation folder.

License Wizard

This section describes the usage of the licensing wizard.

On the initial start of RayQC Advanced, the licensing wizard is shown. If the need to transfer an existing license arises, the license wizard can be started manually. There are a variety of ways in which a license can be activated and below they are described in detail.
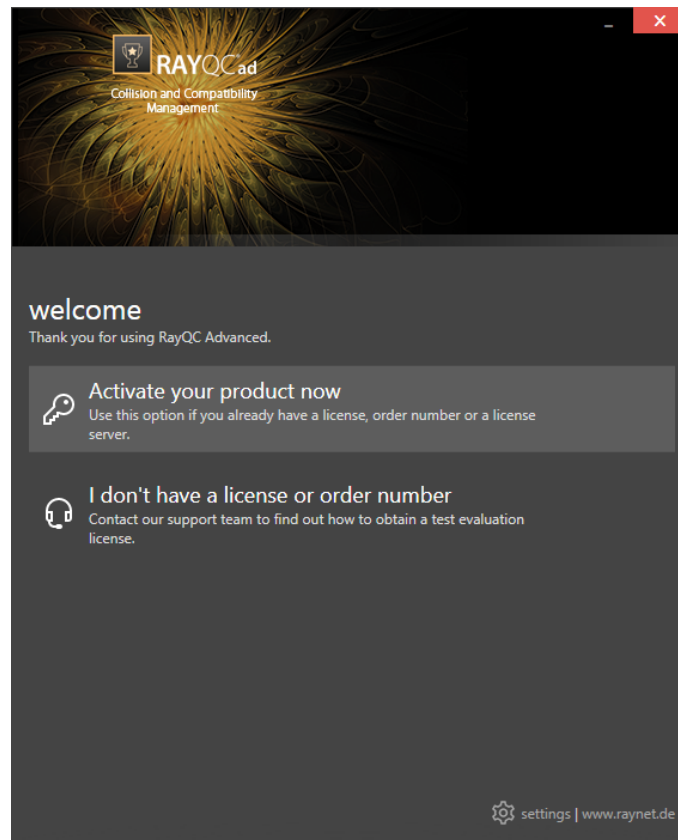
First time activation
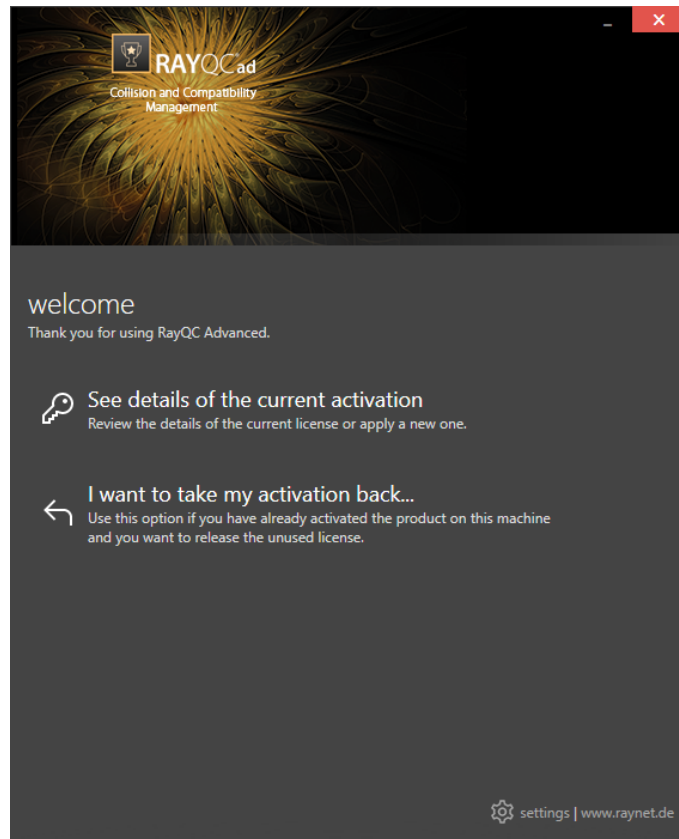
The main screen when the product has been already
activated

Activate your product now

This option should be used to activate the product using one of the following methods:
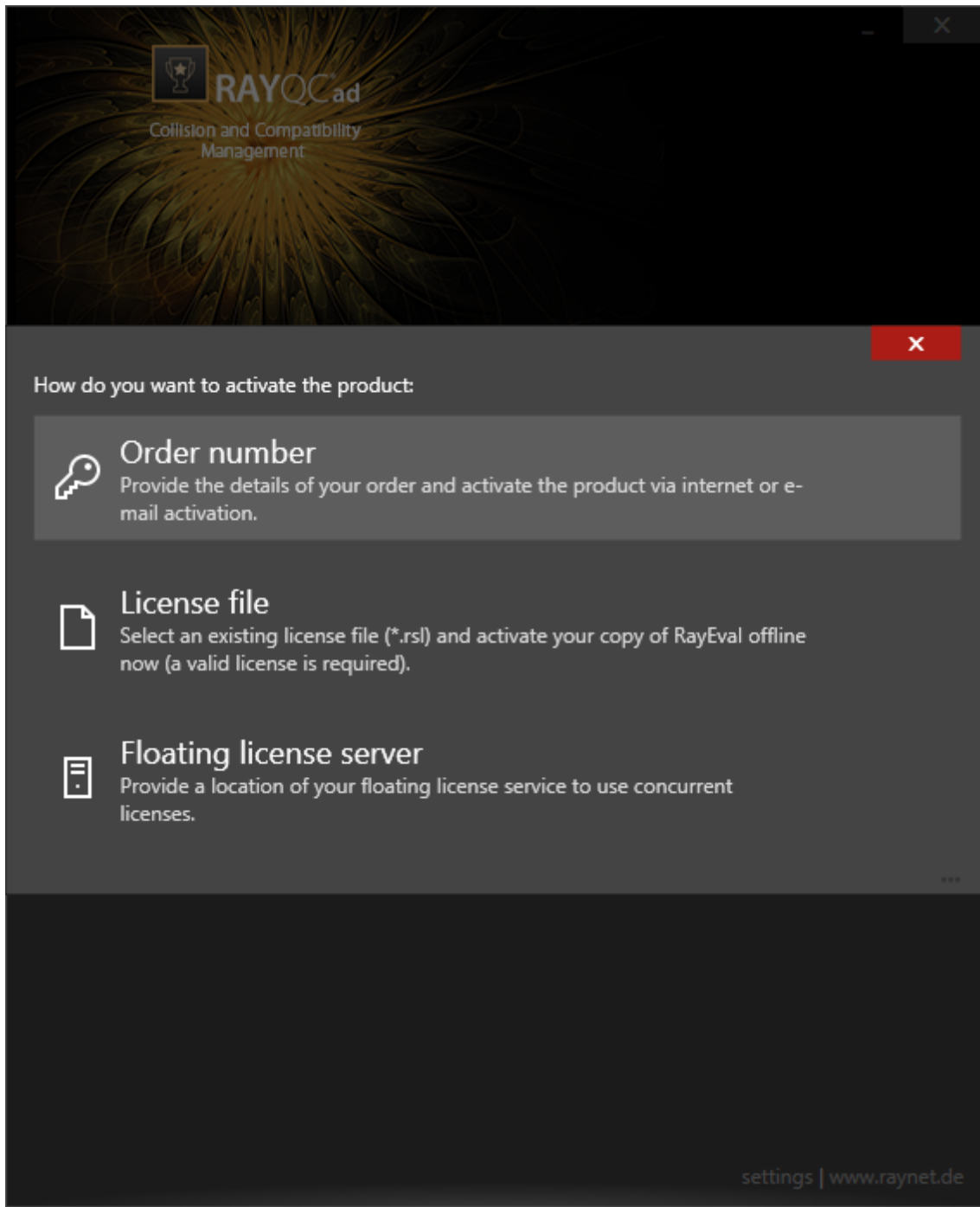
- **Order number**
  Online activation using a valid order number received from Raynet (recommended for most users)

- **License file**
  Offline activation using a license file (`.rsl`) received from Raynet

- **Floating license server**

Activation using a local floating license server.

See details of the current activation
This options shows the details of the current activation. This option is only visible if the product has already been activated or if a floating license server has been configured
This option also allows to reactivate the product using a different order number or a different floating license server connection details.

I don't have a license or order number
Choose this option if there is neither a license nor an order number available. For in-depth information please read this *section*. This option is only visible if the product has not been activated yet.

I want to take my activation back...
Use this option to deactivate a currently licensed version of RayQC Advanced. For in-depth information please read this *section*. This options is only visible if the product has been already activated.

Once the license file has been generated or copied to the correct location the following will be shown...
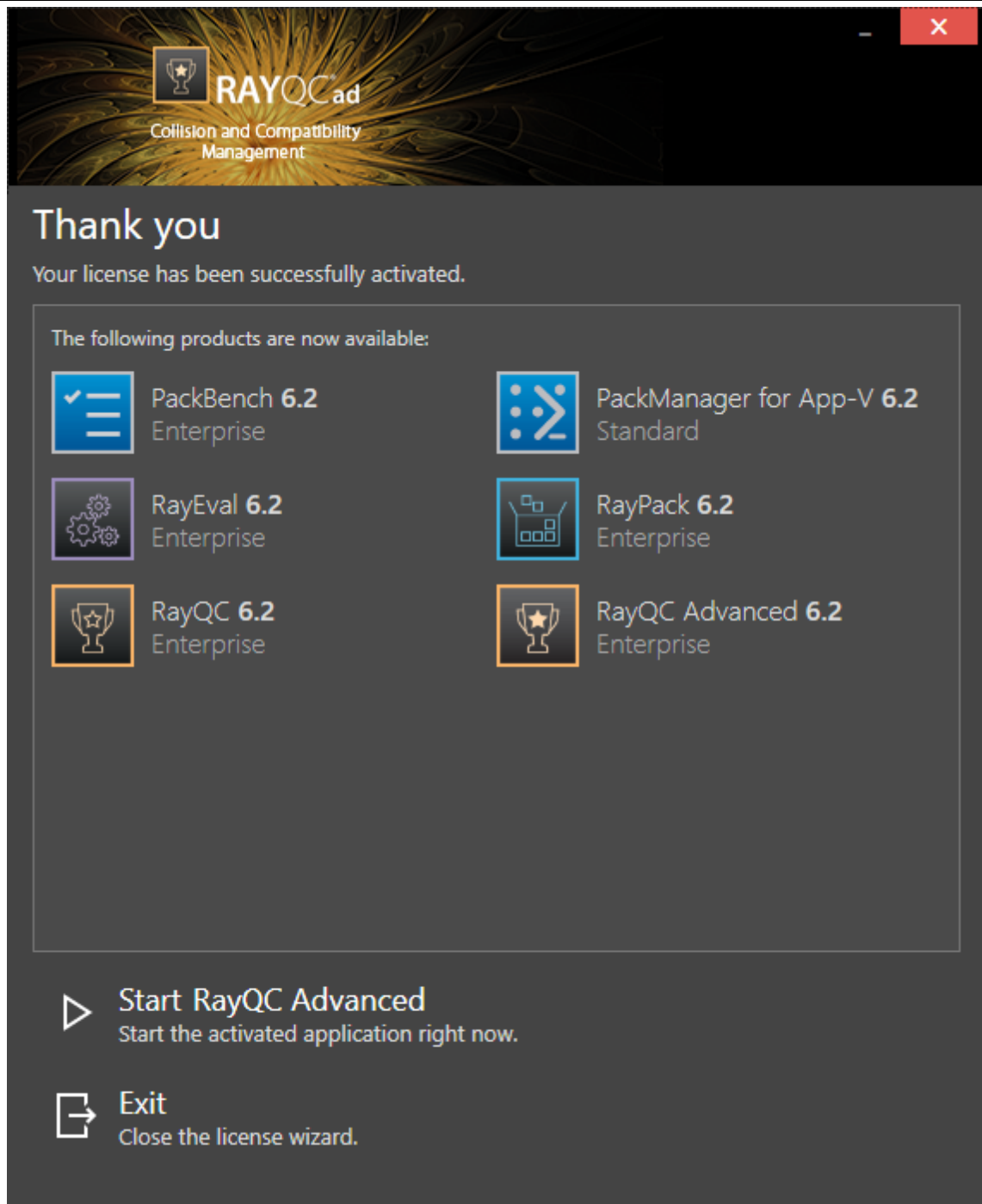
> **Note:**
> Depending on the license, more available products may be shown, as pictured above.

Then the option of starting RayQC Advanced or just closing the activation wizard is made available.

Troubleshooting

If any issues arise during the activation process, please contact our *help desk* to receive assistance in activating RayQC Advanced.

Order Number

RayQC Advanced can be activated either directly online or via email once the order number has been delivered. The activation process generates a license file (`*.rsl`) that is created (or must be copied) to the installation directory of RayQC Advanced (in the same location as the `RayQC Advanced.exe`). When performing an online activation, sufficient permissions must be readily available to allow the creation of the license file in the installation directory. The activation **binds** the license to the machine on which it was activated on. This is the only time that an active connection to the internet is required (if activating online).

Choosing the **ACTIVATE NOW** button, connects to the Raynet license server using the information provided and will dynamically generate a license file. Choosing the **ACTIVATE MANUALLY** button will open a dialog as *shown here*. Choosing the **CANCEL** button will abort the activation process.

Order Details

Order number:
This is the unique order number received when RayQC Advanced has been purchased. If it is necessary to recover the order number, please contact our *sales team*.

User name:
This is the name of the user that is activating RayQC Advanced. It does not need to be the same name used to order RayQC Advanced.

Company:
This is the name of the company for which RayQC Advanced will be licensed. This name will appear in the **License and Edition** view of RayQC Advanced.

E-mail address:
This is the email address of the person that performs the activation. We respect the privacy of our customers, this email address will only be used by Raynet and only when there are any problems or important information regarding the license.

Advanced Options

On choosing the advanced options check box, extended information and possibilities of the licensing and activation of RayQC Advanced are shown.

Hardware ID:
This is a ID calculated based on the hardware on which the activation is taking place on. The ID is unique, but cannot be used to personally identify a user. It is used to generate the license for the machine on which the activation process is carried out on.
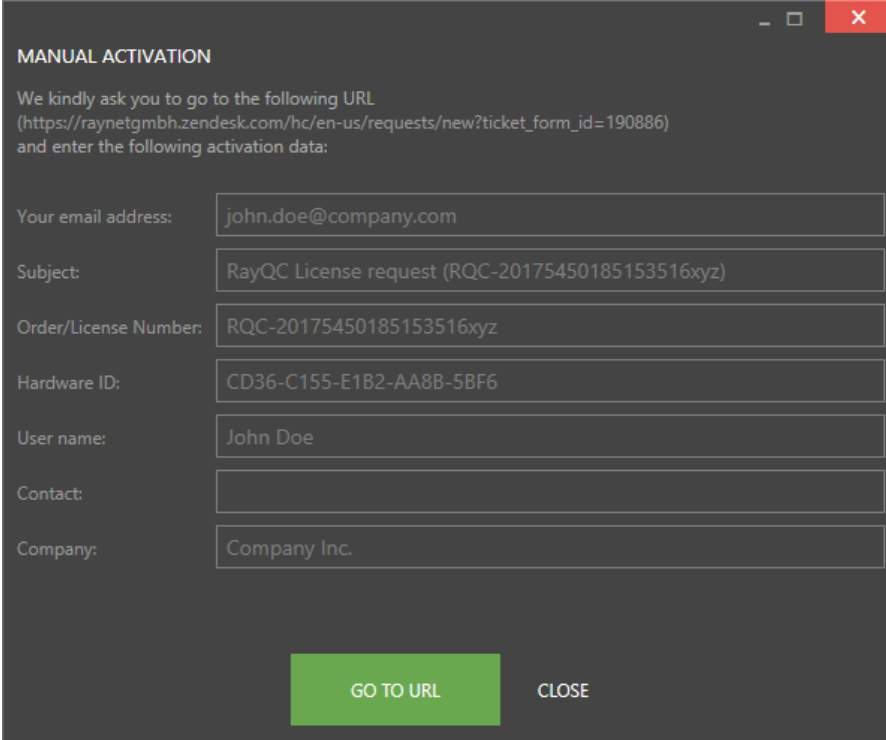
Transfer the license
If this option is selected, the order number and details may be used to activate RayQC Advanced on a second machine, that has differing hardware (which obviously has a different Hardware ID). This assumes that RayQC Advanced has been deinstalled from the machine on which it was previously activated on. The transfer license functionality is logged on our license servers and is periodically checked to ensure that no abuse is made of this functionality.

If the license transfer is part of a regular maintenance and can therefore be prepared and scheduled, it is highly recommended to use the deactivation function first, to disconnect license and packaging machine. This is the standard way for transferring licenses. The option offered here is intended for unscheduled transfers, required if a machine, for whatever reason, cannot be accessed or used operational any longer.

Manual Activation

On choosing the manual activation, the dialog shown below is displayed.

This basically shows the contents of the ticket form that will be opened at Raynet. If there is an internet connection available on the machine, click on the **GO TO URL** button to open the URL shown in the top of the window in the default browser of the system. After a File Order has been opened in the Raynet Support Panel, a license file will be delivered. Information of how to use this file are available here.

If no internet connection is present on the machine on which the activation process is taking place, copy the contents of the dialog onto a machine which has an internet connection and use the URL on that machine. On receiving the ticket, a license file will be generated and sent back. Information on how to use the license file can be found here.

> **Tip:**
> Please ensure that when copying the information from the **MANUAL ACTIVATION** dialog everything is added as shown above.

Once the license file has been generated the following will be shown:
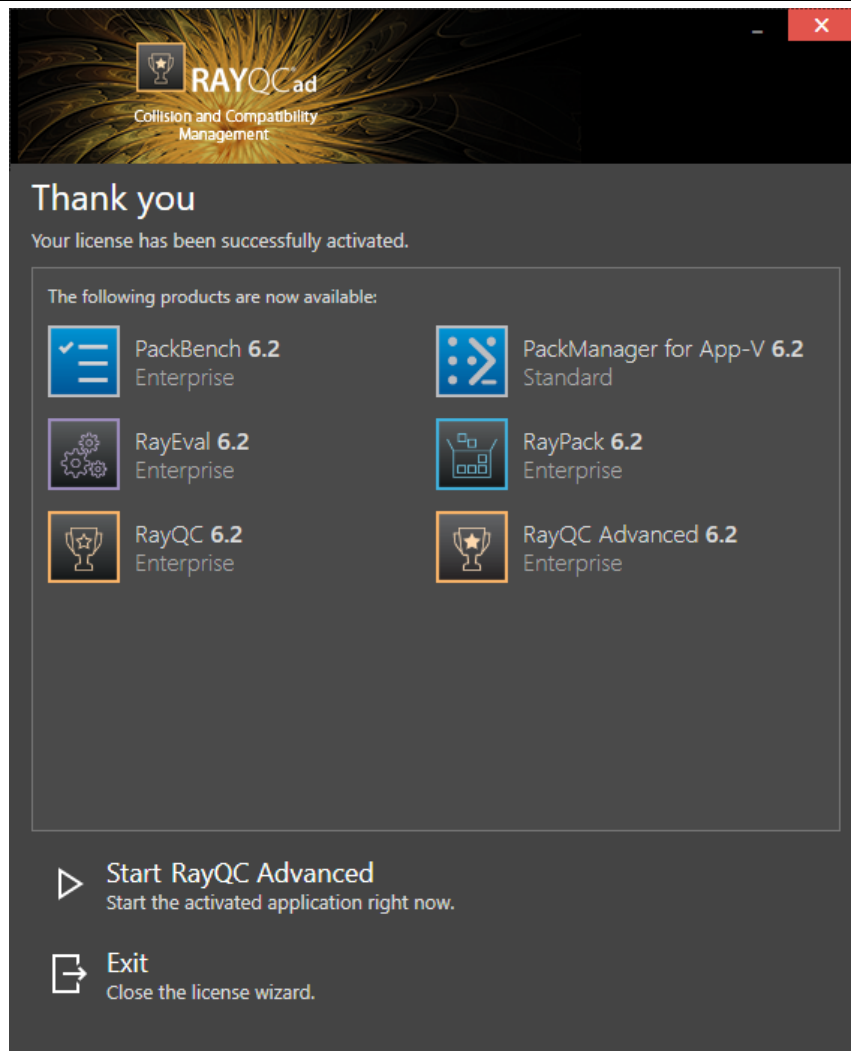
> **Note:**
> Depending on the license, more available products may be shown. As an example, see the image above.

The option of starting RayQC Advanced or just closing the **Activation** wizard are available now.

Troubleshooting

If there are any problems during the activation process, please contact our *help desk* for receiving assistance in activating RayQC Advanced.

License File

If a license is already available, or a license file has been received as a result of activating RayQC Advanced via email, then all that is required is to copy the license file into the installation directory of RayQC Advanced (the directory in which the `RayPack.exe` resides). Clicking on the l

have a license button on the **License wizard** dialog opens a dialog box which allows to choose the license file. Once chosen, the file will be copied automatically to the RayQC Advanced installation directory. Please ensure that sufficient permissions to allow the creation / copying of a file to the installation directory of RayQC Advanced are available.
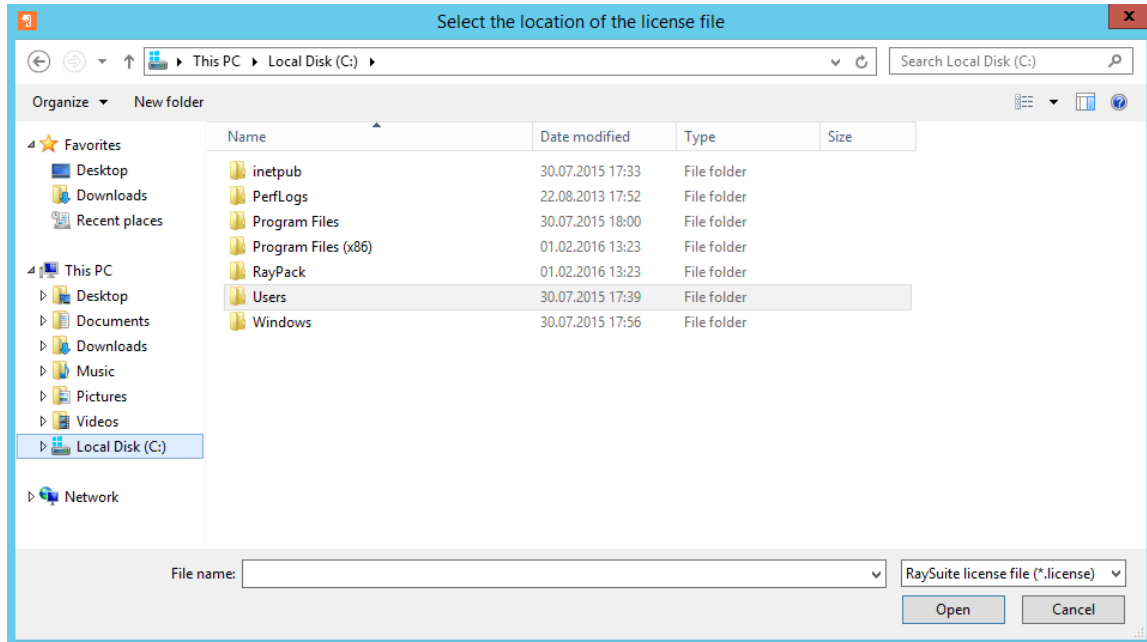
Once the license file has been copied to the correct location the following will be shown:
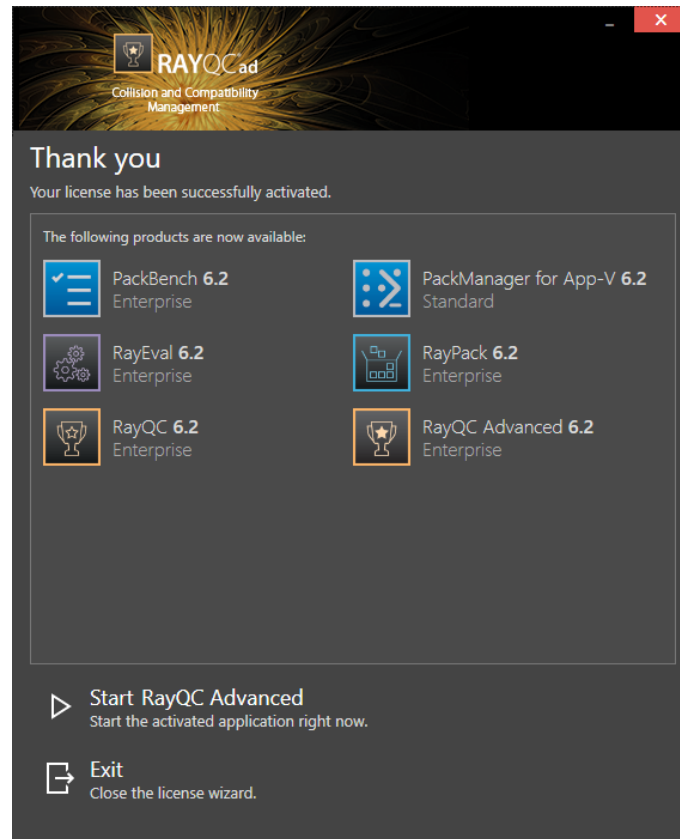
> **Note:**
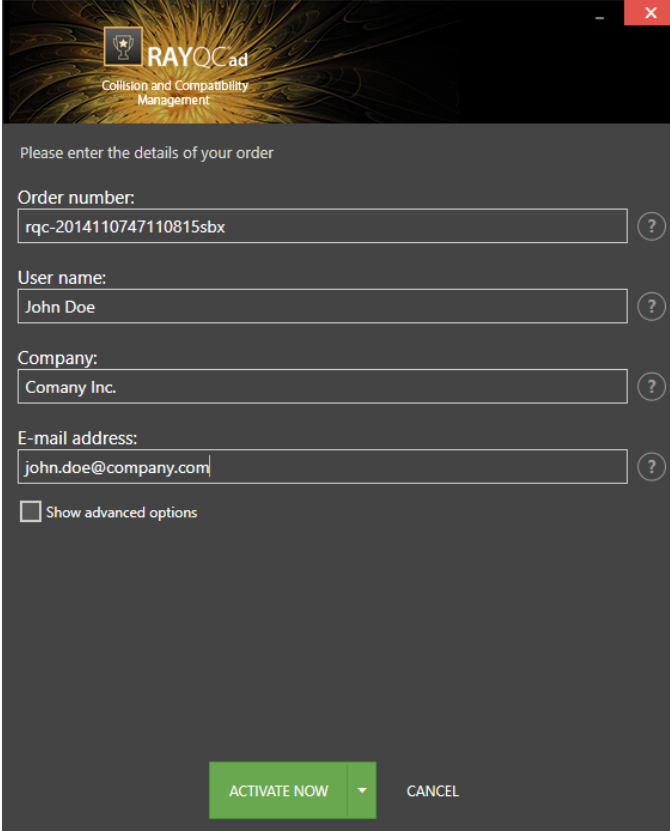> Depending on the license, more available products may be shown. As an example, see the image above.

The option of starting RayQC Advanced or just closing the activation wizard are available now.

Troubleshooting
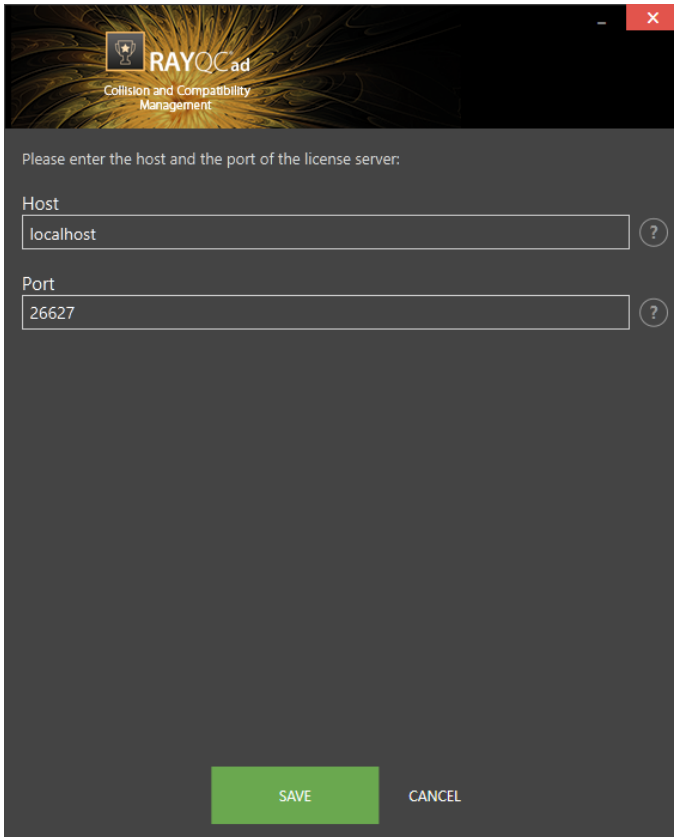
If there are any problems during the activation process, please contact our *help desk* for receiving assistance in activating RayQC Advanced.

Floating License Server

RayQC Advanced can be activated using a local floating license server. This requires that the server component is installed (the installation is available separately from the product installer).

Once the server is configured, the following details are required from the server administrator:

- Server name or IP address
- Configured port (by default `26627`)

Enter required values and confirm them by clicking on the **SAVE** button. The server will be contacted once to verify the correctness of the data. If the server is not available at that time, an option will be presented to write the data anyway.

Once the connection details are saved, please restart the product to activate it using the floating license server.

I Do Not Have a License or Order Number

If neither a license or order number is available, then just simply register with Raynet to download an evaluation license for RayQC Advanced. This allows potential customers to test and work with RayQC Advanced before purchasing. Choosing **I don't have a license or order number** opens the Raynet website in the default browser, allowing potential customers to download an evaluation copy of RayQC Advanced.

I Want to Take my Activation Back

Deactivating an existing license for RayQC Advanced may be required if the packaging machine used has to be switched. Whenever there is a scheduled migration, e. g. when a virtual machine is transferred in a way that affects the **Hardware ID**, or when a physical machine is no longer used for packaging purposes, deactivating the license is the right thing to do.

To deactivate a licensed RayQC Advanced installation

1. Launch RayQC Advanced and open the **license and edition** tab of the **About** area.

2. Click on the **Open the license wizard** button on the lower left hand side of the application window.

3. Use the option **I want to take my activation back...**

4. Enter the **order number** that was originally used to activate RayQC Advanced on the current machine. It was part of the resources and information material delivered during product purchase.

5. If required, adjust the user name already entered into the input field **User name**. The users who activate and deactivate an installation do not necessarily have to be the same.

6. Click on **DEACTIVATE NOW**.

   The license wizard will connect to the Raynet licensing server and send the deactivation information. On success, the number of licenses available for activation, which are bound to the used order number, is incremented by one. With this new free license it is possible to activate any RayQC Advanced installation, on the current machine or any other.

Troubleshooting

If any problems during this process occur, please contact our *help desk* for receiving assistance in deactivating RayQC Advanced.

Working with RayQC Advanced

As mentioned earlier, RayQC Advanced is an extension module of RayQC and availability of its features is controlled via the license file. A user can either use this module in standalone mode or via the RayQC plug-in interface. More information on RayQC plug-ins can be found under the *plug-ins* chapter of the *RayQC User Guide*.

This module can be invoked in standalone mode directly via the application installation directory (e. g., `C:\Program Files (x86)\RayQCAdvanced\RayQCAd.exe`). Whenever this module is launched in standalone mode, this view is the starting point for the new RayQC Advanced session.
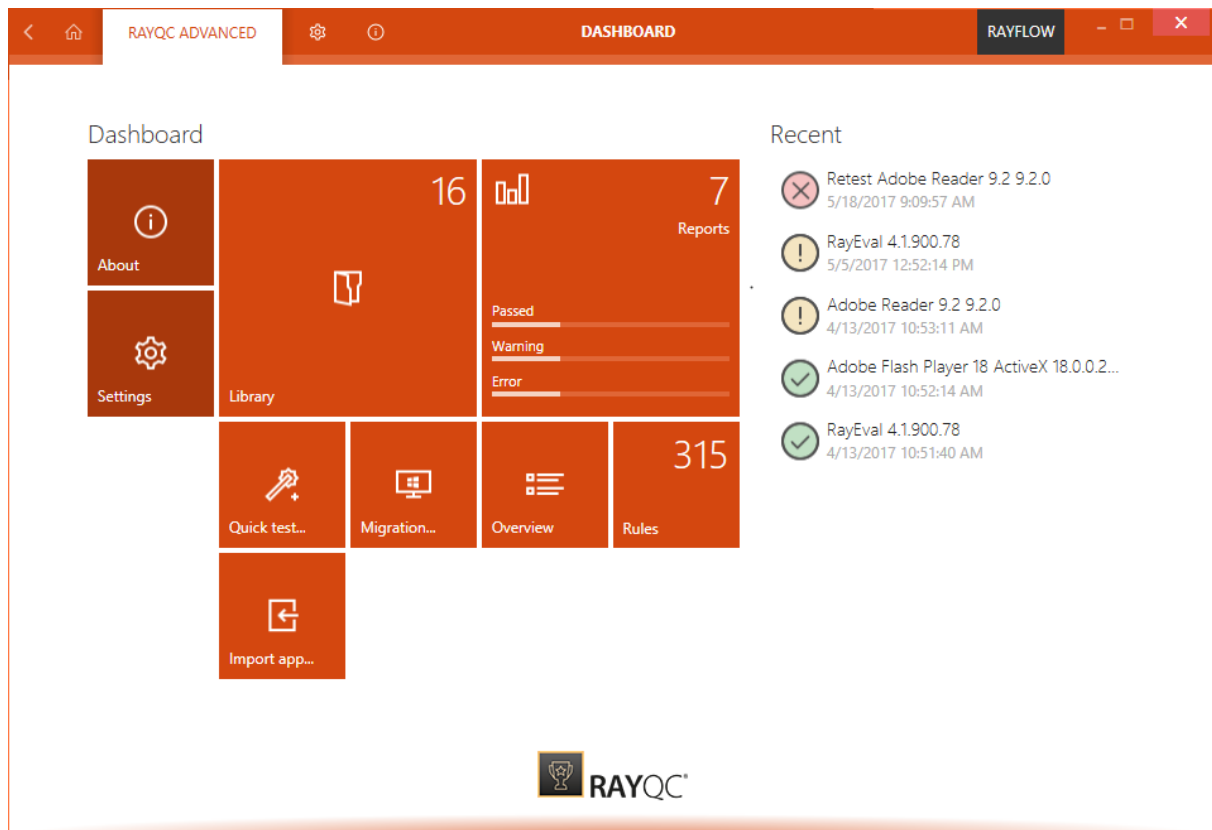
The **Home Screen** is not available to a user, when this module is launched via the RayQC plug-in interface. Just like RayQC, this module contains the **Main Toolbar**, which is available throughout the application.

The Main Toolbar

Throughout RayQC Advanced, the **Main Toolbar** is visible, which, dependent on the contents of the view shown adds or removes menu items dynamically. As a rule of thumb the items shown below are always present on the **Main Toolbar**.

View history

With a left-click on the arrow button, users navigate one step back within the history of recently opened views. Right-clicking the arrow displays the recently visited views, and allows to return to a specific view from that list.

Home

Choosing this button will return you to the **Home Screen**.

View title

The view title specifies which content is currently shown as part of the active application context and module.

Standard window controls

The standard window controls allow to minimize, maximize, resize, and close the application window. The availability of each control follows the Windows schema for standard controls as known from any desktop application.

Application Context

The illustrations above show the main application context status, which is RayQC Advanced. Depending on the set of licensed modules and add-ons, further contexts may be added.

Settings

Loads the **Settings** view for RayQC Advanced.

About

Contains information about the currently active product instance.

Typical Workflows

Working with RayQC Advanced is basically divided into four main areas of activity: The library, the test wizard, the rules catalog, and the report archive. Therefore, the main workflows are bound to these core tasks:

1. **Importing resources into the library**
   In order to get your system ready for usage, it is recommended to import resources into your library first. Even though tests may be performed on temporarily available software packages, it makes sense to import applications that will be a permanent part of the software library into the database.
   Read this section to learn how to do this.
2. **Performing tests**
   Once resources are present, it is possible to perform tests on them. Testing may either be triggered from the Home Screen, or directly from the library.
   Read this section to learn how to do this.
3. **Reviewing reports**
   The result reports are usually stored within an archive. Access it to review former test results.

Read this section to learn how to do this.

4. Managing rule sets
If the default rule set does not cover the actual test needs, they can be adjusted via the rule set catalog.
Read this section to learn how to do this.

The list above is numbered to express the recommended order of activities to get started with RayQC Advanced. Read the following sections in turn to easily dive into a productive usage mode.

What's next?

Now that the most common activities are known, it is time to take a look at the user interface. As outlined before, the starting point of RayQC Advanced daily business is the Home screen with its dashboard and recent list. Advanced RaySuite users may want to skip the in depth description of the Home screen, and directly go ahead to read about the library.

Importing Resources into the Library

> 📎 **Note:**
> This section describes how to import software, merge modules, OS snapshots, and web applications into the library. Please read the library overview to get details on the UI and available additional functionalities.

The library enables the management of four different types of resources:

- **Software Packages**
  In RayQC Advanced, importable software packages are `.msi` files with optional transforms (`.mst`). These resources may either be imported into the database (=library), or be used as a temporary test resource from the file system. Importing is recommended for software that is about to be part of test procedures quite frequently.

- **Merge Modules**
  The second package type that can be imported are merge modules (`.msm`). These resources may either be imported into the database (=library), or be used as a temporary test resource from the file system. Importing is recommended for MSM's that are about to be part of test procedures quite frequently.

- **OS Snapshots**
  Testing in RayQC Advanced may be performed against a standard operating system environment (such as Windows 8.1 or Windows 10), or against a specific device state, represented by an OS snapshot. OS snapshots must be imported to be available for testing. Currently, this application only supports import of OS Snapshots in `.rcs` format.

- **App-V packages**
  Another package type that can be imported into RayQC Advanced are `.appv` files. These resources may either be imported into the database (=library), or be used as a temporary test resource from the file system. They can be tested with a fixed set of rules against different operating systems.

- **Web Apps**
  In RayQC Advanced web applications may be tested against different browsers. Currently

RayQC Advanced offers the possibility to test web applications on Internet Explorer 9, Internet Explorer 10, and Internet Explorer 11. Web applications can be either imported or the test can be launched by using the URL. If imported, when performing the test, a connection to the tested web application is still necessary since the resources are downloaded when the test is actually performed.

> **Tip:**
> In order to be able to check if a software package or merge module installation would cause conflicts on a concrete device, a snapshot has to be taken from that device. To do so, users have to install either RayPack itself, or the Standalone Repackager out of the RayPack toolset, on that device. Whilst the capture wizard is executed, it is possible to save the snapshots that are captured during the wizard run. These `.rcs` files may be copied and used as base for testing in RayQC Advanced.

Open the library

Importing has to be performed directly from the UI of the library.
To open this view:
1. Go to the dashboard on the Home Screen
2. Click on the software tile

Preparing the library folder structure

The library contains three sub-views, one per resource type. In order to import any resource into one of the catalog views, a folder structure has to be implemented first.
To create a folder:
1. Within the library, open the view that matches the type of resource that has to be imported.
2. Right-click the content area at the center of the screen.
3. From the context menu, select the option "+ New Folder"
4. The new folder is created with a default name.

   To rename it, simply start typing the new name, as the folder name is already set into the direct inline edit mode at creation.
   To save the new name, hit enter on the keyboard.
   To rename an existing folder: perform a right-click on the folder name, and select "Rename" from the context menu, or select the folder and hit F2 on the keyboard.
5. Folders may be nested.

   To create a sub-folder instead of a root folder (as described above), right-click a folder, and select the option "+ New Folder" from the context menu.
Now that there is a folder structure, resources may be imported.

To import software packages into the library

The library is the right place for storing packages with long-term relevance. Packages relates to `.msi` files. If required, it is possible to add transform files to the base MSI by selecting them during the import wizard execution.

Be aware:
If an MSI has been imported with additional transforms, all tests against that package will be performed on the combination of MSI and MST(s)!

To import a software package into the library:
1. Click on the software item on the left-hand side of the library view.
2. Right-click the folder the software has to be imported into.
3. Select "Import..." from the context menu.
4. Run through the package import wizard

   Please refer to the Import Wizard section for further details on the steps and options of this procedure.
5. Finish the wizard once the package has been imported.
6. The software package has been added to the catalog and automatically selected within the tree view structure of resources.

At the right-hand side of the application window, there is the details pane. When an object is selected from the center folder hierarchy, the details of the object are displayed within this pane. If required, the name, manufacturer, and version of the software package can be modified from within the details pane. It is also possible to add tags to a resource from the details pane. Tags are quite helpful to organize and look-up resources.

Once the package is imported, testing it may very well be the next step to perform.

To import merge modules into the library

The library is the right place for storing merge modules (MSM files) with long-term relevance.
To import a merge module into the catalog:
1. Click on the merge modules item on the left-hand side of the library view.
2. Right-click the folder the MSM file has to be imported into.
3. Select "Import..." from the context menu.
4. Run through the package import wizard

   Please refer to the Import Wizard section for further details on the steps and options of this procedure.
5. Finish the wizard once the merge module has been imported.
6. The MSM has been added to the library and automatically selected within the tree view structure of resources.

At the right-hand side of the application window, there is the details pane. When an object is selected from the center folder hierarchy, the details of the object are displayed within this pane. If required, the name of the module can be modified from within the details pane.

Once the MSM file is imported, testing it may very well be the next step to perform.

To import OS snapshots into the library

To import an OS snapshot into the library:
1. Click on the OS snapshots item on the left-hand side of the library view.
2. Right-click the folder the snapshot has to be imported into.
3. Select "Import..." from the context menu.
4. Run through the package import wizard

Please refer to the Import Wizard section for further details on the steps and options of this procedure.

5. Finish the wizard once the snapshot has been imported.

6. The snapshot has been added to the library and automatically selected within the tree view structure of resources.

At the right-hand side of the application window, there is the details pane. When an object is selected from the center folder hierarchy, the details of the object are displayed within this pane. If required, the name of the snapshot can be modified from within the details pane.

Once the `.rcs` file is imported, testing packages against it may very well be the next step to perform.

To import App-V packages into the library

To import an App-V package into the library:

1. Click on the App-V item on the left-hand side of the library view.

2. Right-click the folder the software has to be imported into.

3. Select "Import..." from the context menu.

4. Run through the package import wizard

   Please refer to the Import Wizard section for further details on the steps and options of this procedure.

5. Finish the wizard once the package has been imported.

6. The App-v package has been added to the catalog and automatically selected within the tree view structure of resources.

At the right-hand side of the application window, there is the details pane. When an object is selected from the center folder hierarchy, the details of the object are displayed within this pane. If required, the name, manufacturer, and version of the software package can be modified from within the details pane. It is also possible to add tags to a resource from the details pane. Tags are quite helpful to organize and look-up resources.

Once the package is imported, testing it may very well be the next step to perform.

To import web application into the library

To import a web application into the library:

7. Click on the web apps item on the left-hand side of the library view.

8. Right-click the folder the web application has to be imported into.

9. Select "Import..." from the context menu.

10.Run through the package import wizard

    Please refer to the Import Wizard section for further details on the steps and options of this procedure.

11.Finish the wizard once the web application has been imported.

12.The web application has been added to the library and automatically selected within the tree view structure of resources.

At the right-hand side of the application window, there is the details pane. When an object is selected from the center folder hierarchy, the details of the object are displayed within this pane. If required, the name of the module can be modified from within the details pane.

Once the web application is imported, testing it may very well be the next step to perform.

Performing Tests

> 📎 **Note:**
> This section describes how to initiate tests in RayQC Advanced. Please read the test wizard overview to get details on the UI and available additional functionalities.

The center piece of activity in RayQC Advanced is performing tests on software packages, App-V packages, and web applications. The following test procedures are available:

Test software for issue indicators regarding

- conflicts with other software packages (installed on the same device)
- conflicts with specific device environments
- the general ability of the software to be used in a virtualized mode
- conflicts with browser

All test types are bundled within the test wizard. It guides through the test parameter definition and enables quick and easy test setups.

To launch the test wizard:

1. There are two basic wizard modes users may initiate:
   a. The wizard may be called from the **home screen**.

      To do so, users have to click on the quick test tile on the dashboard In this case it opens with a dialog that asks for the resource packages that have to be tested.
   b. It is also possible to launch the wizard from the **library**.

      To do so, users have to select one or more software packages from the catalog folder structure, right-click on one of the selected items, and select "Test Wizard..." from the context menu. In this case it opens with a dialog that asks for the test area selection, as the resource packages to test are already defined. It should be notes that the Test Wizard also be directly initialized by selecting the "quick test" tile from the Dashboard.
2. Walk through the steps of the wizard. Please refer to the Test Wizard section for details regarding available settings and options.
3. Please note that the actual test execution duration depends on the amount of source and target packages, and the number of rules that are applied on them during the test run. For a smooth first test run it is recommended to start with a simple setup, which may later be extended to more complex constellations. A simple setup could be one source and target package that are checked regarding all testing areas .
4. Once the configured test procedures are finished, there is a result summary screen as last step of the wizard.

   The interface of this view provides some optional activities:
   a. Save the report as PDF file. Additionally, an ability exist to export the report in other formats including `.docx, .doc, .html, .xps` and `.xml.`
   b. Open the report as PDF file
   c. Review the command line expression of the test setup (for later reproduction).
   d. The test results may be stored as report within the report archive.
5. Click on finish to close the wizard.

a. If the report has been assigned for archiving, the reports archive is loaded, with the newly added report ready for in-depth review.

b. If the report has not been archived, the initial view (dashboard or software dialog) is loaded next.

Take a look at the reviewing reports section to read some basic information about reviewing options.

> **Note:**
> Only reports pertaining to tests executed on a package from the catalog is stored in the Reports section. Reports generated for a package, tested directly from the disk is only available on temporary basis, after execution of the test.

Reviewing Reports

> **Note:**
> This section describes how to review test results in RayQC Advanced. Please read the reports overview to get details on the UI and available additional functionalities.

As soon as a software package has been tested, and that test result has been added to the reports archive, it can be reviewed from that archive. There are two ways to look up the right report from that archive:

1. To review the results of the last test that has been performed on a package, users select the package within the library.
   a. The details pane at the right-hand side contains two tabs: Details and Test results.
   b. Click on the test results tab. A result summary of the last test is displayed.
   c. To review test details, simply click on the "Show full report..." button at the bottom of the tab.
   d. The report archive is loaded, with the requested report selected and ready for review.

2. To browse the archive for a report, users click on the reports tile on the dashboard of the home screen.
   a. The full archive is loaded, ready for manual browsing.
   b. Use the list of archived reports on the left-hand side to look up the archive.

The report list may be filtered by source packages, and ordered or filtered by one of the list columns (source package name, test date, or test type). Once the desired test is found, simply select it to display its details at the right-hand side of the application window.

The details pane always contains a **GENERAL** tab, which contains

- The general test parameter summary
  Including date, overall result, the resource package list, and an input field for comments that should be archived along with the test report.

- A quick diagram
  Displaying the distribution of rules that were passed, returned a warning or an error as a pie chart.

- The summary of the test results on a single rule level
  All rules that have been applied during the test are listed here. If an error or warning was returned for a specific rule, the rules list item may be expanded to reveal further details. The details help to evaluate the issue relevance, and provides useful hints to the origin of the issue

for precise remediation.

Depending on the testing areas that were analyzed during the test execution, there may be one or several further tabs visible at the top of the details pane:

- **COLLISION**
  For results of tests between software packages
- **VIRTUALIZATION**
  For results of tests regarding fitness for virtualization
- **SYSTEM READINESS**
  For results of tests against environments (static OS or snapshot)
- **APP-V**
  For results of tests on App-V packages.
- **INTERNET EXPLORER 9**
  For results of test against the Internet Explorer 9.
- **INTERNET EXPLORER 10**
  For results of test against the Internet Explorer 10.
- **INTERNET EXPLORER 11**
  For results of test against the Internet Explorer 11.

Click on the tab label to reduce the displayed report content to the results of that specific testing area.

Besides reviewing, the reports archive provides handy features for re-running tests, saving, printing, and exporting them. Please refer to the Reports section for further details.

Managing Rule Sets

> **Note:**
> This section describes how to modify rule sets in RayQC Advanced. Please read the rules overview to get details on the UI and available additional functionalities.

Congratulations! By working through the previous sections it is now possible to perform standard tests on software packages. But what if standard is not enough to cover the actual testing needs? Well, RayQC Advanced provides full access to the rule sets it operates on:

1. Open the rule set library by clicking on the rules tile on the dashboard of the home screen.
2. The displayed view contains an overview of all available rule sets along with the rules that are bundled within them.
3. Browse through the rule set structure on the left hand side, and select any item to be able to see its details within the pane at the right-hand side.
   - For a rule set, the details pane contains the number of rule sets and / or rules that are bundled by it.
   - For a rule, the details pane contains
     - a general description of the tested issue
     - a summary of the test procedure RayQC Advanced applies to find out whether the issue is relevant for a software package
     - a weblink that leads to further information
     - a hint on possible remediation measures that usually solve the issue if it has been detected

To create new rule sets

The default state of the RayQC Advanced installation contains a pre-defined set of rule sets, which may be selected individually to be applied during the execution of the test wizard. Each rule set contains a list of rules the set represents. The default bundling of rules in sets may very well be sufficient for initial test scenarios. However, for advanced test procedures it can be required to create new rule sets with custom rule combinations. Within the "custom" parent rule set, new rule sets may be nested.

Note:
Please note that it is not possible to change the position of a rule set once it has been created. Therefore, it is recommended to think of a speaking rule set naming convention that allows swift interpretation and look-ups.

To create a custom rule set:
1. Right-click the rule set named "custom" (or one of its child-nodes) from within the left-hand side of the rules view.
2. Select "**New folder**" from the context menu
3. A new child-node is added to the structure.
4. To rename the new rule set, right-click it and select "Rename" from the context menu, or select it and hit **F2**.
   To save the new name, hit enter on the keyboard.
   To remove a rule set from a custom parent, right-click it, and select "Delete" from the context menu, or select it and hit **F2**.

To add rules to a rule set

Adding rules is possible for custom rule sets. To do so:
1. Right-click the target rule set, and select "+ Add rule" from the context menu
2. An additional menu is displayed. Select one of the testing areas to reveal the rules that are available within the area
3. Activate the checkboxes at the left-hand side to add rules to the set.
4. With a click anywhere outside the context menu, the assigned rules are added to the parent rule set.
   To remove a rule from a custom rule set, simply right-click the rule and select "Delete" from the context menu.

To add new rules

RayQC Advanced operates on a flexible, plug-in-based model of rule management and application. It is possible to extend the default set of rule plug-ins with custom plug-ins for extended test scenarios.
Please contact your Raynet sales representative to get details on technical requirements and consulting services offered for plug-in development by Raynet consultants.

The Home Screen

The **Home Screen** of RayQC Advanced contains a **Dashboard** and a **Recent** section for quick report access. Just like other RaySuite products, the RayQC Advanced **Dashboard** contain tiles which links to the key features and areas of this module.
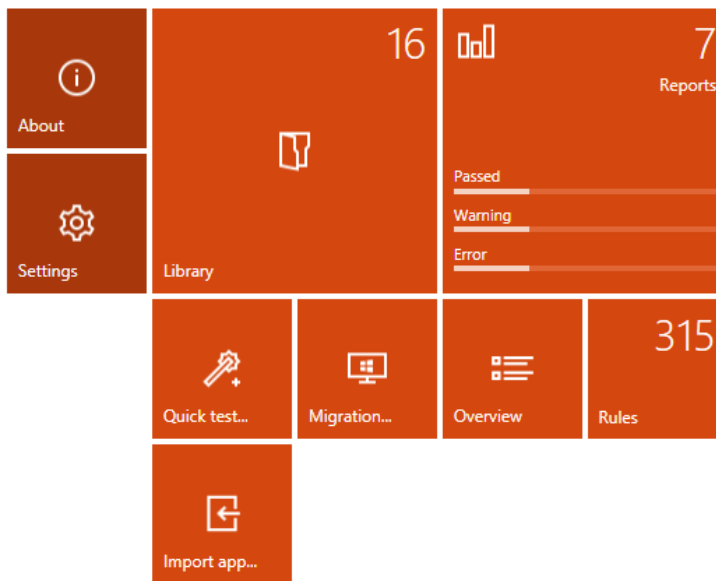
The Dashboard Tiles

Each of the tiles on RayQC Advanced **Dashboard** links to a specific view:

- **About:** Link to various built-in and online resources is available under the **About** view.

- **Settings:** After installation of RayQC Advanced, a user should visit the **Settings** view to verify if the connection to the SQL database is working. Furthermore, if certain rules are missing in the rules view, then a user should recache plug-ins in the **Advanced** section of the **Settings** view.

- **Library**: Links to the **Library** of RayQC Advanced.

- **Reports**: Links to the **Reports** view.

- **Quick test...:** Directly launches the RayQC Advanced **Test** wizard. This option is relevant for scenarios where a user would like to execute test either on a package already in the **Library** or on a package located on disk.

- **Migration...:** Directly launches the RayQC Advanced **Migration** wizard. This option is relevant for scenarios where a migration to another operating system is planned.

- **Import app...:** Opens RMS/SCCM Import Wizard.

- **Overview:** Opens the overview of library packages and presents the overall status.

- **Rules:** Links to the rules library.

Recent List

The **Recent** section of the **Home Screen** shows a list of top five most recent test results stored in the reports view of this module. Selecting an item from this list will open it directly in the **Reports** viewer.

Recent

⊗ **Retest Adobe Reader 9.2 9.2.0**
5/18/2017 9:09:57 AM

⚠ **RayEval 4.1.900.78**
5/5/2017 12:52:14 PM

⚠ **Adobe Reader 9.2 9.2.0**
4/13/2017 10:53:11 AM

✓ **Adobe Flash Player 18 ActiveX 18.0.0.2...**
4/13/2017 10:52:14 AM

✓ **RayEval 4.1.900.78**
4/13/2017 10:51:40 AM

Settings

The **Settings** area of RayQC Advanced can either be accessed via the **Settings** tile on **Dashboard** or from the **Settings** tab in the **Main Toolbar**. It is recommended to check the settings at least once before the productive work with this module begins, since the configuration options offered there determine some properties of the user interface that may help you to gain quick orientation.

The following options can be found in the Settings view:

* **Interface**
* **Database**
* **Deployment**
* **Advanced**
* **Custom fields**
* **Web Apps**
* **RayFlow**
* **Virtual machines**

Saving and Discarding Changes to Settings

To apply changes made in the **Settings** view, click on the **Save changes** button that is located in the bottom swipe-bar of this view. If a user tries to move with unsaved changes in the current view, then a confirmation dialog will be prompted. Selecting **Yes** will save the changes and contrarily clicking on **No** will discard those changes.
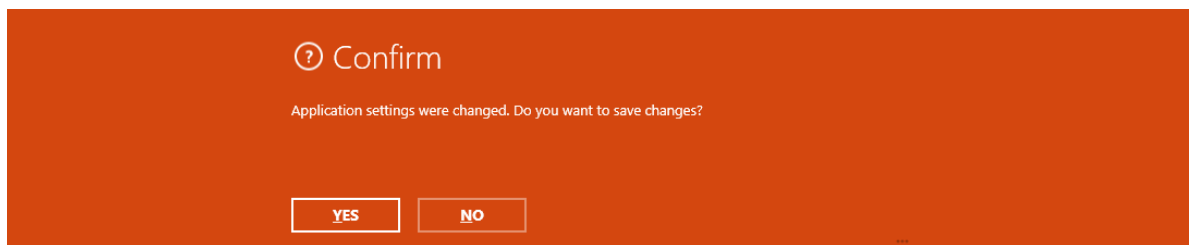
Interface

Underneath this option the settings for the interface can be defined.

Language

User interface language

English

Animations

Enable user interface animations

Yes

Disabling the animations will switch-off the rich user interface transitions, but may help getting a better performance on slow machines or on clients connecting via remote desktop services.

Language
Here users can choose the language for the application by choosing a language from a drop-down menu and clicking on the **Save changes** button. Available languages are English and German. The application needs to be restarted for the changes to be applied.

Animations
This is where users can choose to either enable or disable interface animation. Enabling this option activates rich user interface transition.

Database

Information pertaining to the packages in the **Library** and rules in the **Rule Browser** are stored in a SQL database.

Connection to this database is configured during the installation of RayQC. This settings option allows a user to either modify or test the connection to this database.

Server name
The SQL server is defined here. The server is either defined by its name or by its IP address. It is always defined together with its instance (if an instance is required).

Initial catalog
This is the name of the database which is used by RayQC Advanced as initial catalog.

Connection timeout
Customize the timeframe for the timeout of the connection. It can be specified by clicking on the arrow buttons. For each click a second will be added (arrow button pointing upwards) or subtracted (arrow button pointing downwards).

Authentication
This is where the authentication type is defined. It is possible to choose between Windows Authentication or SQL Authentication. If SQL Authentication is chosen, the user name and the password of a user with read and write access to the database needs to be entered here.

Test database connection
If the **Test database connection** button is used, RayQC Advanced will perform a test to verify that the connection to the database is working.

Deployment

In this tab the settings for the different deployment systems can be configured and information for the configured deployment systems are shown.

SCCM

This is where the connection to the System Center Configuration Manager (SCCM) is configured. The following options are available:

- **Deploying Type:** Select either **Application** or **Package**.
- **Server name**: The name of the server.
- **Share UNC path**: The UNC path.
- **Authentication**: The authentication method that is used for the connection. It can be selected using the dropdown menu.
- **User name**: The user name used for the connection.
- **Password**: The password for the user.

The credentials can be changed using the **Change credentials…** button. Furthermore, the connection to SCCM can be tested using the **Test connection** button.

RMS

To use RayManageSoft the RayManageSoft Console needs to be installed. It this is the case the corresponding information can be found here. Additionally to the information if the RayManageSoft Console is installed or not, the following information can be found here:

- **RayManageSoft version**: The version of RayManageSoft that is used.
- **RayManageSoft server name**: The name of the RayManageSoft server that is used.

This is information from the RayManageSoft Console and cannot be changed.

Advanced

The **Advanced** settings contain five different options. **Plug-ins**, **MSI editor**, **Tags and package families**, **Archive**, and **Console**.

Plugins

Recache plugins and store in catalog: [Recache plugins]

MSI editor

MSI editor location: C:\Program Files (x86)\PackagingSuite\RayPack\RayPack.exe [...]

Tags and package families

Remove not related tags and package families when package is being removed

[●] No

Archive

Remove permanently packages

[Remove...]

Console

Display dialog within the contents of application console

[Open...]

Plug-ins
Under the plug-ins option, the **Recache plug-ins** button is available. When selected, RayQC Advanced connects to its back-end database and updates the **Rules Catalog** in **Rule Browser** view.

MSI editor
Under this option the location of the MSI editor can be defined. Click on the browse button **[...]**, browse to the folder where the executable of the MSI editor is stored and select the .exe which will launch the editor. By default, RayPack is configured as MSI editor.

Tags and package families
Under this option it can be defined if tags and package families should be removed when, after the removal of a package, they have no relations to any packages anymore.

Archive
By using this option it is possible to permanently delete packages.

To delete a package, click on the **Remove...** button. This will open the **REMOVE SELECTED PACKAGES** window. In this view, select the packages that should be permanently removed and click on the **OK** button.

Be aware:
If packages are permanently deleted, all reports related with the packages will also be removed.
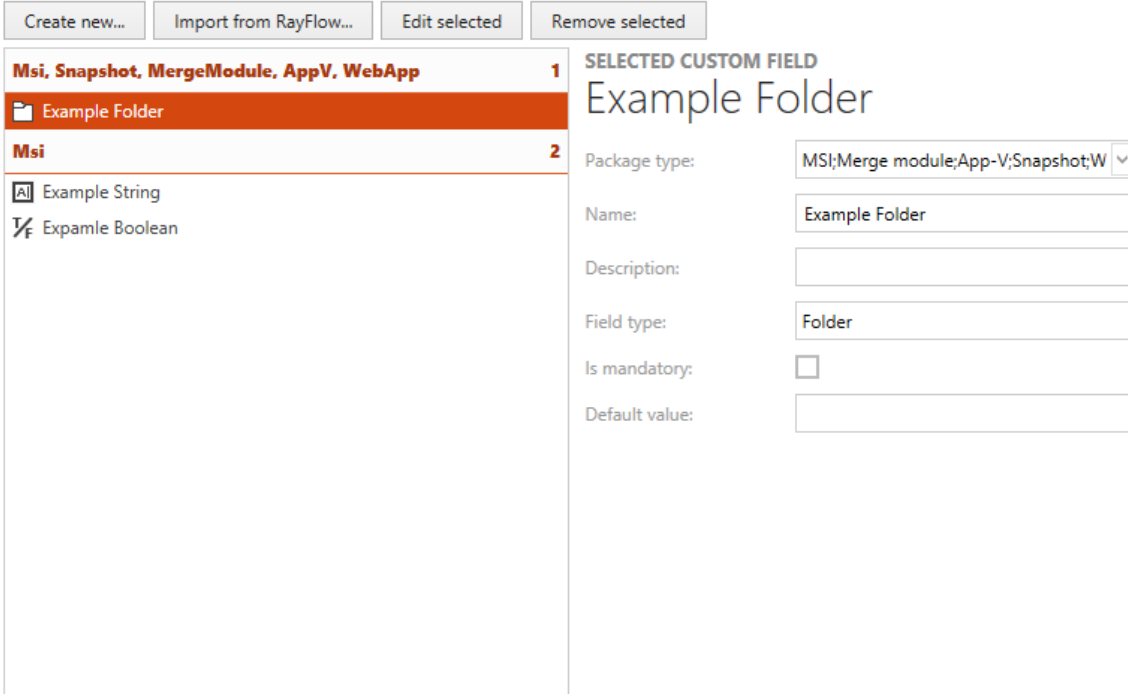
Console

A dialog is displayed within the contents of the application console. To open the **CONSOLE** window click on the **Open...** button underneath this option.

Custom Fields

The **Custom fields** settings contain the **Custom fields** section.

Custom fields which can be added to the package properties are defined here.

New custom fields can be added by clicking on the **Create new...** button. Click on the **Edit selected** button to edit the selected custom field and on the **Remove selected** button to delete a custom field. Editing and deleting a field can also be done by opening the context menu on a field and selecting the respective option. If a field is selected which already is attached to a package or packages, the packages are shown at the bottom of the details section.

For more information on custom fields refer to the *Custom Properties* section of this guide.

Web Apps

Here the settings for the web crawler can be set. There are three different options that can be defined.

Maximum depth

The default maximum depth the web crawler will use can be defined here. When importing a web application this will be taken as the default setting.

Maximum number of links

The default maximum number of links the web crawler will use can be defined here. When importing a web application this will be taken as the default setting.

Crawler URL filter

A default URL filter can be set for the crawler.When importing a web application this filter will be taken as default setting.

RayFlow

This is where the settings for the connection with the RayFlow server can be configured.

The URL address of the RayFlow Server is shown here. Click on the ⊕ button to open the link to the server in a web browser.

Virtual machines

The settings for virtual machines can be configured in this tab of the **Settings** section.
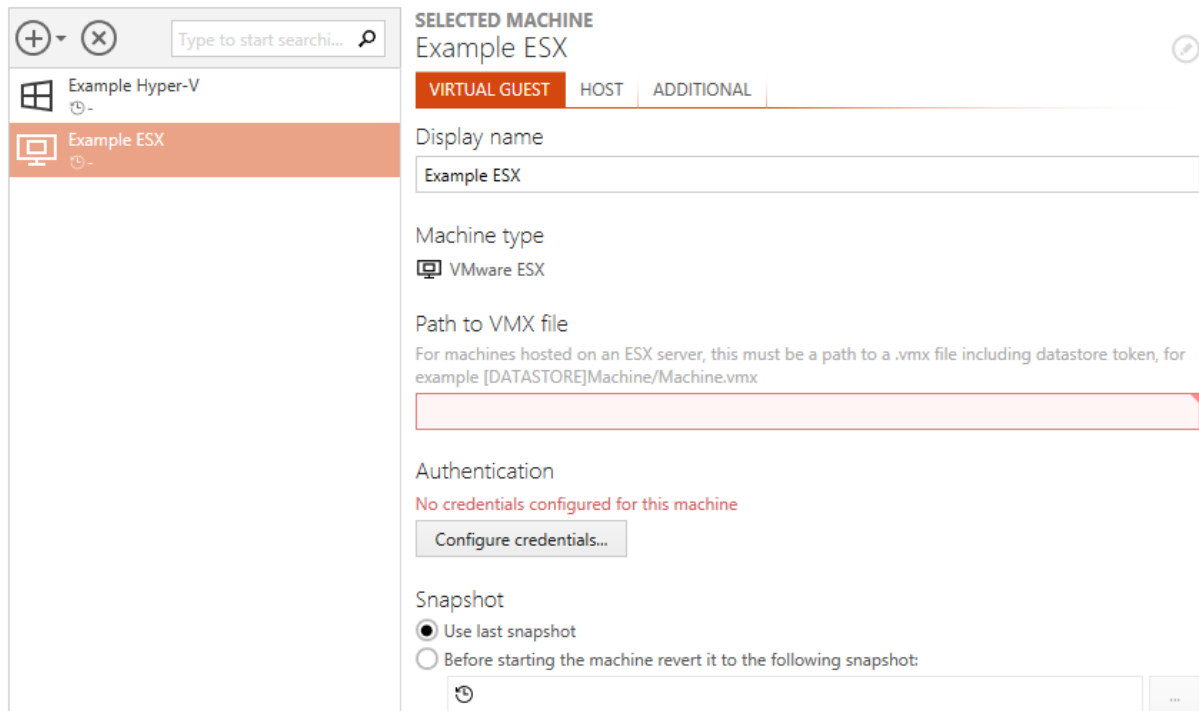
By default, the list of machines is empty. Each machine that needs to be used, has to be imported first. The view is divided into three sections:

- **Function Buttons (Add, Remove, Search)**
  This panel is used to add a new machine, remove a selection and search for machines in the list. In order to filter the list, type a few letters into the search field and the list will be filtered automatically. To clear the results, either click **X** or clear the content of the search box.

- **List of Machines**
  This is a list of all the machines defined for RayPack Studio products. Each machine is represented by an icon representing its type (**VMware Workstation**, **VMWare ESX**, or **Hyper-V**), machine name, and (if configured) the name of the snapshot that is to be used. Select any machine from the list to see its details shown on the right side.

- **Virtual Machine Editor**
  Right panel contains various controls and inputs about the currently selected machine. Further in this chapter their meaning is discussed, together with slight differences between different machine types.

To Import a Virtual Machine...

> ⚠️ **Warning:**
> It is not possible to import virtual machines if RayQC Advanced is already installed on a virtual machine!

1. Press the **+** button to expand the new machine drop-down menu.
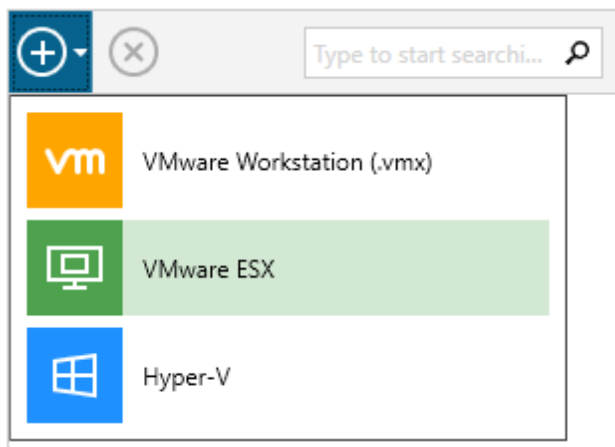
2. Select type of machine to import.
3. The machine will be added to the list. Use the editor to configure the details for the machine.

> **Be aware:**
> Due to technical limitations of the APIs of VMware it is not possible to define both Workstation and ESX machines. Once any of these has been imported, the other type will be disabled!

To Delete a Virtual Machine...

1. Select a machine from the list.
2. Press the **X** button in the functional panel.

Editing Virtual Machines

The virtual machine editor is divided into three tabs. The visibility of tabs depends on the type of the currently selected machine.

Virtual Guest Tab

This tab contains common properties which are valid for all types of supported virtual machines.

- **Display Name**
  This is the name under which the machine is shown in the list. For VMware Workstation and ESX, the name can be an user-friendly string which helps to determine the purpose of the machine (for example *My Repackaging Machine* etc.). For Hyper-V machines, this value must be equal to the name that is visible in the Hyper-V manager.

- **Machine Type**
  The type of the current selection. This setting is read-only.

- **Path to VMX File** (only Workstation and ESX)
  This is the full path to `.vmx` container file. For Workstation machines, this must be a full absolute path to a file, for example `C:\Virtual\Machine\Machine.vmx`). For ESX, the name must include a datastore token (name surrounded by square brackets) followed by relative path of the `.vmx` file. The path can be viewed in the properties dialog directly in a vSphere client. A sample value would be `[DATASTORE]Machine \Machine.vmx`.

> **Be aware:**
> Failure to provide valid file paths to VMX makes the machine unable to work with. Machines with invalid paths or unsupported file formats will be marked as invalid and the user won't be allowed to use them..

- **Computer Name** (Hyper-V only)
  This should be the full DNS computer name of a virtual machine.

- **Authentication**
  This setting configures credentials used to connect to a virtual machine. This field is always required, even if auto-logon is enabled on the guest Operating System. In order to configure the credentials, press the button **Configure credentials...** and enter the user name and password. In order to log in as a domain user, use `DOMAIN\USER` syntax.

> **Be aware:**
> Passwords are stored in an encrypted form in a text file. This however offers by no mean a state-of-art security. Expect that these values can be decrypted easily, and as such never store confidential data on machines with shared access to RayPack configuration files..

- **Snapshot**
  Defines which snapshot is to be used. While it is generally possible to always use the last snapshot (the current one), in a production environment the name of a snapshot should always be specified, either by typing the name manually in the textbox below, or by pressing the **...** button and using the selector dialog.

Host Tab (Only VMware ESX and Hyper-V)

This tab contains the properties of the hypervisor server. Because VMware Workstation uses solely local files, the tab is not visible when working with Workstation machines. When this tab is shown, all values presented here are mandatory.

- **Host Address + Port**
  Defines the location and the port of the host. Contact the responsible administrator to find out these values. By default port 5985 is used for Hyper-V and 443 for ESX machines, but they can be overridden individually.

- **Authentication**
  This setting configures the credentials used to connect to the host. This field is mandatory, even if auto-logon is enabled on the guest Operating System. In order to configure the credentials, press the button **Configure credentials...** and enter the user name and password. In order to log in as a domain user, use the `DOMAIN\USER` syntax.

Note:
The credentials for the host are usually not the same as the credentials that are used to connect to the VM.

Be aware:
Passwords are stored in an encrypted form in a text file. This however offers by no mean a state-of-art security. Expect that these values can be decrypted easily, and as such never store confidential data on machines with shared access to RayPack configuration files..

Additional Tab

- **Comments**
  This is an additional invisible field that can be used for notes and remarks about the machine.

- **Execute tasks on a virtual machine as Administrator**
  By default, the tasks are executed as Administrator, to ensure that the setup files changing machine files and registries are allowed to do it. For certain environments and operations this behavior may not be desired. Unchecking this checkbox makes Raynet start the tasks as the invoker.

Be aware:
This option is only recommended for troubleshooting or for tasks not requiring administrative privileges. Certain Raynet capturing functions may not work when the task is not running as administrator (for example capturing certain shell elements, capturing Windows from higher integrity context, etc.).

Snapshot Selector

To start the **Snapshot Selector** first select the **Before starting the machine revert it to the following snapshot** option that is available beneath the Snapshot heading in the **Virtual Machines** tab in the **Settings**. After the option has been selected, click on the **Browse [...]** button to open the **Snapshot Selector**.
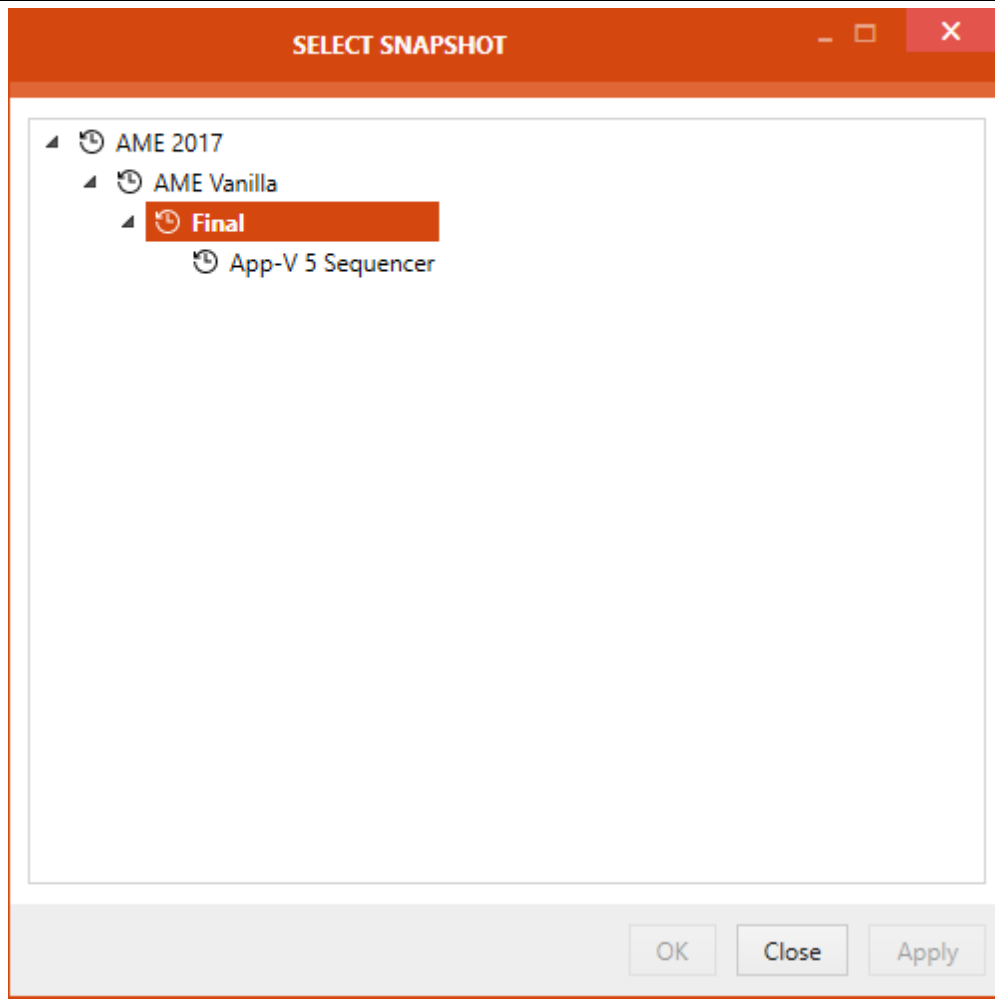
In the **Snapshot Selector** the available snapshots for the virtual machine are shown in a tree structure. Either select a snapshot or close the **Snapshot Selector** without changing the current selection. The following options are available in the **Snapshot Selector**:

- **OK**: This option is used to close the **Snapshot Selector** saving the currently selected status.
- **Close**: This option is used to close the **Snapshot Selector** without saving the changes.
- **Apply**: This option is used to save the currently selected status without closing the **Snapshot Selector**.

Advanced Configuration Options

Besides the product configuration options that are available from the **Settings** section of the application UI, there are some additional configuration settings users may adjust to tailor RayQC Advanced towards their individual requirements.

Logging RayQC Advanced Activity

The program data directory (%`AppData%\Roaming\RayQCAd\Logs`) is used by default to store the application activity log file (`dd-MM-yyyy-HH-mm-ss.log`). If the default settings remain unchanged, RayQC Advanced adds a new line to this log file for every system DEBUG level message that is generated during application use.

The log is by default to be used as in a rolling appender manner, which means that one global log file is permanently extended until a certain file size is reached. As soon as it is reached, the oldest lines are automatically transferred into an archive of log files, which is by default limited to 10 files. When this second limit is reached, the oldest archive is removed to free a slot for the newest archive file.

In order to change the default settings for the log file behavior, users have to manually edit the `log.config` file, which resides in the root of the installation folder of RayQC (usually something like `C:\Program Files (x86)\RayQCAdvanced\`). The settings which are most likely to be of interest for adjustments are:

Log File Storage Location

The log file is by default "`%appdata%\RayQCAd\Logs\dd-MM-yyyy-HH-mm-ss.log`". However, it is possible to define any other absolute local paths as well as shared network locations for logging resource storage.

```
<file type="log4net.Util.PatternString"
      value="%env{AppData}\\RayQC AdvancedAd\\Logs\\%date{yyyy-MM-dd HH-mm-ss}" /
>
```

> **Be aware:**
> The user that runs RayQC Advanced must have write permissions in the log file location in order to initiate and maintain the message flow to the log file. If the user does not have sufficient access rights, there will be no error message, or actual product usage cutback, but simply a loss of system activity documentation. Please refer to the Troubleshooting section for additional instructions in case of missing logs.

Max. Log File Size

The max. log file size may be defined as `KB`, `MB`, or `GB`. The default setting for newly installed RayQC Advanced instances is "`2048KB`"

```
<maximumFileSize value="2048KB" />
```

Log level

The most frequently used log level settings are DEBUG, INFO, WARN, ERROR, FATAL, OFF, whilst OFF prevents logging at all, FATAL is the most restrictive but still writing setting, and DEBUG the most talkative option.

The recommendation is to use the DEBUG level for newly setup systems, since a lot of the information logged in this mode may help to adjust settings regarding access rights, and the like. As soon as the application and system are up and running productively, setting the log level to WARNING should be sufficient for permanent maintenance.

```
<level value="DEBUG" />
```

Default logging configuration

The default configuration file is given below as a review and backup support:

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>

  <configSections>
    <section name="log4net"
type="log4net.Config.Log4NetConfigurationSectionHandler, log4net"/>
  </configSections>

  <log4net>

    <appender name="RayQCAd" type="log4net.Appender.RollingFileAppender">
      <immediateFlush value="true" />
      <file type="log4net.Util.PatternString" value="%property{LogFilePath}\%
date{dd-MM-yyyy-HH-mm-ss}.log" />
      <param name="StaticLogFileName" value="false" />
      <maximumFileSize value="10240KB" />
      <rollingStyle value="Once" />
      <maxSizeRollBackups value="2" />
      <layout type="log4net.Layout.PatternLayout,log4net">
        <param name="header" value="/*************************** LOG HEADER
***************************/&#xD;&#xA;"/>
        <param name="footer" value="/*************************** LOG FOOTER
***************************/&#xD;&#xA;"/>
        <param name="ConversionPattern" value="%d [%t] %-5p %c - %m%n" />
      </layout>
      <threshold value="INFO" />
    </appender>

    <root>
      <level value="ALL" />
      <appender-ref ref="RayQCAd" />
    </root>
```

```
    </log4net>
</configuration>
```

Further Information

RayQC Advanced uses an external library to provide logging functionality. Please refer to the online-documentation provided for the log4net project (http://logging.apache.org/log4net/) in order to get further details regarding available configuration and usage options. log4net can be adjusted to connect directly with databases or event-loggers. There are numerous options for layout and behavior manipulations. RayQC Advanced system administrators with a slight affection for perfection are highly welcome to configure their very own logger version.

About
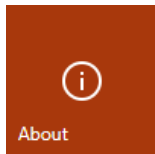
Choosing the **About** tile from the **Home Screen** displays the **About** area. It contains the get started view, providing information about the individual tools of RayQC, links to various resources pertaining to this module. Additional supportive views regarding license and edition as well as troubleshooting are available by clicking on the other view tabs of the **About** area.

Get Started

This section is meant to provide a starting point to new users of RayQC Advanced. This section allows user to directly access various help and online resources.
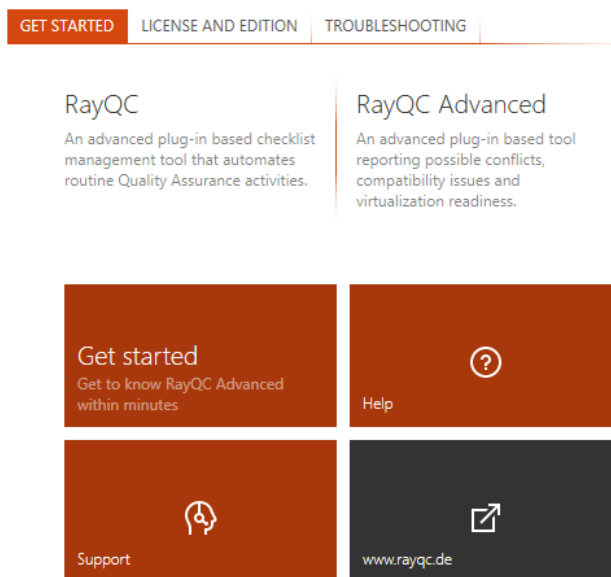
Resources

RayQC Advanced includes various resources that can be used to make the experience with this module more productive and provide help where needed. Please note that some resources (including some items in this help file) are only available on-line or with an internet connection.

Get started
Opens the *Get Started Guide* for RayQC Advanced.

help
Opens the help document.

support
Opens the website for product support contact.

www.rayqc.de
RayQC Advanced on the web.

ad

License and Edition

The **About** area contains the **LICENSE AND EDITION** view, providing all usage relevant license information about the current product instance.

Here, a variety of information is shown regarding the current version of RayQC Advanced and the applied license file. Changing the license can be achieved using the license wizard by choosing **Open the license wizard**.

Troubleshooting

The about area contains the **TROUBLESHOOTING** view, providing handy information about the crucial system paths defined for the current product instance.

Any information displayed within this tab is read-only. It is provided to ensure transparency about the current instance settings, which is vital for proper troubleshooting measures in case of support relevant issues.

Installation Folder

This path shows where the currently running instance of RayQC Advanced is located. Click on the **Open installation folder** link to open a windows explorer instance at the displayed location for further instance resource review.

Logging and Performance Diagnostic

RayQC Advanced is by default configured to write log files with information about each product work session. A new log file will be generated for every launch of the current application instance. These log files contain vital information for any troubleshooting or help desk measure, such as environment information about the physical machine RayQC Advanced resides on, the steps performed during a session, and exception details thrown by the application in case of operational issues. Please make sure that the target directory displayed here provides sufficient disk space and is accessible for the currently logged in user. Click on the Open logs folder link to open a windows explorer instance at the displayed location for further instance resource review.

Extracted Data

This path shows the extraction location for imported packages in software library. During a package import a user can choose to extract the package files. Doing so creates a new folder under this path and the related files are extracted under it.

Library

The **Library** catalogs the packages imported by users for testing. This library can be accessed by selecting software element on the RayQC Advanced **Dashboard**. This library is basically a front-end for packages which are imported by users and stored in the back-end SQL database.

The library categorize packages into five types: **SOFTWARE**, **MERGE MODULES**, **OS SNAPSHOTS**, **APP-V**, and **WEB APPS**. Within each of the categories a user can arrange packages using hierarchical folder structures.
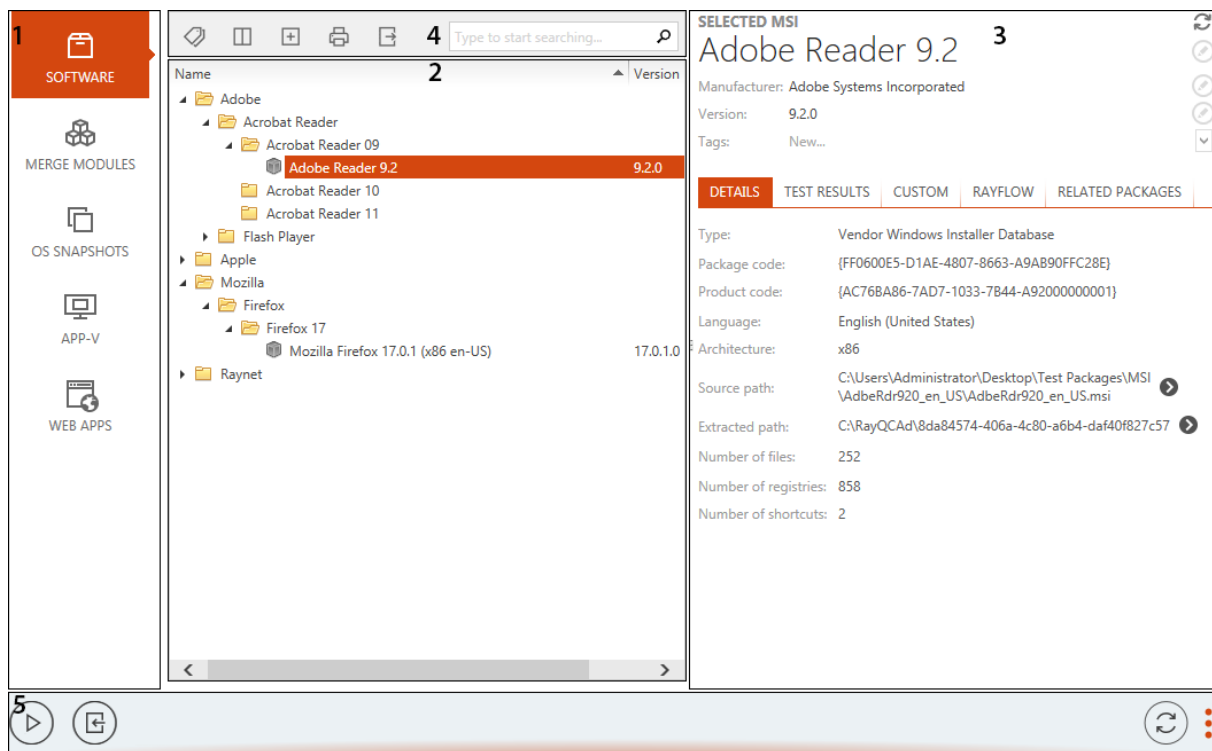
The Library interface can be divided into five areas:

1. Imported file type
2. Content area
3. Side bar
4. Functional Tool Bar
5. Swipe bar

Imported File Type

As previously mentioned, the **Library** categorizes packages based on their type. These types include software(`.msi`), merge module(`.msm`), OS snapshot(`.rcs`), APP-V (`.appv`) and web applications. To import a package in the content area, a user first need to select the package type from this area.
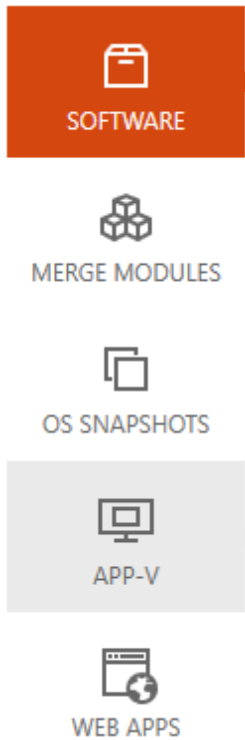
Content Area

Content area of the **Library** is the area where packages are stored and cataloged. For an imported package, the name and version of the package is shown under the **Name** and **Version** column headers.
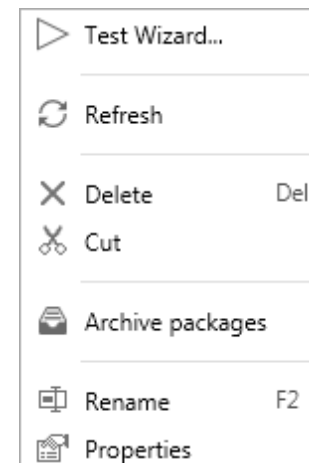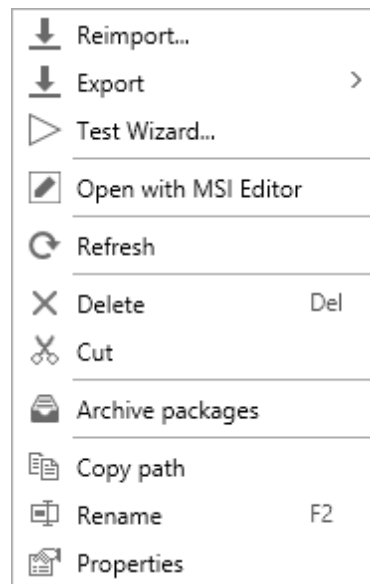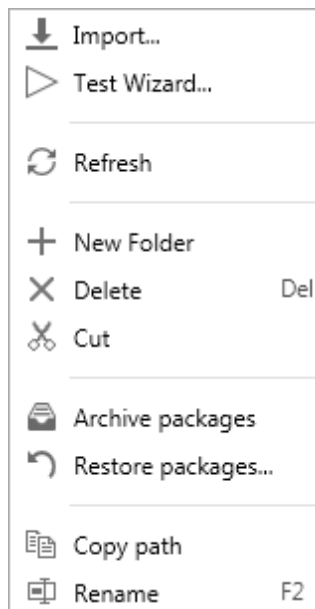
context menu: folder	context menu: package	context menu: web application

Functional options available in this area can be accessed by the context menu. This menu is available when a user right clicks within this area. Options available through context menu include:

- **Import...**: When selected, the **import package** wizard is launched. It is important to note that, a package can only be imported inside a folder. Hence this option only gets activated when a user right clicks on a folder.

- **Reimport...**: Allows a user to reimport a package into the **Library**

- **Export**
  This option can be used to start the **Deployment Wizard** and export the selected package.

- **Test Wizard...**
  When chosen on a package, this option launches the **test** wizard with the selected package as source package for testing.

- **Link RayFlow package**
  Allows a user to link the selected package with a RayFlow package.

- **Unlink RayFlow package**
  Allows a user to unlink the selected package with a RayFlow package.

- **Open with MSI Editor**
  This option is only available if an MSI editor is installed. The source package that has been imported can be edited in the configured MSI editor. By default, RayPack is the configured MSI editor.

- **Refresh**
  Refresh the content area

- **New Folder**
  Creates a new folder

- **Delete**
  Allows a user to delete a folder or package from the content area. Can also be used by using the **Del** shortcut.

- **Cut**
  This allows the user to move an item or a folder to another folder. Clicking on **Cut** after the context menu has been opened on an item or a folder will enable the **Paste** option. If the **Paste** option is used on a target folder, the item or folder on which the **Cut** option was used will be moved to the selected folder. Be aware, that a folder cannot be moved to its sub-folder

but only to a different folder. Items and folders can also be moved by drag and drop.

- **Archive**
  This function is used to archive packages together with the corresponding reports in the database. Archived packages are not shown in the library and cannot be used as target packages.

- **Restore...**
  This function opens a window which shows all packages which are archived in the database. The archived packages can be restored to the library. The **Restore...** function is only visible if the context menu is opened on a folder.

- **Copy path**
  Copies the path under which the target package is stored in the database into the cache.
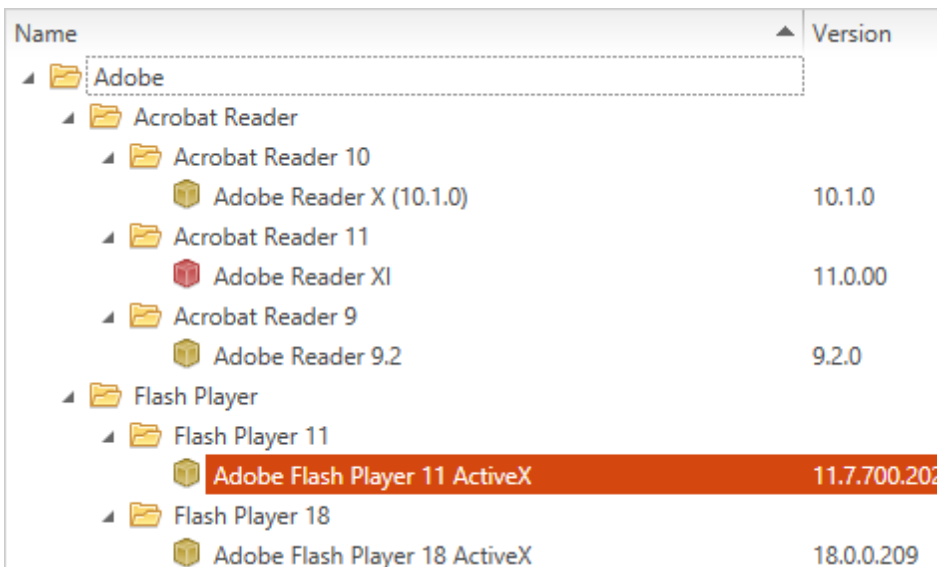
- **Rename**
  Allows a user to rename an imported package or folder. This function is also accessible via **F2** shortcut.

- **Properties**
  When selected on a package within the **Library**, a properties wizard is available. This wizard shows details pertaining to a package. For more on properties refer to this *section*.

Content Management

Within the content area of the **Library**, users can define folder structure to arrange packages in a hierarchical fashion.
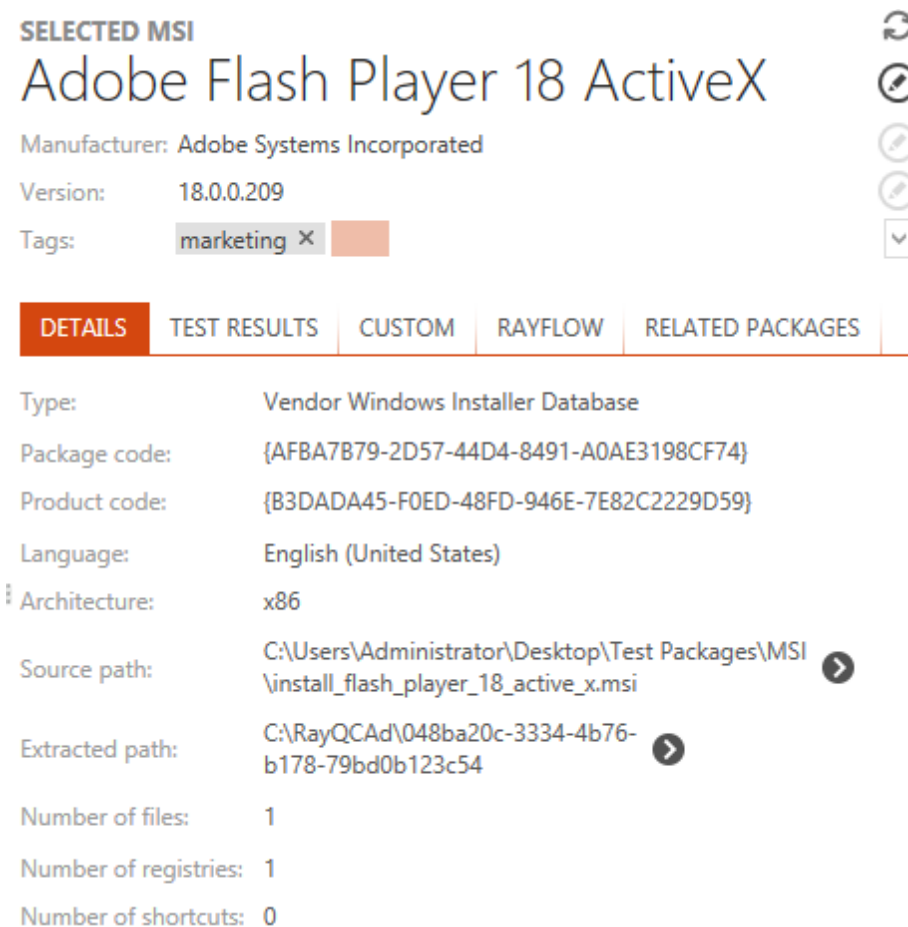
Name	Version
◢ 📂 Adobe	
◢ 📂 Acrobat Reader	
◢ 📂 Acrobat Reader 10	
📦 Adobe Reader X (10.1.0)	10.1.0
◢ 📂 Acrobat Reader 11	
📦 Adobe Reader XI	11.0.00
◢ 📂 Acrobat Reader 9	
📦 Adobe Reader 9.2	9.2.0
◢ 📂 Flash Player	
◢ 📂 Flash Player 11	
📦 Adobe Flash Player 11 ActiveX	11.7.700.202
◢ 📂 Flash Player 18	
📦 Adobe Flash Player 18 ActiveX	18.0.0.209

Side Bar

Side bar is available on the right side of the **Library**. When a package is selected in the content area, properties and test result pertaining to it, is shown in this area.

DETAILS

As shown in the image above, the swipe bar on top shows the basic properties of the package including its name, manufacturer, version, and tags. A user can modify these properties by selecting the edit tool, which is available on the right side of each property.

Further information on the selected package is divided under the tabs: details and test results. Under the details tab following properties are shown for the selected package:

- **Type**
  The type of the imported MSI (Vendor / Self-made / Wrapper).

- **Package code**
  The unique identifier of the package.

- **Product code**
  The unique identifier of the product.

- **Language**
  The application language is shown as string and the related language code is shown as tooltip.

- **Source path**
  The path from which `.msi` file was uploaded.

- **Extracted path**
  The extract path where the file from Windows Installer has been extracted.

- **Number of files**
  The number of files from the package.

- **Number of registries**
  The number of registry entries.

- **Number of shortcuts**
  The number of shortcuts in the package.

TEST RESULTS

Current and historical test results for a selected package are available under the **TEST RESULTS** tab. Information available under this tab is interpreted using raw data, symbols, and a graphical chart.

SELECTED MSI

Adobe Reader 9.2

Manufacturer: Adobe Systems Incorporated

Version: 9.2.0

Tags: New...

DETAILS | **TEST RESULTS** | CUSTOM | RAYFLOW | RELATED PACKAGES

Adobe Reader 9.2 9.2.0

✖ Error
errors have been found

Passed	Warning	Errors	Skipped	Approved	Fixed
114	31	4			5

Show full report...
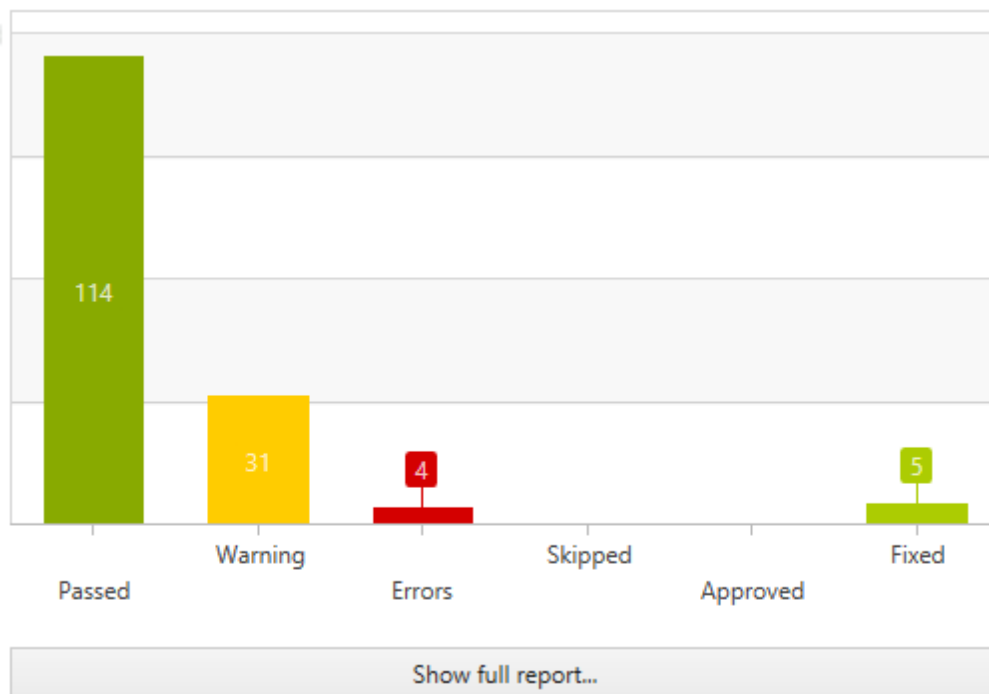
Just under the **TEST RESULTS** tab, the name of the package is shown. Clicking on the edit tool, next to this name will show the historical test result for the package.

A user can access the full test report for the selected package by clicking on the **Show full report...** button, which is available at the bottom of this tab.

RELATED PACKAGES

Packages belonging to the package family of currently selected package are shown under the **RELATED PACKAGES** tab of the side bar. For more information on **Package Families** see the *Package Families and Tags* section of this document.

RAYFLOW

Details about linked RayFlow packages are available in the **RAYFLOW** tab. A user can find package information as well as change the current trigger or add a new comment.

Functional Toolbar

A **Functional Toolbar** is located above the content area of the **Library** view. Each of the functionality offered through is toolbar are described in turn in the following sections.
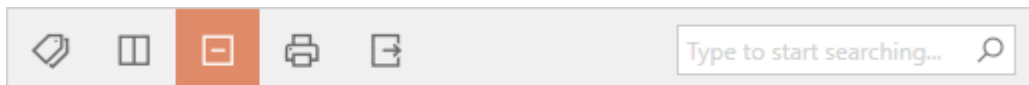
Filtering Data Based on Tags

Tags can also be used to filter data within the library. For more information on **Tags** see the *Package Families and Tags* section of this document.

Click on the tags icon to show a list of existing tags. Select the target tags for filtering and then click on the **OK** button.
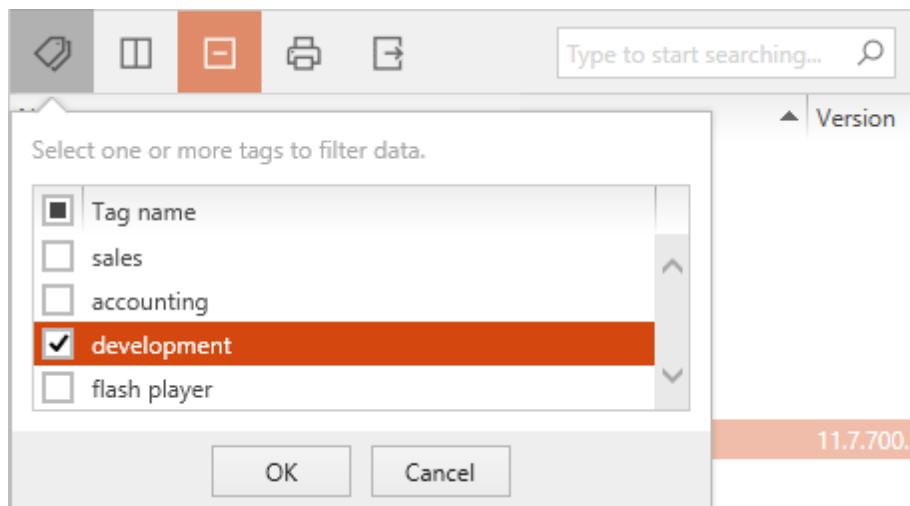
Column Chooser

A user can change the position of each column by dragging it to the desired position. During dragging blue arrows indicate the target position when the column is dropped at this point

Click on the **Column Chooser** icon to display the **Column Chooser** menu. It contains all the available columns, that are not displayed in the current list setting. To add a column to the view, simply drag it from the menu to the header section of the **Library**. To remove a column, drag the column header to the **Column Chooser** menu.
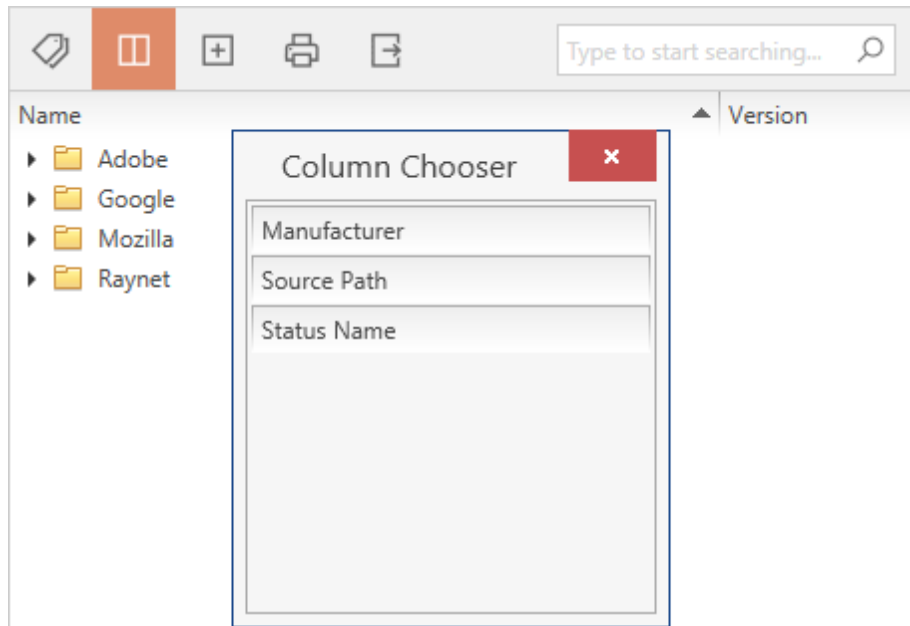
To close the **Column Chooser** menu, click on the close icon at the upper right corner of the menu, or use the choose columns icon.

Collapse All Groups

The **Collapse all groups** button is automatically shown and highlighted when one or more groups have been expanded either manually or by using the **Expand all groups** button. If clicking on the **Collapse all groups** button, all groups in the **Library** will be collapsed and the button will be replaced by the **Expand all groups** button.

Expand All Groups

The **Expand all groups** button is automatically shown when all groups have been collapsed. As soon as one group is expanded the button is replaced by the **Collapse all groups** button. If clicking on the **Expand all groups** button, all groups in **Library** will be expanded and the button will be replaced by the **Collapse all groups** button.

Print

To print the currently displayed content of the **Library** view, hit the print icon. A dialog opens, that allows a user to select the desired printer and printing options.

Export

Exporting the library contents can be handy for communication on certain items or structures.

The currently displayed contents of the **Library** view can be exported to the following formats:

- Excel
- PDF
- HTML
- CSV

To export data:

1. Click on the **export** icon.

   A dialog opens, in which a user can select the desired format and target location for the export.

2. Click **OK** to start the export.

Search
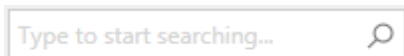
A user can search through the **Library** by using the search bar. Based upon the entered search keyword, the catalog will be filtered to show the related content.

Swipe Bar

Swipe bar is available at the bottom of **Software** view. The swipe bar comes along in two display states: expanded and collapsed. In the collapsed state, there are only button icons while the expanded mode displays additional text information about functionality related to each button provided within the swipe bar. To switch between two, described states, user have to click on the dot icons at the right-hand side of the swipe bar.

Following functions are available through this bar:

- **Run tests**: Launches the **test** wizard

- **Import package**: When selected, the **package import** wizard is initialized

- **Refresh**: Refresh the content area

Properties of packages

When opening the context menu on a package and selecting **Properties** from the context menu there are two tabs available. The **BASIC INFORMATION** tab, which offers editable information about the selected package, and the **PACKAGE FAMILY** tab, where the Package Families of a package can be edited. The changes made by the user can be applied by using the **Apply** button at the bottom right corner of the **PROPERTIES** window. For more on the **PACKAGE FAMILY** tab and the function of Package Families refer to the *Package Families and Tags* section of this document.
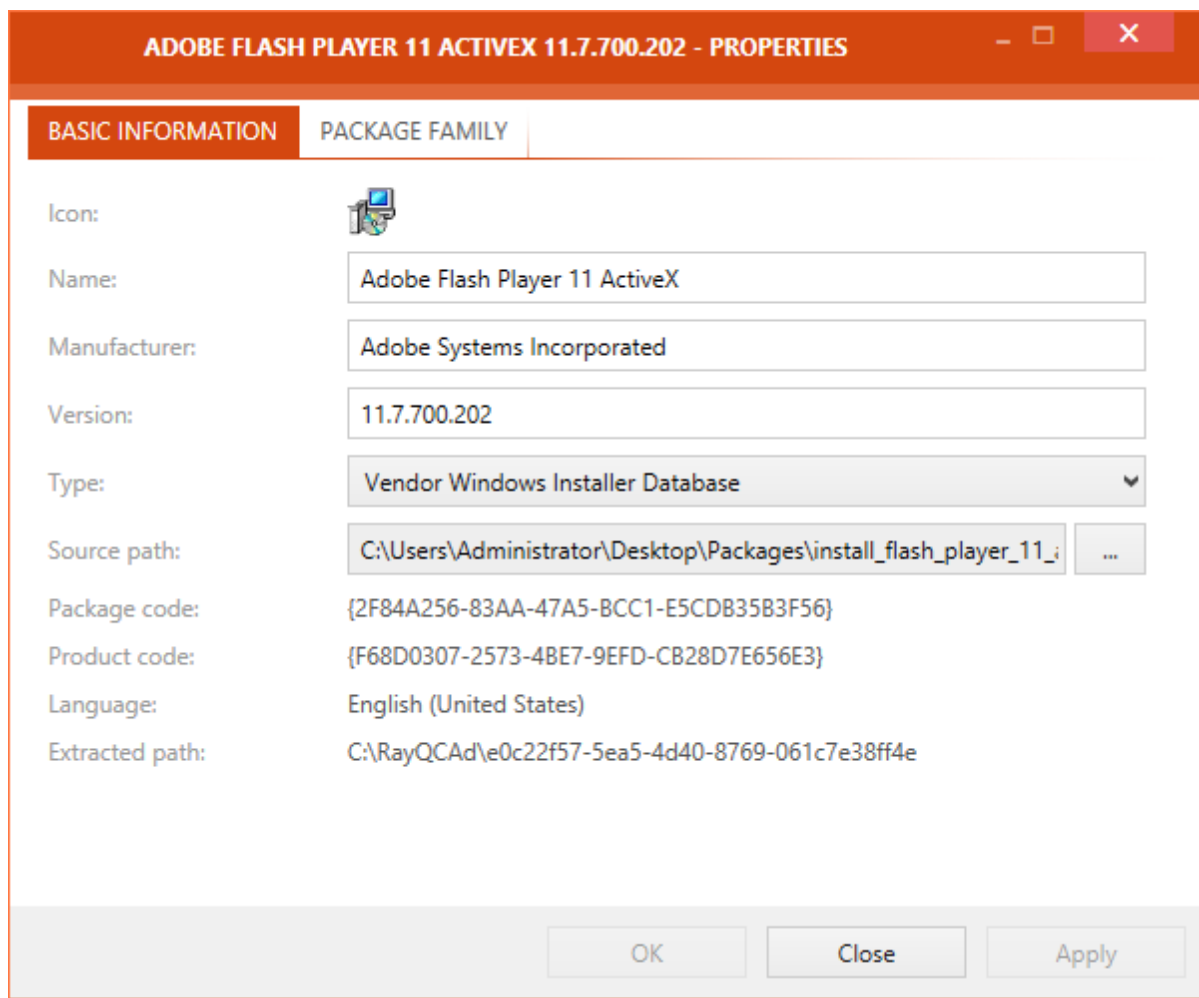
In the **BASIC INFORMATION** tab the following information are available:

- **Name**
  This field contains the name of the package. This field can be edited.

- **Manufacturer**
  This field contains the name of the manufacturer of the package. It can be edited.

- **Version**
  This field contains the version number of the package and can be edited.

- **Type**
  The type of the package can be set to either Vendor Windows Installer Database, Self-Made Windows Installer Database or Wrapper Windows Installer Database. The respective type can be chosen by using the drop-down menu.
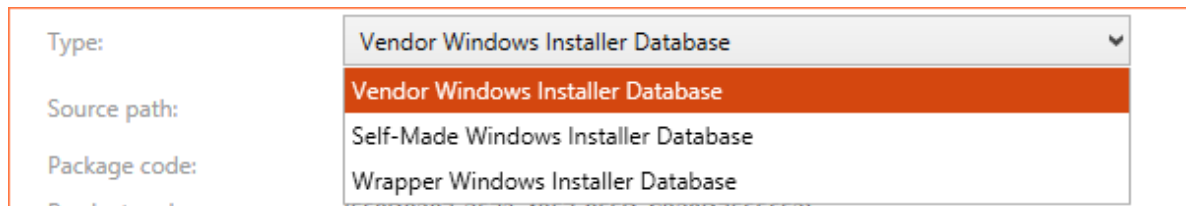
- **Source path**
  The path to the source package an be set here. By default, this is the path from where the package has been imported into RayQC Advanced Advance. This field is editable.

- **Package code**
  The package code is shown here. The package code cannot be edited by the user.

- **Product code**
  The product code is shown here. The product code cannot be edited by the user.
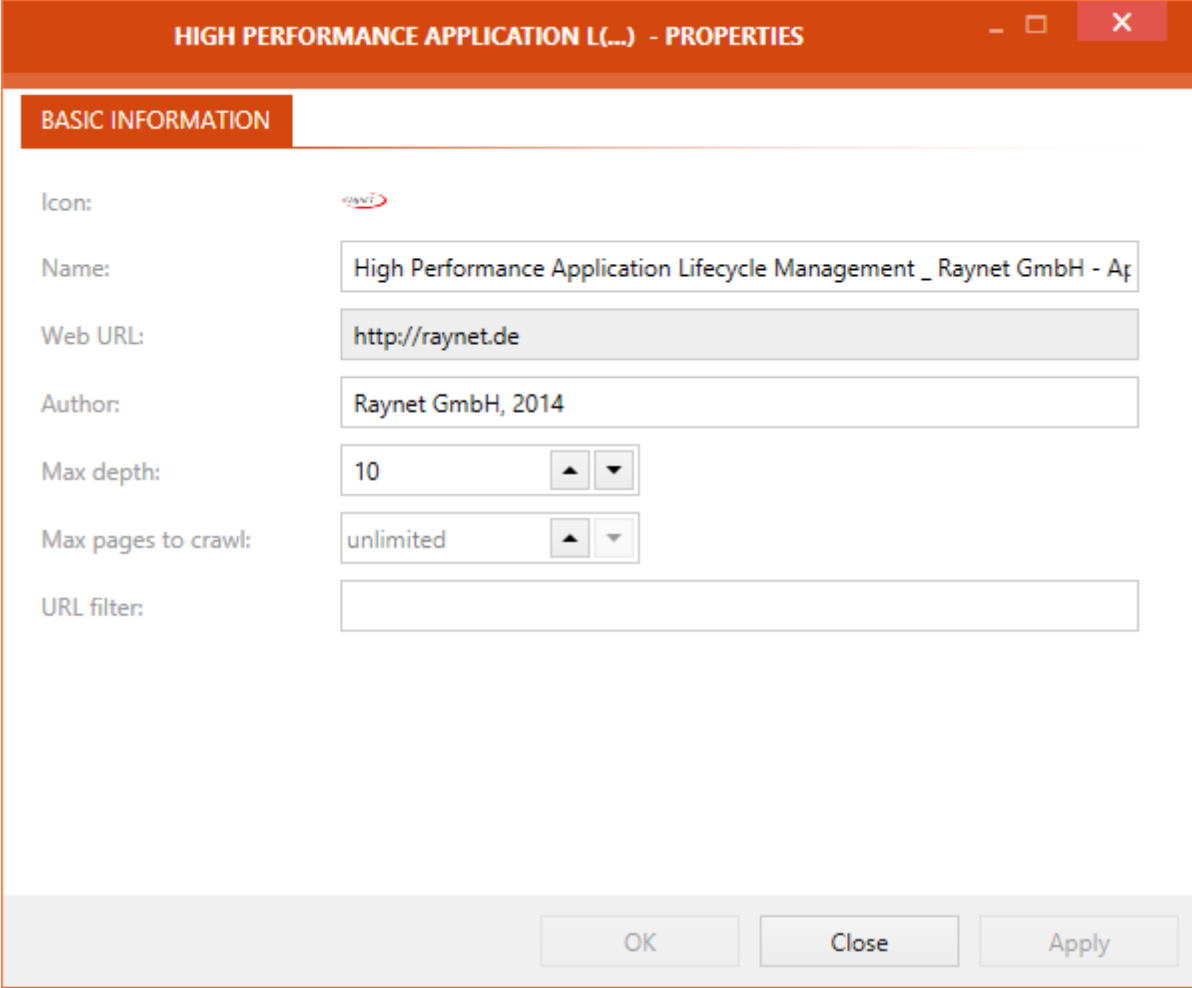
- **Language**
  The language of the package is shown here. This information cannot be edited by the user.

- **Extracted path:**
  The extraction path of the package is given here. It consists of the normal extraction path and the specific folder to where the package has been extracted.

Properties of Web Applications

When opening the context menu on a web application and selecting **Properties** from the context menu the **Properties** screen for the web application is shown.

In the **BASIC INFORMATION** tab of the **PROPERTIES** window the following information are available. Most of the fields are editable and changes can be saved by using the **Apply** button:

- **Icon**
  This field contains the icon of the web application. This is one of two fields in the **PROPERTIES** window of the web application that is not editable by the user.

- **Name**
  This field contains the name of the web application and is editable by the user.

- **Web URL**
  This field contains the URL of web application. This is is one of two fields in the **PROPERTIES** window of the web application that is not editable by the user.

- **Author**
  This field contains the name of the author of the web application and is editable.

- **Max depth**

This field contains the Max depth that will be used when scanning the web application. This option defines the maximum number of links the web crawler will follow (e.g. the target application contains a link to another web application which links to the next web application etc.). This field is editable by the user.

- **Max pages to crawl**
  This field contains the maximum number of pages to be crawled by a scan of the web application. This option defines the maximum number of pages that will be scanned. This field is editable by the user.

- **URL filter:**
  The URL filter can be set here. A scan will only include pages matching the filter and exclude all other pages. For example, if `*.raynet.*` is set as filter, the web crawler will only scan pages where the URL contains "`.raynet.`". This field is editable by the user.

Package Import Wizard

Package import wizard allows a user to import/re-import a software packages into the library. This wizard can be accessed either via the context menu within the library or using the **Import...** option in swipe-bar.

In order to maintain a coherent structure within the library, a user can only import a package under a folder. Hence, the **Import...** and **Reimport...** option is only activated when a user access the context menu either over a folder or an existing package.

In comparison to being launched via the context menu, the Import Package Wizard shows additional steps when initialized via the swipe-bar. These steps include specifying the package type and destination folder.

Importing a package via the context menu

Using the **Import...** option in the context menu, a user can import a package of type software, merge module, OS snapshot, or web application; under the respective categories of the library.

Importing a Software Package

An active **Import...** option is available in the context menu, launched over a child element (folder or package) of a parent folder.

The following steps, precisely describe the steps required in order to import a software package:

1. From the application dashboard, select the **library** item to load the **SOFTWARE** view

2. Within the library, either create a new folder or navigate to an existing folder, under which the package is to be imported

3. Right click upon the target folder, to show the context menu
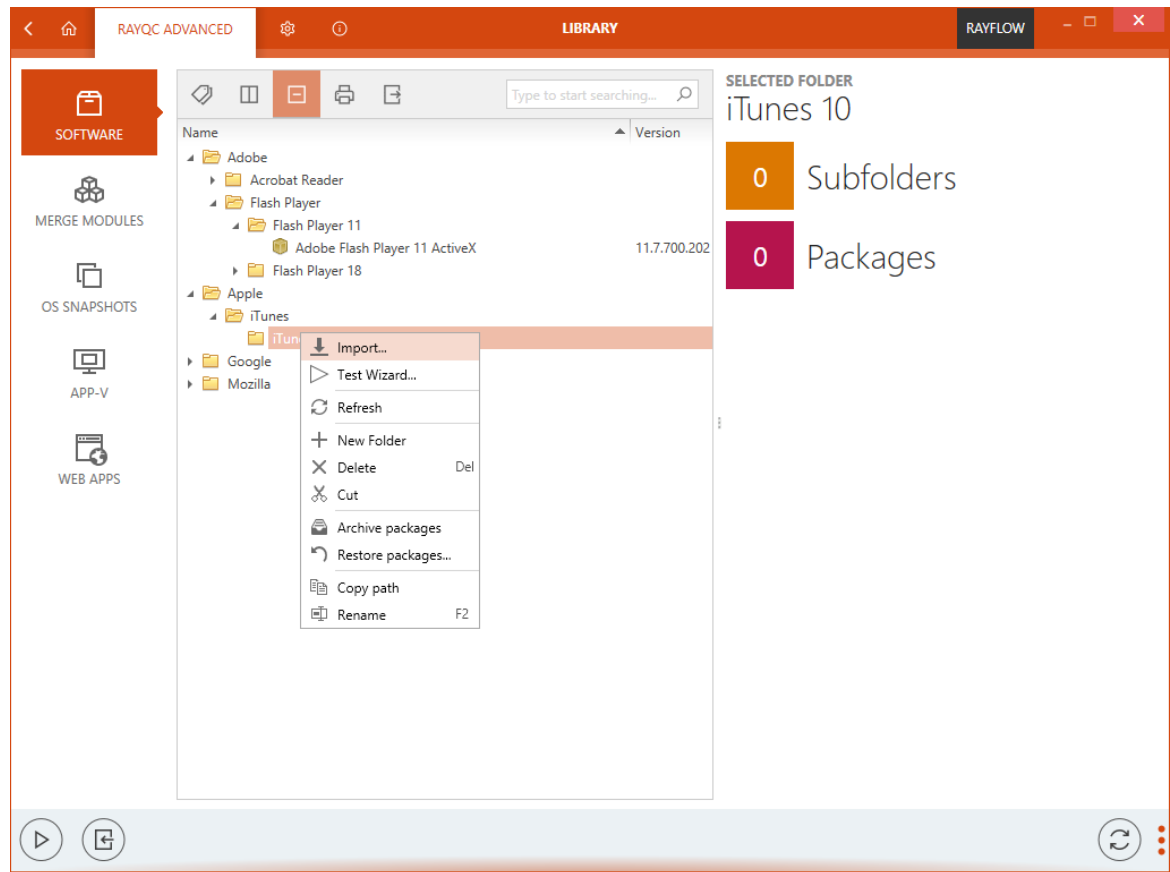
4. Select the **Import...** option from this menu
   IMPORT PACKAGE WIZARD is launched
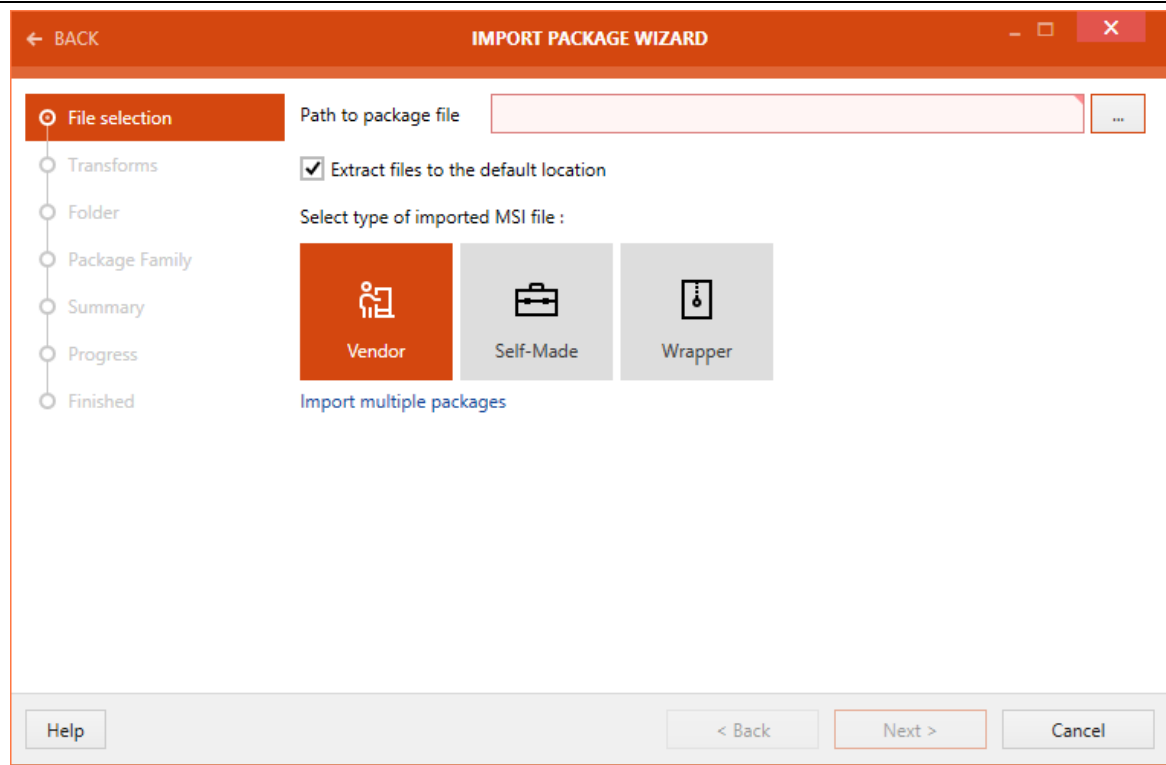
5. In this wizard, the first view shown is the **File selection** view. This view allows a user to specify the `.msi` file, its type and an option to extract the `.msi` to the default extraction folder. Additionally, the **Import multiple package** option, allows a user to import multiple packages at the same time.

- **Type of MSI imported file**: In RayQC Advanced, an imported `.msi` file can be of three types: **Vendor**, **Self-Made** and **Wrapper**.

  o **Vendor**: A `.msi` file delivered by a vendor and includes a valid signature.
  o **Self-Made**: A `.msi` file provided by a packager and may contain a signature.
  o **Wrapper**: A wrapper `.msi` file is usually a program used to execute one or more other installation programs.

- Extract files to the default location: This option that is by default enabled, extracts the imported `.msi` file to the default extraction directory. Link to this extraction directory is shown under the **TROUBLESHOOTING** tab of the **ABOUT** view.

6. After selecting a path to the `.msi` file being imported, click on the **Next >** button to proceed **Transforms** view is shown.

7. Click on the **Add** button, to add transform to the package being imported. An existing transform can be removed and arranged using the **Remove**, **Up**, and **Down** buttons.
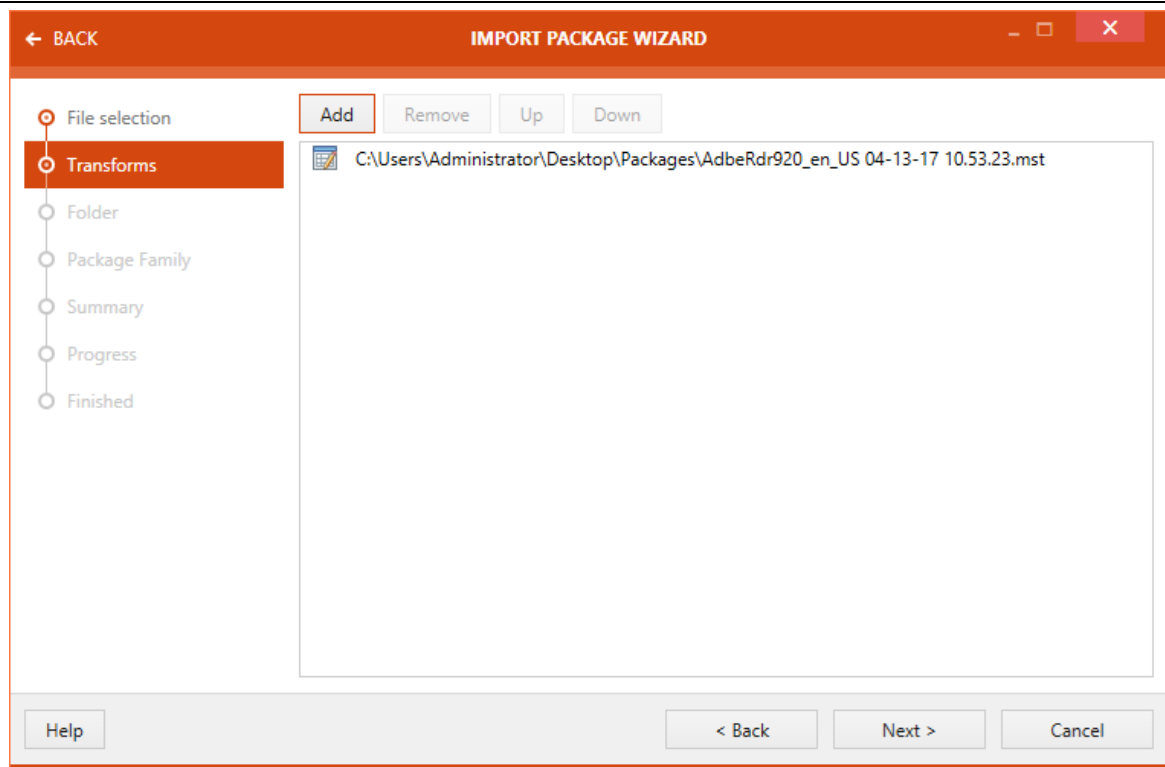
Click on the **Next >** button to proceed further.

8. A target folder can be selected in the Folder section of the wizard.
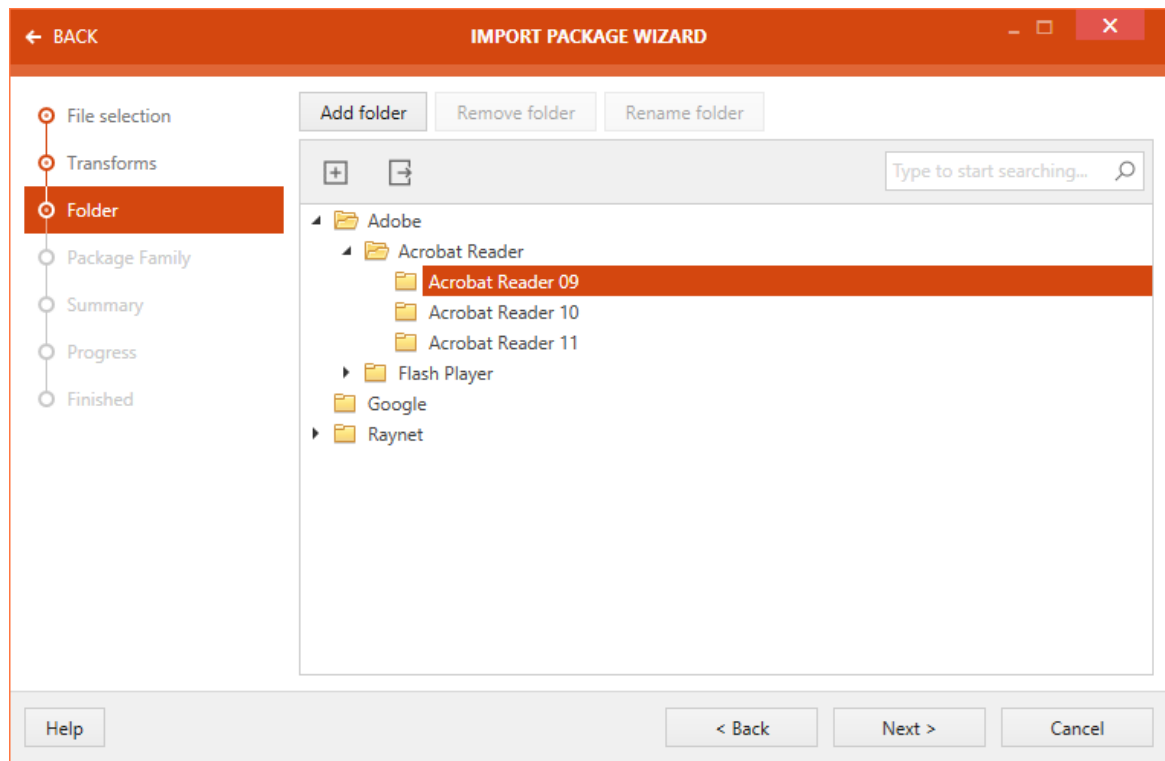
There are three buttons available at the top of the wizard.

- **Add folder**: This button can be used to add a new folder.
- **Remove folder**: This button can be used to remove the selected folder.
- **Rename folder**: This button can be used to rename the selected folder.

Select the target folder and click on the **Next >** button to proceed further.

9. If applicable, assign a package family to the package.
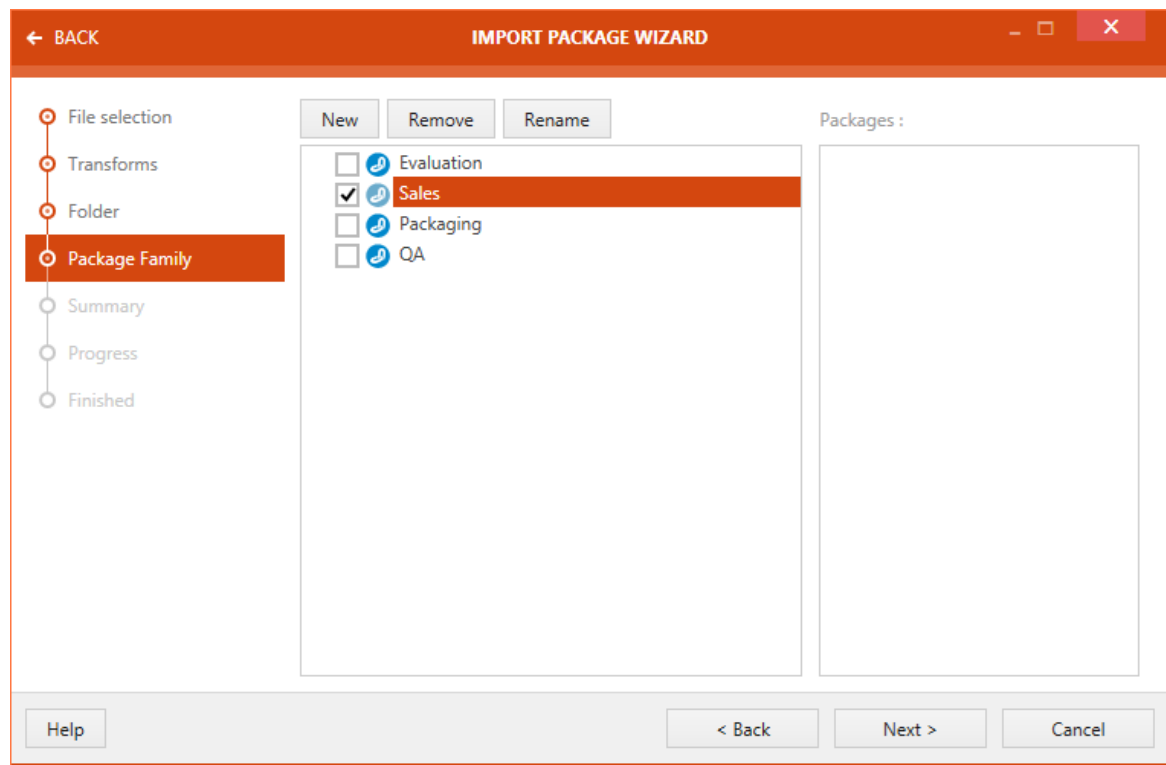
Click on the **Next >** button to proceed to the **Summary** view.

10. A summary of package import properties is shown on the **Summary** view.
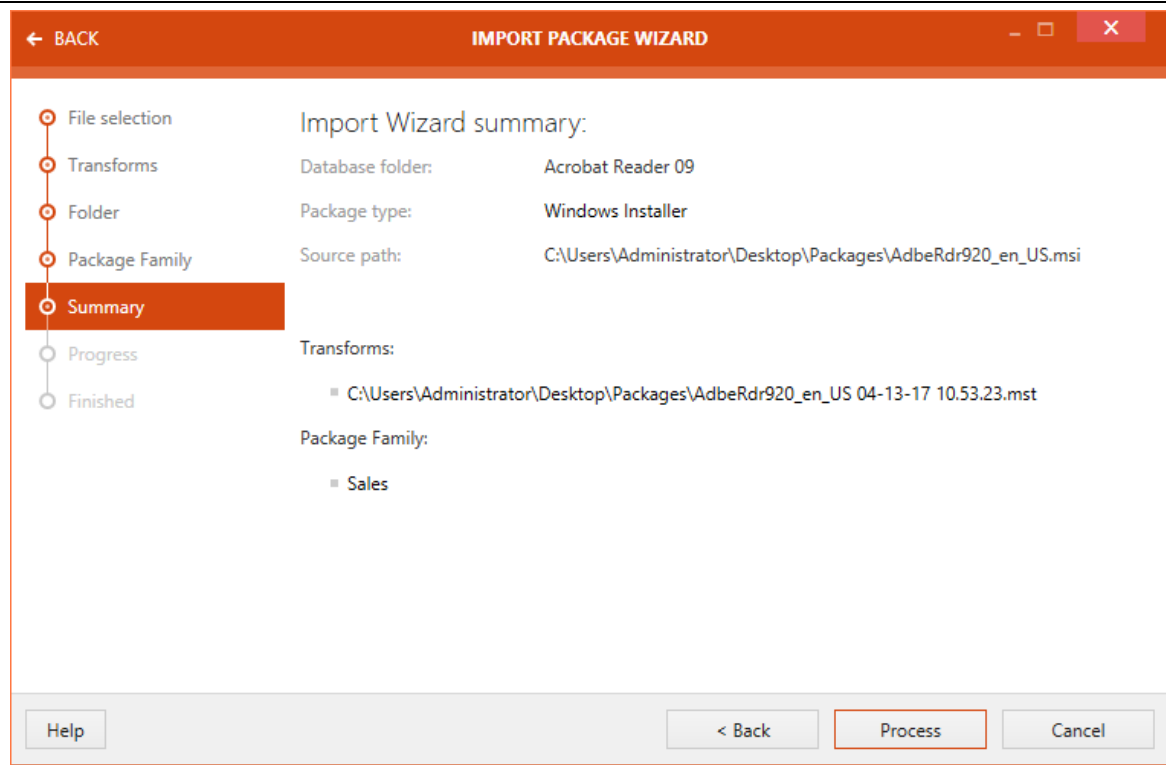
11. Click on the **Process** button to initialize the package import.

12. The package import is initialized and a progress bar is shown.
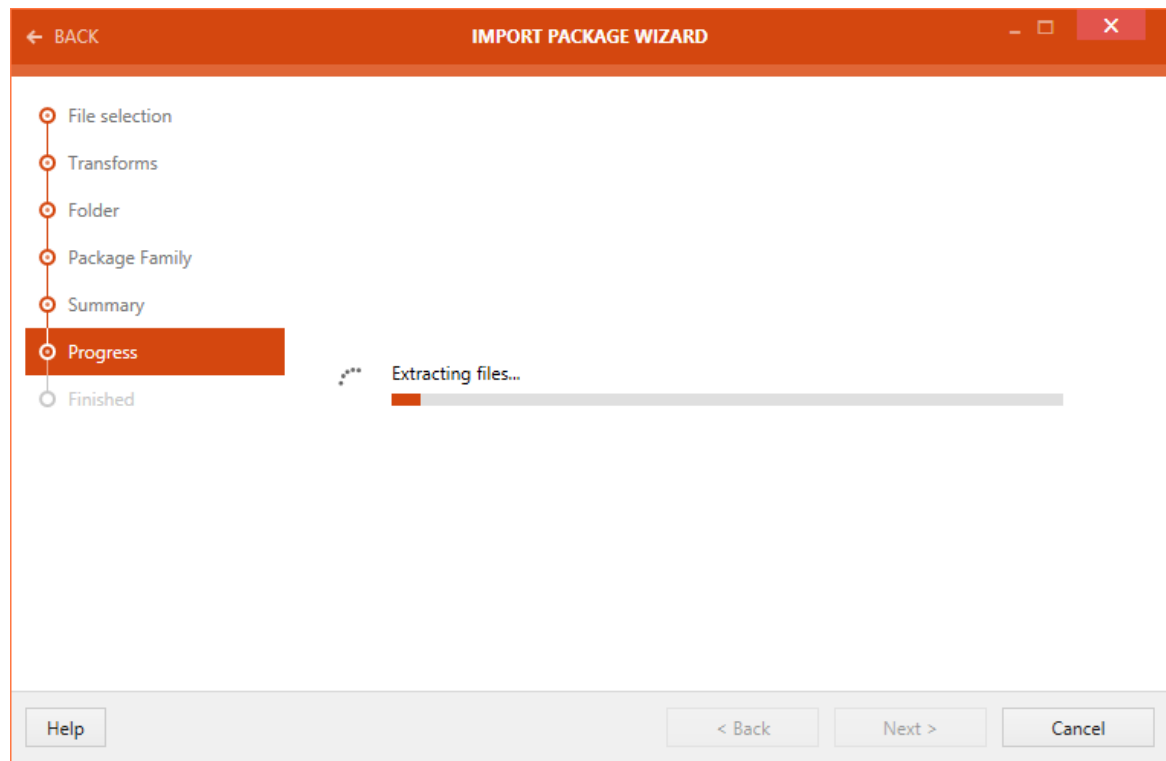
13. Status pertaining to the package import is shown on the **Finished** view.
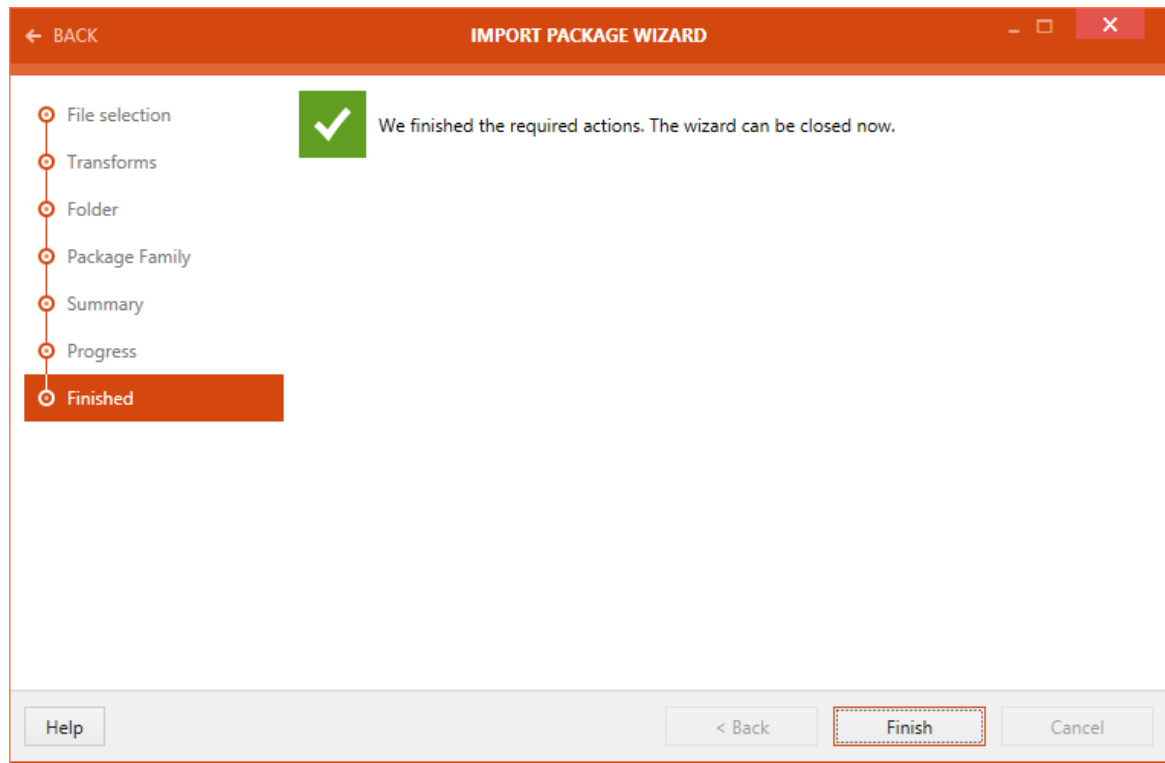
14. Click on the **Finish** button to finalize the package import.

Importing a Merge Module

To import a merge module (`.msm`) file into the library, first select the **Merge modules** from the *file type section* in the Library view. Either select an existing folder or create a new folder for importing a merge module into the library. Right click upon the target folder to show the context menu:

Select the **Import....** item from the context menu. This will launch the Package import wizard. As shown in the image below, specify following properties on the **File selection** view:

- **Path to the package file**: A path to the merge module file is set here.
- **Select type of imported MSM file**: A user can specify the type of `.msm` file being imported. Two options are available to a user:
  o **Vendor**: A `.msm` file delivered by a vendor and includes a valid signature.
  o **Self-Made**: A `.msm` file provided by a packager and may contain a signature.
- **Import multiple packages**: In case a user wish to import multiple merge module file at the same time, this option is selected.

Click on the **Next >** button to proceed further with the import.

A target folder can be selected in the Folder section of the wizard.

There are three buttons available at the top of the wizard.

- **Add folder**: This button can be used to add a new folder.
- **Remove folder**: This button can be used to remove the selected folder.
- **Rename folder**: This button can be used to rename the selected folder.

Select the target folder and click on the **Next >** button to proceed further.

A summary of package import properties is shown on the **Summary** view.

Click on the **Process** button to initialize package import. After the package import is complete, the import status is shown on the **FINISHED** view.

Click on the **Finish** button to finalize the package import.

Importing an OS Snapshot

To import an OS Snapshot (`.rcs`) file into the library, first select the OS Snapshots from the *file type section* in the **library** view.

Tip:
OS Snapshots in the `.rcs` format can be created by using RayPack. For information on how to create an OS Snapshot using RayPack refer to the *RayPack User Guide.* The *RayPack User Guide* can be found on the RayPack Product Homepage.

Either select an existing folder or create a new folder for importing a OS Snapshot into the **Library**. Right click upon the target folder to show the context menu:

The **IMPORT SNAPSHOT WIZARD** is launched. On the **File selection** view, specify the path to the OS Snapshot that is to be imported.
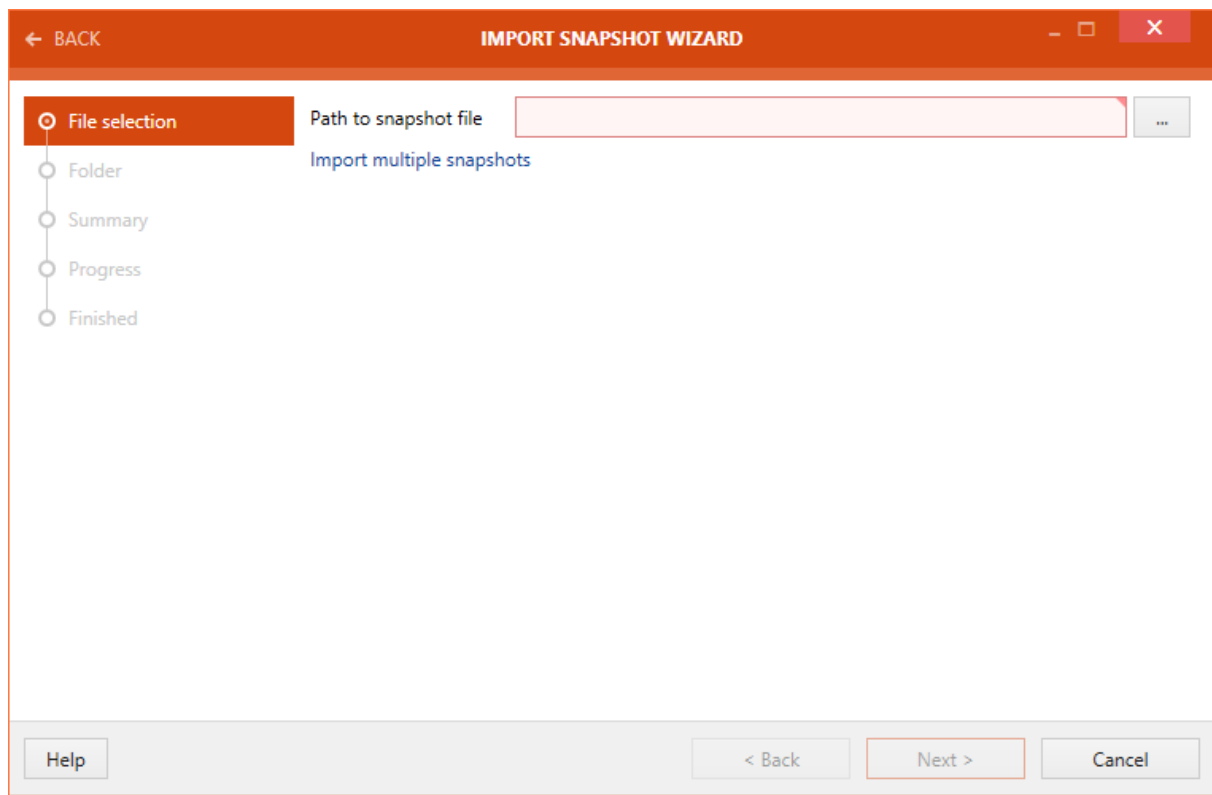
Click on the **Next >** button to proceed further with the import.

A target folder can be selected in the **Folder** section of the wizard.

There are three buttons available at the top of the wizard.

- **Add folder**: This button can be used to add a new folder.
- **Remove folder**: This button can be used to remove the selected folder.
- **Rename folder**: This button can be used to rename the selected folder.

Select the target folder and click on the **Next >** button to proceed further.

A summary of package import properties is shown on the **Summary** view.
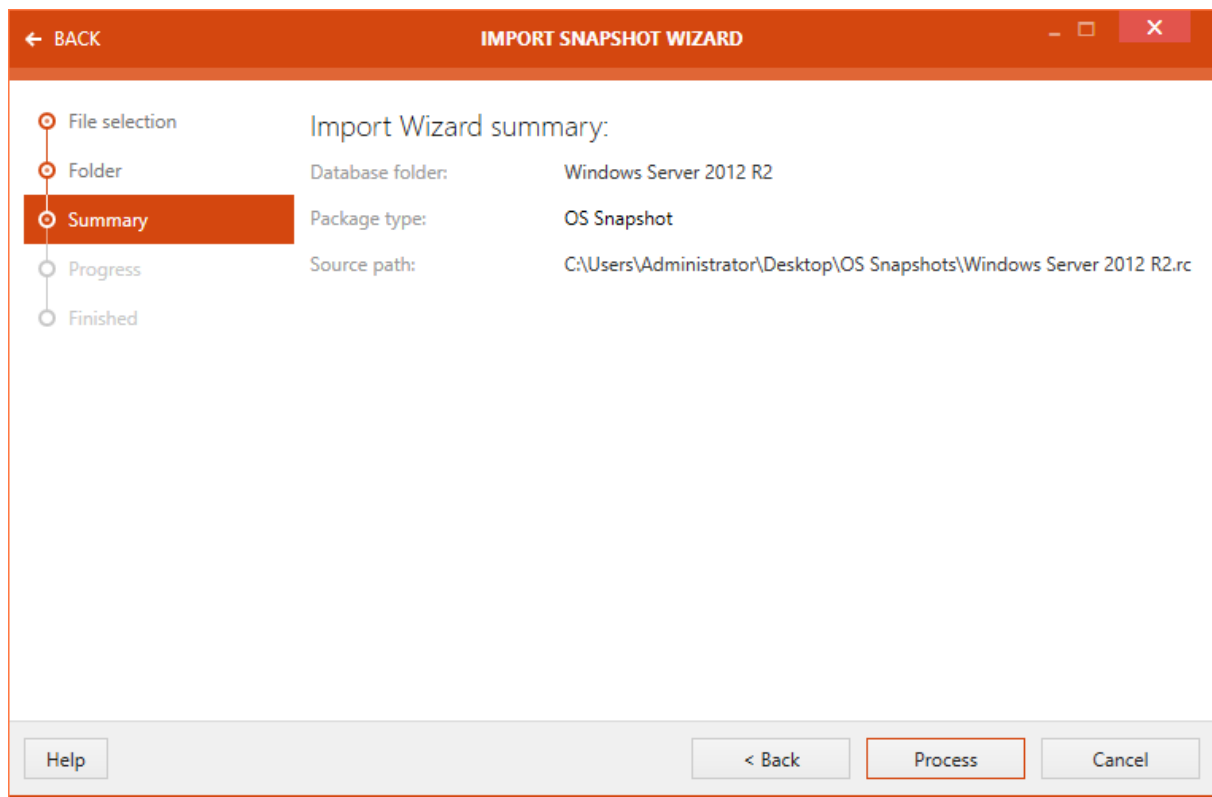
Click on the **Process** button to initialize the snapshot import. After the package import is complete, the import status is shown on the **FINISHED** view.
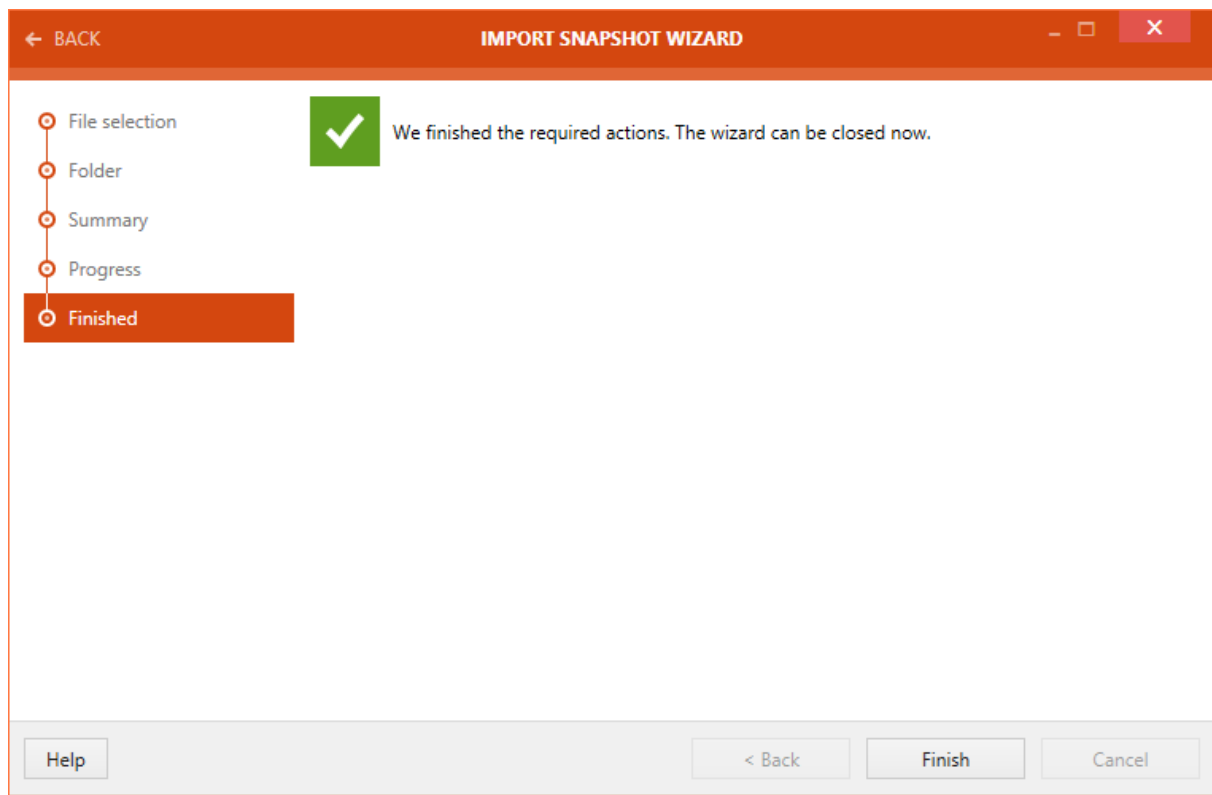
Click on the **Finish** button to close the **IMPORT SNAPSHOT WIZARD**.
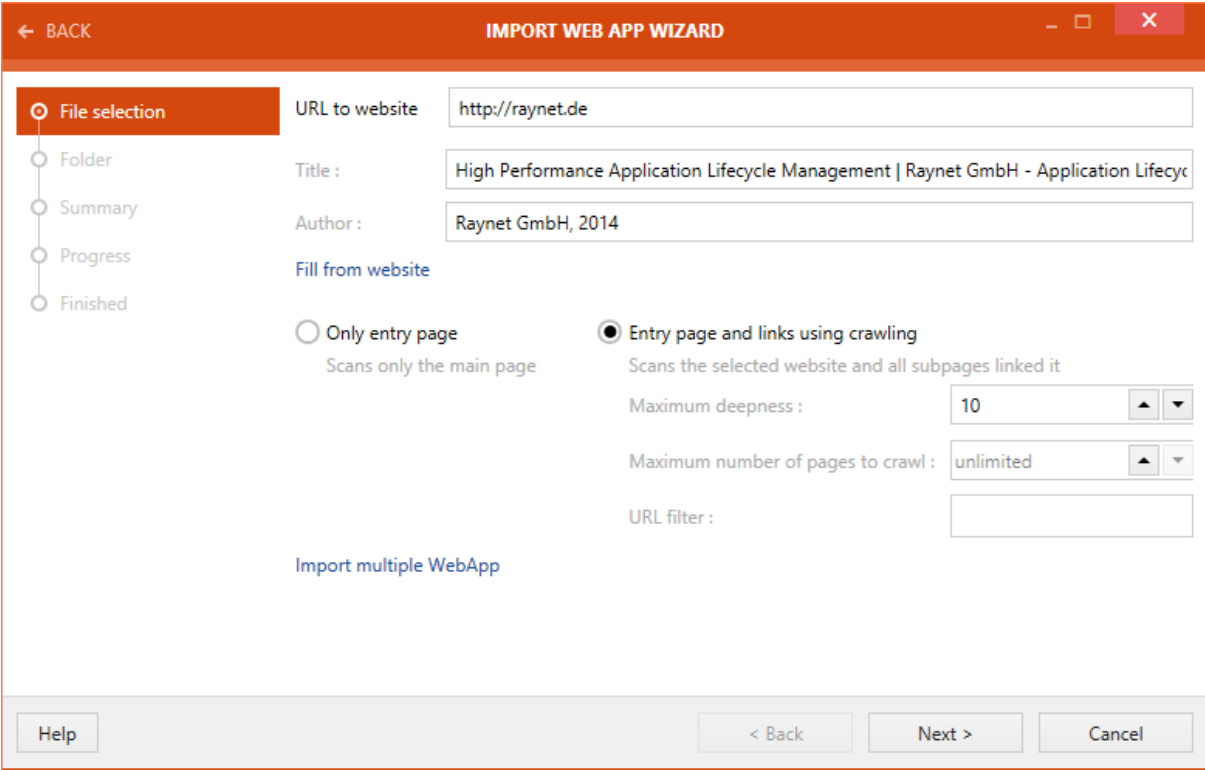
Importing a Web Application

Importing a Web Application

To import a web application into the library, first select **Web Apps** from the *file type section* in the **Library** view. Either select an existing folder or create a new folder for importing a web application into the library. Right-click upon the target folder to show the context menu.

The **IMPORT WEB APP WIZARD** is launched. On he **File selection** view, specify the URL to the website of the web application that is to be imported. Choose if only the entry page should be scanned or specify the maximum deepness and the maximum number of pages to crawl for the scan. It is also possible to set an URL filter. If the filter is set, the scan will only include those pages matching the filter and exclude other pages (e.g. if `*.raynet.*` is set as filter, only pages where the URL contains "raynet" are included).

Title and **Author** of the web application are optional and can be filled in either manually or automatically by clicking on the **Fill from website** option.

Click on the **Next >** button to proceed further with the import.

A target folder can be selected in the **Folder** section of the wizard.

There are three buttons available at the top of the wizard.

- **Add folder**: This button can be used to add a new folder.
- **Remove folder**: This button can be used to remove the selected folder.
- **Rename folder**: This button can be used to rename the selected folder.

Select the target folder and click on the **Next >** button to proceed further.

A summary of package import properties is shown on the **Summary** view.

Click on the **Process** button to initialize the import of the Web Application. After the import is complete, the import status is shown on the **FINISHED** view.
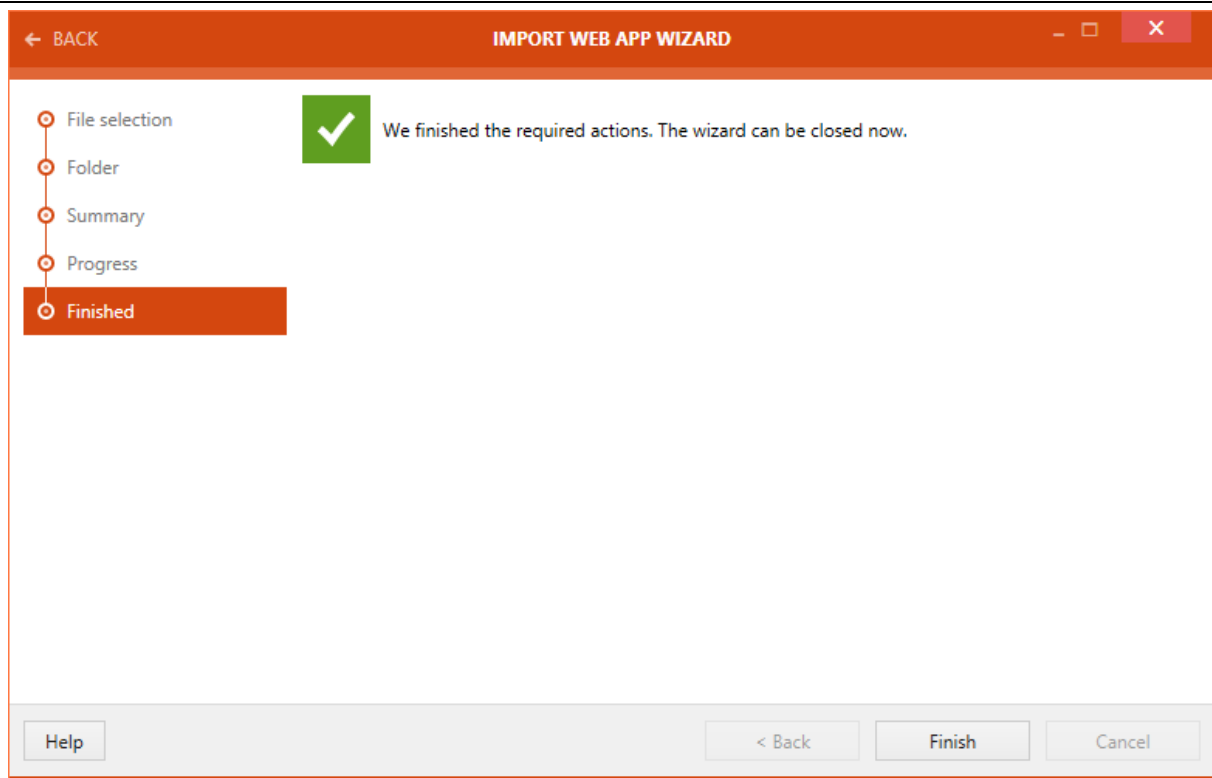
Click on the **Finish** button to close the **IMPORT WEB APP WIZARD**.

Importing an App-V Package

To import an App-V (`.appv`) file into the library, first select **APP-V** from the *file type section* in the **Library** view. Either select an existing folder or create a new folder for importing an App-V file into the library. Right click upon the target folder to show the context menu:

Select the **Import....** item from the context menu. This will launch the Package import wizard. As shown in the image below, specify following properties on the **File selection** view:

- **Path to the package file**: A path to the merge module file is set here.
- **Extract files to the default location**: Check the checkbox to extract the files to the default location.
- **Import multiple packages**: In case a user wish to import multiple merge module file at the same time, this option is selected.
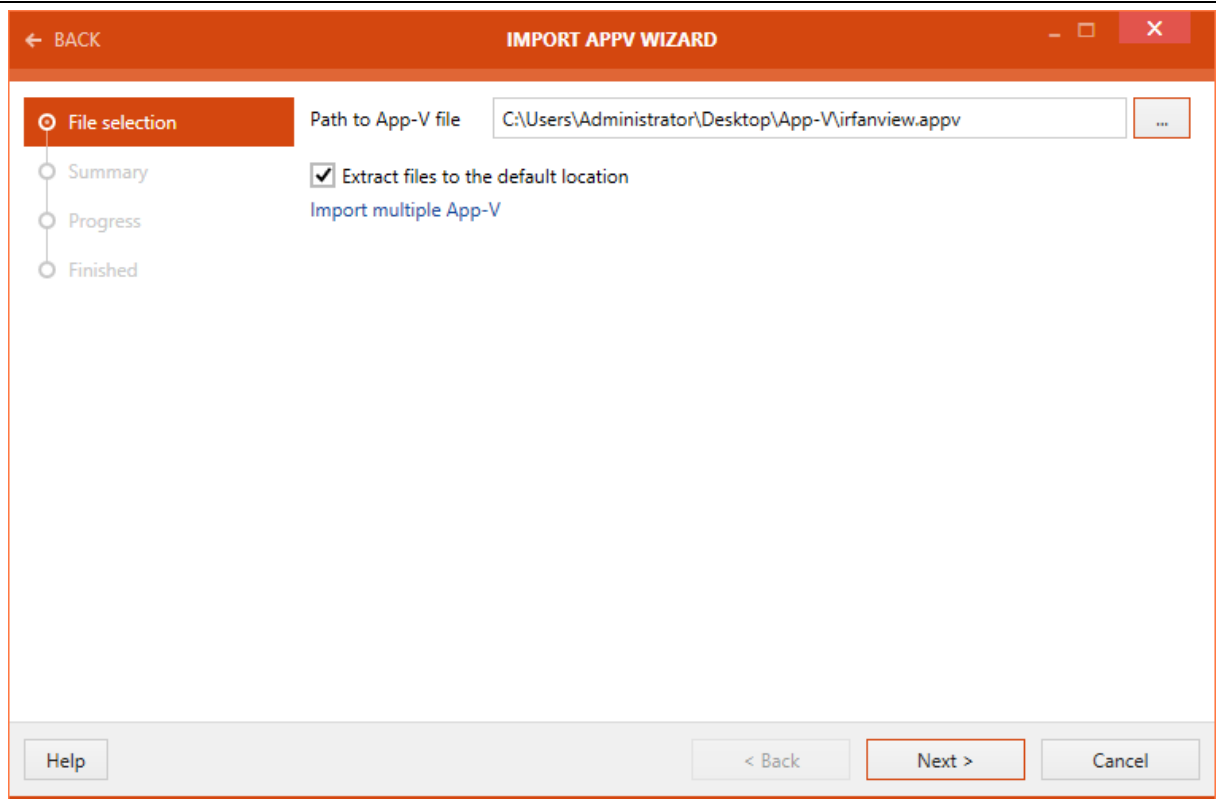
Click on the **Next >** button to proceed further with the import.

A summary of package import properties is shown on the **Summary** view.
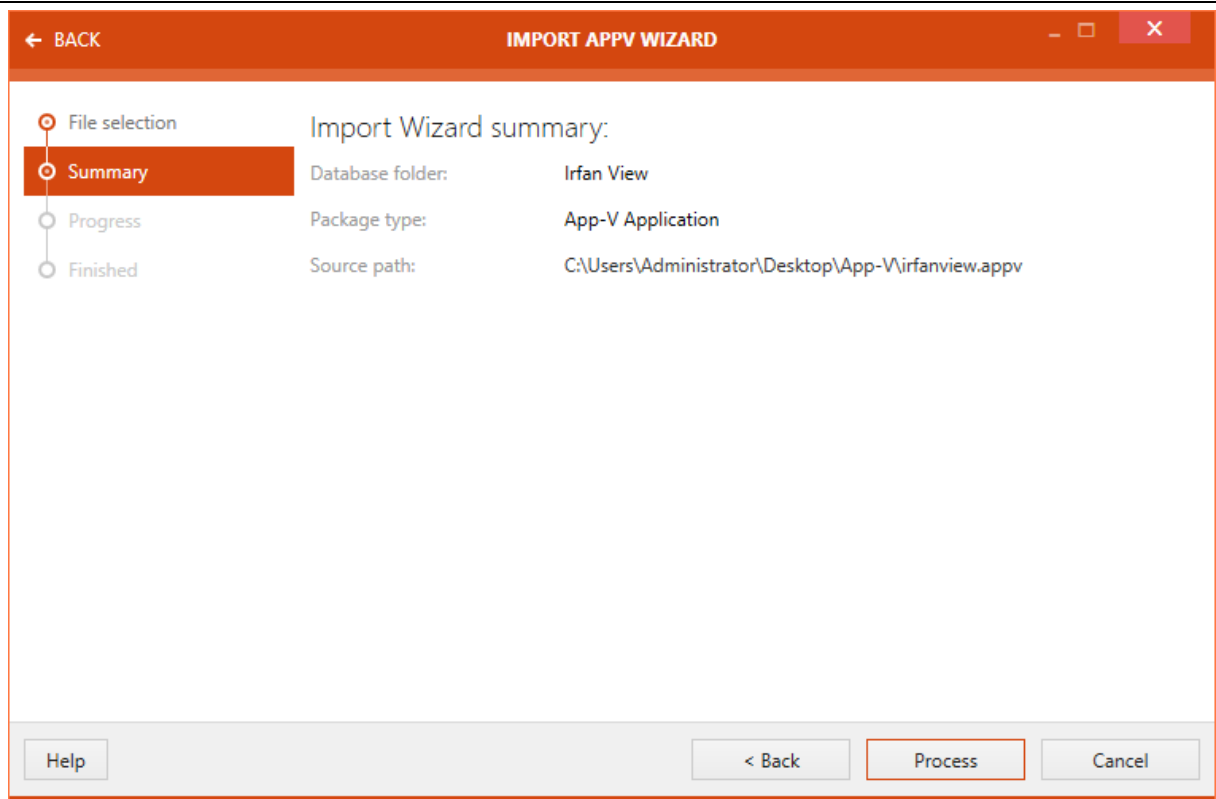
Click on the **Process** button to initialize package import. After the package import is complete, the import status is shown on the **FINISHED** view.
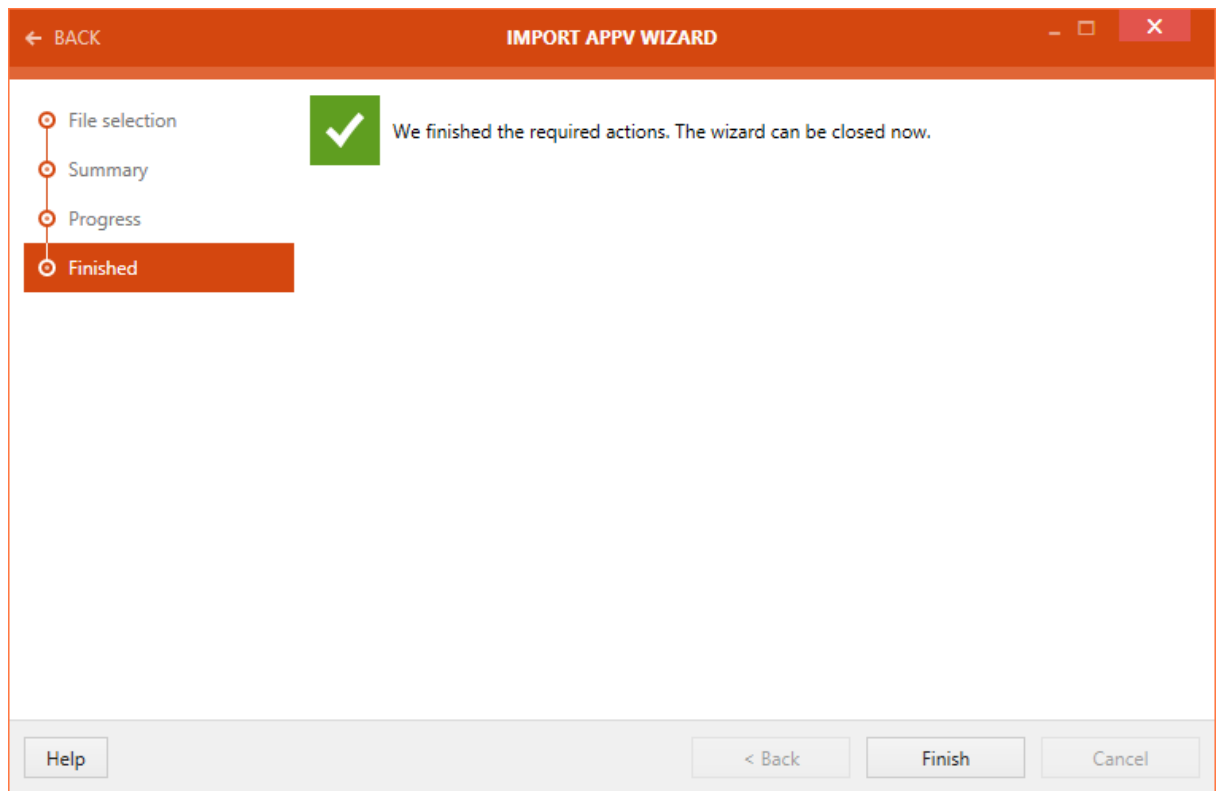
Click on the **Finish** button to finalize the package import.

Importing Multiple Packages

The Import package wizard offers a user an ability to import multiple packages at the same time. To do this, click on the **Import multiple packages** option on the **File selection** view.
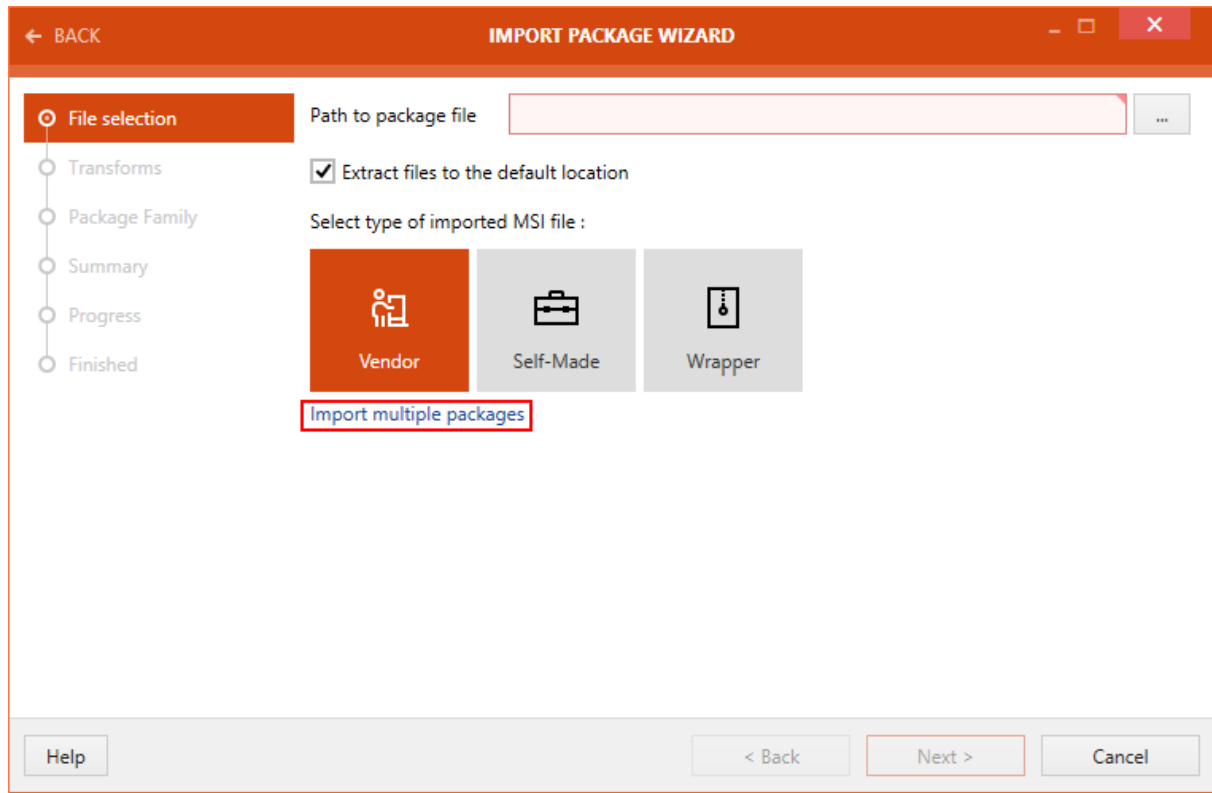
The **File Selection** view is now available to allow importing multiple packages at the same time.
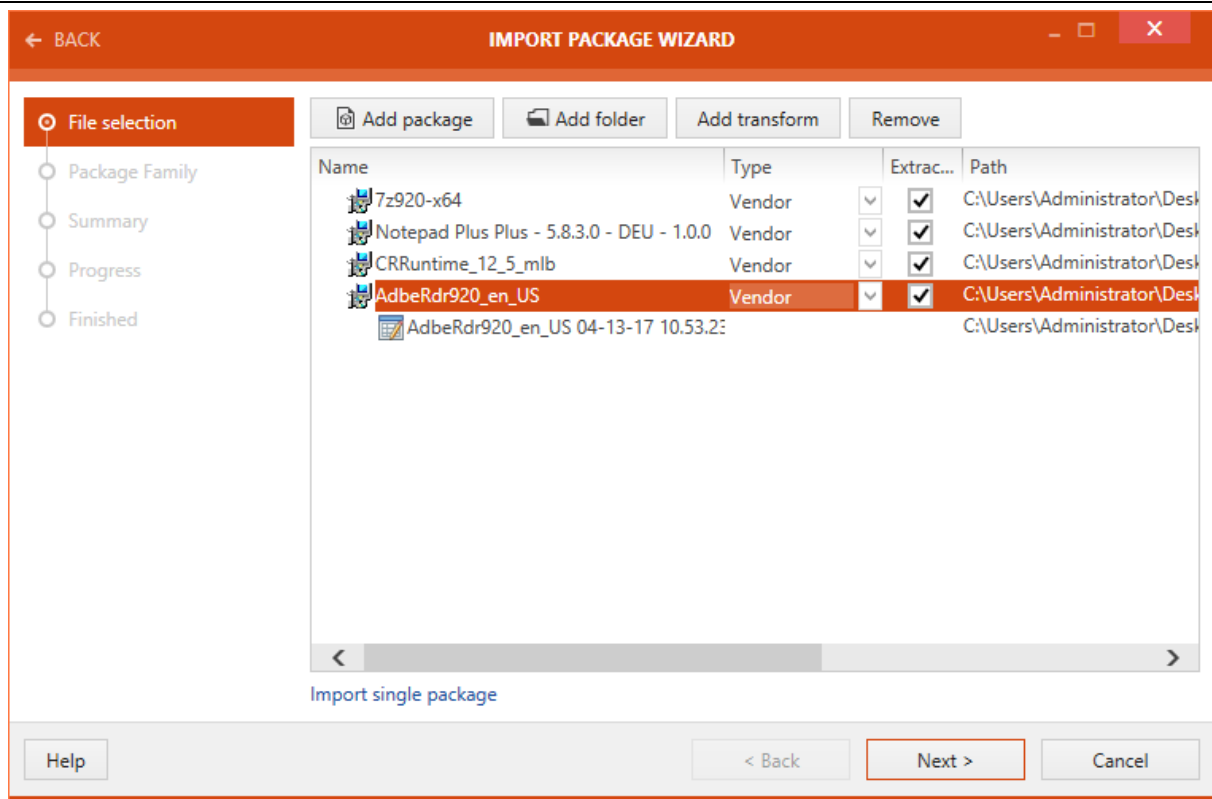
Click on the **Add package** button to add packages for import. To add a transform file to a package being imported, click on the **Add transform** button. Options to extract the `.msi` file and to specify the type of `.msi` file are available under **Type** and **ExtractFiles** column header, respectively.

To proceed further, follow the steps 8 to 12 mentioned under the topic *Importing a software package*.

Importing a Package Using the Import Package Option in the Swipe-bar

Following steps illustrate how to import a package into the **Library** using **IMPORT PACKAGE WIZARD**:

1. Select the item **Import package** from the swipe-bar.
   The IMPORT PACKAGE WIZARD is initialized.

2. Select the package type from the available options. These options include:

- **MSI**: Imports Windows Installer database file (`.msi`).
- **Merge Module**: Imports a Merge Module file (`.msm`).
- **Snapshot**: Imports a snapshot file captured with RayPack (`.rcs`).
- **Legacy Setup**: Imports legacy setup exe installer (`.exe`).
- **Web Application**: Imports a web application.
- **App-V Application**: Imports an App-V application (`.appv`).
- **RayFlow**: Imports a package from RayFlow.

> ⚠️ **Warning:**
> To import a legacy package (`.exe`) a version of RayPack must be available either on the local system or on a virtual machine that is configured for RayQC Advanced!
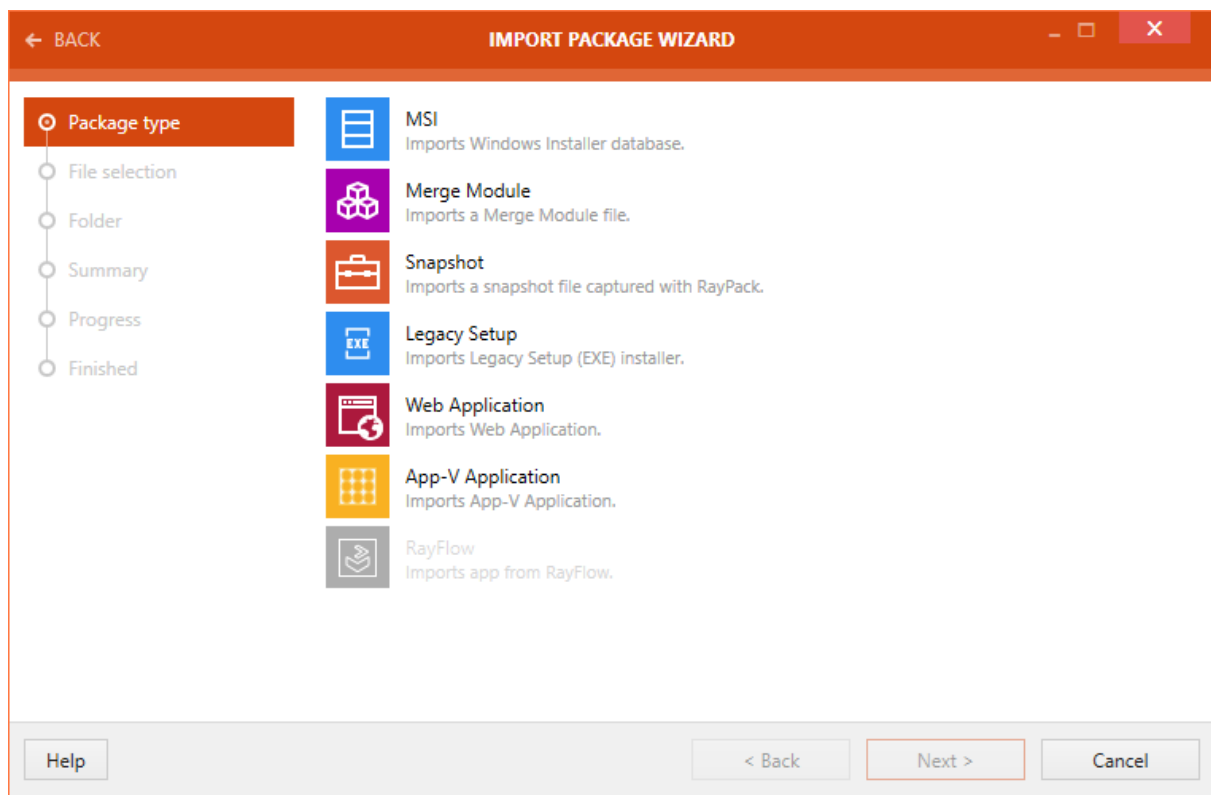
3. Click on the **Next >** button
   File selection page is now available. Based on the package type initially selected, this page will show relevant options for that package type.

4. Select the path to package file (for this example MSI is chosen as the package type for import)
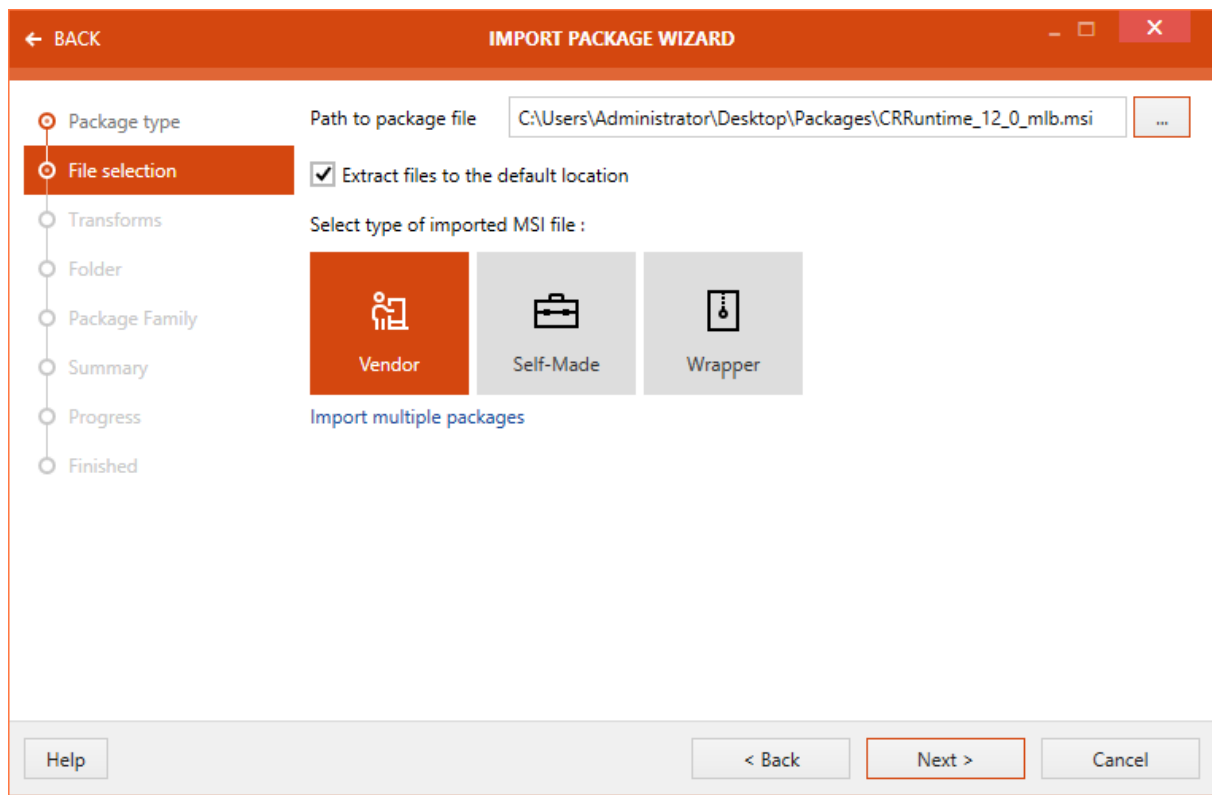
5. If the selected package already exists in the database, then a confirmation message is shown. A user can select **RELOAD** to overwrite the package in the **Library** or can select **CONTINUE** to import a second copy of the package.
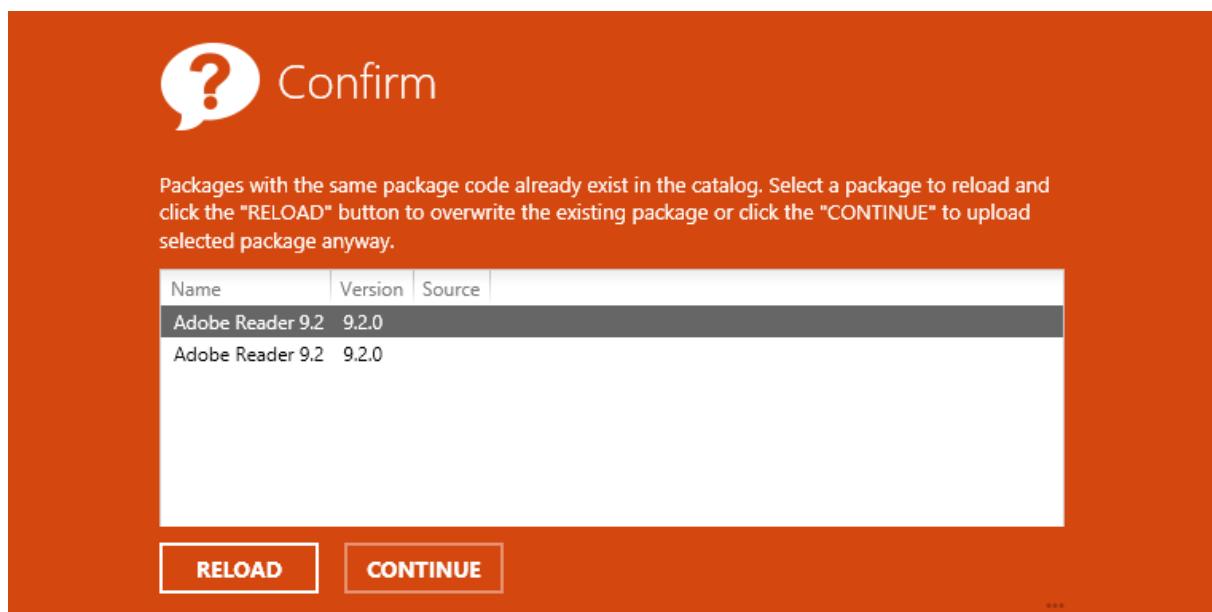
6. If a user has selected `.msi` as package import type, then the **Transforms** page is shown next.

In this page a user can add transform files for the package which is being imported.

Click on the **Next >** button to proceed.
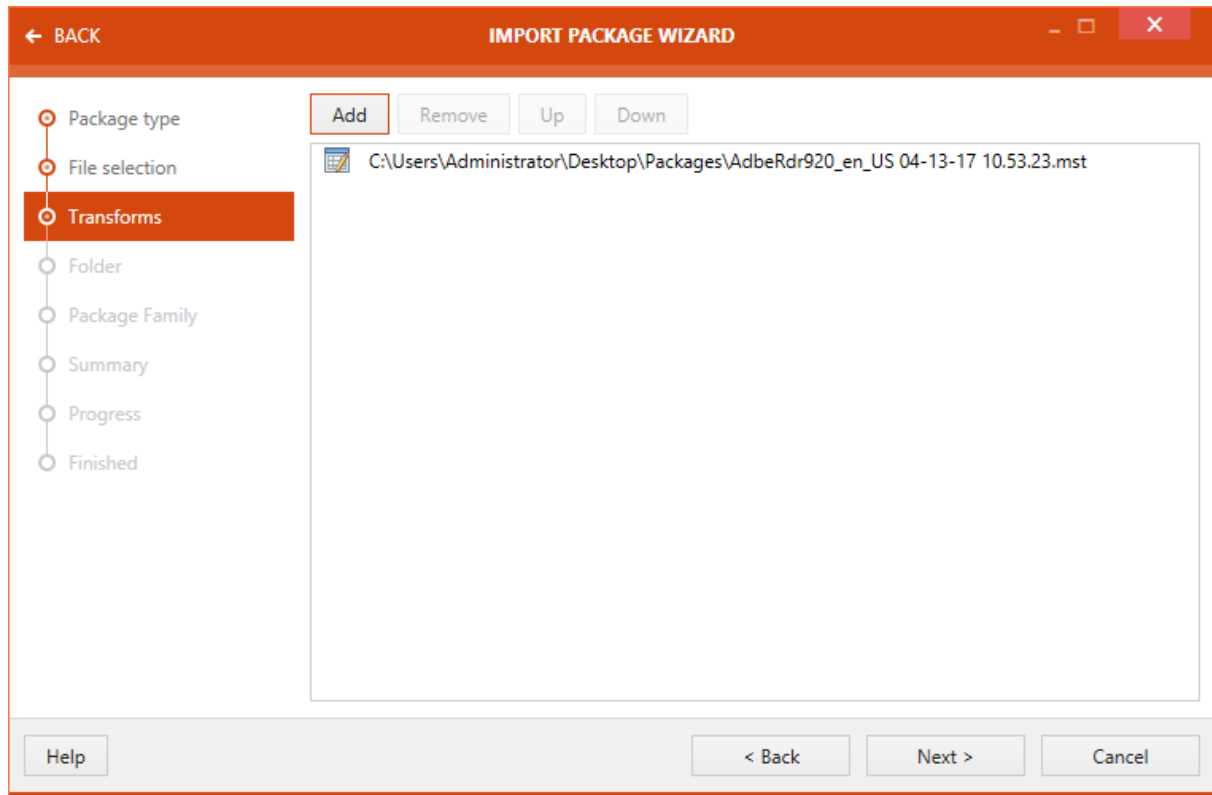
7. Select **Add folder** as destination for the imported package. The folders shown or created here are related to the package type previously selected. This means that if a user has selected OS Snapshot as package type, then the existing folders within the OS Snapshots area of the library will be shown here.
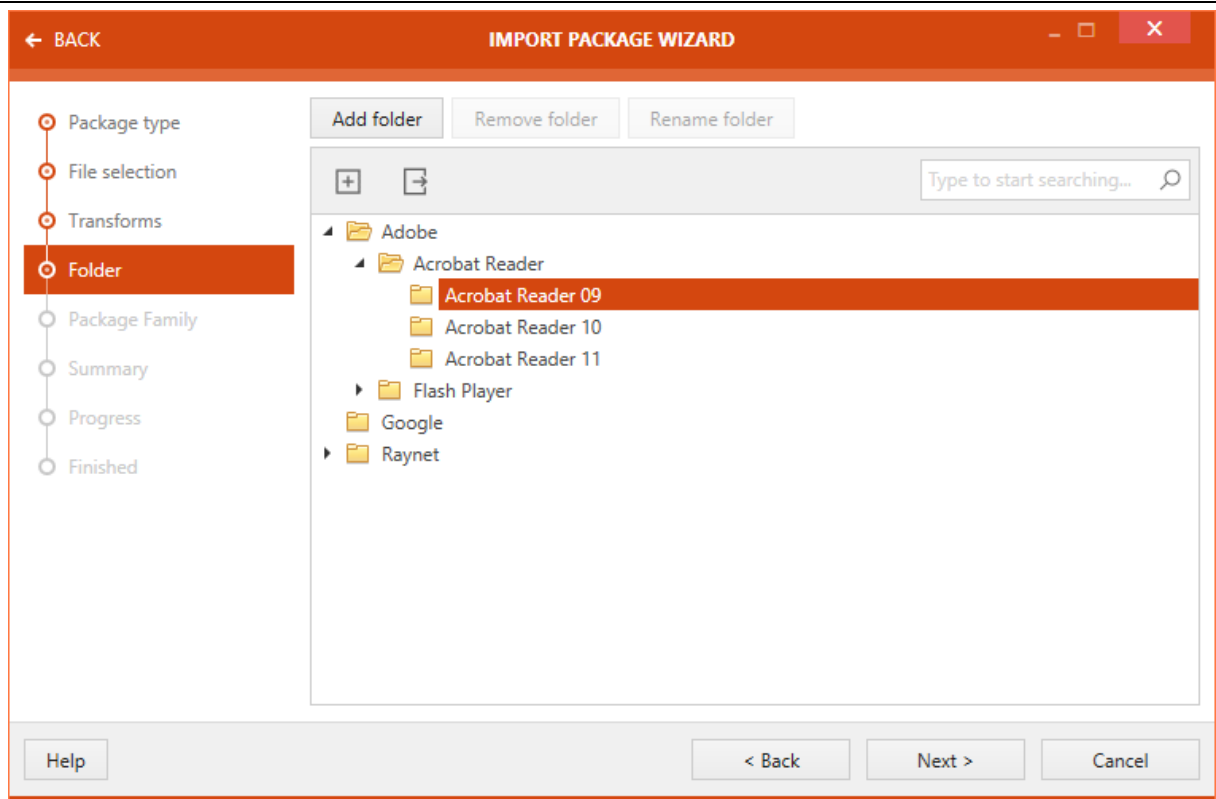
8. On the **Package Family** page, a user can specify the Package Family to which the package belongs. This page offers the ability to either use an existing package family or create a new one.
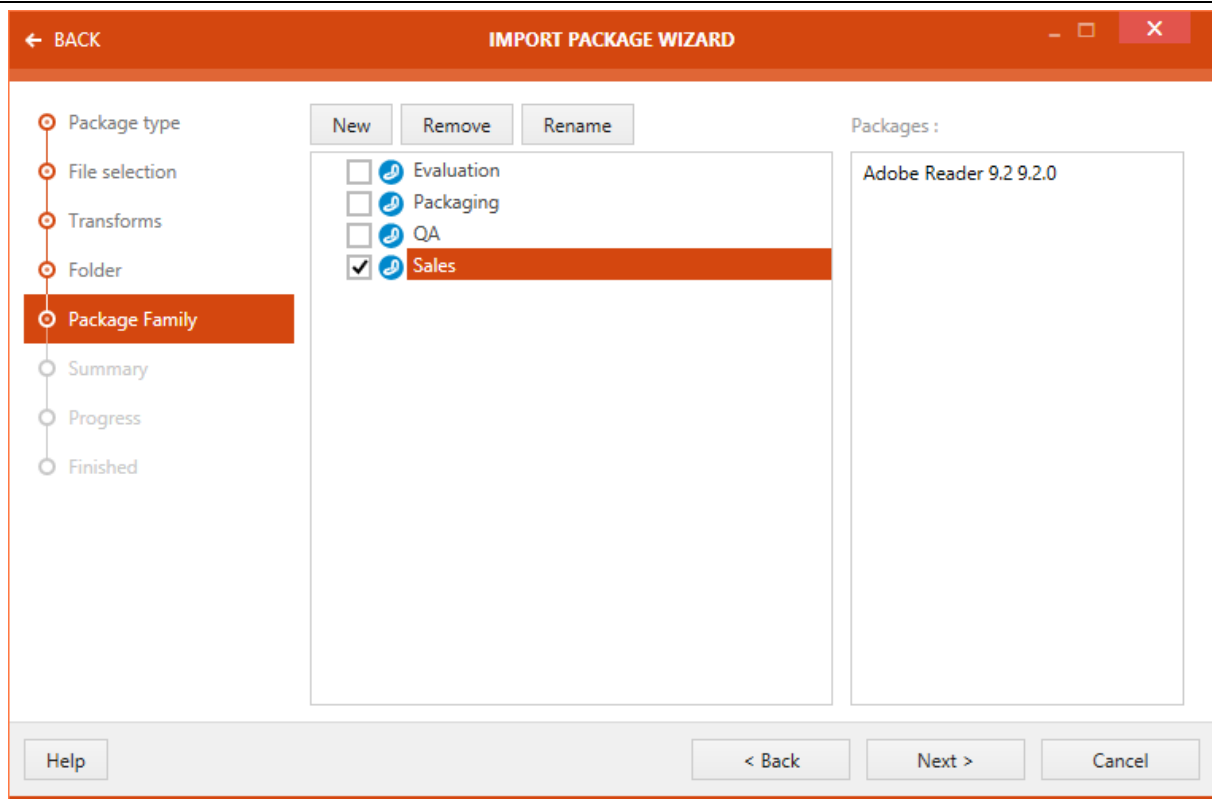
Next, the **Summary** page is shown. The user input for the package import is summarized on this page.
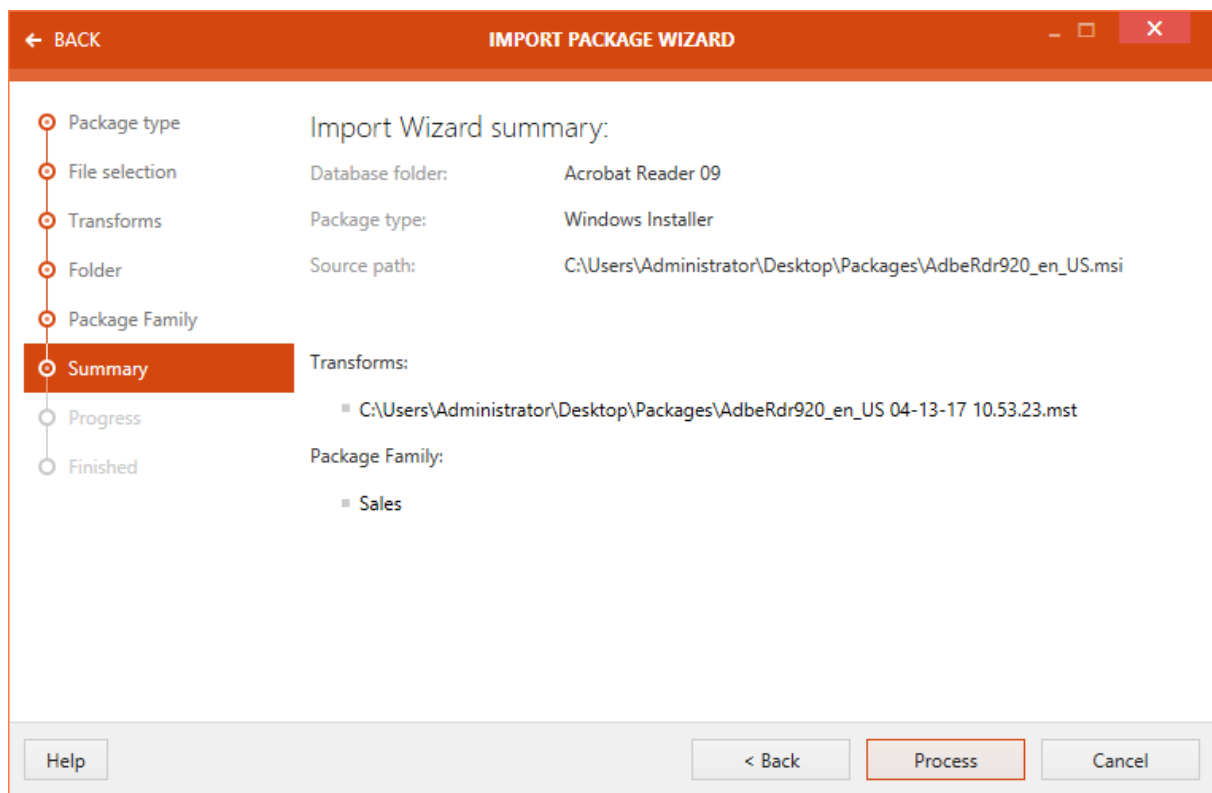
9. Click on the **Process** button to start importing the package.
   A progress bar is shown.

10. Confirmation on successful package import is shown on the **Finished** page.
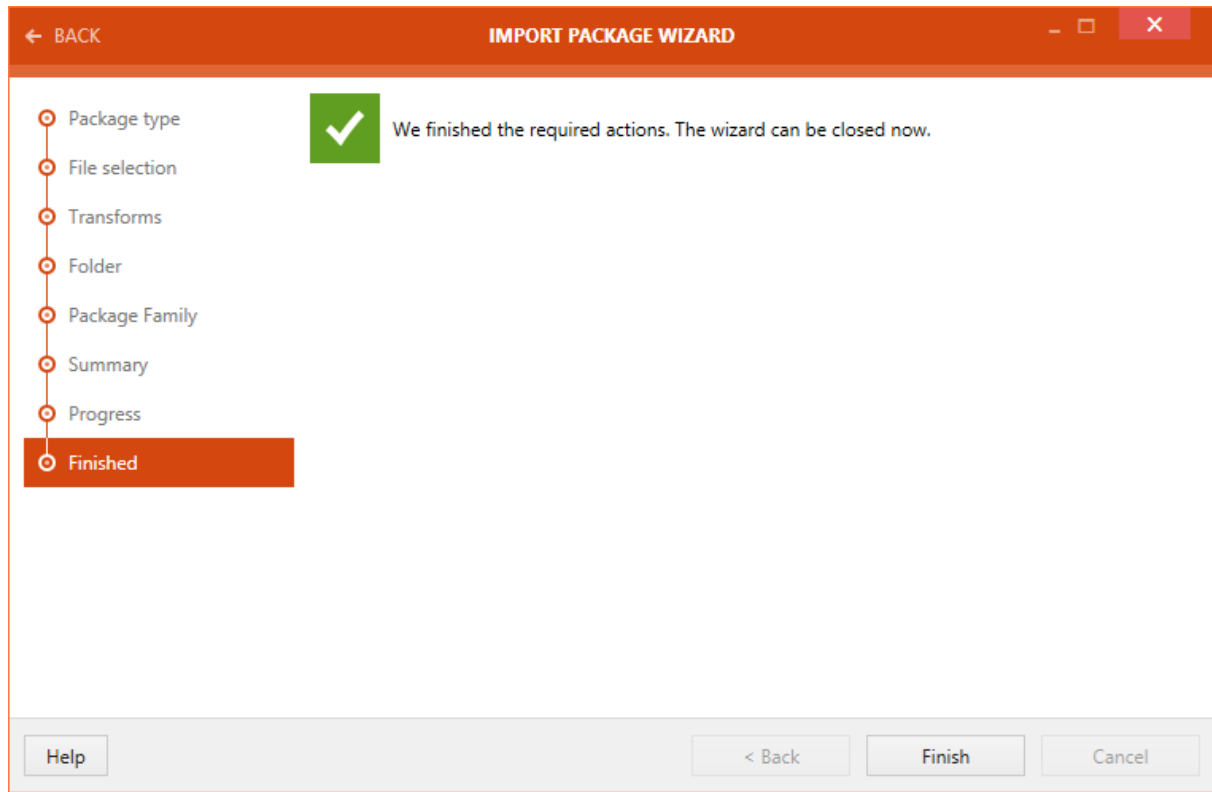
Click on the **Finish** button to close the **IMPORT PACKAGE WIZARD**.

Importing a Legacy Setup

1. Select the item **Import package** from the swipe-bar.
   The IMPORT PACKAGE WIZARD is initialized.

2. Select the **Legacy Setup** option.

> ⚠ **Warning:**
> To import a legacy package (`.exe`) a version of RayPack must be available on the local system (the one that is running RayQC Advanced).

---
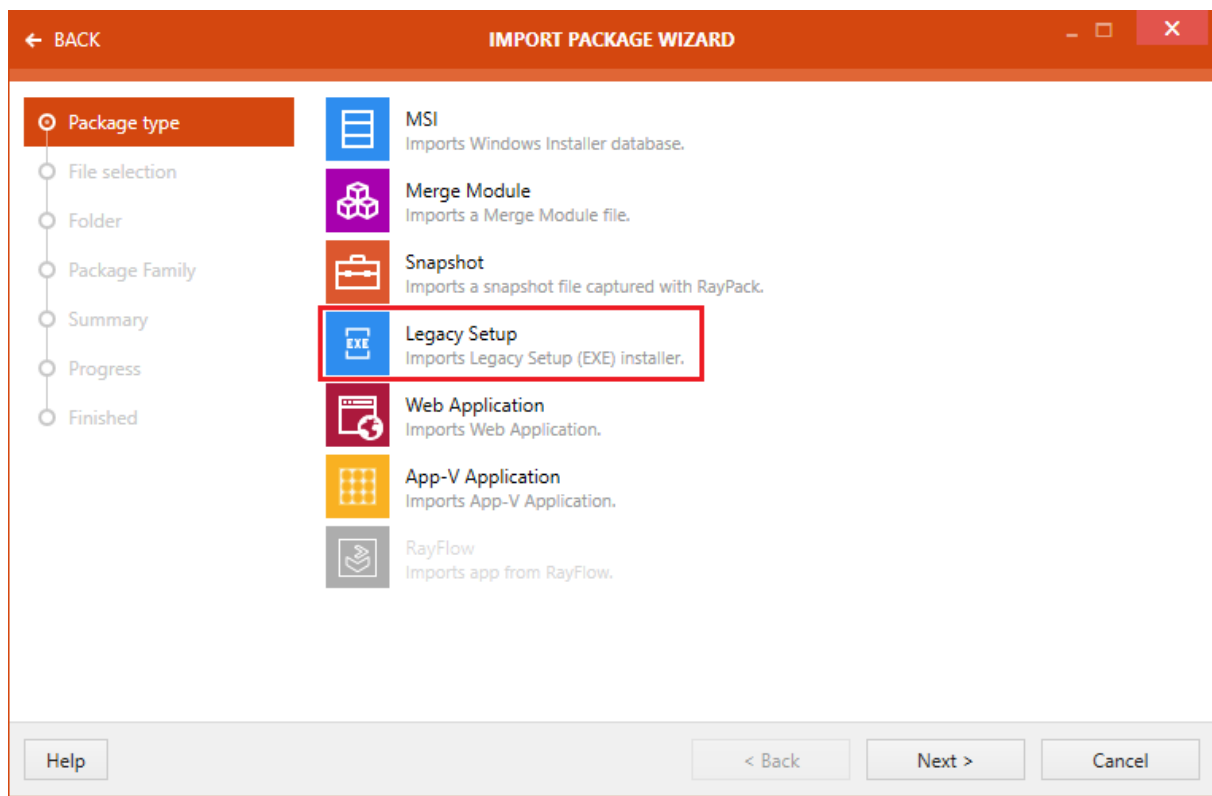
3. Click on the **Next >** button
   File selection page is now available. When importing a legacy file, the following options are available.

   - **Path to package file**: The path to the .exe file is configured in this field. Either type the exact path or use the **Browse** [...] button to select the file browsing to the folder that contains the file..
   - **Setup parameters**: Parameters for the setup of the file can be entered here.
   - **Use virtual machine**: When the checkbox is checked a virtual machine from the configured virtual machines can be chosen using the drop-down list. This option is used to convert the legacy file into a temporary `.msi` using a virtual machine with an installed RayPack. If the box is not checked, the conversion will be done on the local machine, which then needs an

installed RayPack instance.
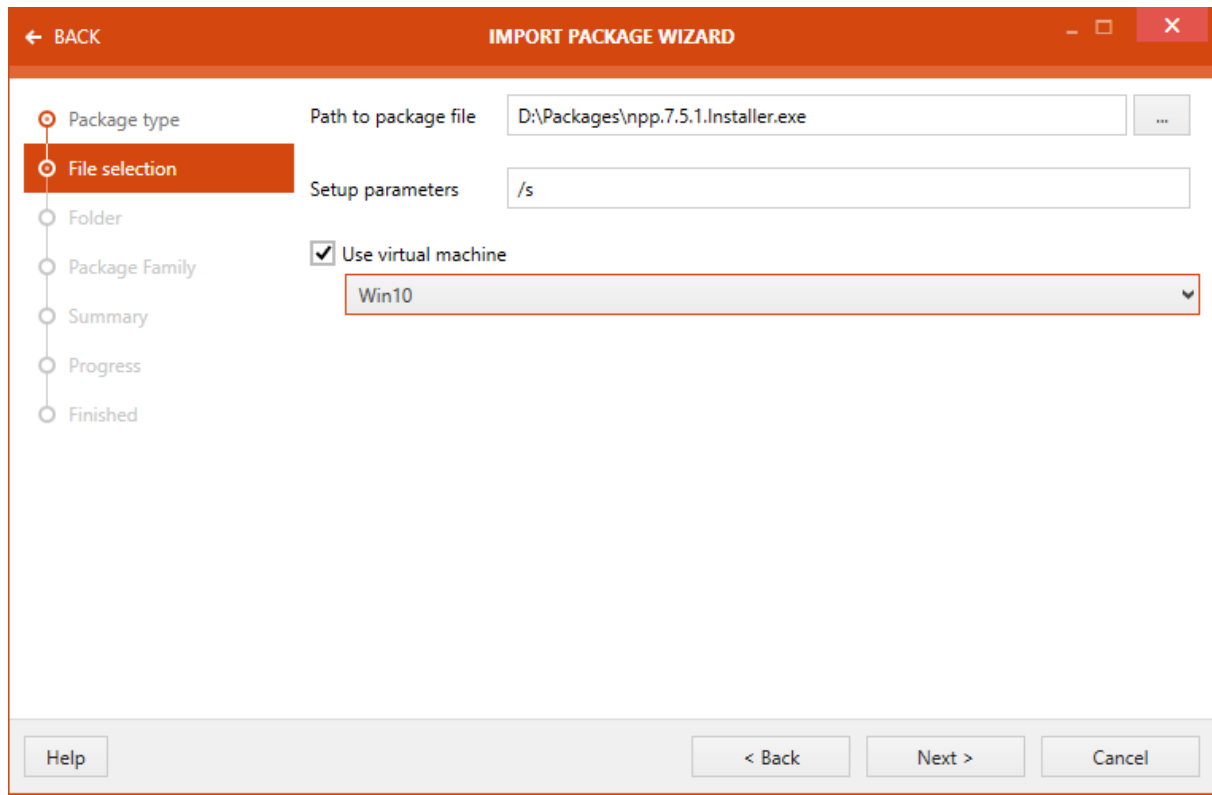
The machines must be configured prior to starting the wizard. Refer to chapter Virtual Machines for more information.

4. Select **Add folder** as destination for the imported package. The folders shown or created here are related to the package type previously selected. This means that if a user has selected OS Snapshot as package type, then the existing folders within the OS Snapshots area of the library will be shown here.
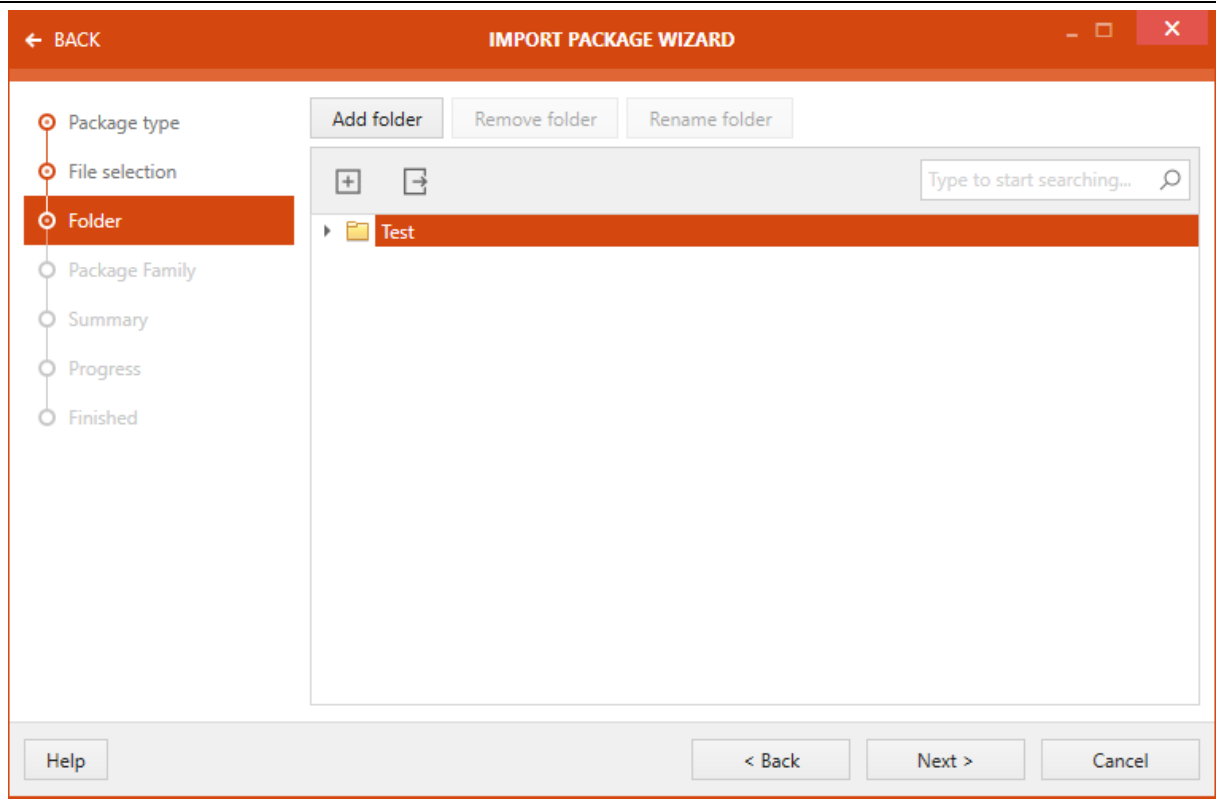
5. On the **Package Family** page, a user can specify the Package Family to which the package belongs. This page offers the ability to either use an existing package family or create a new one.
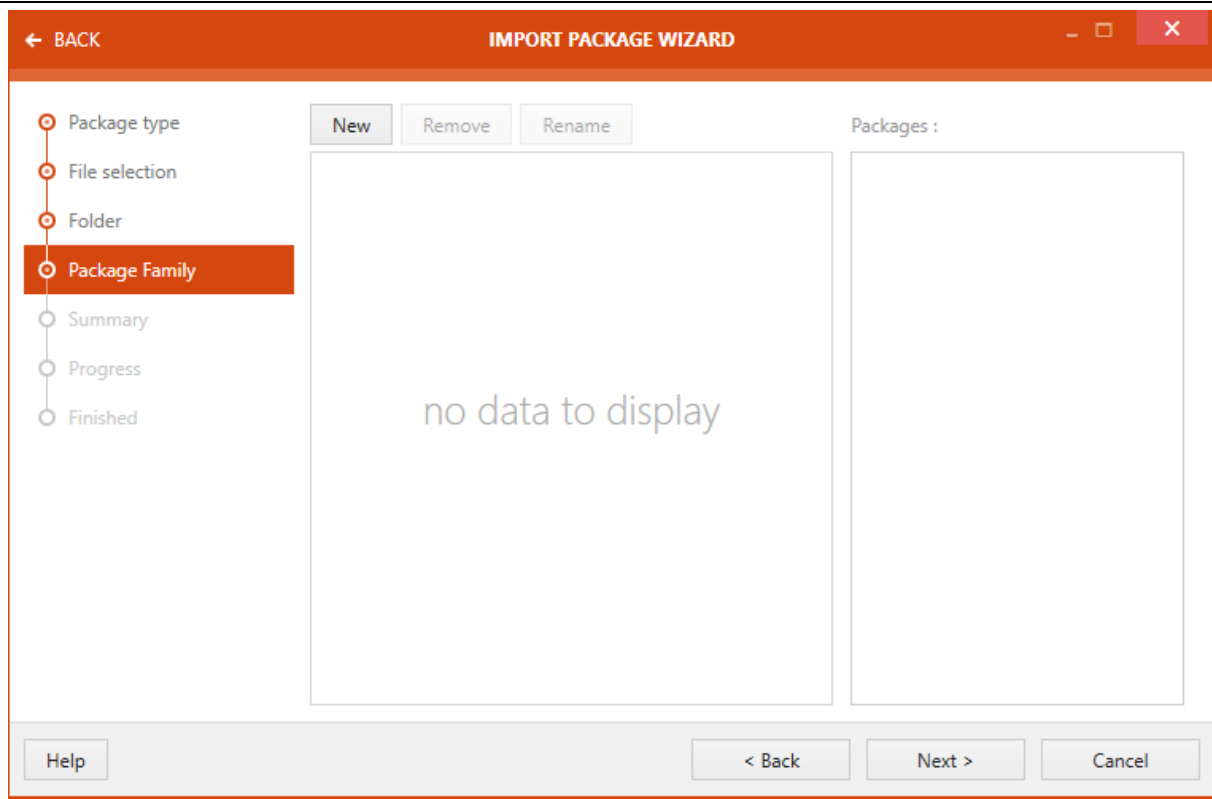
6. Next, the **Summary** page is shown. The user input for the package import is summarized on this page.
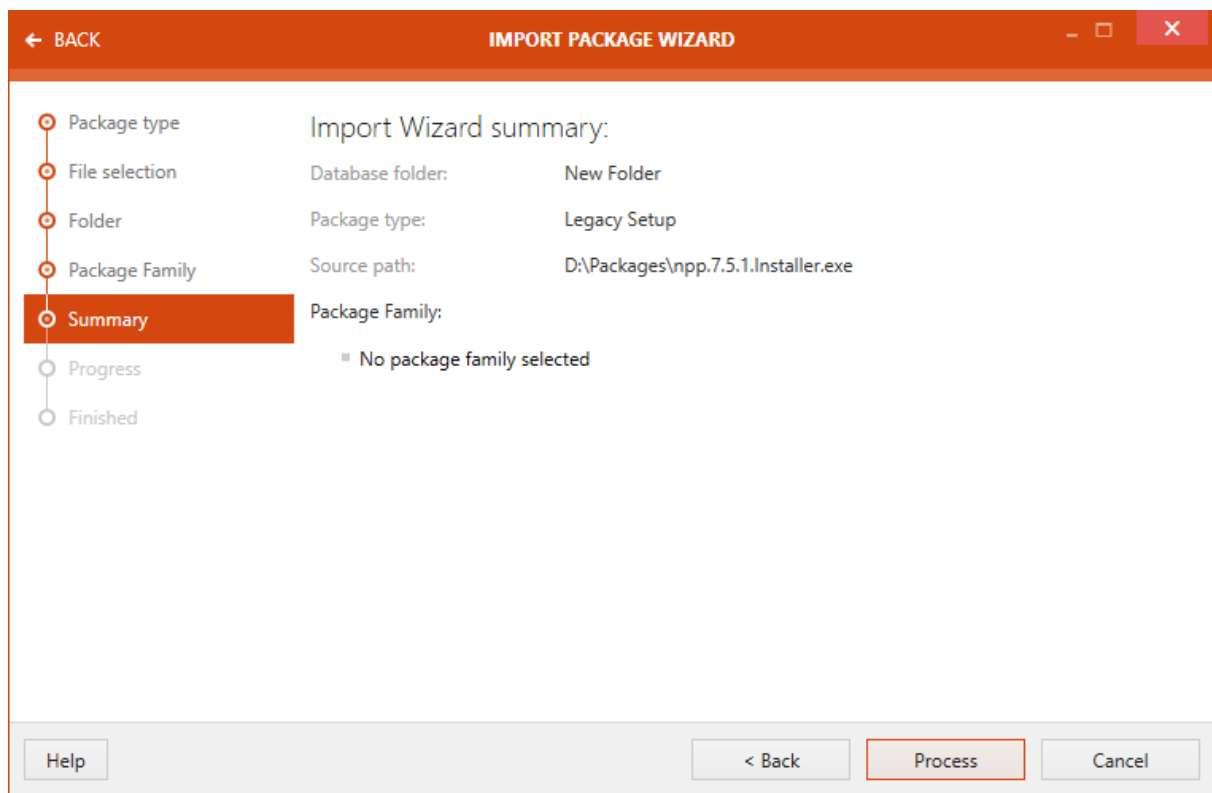
7. Click on the **Process** button to start the conversion and the import of the package. If a virtual machine has been selected, the Progress bar will also show the single steps that are needed to activate the virtual machine.
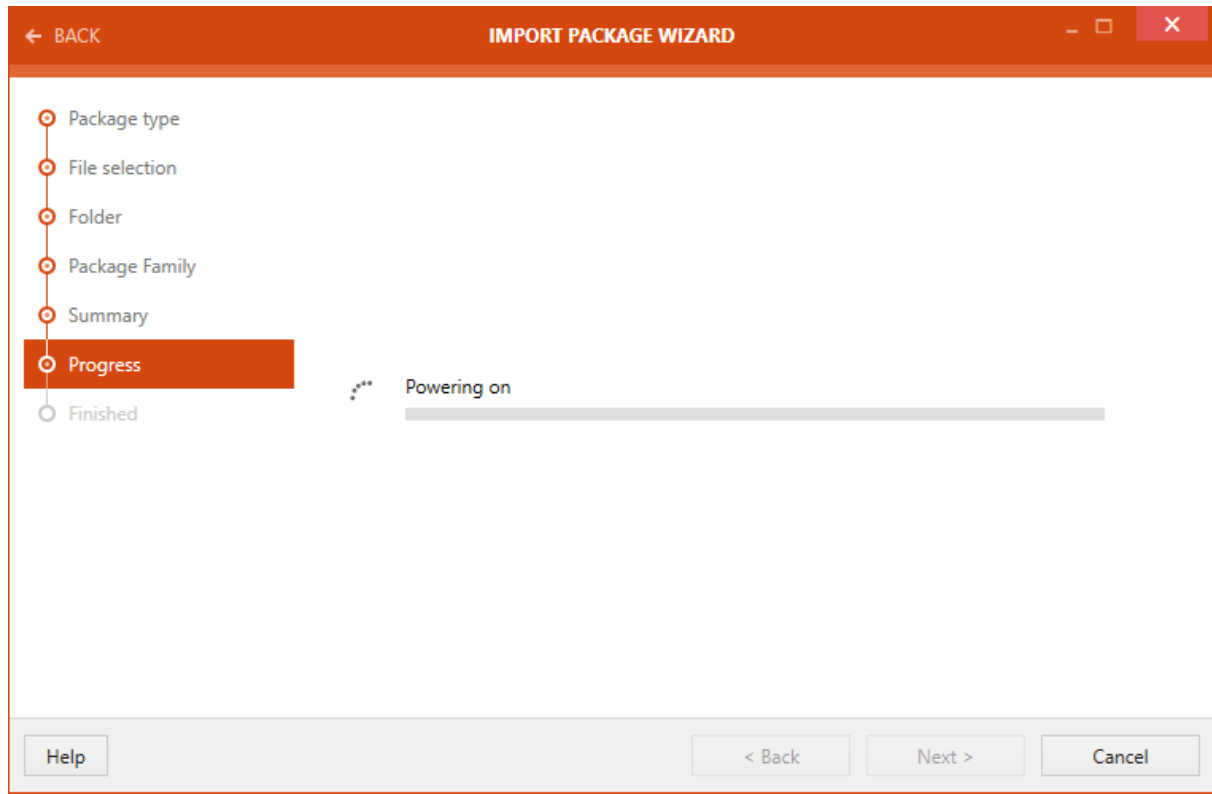
8. Confirmation on successful package import is shown on the **Finished** page.
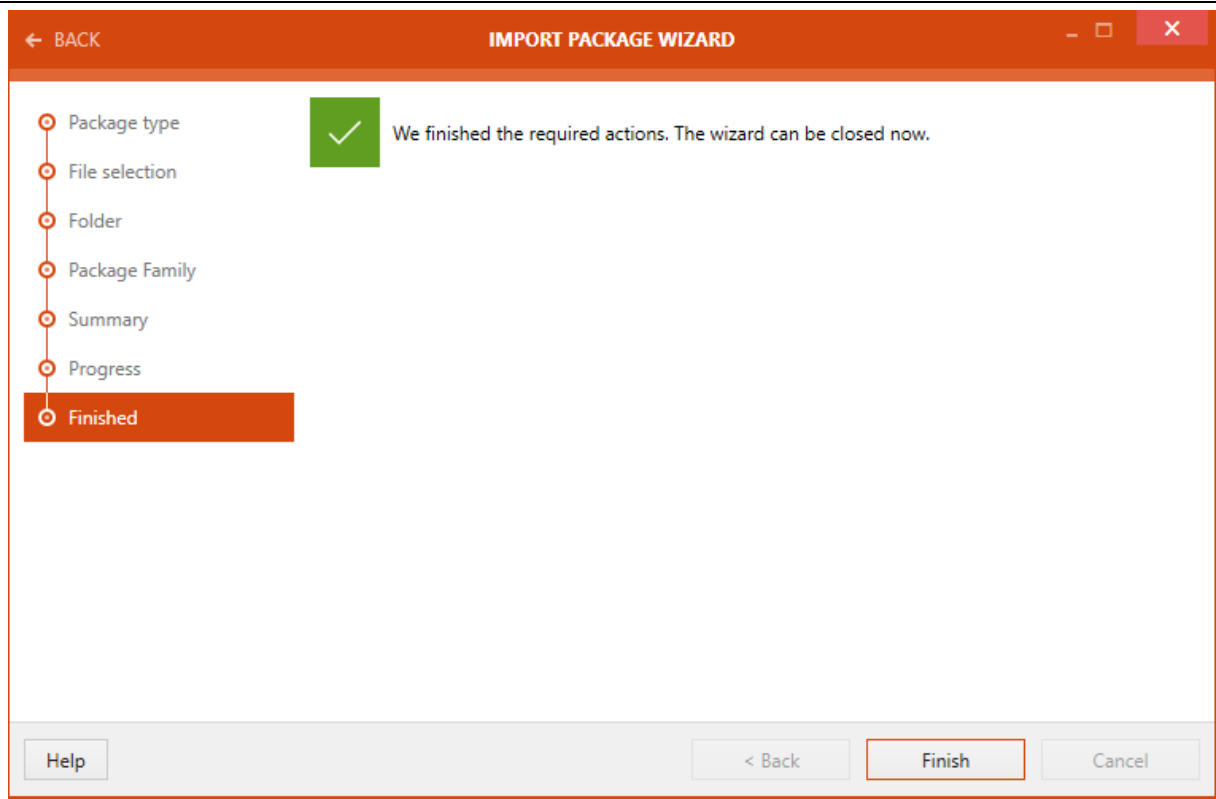
Click on the **Finish** button to close the **IMPORT PACKAGE WIZARD**.

RMS/SCCM Import Wizard

Deployment Type page

On the **Deployment Type** page users can choose their deployment type. The chosen type will then be used for the export of the package. The following deployment types are available:
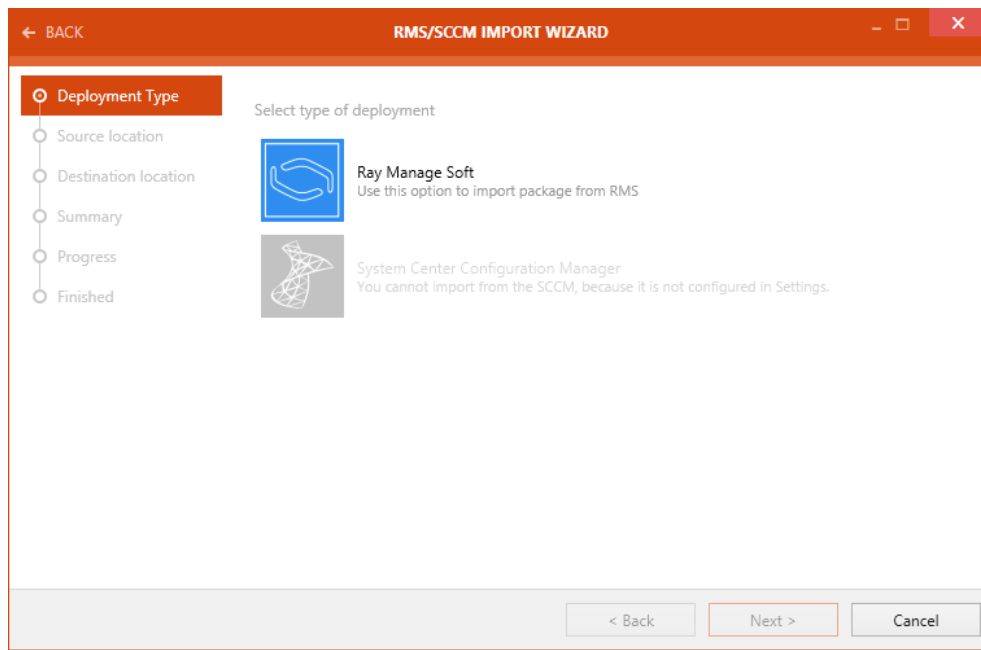
- **RayManageSoft**: If this option is chosen, the package will be exported using RayManageSoft. Be aware, that the RMS Console needs to be installed. If this is not the case, the option will be grayed out.
- **System Center Configuration Manager**: If this option is chosen, the package will be exported using the System Center Configuration Manager (SCCM). Be aware, that SCCM needs to be configured. If this is not the case, the option will be grayed out.

After a type has been chosen, click on the **Next >** button to proceed.

Source location page

On the **Source location** page the target package needs to be selected.
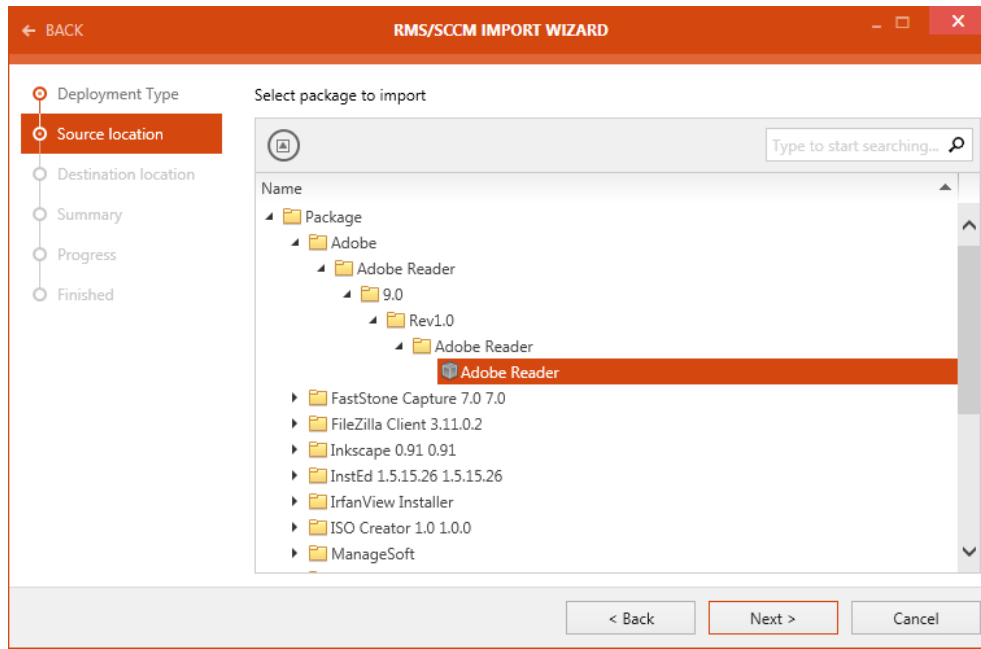
Select the target package from the library structure that is shown and after the package has been selected, click on the **Next >** button to proceed to the next step.

Destination location page

On the **Destination location page** the location to which the package shall be imported can be chosen.
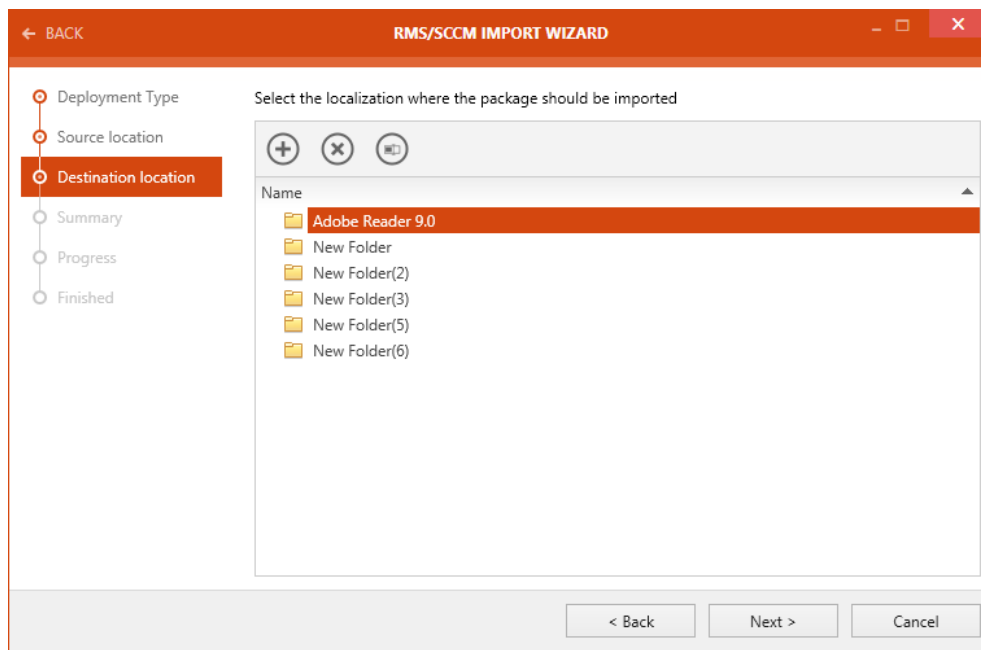
Choose the destination for the import by selecting the target folder from the tree structure.

Click on the **Next >** button to continue.

Summary page

The **Summary page** summarizes the settings for the export.
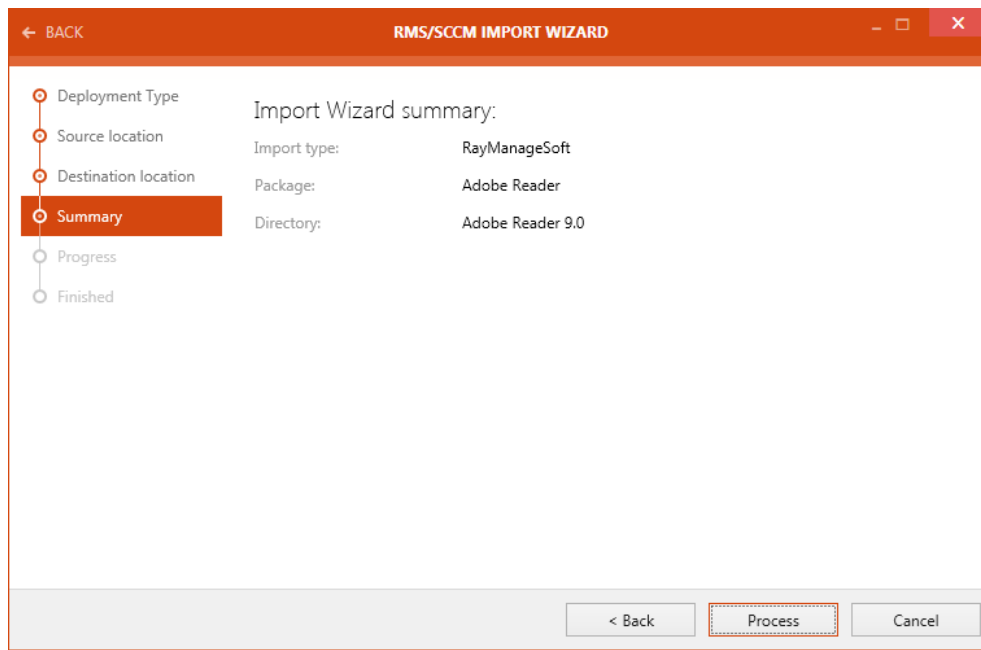
Check if all the settings are correct and then either proceed with the import or jump back to the stage where other settings need to be configured.

Click on the **Process** button to execute the import.

Progress page

On the **Progress page** the progress of the import is shown.
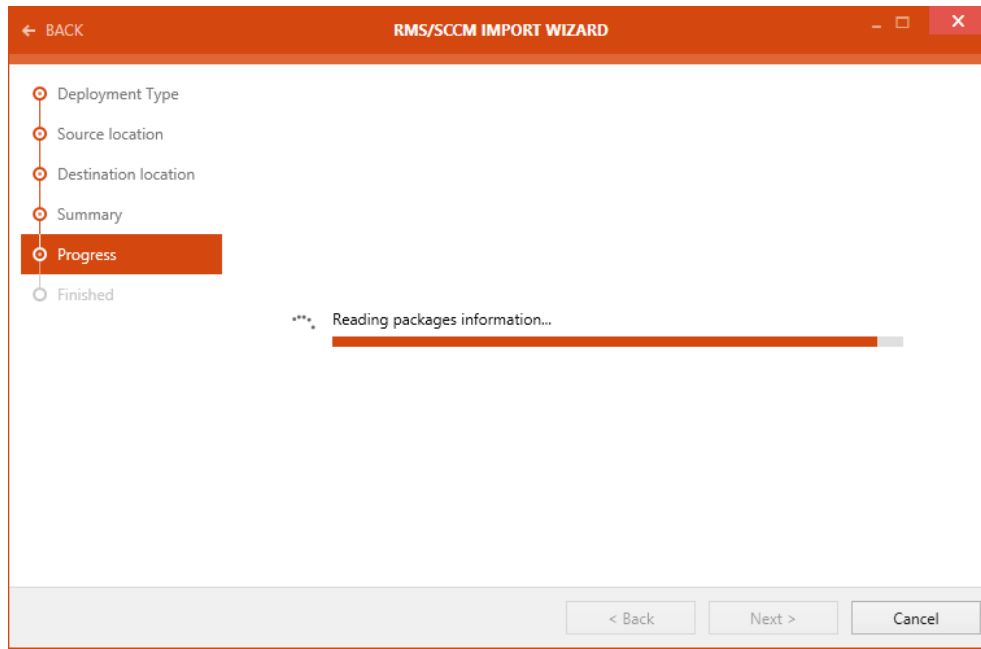
After the import has been finished the wizard will automatically continue to the next page.

Finished page

The **Finished page** contains the information if the import has been successful.
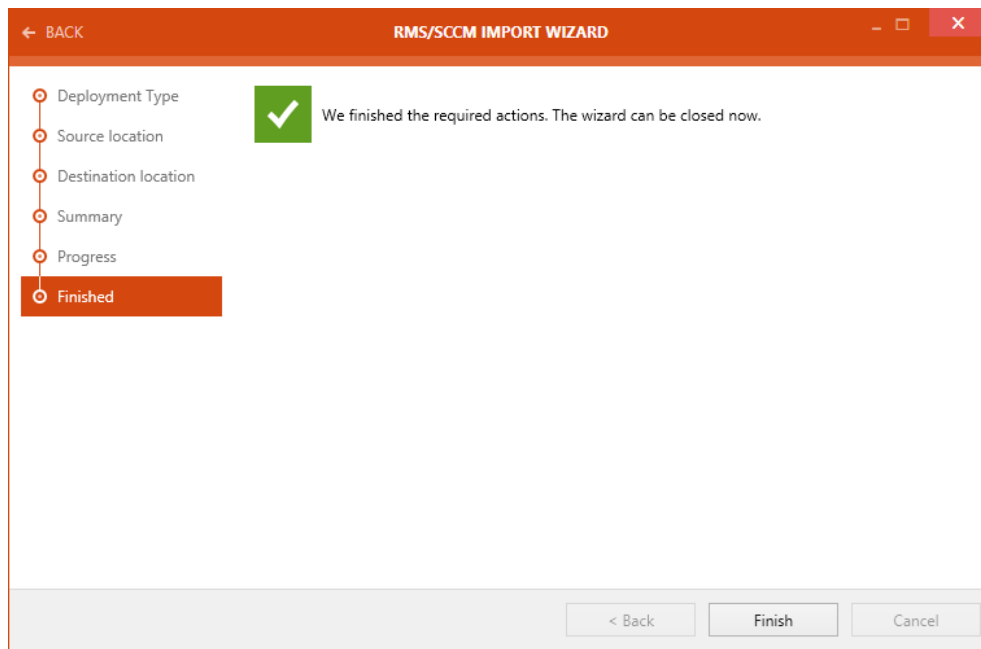
Click on the **Finished** button to close the wizard.

Package Families and Tags

Package Families and Tags can be used for the sorting and differentiating of packages. They can be assigned to packages and thereby enable the user to find packages easier and distinguish between similar packages.

Under the **SETTINGS** in the *Advanced* tab it is possible to define if a **Package family** or a tag will be deleted if the last package that is related to the tag or **Package family**.

Package Families

A **Package Family** can be assigned to a package during the import of a package in the **Package Family** window of the **IMPORT PACKAGE WIZARD**.

One way to use the **Package Family** is to assign the type of application as Package Family to a package. For example, the **Package family** PDF Reader can be assigned to a package which contains an Adobe Acrobat Reader or the **Package family** Browser can be assigned to a package which contains either Mozilla Firefox or Google Chrome.

In the Library the related packages (packages which share a **Package Family** with a selected package) are shown in the **RELATED PACKAGES** tab which is part of the side bar if a package is selected.

In the screenshot above the package named Google Chrome shares the **Package Family** Browser with the package Mozilla Firefox.

In the **PROPERTIES** tab of a package, which can be opened by selecting **Properties** in a context menu, there is a **PACKAGE FAMILY** tab. Here, the **Package Families** belonging to a package can be edited.
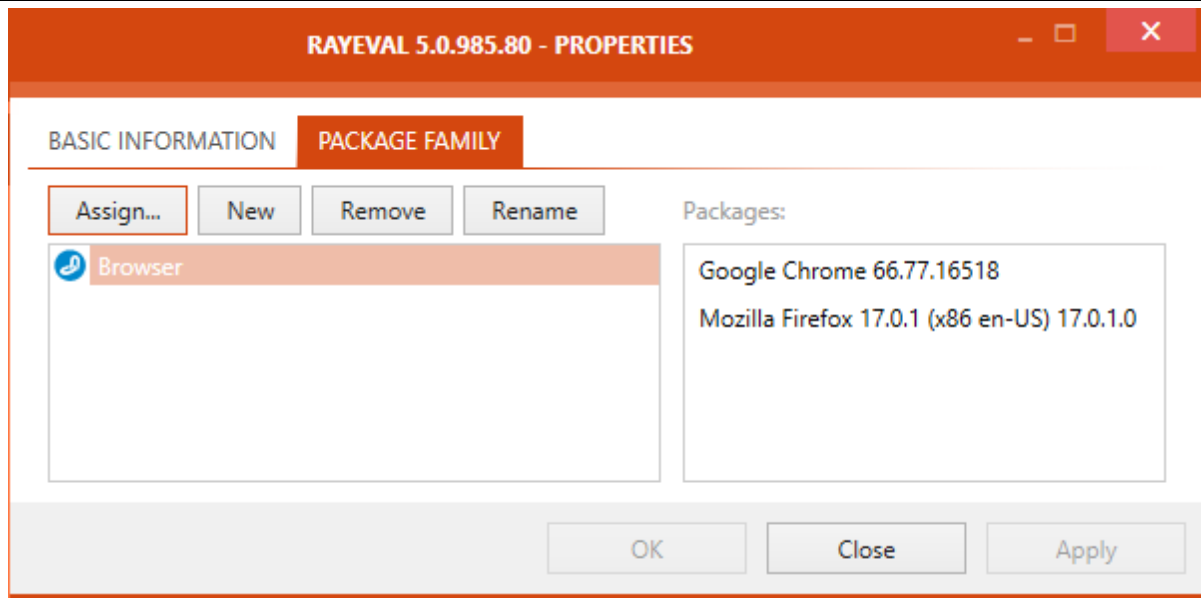
There are different buttons inside the tab. **Assign...**, **New**, **Remove**, and **Rename**. Furthermore, there are **OK**, **Close**, and **Apply** which can be used to save or discard changes made in the tab.

Assigning a Package Family

Clicking on the **Assign...** button will open the **SELECT PACKAGE FAMILY** window. In this window all **Package Families** available for assignment are shown.
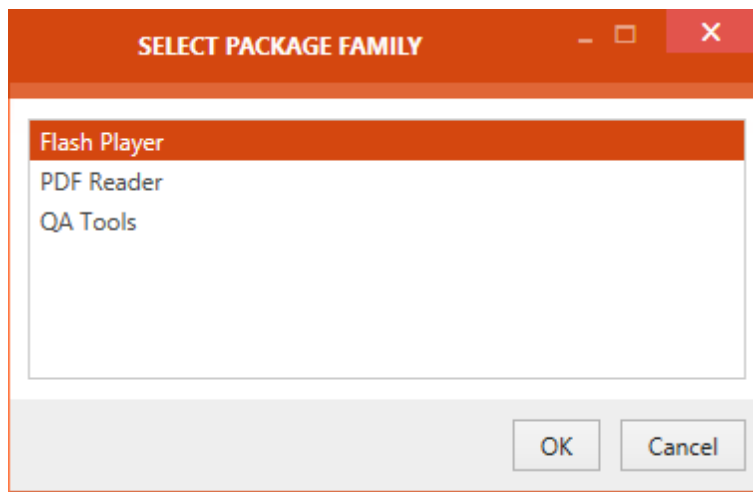
Select the target **Package Family** and click on the **OK** button to assign a package family to the package.

Creating a New Package Family

To create a new **Package Family** click on the **New** button in the **PROPERTIES** window of the select package.
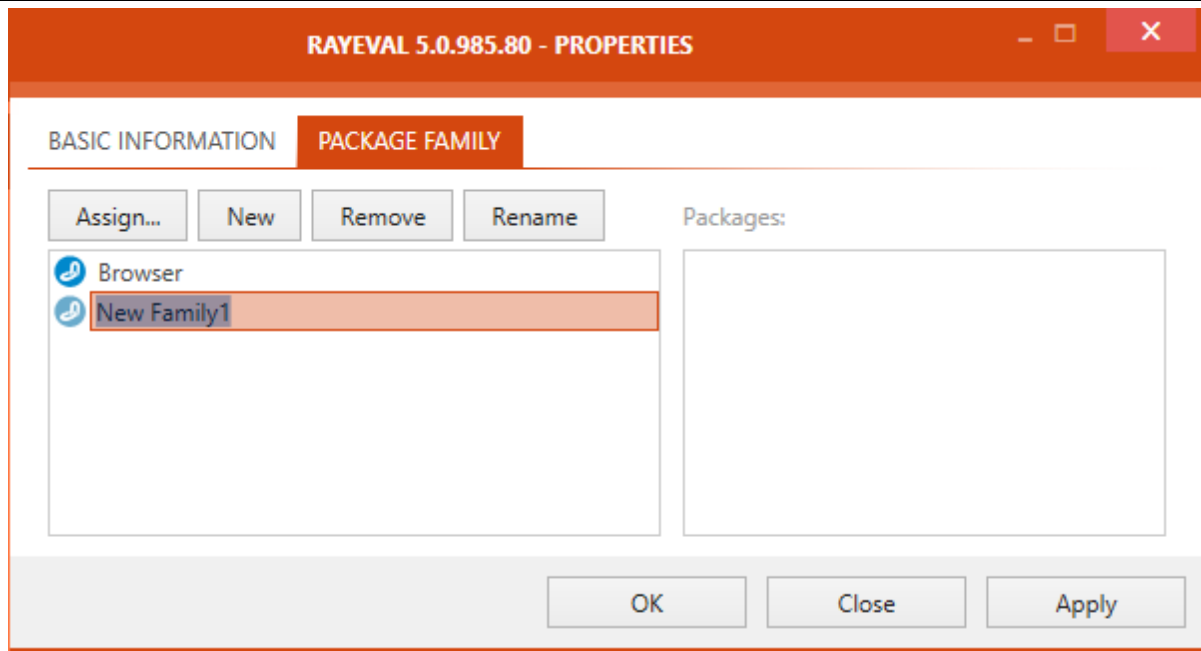
The newly created **Package Family** can be assigned to the selected package by clicking the **Apply** button.

Remove a Package Family

A **Package Family** can be removed from a package by selecting the target **Package Family** in the **PROPERTIES** view of the selected package and clicking on the **Remove** button. A confirmation window will be shown in which the removal of the **Package Family** from the package needs to be confirmed. There are two different confirmation windows that may appear. It depends on the number of packages a **Package Family** is assigned to.
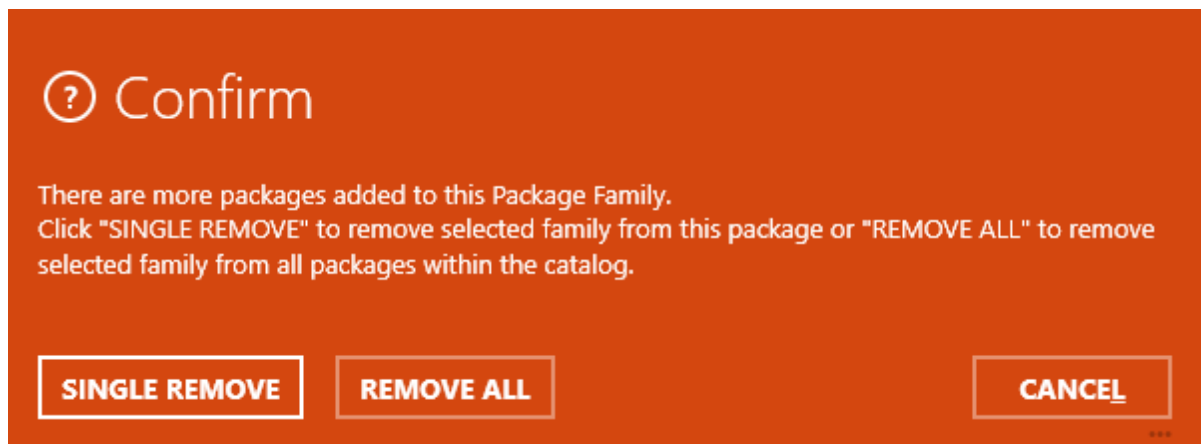
The above confirmation window will appear if a **Package Family** is assigned to more than one package. For the removal of the **Package Family** from the selected package only the **SINGLE REMOVE** button needs to be clicked. To remove the **Package Family** from all packages that it is assigned to the **REMOVE ALL** button needs to be clicked. If a **Package Family** is removed from all packages the **Package Family** will be deleted automatically.
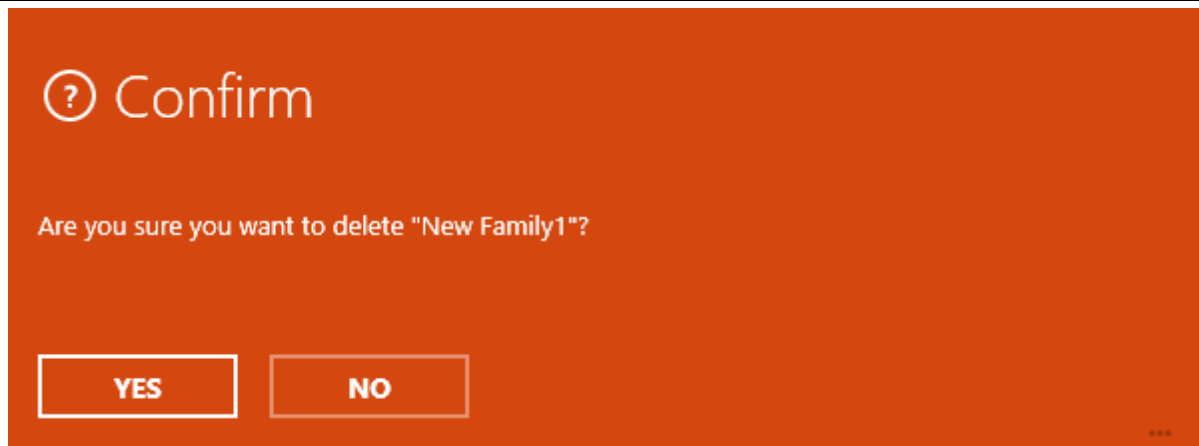
If the target **Package Family** is connected to the selected package only the above confirmation window will appear. Click on the **YES** button to proceed with the action. The **Package Family** will be deleted.

Rename a Package Family

A **Package Family** can be renamed by selecting the target **Package Family** and clicking on the **Rename** button.

Package Family Context Menu

The context menu can be opened by either clicking on a **Package Family** or in the area containing the Package Families. If the context menu is not opened directly on a **Package Family**, there will only be the **New** option available. With this option a new **Package Family** can be created. If opened directly on a **Package Family**, in addition to the **New** option, **Remove** and **Rename** will be available. The **Remove** option can be used to either **Remove** a **Package Family** from the target package or delete it completely if, after the **Remove** action has been executed, the **Package Family** will not be assigned to any package in the **Library** anymore. The **Rename** option can be used to rename a **Package Family**.
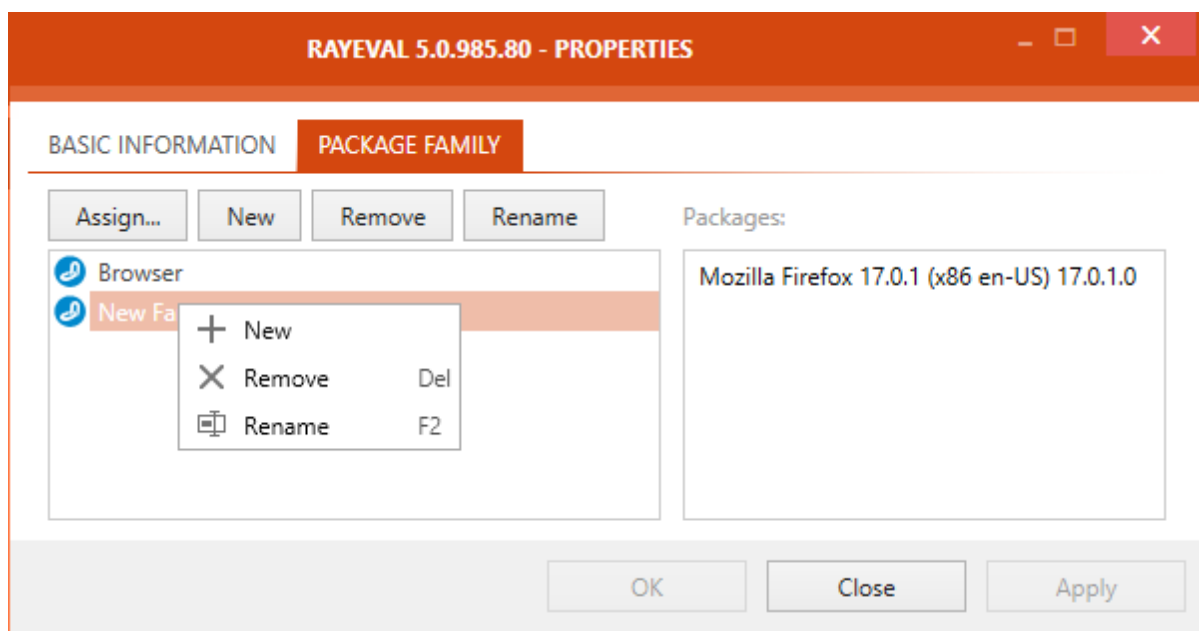
Saving and closing the window

After all changes have been applied, the **PROPERTIES** window can be closed by either using the **OK** button or the **Close** button. The **OK** button will save any changes and close the **PROPERTIES** window. The **Close** option will close the **PROPERTIES** window without saving the changes. A warning will appear that all unsaved changes will be lost. With the **Apply** button changes can be saved without closing the **PROPERTIES** window.

Tagging

A tag is a label which can be used to mark packages within the **Library**. Normally, a user can use a hierarchical folder structure to manage packages within the **Library**, however tags allow users to achieve a higher level of functional grouping.

A possible use case scenario for tags can be that of an enterprise using RayQC Advanced for package testing. Now suppose that certain packages are used by multiple departments within that enterprise and at times all the packages belonging to a single department needs to be tested. In this case, if folders are used to arrange packages based on the departments, then this will lead to redundancy of packages, as some of the package is used by more than one department. For this scenario, it will be more suitable to use folders to arrange packages based upon their manufacturer or type and then further tag them with department which uses it.

To tag a package, a user will need to select that package from the **Library** and then either create a new tag for it or select an existing one from the drop-down list.

To create a new tag, type in the name of this tag and then press **ENTER**. These tags can be used to filter packages both in within the catalog and in *Test Wizard.*

Custom Properties

Custom Properties are properties that can be added to packages in the **CUSTOM** tab of the side bar of a selected package in the **Library**. By default, the tab is empty until a user adds a custom variable to a package by clicking on the **Edit** button at the bottom of the tab.
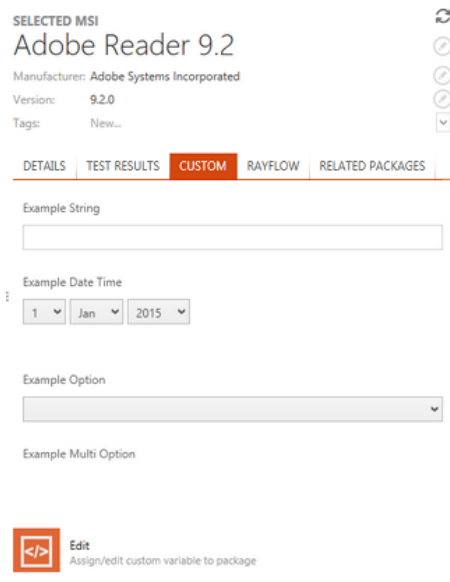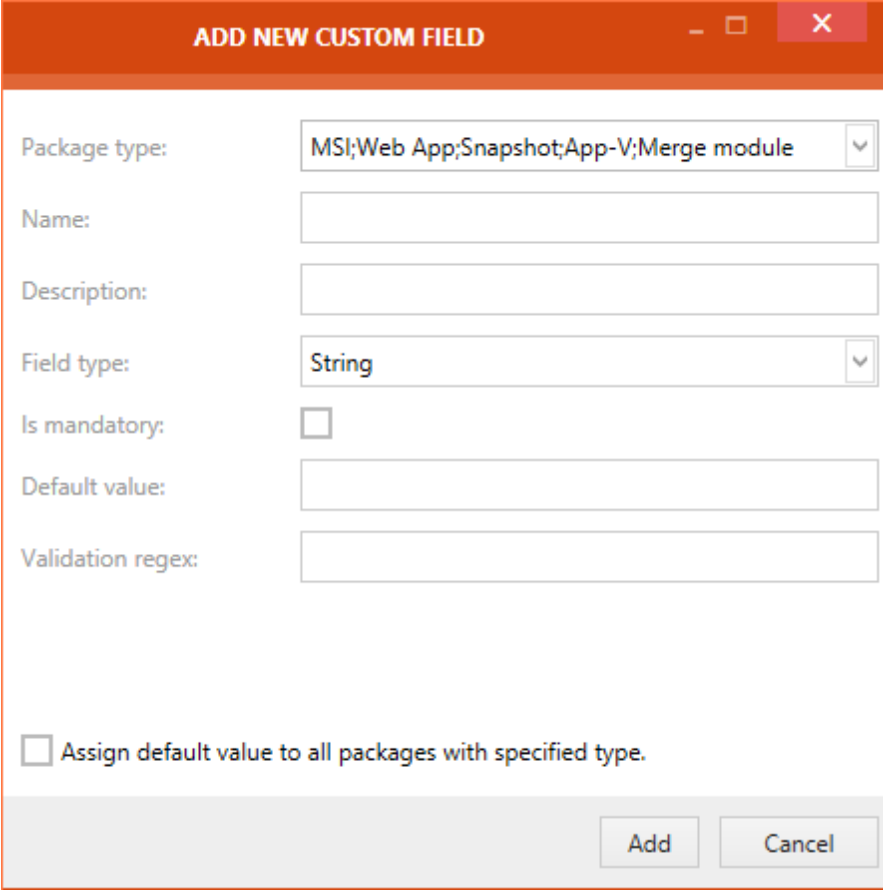
In the **PROPERTIES** window all valid variables for the package will be shown. A variable can be added by clicking on the **+** icon that is shown on next to the variable on the left when the variable is selected. Variables with an invalid value can not be added and will be highlighted in red. Furthermore, a short description why the value is invalid will be shown.
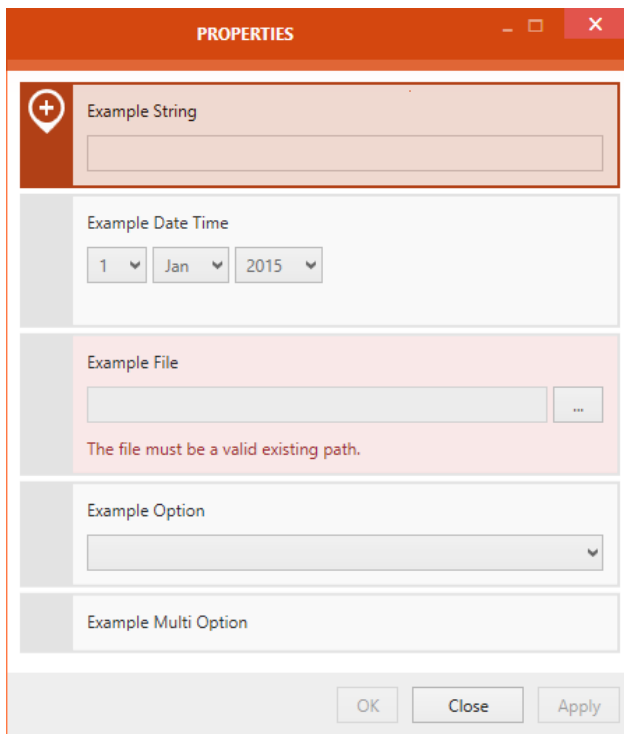
Click on the **Apply** button to apply the changes to the package without closing the window. Click on the **OK** button to apply the changes and close the **PROPERTIES** window.

In the following the different available custom fields are described.
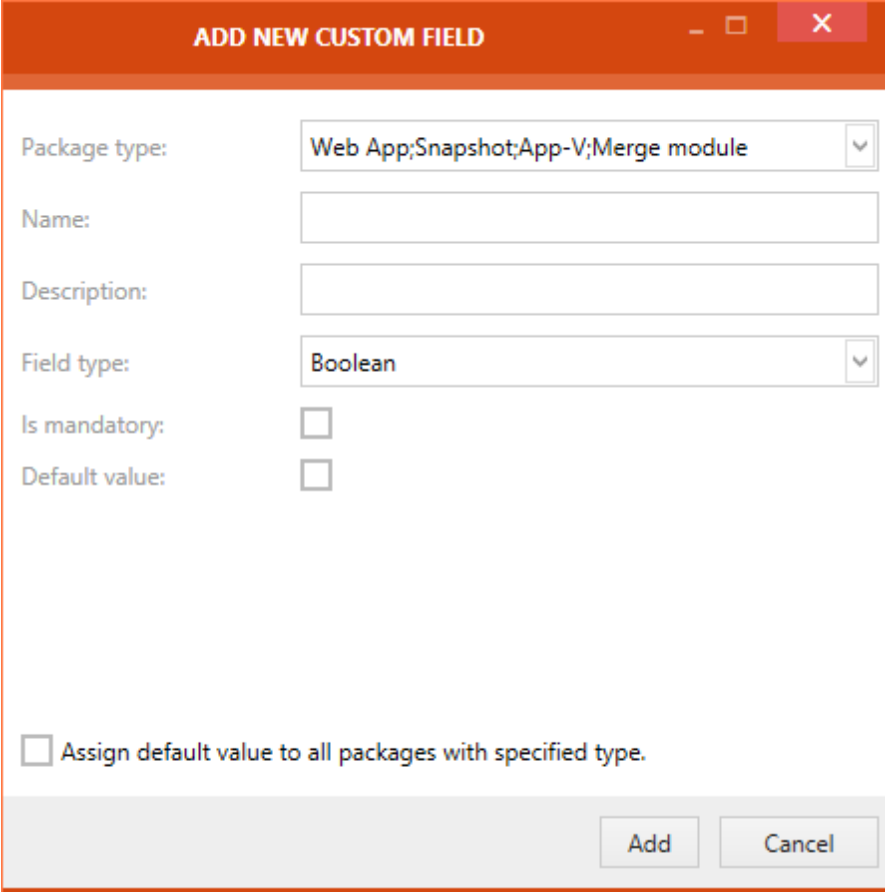
String

- **Package type**: The package type can be selected by using the dropdown menu and select the package type by checking the checkboxes to the left of the package type. It is possible to select multiple package types. The custom field will be available for all packages of the chosen package type. Click on the **OK** button to confirm the selection. Available package types are: **MSI**, **Merge module**, **App-V**, **Snapshot**, and **Web App**.
- **Name**: The name for the new text field can be entered here.
- **Description**: A description of the field can be entered here.
- **Field type**: The field type is selected here by using the dropdown menu. Only one type can be chosen. The fields beneath this field vary depending on the chosen type.
- **Is mandatory**: If this option is checked, the field is defined as a mandatory field.
- **Default value**: The default value of the field is entered here.
- **Validation regex**: The regular expression for the validation of a given value is entered here. (Example: "`PKG_[\d]+`" means that the given value has to start with "`[PKG_[at_least_one_digit]`")

Assign default value to all packages with specified type.: Checking this box will assign the newly generated custom property to all packages of the chosen package type. (This option is only available when the field is created for the first time)

Boolean

- **Package type**: The package type can be selected by using the dropdown menu and select the package type by checking the checkboxes to the left of the package type. It is possible to select multiple package types. The custom field will be available for all packages of the chosen package type. Click on the **OK** button to confirm the selection. Available package types are: **MSI**, **Merge module**, **App-V**, **Snapshot**, and **Web App**.
- **Name**: The name for the new text field can be entered here.
- **Description**: A description of the field can be entered here.
- **Field type**: The field type is selected here by using the dropdown menu. Only one type can be chosen. The fields beneath this field vary depending on the chosen type.
- **Is mandatory**: If this option is checked, the field is defined as a mandatory field.
- **Default value**: The default value of the field is entered here.

Assign default value to all packages with specified type.: Checking this box will assign the newly generated custom property to all packages of the chosen package type. (This option is only available when the field is created for the first time)

Date Time

- **Package type**: The package type can be selected by using the dropdown menu and select the package type by checking the checkboxes to the left of the package type. It is possible to select multiple package types. The custom field will be available for all packages of the chosen package type. Click on the **OK** button to confirm the selection. Available package types are: **MSI**, **Merge module**, **App-V**, **Snapshot**, and **Web App**.
- **Name**: The name for the new text field can be entered here.
- **Description**: A description of the field can be entered here.
- **Field type**: The field type is selected here by using the dropdown menu. Only one type can be chosen. The fields beneath this field vary depending on the chosen type.
- **Is mandatory**: If this option is checked, the field is defined as a mandatory field.
- **Default date**: The default date of the field is entered here.

Assign default value to all packages with specified type.: Checking this box will assign the newly generated custom property to all packages of the chosen package type. (This option is only available when the field is created for the first time)

File

- **Package type**: The package type can be selected by using the dropdown menu and select the package type by checking the checkboxes to the left of the package type. It is possible to select multiple package types. The custom field will be available for all packages of the chosen package type. Click on the **OK** button to confirm the selection. Available package types are: **MSI**, **Merge module**, **App-V**, **Snapshot**, and **Web App**.
- **Name**: The name for the new text field can be entered here.
- **Description**: A description of the field can be entered here.
- **Field type**: The field type is selected here by using the dropdown menu. Only one type can be chosen. The fields beneath this field vary depending on the chosen type.
- **Is mandatory**: If this option is checked, the field is defined as a mandatory field.
- **Default value**: The default value of the field is entered here.
- **Filter**: By using this field the file type can be defined (Example: "`INI file (*.ini | *.ini`" will open the Open dialog for INI files only).
- **Dialog mode**: This field defines if an **Open** or as **Save** file dialog will be shown. Select either **Open** or **Save** as option from the dropdown menu.

Assign default value to all packages with specified type.: Checking this box will assign the newly generated custom property to all packages of the chosen package type. (This option is only available when the field is created for the first time)

Folder

- **Package type**: The package type can be selected by using the dropdown menu and select the package type by checking the checkboxes to the left of the package type. It is possible to select multiple package types. The custom field will be available for all packages of the chosen package type. Click on the **OK** button to confirm the selection. Available package types are: **MSI**, **Merge module**, **App-V**, **Snapshot**, and **Web App**.
- **Name**: The name for the new text field can be entered here.
- **Description**: A description of the field can be entered here.
- **Field type**: The field type is selected here by using the dropdown menu. Only one type can be chosen. The fields beneath this field vary depending on the chosen type.
- **Is mandatory**: If this option is checked, the field is defined as a mandatory field.
- **Default value**: The default value of the field is entered here.

Assign default value to all packages with specified type.: Checking this box will assign the newly generated custom property to all packages of the chosen package type. (This option is only available when the field is created for the first time)

Option

- **Package type**: The package type can be selected by using the dropdown menu and select the package type by checking the checkboxes to the left of the package type. It is possible to select multiple package types. The custom field will be available for all packages of the chosen package type. Click on the **OK** button to confirm the selection. Available package types are: **MSI**, **Merge module**, **App-V**, **Snapshot**, and **Web App**.
- **Name**: The name for the new text field can be entered here.
- **Description**: A description of the field can be entered here.
- **Field type**: The field type is selected here by using the dropdown menu. Only one type can be chosen. The fields beneath this field vary depending on the chosen type.
- **Is mandatory**: If this option is checked, the field is defined as a mandatory field.
- **Option with values**: Check this box to enable the value field for the option.

Click inside the table under the **Option with values** checkbox to enter the **Name** and, if selected, the value of the option.

Assign default value to all packages with specified type.: Checking this box will assign the newly generated custom property to all packages of the chosen package type. (This option is only available when the field is created for the first time)

Multi Option

- **Package type**: The package type can be selected by using the dropdown menu and select the package type by checking the checkboxes to the left of the package type. It is possible to select multiple package types. The custom field will be available for all packages of the chosen package type. Click on the **OK** button to confirm the selection. Available package types are: **MSI**, **Merge module**, **App-V**, **Snapshot**, and **Web App**.
- **Name**: The name for the new text field can be entered here.
- **Description**: A description of the field can be entered here.
- **Field type**: The field type is selected here by using the dropdown menu. Only one type can be chosen. The fields beneath this field vary depending on the chosen type.
- **Is mandatory**: If this option is checked, the field is defined as a mandatory field.
- **Option with values**: Check this box to enable the value field for the option.

Click inside the table under the **Option with values** checkbox to enter a **Name** of an option and, if selected, the value of the option.

Assign default value to all packages with specified type.: Checking this box will assign the newly generated custom property to all packages of the chosen package type. (This option is only available when the field is created for the first time)

Numeric

ADD NEW CUSTOM FIELD

Package type: MSI

Name:

Description:

Field type: Numeric

Is mandatory:

Minimum: 0

Default: 0

Maximum: 2147483647
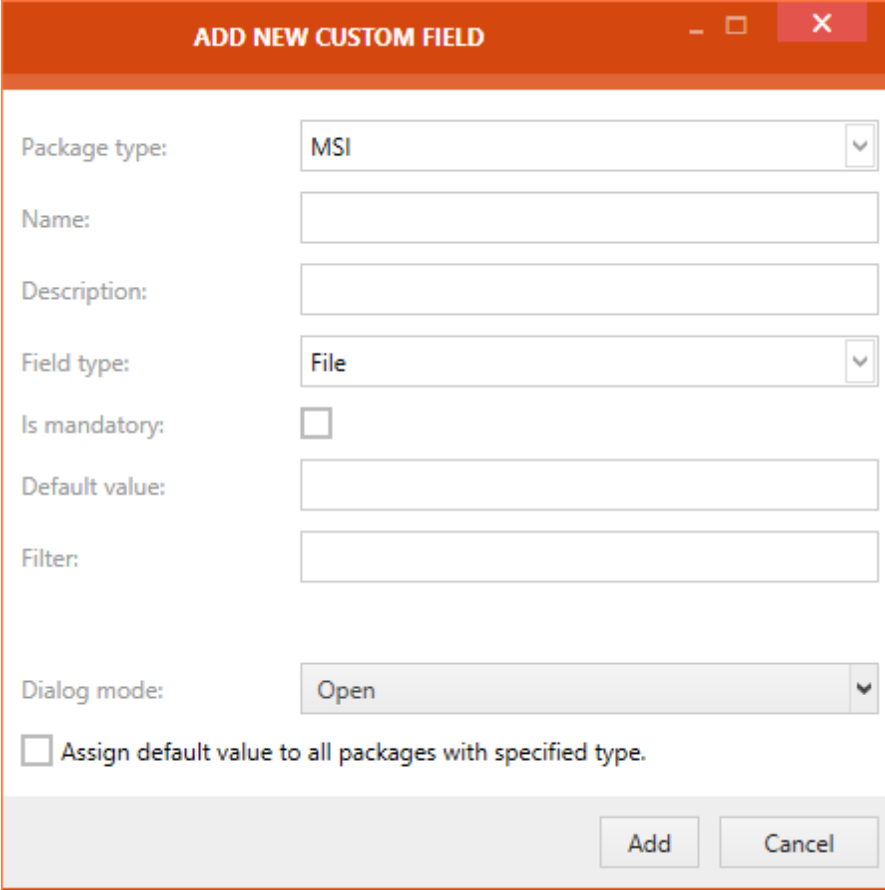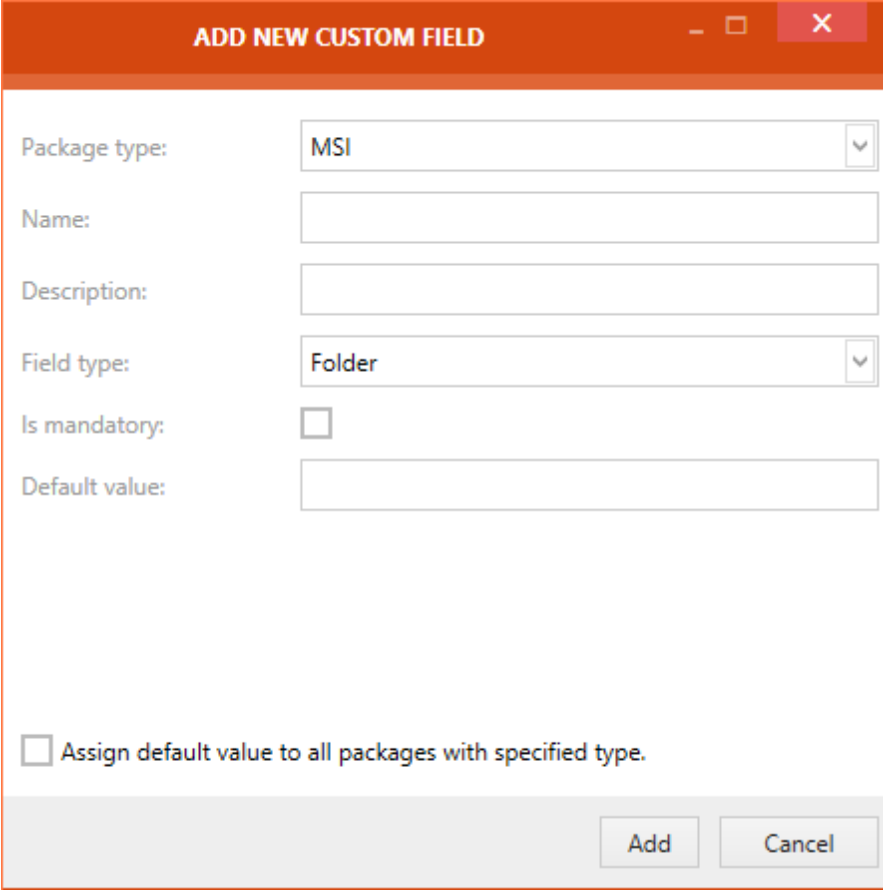
Assign default value to all packages with specified type.
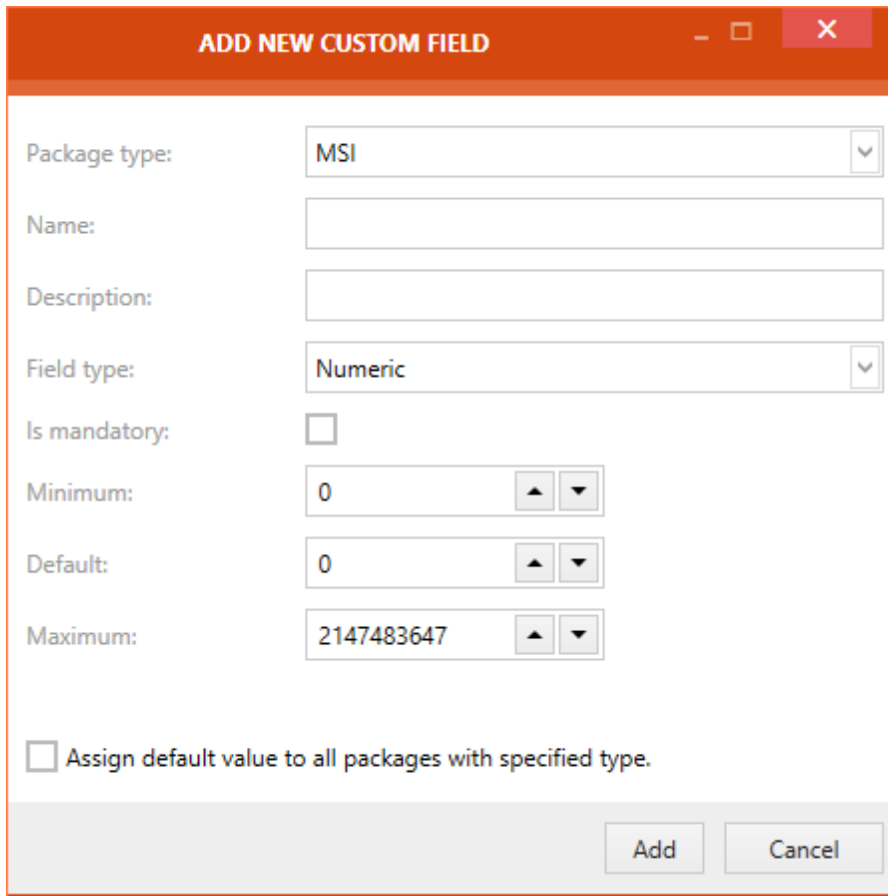
Add   Cancel

- **Package type**: The package type can be selected by using the dropdown menu and select the package type by checking the checkboxes to the left of the package type. It is possible to select multiple package types. The custom field will be available for all packages of the chosen package type. Click on the **OK** button to confirm the selection. Available package types are: **MSI**, **Merge module**, **App-V**, **Snapshot**, and **Web App**.
- **Name**: The name for the new text field can be entered here.
- **Description**: A description of the field can be entered here.
- **Field type**: The field type is selected here by using the dropdown menu. Only one type can be chosen. The fields beneath this field vary depending on the chosen type.
- **Is mandatory**: If this option is checked, the field is defined as a mandatory field.
- **Minimum**: The minimum value for the field is entered here by either typing it in directly or using the upwards and downwards arrow. The value of the **Minimum** field may not exceed the value of the **Maximum** field.
- **Default**: The default value for the field is entered here by either typing it in directly or using the upwards and downwards arrow. The value of the **Default** field may not exceed the value of the **Maximum** field and may not be lower than the value of the **Minimum** field..
- **Maximum**: The maximum value for the field is entered here by either typing it in directly or using the upwards and downwards arrow. The value of the **Maximum** field may not be lower than the value of the **Minimum** field.

Assign default value to all packages with specified type.: Checking this box will assign the newly generated custom property to all packages of the chosen package type. (This option is only available when the field is created for the first time)

Date Extended

- **Package type**: The package type can be selected by using the dropdown menu and select the package type by checking the checkboxes to the left of the package type. It is possible to select multiple package types. The custom field will be available for all packages of the chosen package type. Click on the **OK** button to confirm the selection. Available package types are: **MSI**, **Merge module**, **App-V**, **Snapshot**, and **Web App**.
- **Name**: The name for the new text field can be entered here.
- **Description**: A description of the field can be entered here.
- **Field type**: The field type is selected here by using the dropdown menu. Only one type can be chosen. The fields beneath this field vary depending on the chosen type.
- **Is mandatory**: If this option is checked, the field is defined as a mandatory field.
- **Default date**: The default date of the field is entered here. Other than the **Date** custom field the **Date Extended** custom field also includes the exact time.

Assign default value to all packages with specified type.: Checking this box will assign the newly generated custom property to all packages of the chosen package type. (This option is

only available when the field is created for the first time)

Rules Overview

Supported by a pre-defined set of rules, a user has an ability to execute collision, conformity, and virtualization tests, either on a single package or a set of packages, and conformity tests on web applications.These tests can be executed either individually or in a mixed mode. Further details on test execution can be found in the *Test Wizard* chapter of this document.

These rules are the backbone of this module and their algorithm not only reflects the current industry practices but also Raynet's vast experience in the fields of software packaging.

The following section provides an overview of currently existing rules in the RayQC Advanced module. These rules have been categorized based on the respective test types, supported by them.

These rules are cataloged and can be accessed via the Rule Browser. For information on Rule Browser and how to create custom rule sets, please refer to the *Rule Browser* section of this document.

App-V Test

The App-V test is carried out to test the conformity of an App-V package against a given operating system.

Windows 7 32-bit

AV001 - .NET framework Compatibility

Description: RayQC Advanced scans the App-V package for a presence of applications using .NET Framework 1.0, 1.1, 2.0, 3.0 or 3.5.

Background: Since Windows 7, .NET Framework 1.0 and 1.1 are not supported. Although it may be possible to deploy deprecated .NET components, there is no support for these configurations provided by Microsoft. Additionally, .NET Framework 2.0, 3.0 and 3.5 is not included in the default configuration of Windows 8 and later operating systems.

More Information: http://support.microsoft.com/kb/2489698

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should be converted to newer .NET Framework version.

AV002 - Launch conditions

Description: The launch conditions in App-V package is checked for existing selected operating system on the targets list.

Background: Launch conditions specify the operating systems that can run this package. If the target operating system does not fulfill conditions, it prevents running this package.

More Information: None available.

Manual Remediation: Contact the manufacturer to obtain compatible software. In self-developed software the 'TargetOperatingSystem' parameter should be modified.

AV003 - Session 0 isolation

Description: RayQC Advanced scans the App-V package for the presence of interactive services running in session 0.

Background: Session 0 isolation is example of security improvement introduced to prevent malicious software from compromising the security of the operating systems. They provide a separation between interactive user sessions and non-interactive session 0 devoted for services. Modern software has to comply to these restrictions in order to function correctly.

More Information: https://msdn.microsoft.com/en-us/library/windows/hardware/dn653293(v=vs.85).aspx

Manual Remediation: None available.

AV004 - Deprecated and obsolete API Calls

Description: RayQC Advanced scans the App-V package for a presence of API calls that are deprecated or obsolete.

Background: Certain APIs present in previous versions of Microsoft Windows are now officially deprecated or obsoleted by Microsoft. Obsolete APIs may not work anymore, or their behavior may be different leading to unexpected results. The deprecated APIs may be still working, but there is no guarantee they will function correctly or at all after any update or security patch. Usually, there is a replacement API that should be used in favor of deprecated or obsolete API call.

More Information: None available.

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should not use obsolete functions anymore and switch to replacements as described by Microsoft in Microsoft SDK Updates.

Windows 7 64-bit

AV001 - .NET framework Compatibility

Description: RayQC Advanced scans the App-V package for a presence of applications using .NET Framework 1.0, 1.1, 2.0, 3.0 or 3.5.

Background: Since Windows 7, .NET Framework 1.0 and 1.1 are not supported. Although it may be possible to deploy deprecated .NET components, there is no support for these configurations provided by Microsoft. Additionally, .NET Framework 2.0, 3.0 and 3.5 is not included in the default configuration of Windows 8 and later operating systems.

More Information: http://support.microsoft.com/kb/2489698

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should be converted to newer .NET Framework version.

AV002 - Launch conditions

Description: The launch conditions in App-V package is checked for existing selected operating system on the targets list.

Background: Launch conditions specify the operating systems that can run this package. If the target operating system does not fulfill conditions, it prevents running this package.

More Information: None available.

Manual Remediation: Contact the manufacturer to obtain compatible software. In self-developed software the 'TargetOperatingSystem' parameter should be modified.

AV003 - Session 0 isolation

Description: RayQC Advanced scans the App-V package for the presence of interactive services running in session 0.

Background: Session 0 isolation is example of security improvement introduced to prevent malicious software from compromising the security of the operating systems. They provide a separation between interactive user sessions and non-interactive session 0 devoted for services. Modern software has to comply to these restrictions in order to function correctly.

More Information: https://msdn.microsoft.com/en-us/library/windows/hardware/dn653293(v=vs.85).aspx

Manual Remediation: None available.

AV004 - Deprecated and obsolete API Calls

Description: RayQC Advanced scans the App-V package for a presence of API calls that are deprecated or obsolete.

Background: Certain APIs present in previous versions of Microsoft Windows are now officially deprecated or obsoleted by Microsoft. Obsolete APIs may not work anymore, or their behavior may be different leading to unexpected results. The deprecated APIs may be still working, but there is no guarantee they will function correctly or at all after any update or security patch. Usually, there is a replacement API that should be used in favor of deprecated or obsolete API call.

More Information: None available.

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should not use obsolete functions anymore and switch to replacements as described by Microsoft in Microsoft SDK Updates.

Windows 8 32-bit

AV001 - .NET framework Compatibility

Description: RayQC Advanced scans the App-V package for a presence of applications using .NET Framework 1.0, 1.1, 2.0, 3.0 or 3.5.

Background: Since Windows 7, .NET Framework 1.0 and 1.1 are not supported. Although it may be possible to deploy deprecated .NET components, there is no support for these configurations provided by Microsoft. Additionally, .NET Framework 2.0, 3.0 and 3.5 is not included in the default configuration of Windows 8 and later operating systems.

More Information: http://support.microsoft.com/kb/2489698

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should be converted to newer .NET Framework version.

AV002 - Launch conditions

Description: The launch conditions in App-V package is checked for existing selected

operating system on the targets list.

Background: Launch conditions specify the operating systems that can run this package. If the target operating system does not fulfill conditions, it prevents running this package.

More Information: None available.

Manual Remediation: Contact the manufacturer to obtain compatible software. In self-developed software the 'TargetOperatingSystem' parameter should be modified.

AV003 - Session 0 isolation

Description: RayQC Advanced scans the App-V package for the presence of interactive services running in session 0.

Background: Session 0 isolation is example of security improvement introduced to prevent malicious software from compromising the security of the operating systems. They provide a separation between interactive user sessions and non-interactive session 0 devoted for services. Modern software has to comply to these restrictions in order to function correctly.

More Information: https://msdn.microsoft.com/en-us/library/windows/hardware/dn653293(v=vs.85).aspx

Manual Remediation: None available.

AV004 - Deprecated and obsolete API Calls

Description: RayQC Advanced scans the App-V package for a presence of API calls that are deprecated or obsolete.

Background: Certain APIs present in previous versions of Microsoft Windows are now officially deprecated or obsoleted by Microsoft. Obsolete APIs may not work anymore, or their behavior may be different leading to unexpected results. The deprecated APIs may be still working, but there is no guarantee they will function correctly or at all after any update or security patch. Usually, there is a replacement API that should be used in favor of deprecated or obsolete API call.

More Information: None available.

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should not use obsolete functions anymore and switch to replacements as described by Microsoft in Microsoft SDK Updates.

Windows 8 64-bit

AV001 - .NET framework Compatibility

Description: RayQC Advanced scans the App-V package for a presence of applications using .NET Framework 1.0, 1.1, 2.0, 3.0 or 3.5.

Background: Since Windows 7, .NET Framework 1.0 and 1.1 are not supported. Although it may be possible to deploy deprecated .NET components, there is no support for these configurations provided by Microsoft. Additionally, .NET Framework 2.0, 3.0 and 3.5 is not included in the default configuration of Windows 8 and later operating systems.

More Information: http://support.microsoft.com/kb/2489698

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-

developed software should be converted to newer .NET Framework version.

AV002 - Launch conditions

Description: The launch conditions in App-V package is checked for existing selected operating system on the targets list.

Background: Launch conditions specify the operating systems that can run this package. If the target operating system does not fulfill conditions, it prevents running this package.

More Information: None available.

Manual Remediation: Contact the manufacturer to obtain compatible software. In self-developed software the 'TargetOperatingSystem' parameter should be modified.

AV003 - Session 0 isolation

Description: RayQC Advanced scans the App-V package for the presence of interactive services running in session 0.

Background: Session 0 isolation is example of security improvement introduced to prevent malicious software from compromising the security of the operating systems. They provide a separation between interactive user sessions and non-interactive session 0 devoted for services. Modern software has to comply to these restrictions in order to function correctly.

More Information: https://msdn.microsoft.com/en-us/library/windows/hardware/dn653293(v=vs.85).aspx

Manual Remediation: None available.

AV004 - Deprecated and obsolete API Calls

Description: RayQC Advanced scans the App-V package for a presence of API calls that are deprecated or obsolete.

Background: Certain APIs present in previous versions of Microsoft Windows are now officially deprecated or obsoleted by Microsoft. Obsolete APIs may not work anymore, or their behavior may be different leading to unexpected results. The deprecated APIs may be still working, but there is no guarantee they will function correctly or at all after any update or security patch. Usually, there is a replacement API that should be used in favor of deprecated or obsolete API call.

More Information: None available.

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should not use obsolete functions anymore and switch to replacements as described by Microsoft in Microsoft SDK Updates.

Windows 8.1 32-bit

AV001 - .NET framework Compatibility

Description: RayQC Advanced scans the App-V package for a presence of applications using .NET Framework 1.0, 1.1, 2.0, 3.0 or 3.5.

Background: Since Windows 7, .NET Framework 1.0 and 1.1 are not supported. Although it may be possible to deploy deprecated .NET components, there is no support for these configurations provided by Microsoft. Additionally, .NET Framework 2.0, 3.0 and 3.5 is not

included in the default configuration of Windows 8 and later operating systems.

More Information: http://support.microsoft.com/kb/2489698

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should be converted to newer .NET Framework version.

AV002 - Launch conditions

Description: The launch conditions in App-V package is checked for existing selected operating system on the targets list.

Background: Launch conditions specify the operating systems that can run this package. If the target operating system does not fulfill conditions, it prevents running this package.

More Information: None available.

Manual Remediation: Contact the manufacturer to obtain compatible software. In self-developed software the 'TargetOperatingSystem' parameter should be modified.

AV003 - Session 0 isolation

Description: RayQC Advanced scans the App-V package for the presence of interactive services running in session 0.

Background: Session 0 isolation is example of security improvement introduced to prevent malicious software from compromising the security of the operating systems. They provide a separation between interactive user sessions and non-interactive session 0 devoted for services. Modern software has to comply to these restrictions in order to function correctly.

More Information: https://msdn.microsoft.com/en-us/library/windows/hardware/dn653293(v=vs.85).aspx

Manual Remediation: None available.

AV004 - Deprecated and obsolete API Calls

Description: RayQC Advanced scans the App-V package for a presence of API calls that are deprecated or obsolete.

Background: Certain APIs present in previous versions of Microsoft Windows are now officially deprecated or obsoleted by Microsoft. Obsolete APIs may not work anymore, or their behavior may be different leading to unexpected results. The deprecated APIs may be still working, but there is no guarantee they will function correctly or at all after any update or security patch. Usually, there is a replacement API that should be used in favor of deprecated or obsolete API call.

More Information: None available.

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should not use obsolete functions anymore and switch to replacements as described by Microsoft in Microsoft SDK Updates.

Windows 8.1 64-bit

AV001 - .NET framework Compatibility

Description: RayQC Advanced scans the App-V package for a presence of applications using

.NET Framework 1.0, 1.1, 2.0, 3.0 or 3.5.

Background: Since Windows 7, .NET Framework 1.0 and 1.1 are not supported. Although it may be possible to deploy deprecated .NET components, there is no support for these configurations provided by Microsoft. Additionally, .NET Framework 2.0, 3.0 and 3.5 is not included in the default configuration of Windows 8 and later operating systems.

More Information: http://support.microsoft.com/kb/2489698

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should be converted to newer .NET Framework version.

AV002 - Launch conditions

Description: The launch conditions in App-V package is checked for existing selected operating system on the targets list.

Background: Launch conditions specify the operating systems that can run this package. If the target operating system does not fulfill conditions, it prevents running this package.

More Information: None available.

Manual Remediation: Contact the manufacturer to obtain compatible software. In self-developed software the 'TargetOperatingSystem' parameter should be modified.

AV003 - Session 0 isolation

Description: RayQC Advanced scans the App-V package for the presence of interactive services running in session 0.

Background: Session 0 isolation is example of security improvement introduced to prevent malicious software from compromising the security of the operating systems. They provide a separation between interactive user sessions and non-interactive session 0 devoted for services. Modern software has to comply to these restrictions in order to function correctly.

More Information: https://msdn.microsoft.com/en-us/library/windows/hardware/dn653293(v=vs.85).aspx

Manual Remediation: None available.

AV004 - Deprecated and obsolete API Calls

Description: RayQC Advanced scans the App-V package for a presence of API calls that are deprecated or obsolete.

Background: Certain APIs present in previous versions of Microsoft Windows are now officially deprecated or obsoleted by Microsoft. Obsolete APIs may not work anymore, or their behavior may be different leading to unexpected results. The deprecated APIs may be still working, but there is no guarantee they will function correctly or at all after any update or security patch. Usually, there is a replacement API that should be used in favor of deprecated or obsolete API call.

More Information: None available.

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should not use obsolete functions anymore and switch to replacements as described by Microsoft in Microsoft SDK Updates.

Windows 10 32-bit

AV001 - .NET framework Compatibility

Description: RayQC Advanced scans the App-V package for a presence of applications using .NET Framework 1.0, 1.1, 2.0, 3.0 or 3.5.

Background: Since Windows 7, .NET Framework 1.0 and 1.1 are not supported. Although it may be possible to deploy deprecated .NET components, there is no support for these configurations provided by Microsoft. Additionally, .NET Framework 2.0, 3.0 and 3.5 is not included in the default configuration of Windows 8 and later operating systems.

More Information: http://support.microsoft.com/kb/2489698

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should be converted to newer .NET Framework version.

AV002 - Launch conditions

Description: The launch conditions in App-V package is checked for existing selected operating system on the targets list.

Background: Launch conditions specify the operating systems that can run this package. If the target operating system does not fulfill conditions, it prevents running this package.

More Information: None available.

Manual Remediation: Contact the manufacturer to obtain compatible software. In self-developed software the 'TargetOperatingSystem' parameter should be modified.

AV003 - Session 0 isolation

Description: RayQC Advanced scans the App-V package for the presence of interactive services running in session 0.

Background: Session 0 isolation is example of security improvement introduced to prevent malicious software from compromising the security of the operating systems. They provide a separation between interactive user sessions and non-interactive session 0 devoted for services. Modern software has to comply to these restrictions in order to function correctly.

More Information: https://msdn.microsoft.com/en-us/library/windows/hardware/dn653293(v=vs.85).aspx

Manual Remediation: None available.

AV004 - Deprecated and obsolete API Calls

Description: RayQC Advanced scans the App-V package for a presence of API calls that are deprecated or obsolete.

Background: Certain APIs present in previous versions of Microsoft Windows are now officially deprecated or obsoleted by Microsoft. Obsolete APIs may not work anymore, or their behavior may be different leading to unexpected results. The deprecated APIs may be still working, but there is no guarantee they will function correctly or at all after any update or security patch. Usually, there is a replacement API that should be used in favor of deprecated or obsolete API call.

More Information: None available.

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should not use obsolete functions anymore and switch to replacements as described by Microsoft in Microsoft SDK Updates.

Windows 10 64-bit

AV001 - .NET framework Compatibility

Description: RayQC Advanced scans the App-V package for a presence of applications using .NET Framework 1.0, 1.1, 2.0, 3.0 or 3.5.

Background: Since Windows 7, .NET Framework 1.0 and 1.1 are not supported. Although it may be possible to deploy deprecated .NET components, there is no support for these configurations provided by Microsoft. Additionally, .NET Framework 2.0, 3.0 and 3.5 is not included in the default configuration of Windows 8 and later operating systems.

More Information: http://support.microsoft.com/kb/2489698

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should be converted to newer .NET Framework version.

AV002 - Launch conditions

Description: The launch conditions in App-V package is checked for existing selected operating system on the targets list.

Background: Launch conditions specify the operating systems that can run this package. If the target operating system does not fulfill conditions, it prevents running this package.

More Information: None available.

Manual Remediation: Contact the manufacturer to obtain compatible software. In self-developed software the 'TargetOperatingSystem' parameter should be modified.

AV003 - Session 0 isolation

Description: RayQC Advanced scans the App-V package for the presence of interactive services running in session 0.

Background: Session 0 isolation is example of security improvement introduced to prevent malicious software from compromising the security of the operating systems. They provide a separation between interactive user sessions and non-interactive session 0 devoted for services. Modern software has to comply to these restrictions in order to function correctly.

More Information: https://msdn.microsoft.com/en-us/library/windows/hardware/dn653293(v=vs.85).aspx

Manual Remediation: None available.

AV004 - Deprecated and obsolete API Calls

Description: RayQC Advanced scans the App-V package for a presence of API calls that are deprecated or obsolete.

Background: Certain APIs present in previous versions of Microsoft Windows are now officially deprecated or obsoleted by Microsoft. Obsolete APIs may not work anymore, or their behavior may be different leading to unexpected results. The deprecated APIs may be still working, but there is no guarantee they will function correctly or at all after any update or security patch.

Usually, there is a replacement API that should be used in favor of deprecated or obsolete API call.

More Information: None available.

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should not use obsolete functions anymore and switch to replacements as described by Microsoft in Microsoft SDK Updates.

Windows Server 2008 R2

AV001 - .NET framework Compatibility

Description: RayQC Advanced scans the App-V package for a presence of applications using .NET Framework 1.0, 1.1, 2.0, 3.0 or 3.5.

Background: Since Windows 7, .NET Framework 1.0 and 1.1 are not supported. Although it may be possible to deploy deprecated .NET components, there is no support for these configurations provided by Microsoft. Additionally, .NET Framework 2.0, 3.0 and 3.5 is not included in the default configuration of Windows 8 and later operating systems.

More Information: http://support.microsoft.com/kb/2489698

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should be converted to newer .NET Framework version.

AV002 - Launch conditions

Description: The launch conditions in App-V package is checked for existing selected operating system on the targets list.

Background: Launch conditions specify the operating systems that can run this package. If the target operating system does not fulfill conditions, it prevents running this package.

More Information: None available.

Manual Remediation: Contact the manufacturer to obtain compatible software. In self-developed software the 'TargetOperatingSystem' parameter should be modified.

AV003 - Session 0 isolation

Description: RayQC Advanced scans the App-V package for the presence of interactive services running in session 0.

Background: Session 0 isolation is example of security improvement introduced to prevent malicious software from compromising the security of the operating systems. They provide a separation between interactive user sessions and non-interactive session 0 devoted for services. Modern software has to comply to these restrictions in order to function correctly.

More Information: https://msdn.microsoft.com/en-us/library/windows/hardware/dn653293(v=vs.85).aspx

Manual Remediation: None available.

AV004 - Deprecated and obsolete API Calls

Description: RayQC Advanced scans the App-V package for a presence of API calls that are deprecated or obsolete.

Background: Certain APIs present in previous versions of Microsoft Windows are now officially deprecated or obsoleted by Microsoft. Obsolete APIs may not work anymore, or their behavior may be different leading to unexpected results. The deprecated APIs may be still working, but there is no guarantee they will function correctly or at all after any update or security patch. Usually, there is a replacement API that should be used in favor of deprecated or obsolete API call.

More Information: None available.

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should not use obsolete functions anymore and switch to replacements as described by Microsoft in Microsoft SDK Updates.

Windows Server 2012

AV001 - .NET framework Compatibility

Description: RayQC Advanced scans the App-V package for a presence of applications using .NET Framework 1.0, 1.1, 2.0, 3.0 or 3.5.

Background: Since Windows 7, .NET Framework 1.0 and 1.1 are not supported. Although it may be possible to deploy deprecated .NET components, there is no support for these configurations provided by Microsoft. Additionally, .NET Framework 2.0, 3.0 and 3.5 is not included in the default configuration of Windows 8 and later operating systems.

More Information: http://support.microsoft.com/kb/2489698

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should be converted to newer .NET Framework version.

AV002 - Launch conditions

Description: The launch conditions in App-V package is checked for existing selected operating system on the targets list.

Background: Launch conditions specify the operating systems that can run this package. If the target operating system does not fulfill conditions, it prevents running this package.

More Information: None available.

Manual Remediation: Contact the manufacturer to obtain compatible software. In self-developed software the 'TargetOperatingSystem' parameter should be modified.

AV003 - Session 0 isolation

Description: RayQC Advanced scans the App-V package for the presence of interactive services running in session 0.

Background: Session 0 isolation is example of security improvement introduced to prevent malicious software from compromising the security of the operating systems. They provide a separation between interactive user sessions and non-interactive session 0 devoted for services. Modern software has to comply to these restrictions in order to function correctly.

More Information: https://msdn.microsoft.com/en-us/library/windows/hardware/dn653293(v=vs.85).aspx

Manual Remediation: None available.

AV004 - Deprecated and obsolete API Calls

Description: RayQC Advanced scans the App-V package for a presence of API calls that are deprecated or obsolete.

Background: Certain APIs present in previous versions of Microsoft Windows are now officially deprecated or obsoleted by Microsoft. Obsolete APIs may not work anymore, or their behavior may be different leading to unexpected results. The deprecated APIs may be still working, but there is no guarantee they will function correctly or at all after any update or security patch. Usually, there is a replacement API that should be used in favor of deprecated or obsolete API call.

More Information: None available.

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should not use obsolete functions anymore and switch to replacements as described by Microsoft in Microsoft SDK Updates.

Windows Server 2012 R2

AV001 - .NET framework Compatibility

Description: RayQC Advanced scans the App-V package for a presence of applications using .NET Framework 1.0, 1.1, 2.0, 3.0 or 3.5.

Background: Since Windows 7, .NET Framework 1.0 and 1.1 are not supported. Although it may be possible to deploy deprecated .NET components, there is no support for these configurations provided by Microsoft. Additionally, .NET Framework 2.0, 3.0 and 3.5 is not included in the default configuration of Windows 8 and later operating systems.

More Information: http://support.microsoft.com/kb/2489698

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should be converted to newer .NET Framework version.

AV002 - Launch conditions

Description: The launch conditions in App-V package is checked for existing selected operating system on the targets list.

Background: Launch conditions specify the operating systems that can run this package. If the target operating system does not fulfill conditions, it prevents running this package.

More Information: None available.

Manual Remediation: Contact the manufacturer to obtain compatible software. In self-developed software the 'TargetOperatingSystem' parameter should be modified.

AV003 - Session 0 isolation

Description: RayQC Advanced scans the App-V package for the presence of interactive services running in session 0.

Background: Session 0 isolation is example of security improvement introduced to prevent malicious software from compromising the security of the operating systems. They provide a separation between interactive user sessions and non-interactive session 0 devoted for services. Modern software has to comply to these restrictions in order to function correctly.

More Information: https://msdn.microsoft.com/en-us/library/windows/hardware/dn653293(v=vs.85).aspx

Manual Remediation: None available.

AV004 - Deprecated and obsolete API Calls

Description: RayQC Advanced scans the App-V package for a presence of API calls that are deprecated or obsolete.

Background: Certain APIs present in previous versions of Microsoft Windows are now officially deprecated or obsoleted by Microsoft. Obsolete APIs may not work anymore, or their behavior may be different leading to unexpected results. The deprecated APIs may be still working, but there is no guarantee they will function correctly or at all after any update or security patch. Usually, there is a replacement API that should be used in favor of deprecated or obsolete API call.

More Information: None available.

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should not use obsolete functions anymore and switch to replacements as described by Microsoft in Microsoft SDK Updates.

Collision Test

Collision test is carried out to identify common conflicts between different applications, which hinder achieving required level of application isolation.

CA001 - Identical Component Identifiers

Description: The Windows Installer databases are scanned for the presence of identical Component IDs. A collision occurs when two or more packages contain the same Component ID with different content or different installation path.

Background: A component is a piece of the application to be installed. The Windows Installer service installs or removes a component as a single coherent piece. It tracks every component by its respective Component ID GUID specified in the Component column of the Component table.
Two components that share the same component ID are treated as multiple instances of the same component regardless of their actual content. Only a single instance of any component is installed on a user's computer. Therefore the install location and the content of components with the same Component ID should be identical.

More Information: https://msdn.microsoft.com/en-us/library/aa368007%28v=vs.85%29.aspx

Manual Remediation: A new Component ID should be generated for the Component(s) that unintentionally share the same GUID.

CA002 - Identical Product Codes

Description: The Windows Installer databases are scanned for the presence of identical Product Codes. A collision may occur when two or more packages have the same Product Code.

Background: The product code is a GUID that is the principal identification of an application or product.Two products with the same Product Code can not be installed on the same

computer. If significant changes are made to a product then the product code should also be changed to reflect this. However, when only minor changes are made, it is not required to change the Product Code.

More Information: https://msdn.microsoft.com/en-us/library/aa370854%28v=vs.85%29.aspx

Manual Remediation: A new Product Code should be generated for the package(s) that unintentionally shares the same Product Code GUID.

CA003 – Identical Package Codes

Description: The Windows Installer databases are scanned for the presence of identical Package Codes. A collision occurs when two or more packages have the same Package Code.

Background: The Package Code is a GUID that identifies a specific MSI file. No two MSIs should ever have the same Package Code unless they are identical copies of each other.

More Information: https://msdn.microsoft.com/pl-pl/library/aa370568%28v=vs.85%29.aspx

Manual Remediation: A new Package Code should be generated for the package(s) that share the same Package Code GUID.

CA004 – Identical Upgrade Codes

Description: The Windows Installer databases are scanned for the presence of identical Upgrade Codes. A collision may occur when two or more packages have the same Upgrade Code.

Background: The Upgrade Code is a GUID representing a related set of products. A set of different versions of one application will have the same Upgrade Code. This enables newer versions of the application to search and upgrade previous versions already installed on the same computer.

More Information: https://msdn.microsoft.com/en-us/library/aa372375%28v=vs.85%29.aspx

Manual Remediation: A new Upgrade Code should be generated for the package(s) that unintentionally share the same Upgrade Code GUID.

CA005 – Files

Description: The Windows Installer database is compared to the snapshot and/or MSI packages and scanned for the presence of identical file names in the same folder but with different attributes. A collision may occur when a different version of the same file name in the same folder is installed.

Background: Files are the main element of nearly every application. Proper working of the application depends on the availability of specific versions of these files in the appropriate locations. If different applications install different versions of the same file in the same location, then it might cause a collision between them.

More Information: https://msdn.microsoft.com/en-us/library/aa368596%28v=vs.85%29.aspx

Manual Remediation: Self-developed software should be re-authored to access the colliding files in a different location.

CA006 – Registry

Description: The Windows Installer database is compared to the snapshot and/or MSI packages and scanned for the presence of identical registry value names containing different

data.

Background: The Windows registry contains 3 basic elements: keys, values and data. A collision occurs if multiple applications add the same registry value with different data.

More Information: https://msdn.microsoft.com/en-us/library/aa371168%28v=vs.85%29.aspx

Manual Remediation: Self-developed software should be re-authored to read the registry values from a different key or different value name.

CA007 - INI Files

Description: The Windows Installer databases are scanned for the presence of identical INI file names in the same location but with colliding values.

Background: INI files are used to store application configuration. The proper working of the application often depends on the configurations in the INI file. Collisions may occur if different applications use the same INI file with colliding values.

More information: https://msdn.microsoft.com/en-us/library/aa369282%28v=vs.85%29.aspx

Manual Remediation: Self-developed software should be re-authored to use unique values / sections in shared INI files.

CA008 - Mismatch between INI File and File

Description: The Windows Installer database is compared to the snapshot and/or MSI packages and scanned for the presence of INI files that are installed from different sources (INI File table and File table).

Background: INI files can be installed either as flat files (from the File table) or as modular files (from the INI File table). If the INI file already exists on the target system and a Windows Installer package is installed that contains an INI file in the File table, the complete INI file will be overwritten. However, if the INI file is installed with the IniFile table, Windows Installer will edit the existing INI file and add the new content. Collisions may occur if the same INI file is installed from the INI File table and the File table.

More Information: https://msdn.microsoft.com/en-us/library/aa369282%28v=vs.85%29.aspx

Manual Remediation: The INI file should be removed from the File table and added to the IniFile table.

CA009 - Shortcuts

Description: The Windows Installer database is compared to the snapshot and/or MSI packages and scanned for the presence of identical shortcut names with different data.

Background: If multiple applications install the same shortcut name pointing to a different file or a different file location, collisions may occur.

More Information: https://msdn.microsoft.com/en-us/library/aa371847%28v=vs.85%29.aspx

Manual Remediation: Self-developed software should be re-authored to change the colliding shortcut name.

CA010 - File Associations

Description: The Windows Installer database is compared to the snapshot and/or MSI packages and scanned for the presence of identical file extensions pointing to different programs.

Background: A File Association links a file extension to an application capable of opening that file. A collision occurs if different applications associate the same file extension to a different program.

More Information: https://msdn.microsoft.com/en-us/library/aa368571%28v=vs.85%29.aspx

Manual Remediation: Self-developed software should be re-authored to change the colliding file association.

CA011 – Fonts

Description: The Windows Installer database is compared to the snapshot and/or MSI packages and scanned for the presence of identical font file names but with different font names.

Background: Windows Installer tracks all fonts by checking the columns "File_" and "FontTitle" in the Font table. A collision occurs if the same font file name is found with different font names (FontTitle).

More Information: https://msdn.microsoft.com/en-us/library/aa368606%28v=vs.85%29.aspx

Manual Remediation: Self-developed software should be re-authored to change the font file name to a new unique name.

CA012 – Services

Description: The Windows Installer database is compared to the snapshot and/or MSI packages and scanned for the presence of identical Service names but with different configurations.

Background: Windows Service Applications enable you to create long-running executable applications that run in their own Windows sessions. These services can be automatically started when the computer boots, can be paused and restarted, and do not show any user interface. Services can also run in the security context of a specific user account that is different from the logged-on user. A collision may occur if different applications install the same service but with different configuration options.

More Information: https://msdn.microsoft.com/en-us/library/aa371637%28v=vs.85%29.aspx

Manual Remediation: Self-developed software should be re-authored to use unique Service names.

CA013 – ODBC Data Sources and drivers

Description: The Windows Installer database is compared to the snapshot and/or MSI packages and scanned for the presence of identical ODBC Driver names pointing to different source files and for identical ODBC Data Source names with different configuration settings.

Background: ODBC (Open Database Connectivity) is a standard interface for accessing database management systems. A collision may occur if more than one application registers the same ODBC driver or Data Source but with different configuration options.

More Information: https://msdn.microsoft.com/en-us/library/aa370547(v=vs.85).aspx
https://msdn.microsoft.com/en-us/library/aa370546(v=vs.85).aspx

Manual Remediation: Self-developed software should be re-authored to use unique ODBC drivers and / or Data Sources.

CA014 - Environment Variables

Description: The Windows Installer database is compared to the snapshot and/or MSI packages and scanned for the presence of identical Environment Variable names. A collision occurs when at least one uses the "overwrite" option and has a different value to be set.

Background: Environment Variables are dynamic objects that store values to be referenced by applications.
Data can be appended to Environment Variables but it is also possible to overwrite the complete content of the Environment Variable with new data in which case a collision will occur.

More Information: https://msdn.microsoft.com/en-us/library/aa368369%28v=vs.85%29.aspx

Manual Remediation: Self-developed software should be re-authored to append the data to the existing content of the Environment Variable instead of overwriting it.

CA015 - Legacy Files

Description: The Windows Installer database is compared to the snapshot and/or other Windows Installer databases and scanned for the presence of `Autoexec.bat` and/or `Config.sys` files installed in the root of the System Drive.

Background: `Autoexec.bat` and `Config.sys` files are the primary automatic execution and configuration system files that were originally on DOS-type operating systems. Since Windows NT the content of those files is mostly ignored and only environment variables are taken into account.

More Information: None available.

Manual Remediation: Functionalities included in the `Autoexec.bat` and `Config.sys` files should be moved using new technologies.

CA016 - Executables Registration

Description: The Windows Installer databases are scanned for the presence of the same executables (`.dll`, `.exe`, `.ocx`) but are registered from different locations.

Background: Registering a DLL puts the path to the file in the registry where it can be looked up. That eliminates the problem of the program (or another program that also uses that same DLL) from having to hunt around for it.

More Information: None available.

Manual Remediation: None available.

Virtualization Test

Based upon the below listed rules, this test type is meant to verify that an application is ready for virtualization..

App-V 4.x

VA001 - Missing Shortcuts

Description: The Windows Installer database is scanned for the presence of at least one shortcut.

Background: At least one shortcut should be present in the package as it is necessary to act as entry point for the virtualized application.

More Information: None available.

Manual Remediation: A shortcut can be created to an existing or dummy file in the package. The users have to be made aware that they will have to start the application through this shortcut to activate it.

VA002 - Drivers

Description: The Windows Installer database is scanned for the presence of drivers.

Background: Most drivers cannot be virtualized and will not work in the virtualized application.

More Information: None available.

Manual Remediation: The driver should be removed from the virtual packaage and be installed physically on the machine.

VA003 - Fonts

Description: The Windows Installer database is scanned for the presence of fonts in the File, Registry, and Font table.

Background: Fonts that are installed with a virtual application will only be available for that software. Issues may occur in case the font should also be available for other (physically installed) software.

More Information: None available.

Manual Remediation: The font should be removed from the virtual package and be installed physically on the machine.

VA004 - Custom Actions

Description: The Windows Installer database is scanned for the presence of Custom Actions.

Background: Custom Actions may contain operations that alter existing or add new resources (not being part of the standard MSI tables) to the system. As Custom Actions are discarded when converting the package into a virtual format, all changes made by them will not be part of the virtualized application which will cause the package to be incomplete.

More Information: None available.

Manual Remediation: None available.

VA005 - Conditions on Components

Description: The Windows Installer database is scanned for the presence of Conditions on Components.

Background: Components can contain a conditional statement that controls whether or not a component is installed. As Component Conditions are discarded when converting a package into a virtual format, the content of all components will be part of the virtualized application which may result in undesired content.

More Information: None available.

Manual Remediation: None available.

VA006 – Hardcoded shortcuts

Description: The Windows Installer database is scanned for the presence of hardcoded shortcuts.

Background: Shortcuts are used as entry points for the virtualized application. As the installation folder for virtual software may vary, these shortcuts should contain relative paths to the target, working directory, and arguments.

More Information: None available.

Manual Remediation: All hardcoded paths in the properties of the shortcut should be changed to relative paths.

VA007 – Shell extensions

Description: The Windows Installer database is scanned for the presence of shell extensions.

Background: If application contains shell extensions cannot be convert to virtual format.

More information: None available.

Manual Remediation: Please note that for App-V this rule can be ignored from version 5.0 SP2 onwards.

VA008 – App-V filename length limitation

Description: The length of the Windows installer database filename is checked. It should not exceed 56 characters.

Background: Microsoft App-V stores the name of the `.sft` file in the Name field of `DBO.Packages` table in the SQL database. This Name filed has a length limitation of 64 characters and is made up of the name of the `.sft` file followed by "`_Package`", thus limiting the name of the `.sft` file to 56 characters.

More Information: None available.

Manual Remediation: The name of the Windows Installer database file should be limited to 56 characters.

VA010 – Office Add-ins

Description: Scan the Registry table for existence of Office Add-ins

Background: Office add-ins are not supported and they will not work in virtual applications. To work properly, add-ins should be installed physically on the machine.

More Information: https://msdn.microsoft.com/en-us/library/aa371168%28v=vs.85%29.aspx

Manual Remediation: The Office Add-ins should be removed from the virtual package and be installed physically on the machine.

VA011 – Services

Description: The Windows Installer database is scanned for the presence of services with automatic Startup Type.

Background: Services with Startup Type equal to Automatic (boot services) are not supported for virtualization.

More Information: None available.

Manual Remediation: the Startup Type for each service should be changed from **Automatic** to **Manual**.

VA012 - RELS files

Description: Scan the file table for the existence of files with extension `.rels`.

Background: If an application contains an OPC relationship part (`.rels`) file, the Microsoft App-V 5.0 sequencer fails to package the application.

More Information: https://support.microsoft.com/en-us/kb/2843030

Manual Remediation: To work around the limitation, manually delete all relationship files from the package source folder prior to saving the package.

VA013 - Hosts file

Description: The Windows Installer database is scanned for the presence of hosts file.

Background: The packages that update the hosts file cannot be virtualized.

More Information: None available.

Manual Remediation: None available.

VA014 - Hard-coded Paths

Description: The Windows Installer database is scanned for the presence of hard-coded paths.

Background: Paths should be relative...

More Information: None available.

Manual Remediation: All hard-coded paths should be changed to relative paths.

App-V 5.x

App-V 5.x Ruleset has several subeditions:

- App-V 5.0
- App-V 5.0 Service Pack 2
- App-V 5.0 Service Pack 2 (Hotfix 4)
- App-V 5.0 Service Pack 3
- App V 5.1
- App-V for Windows 10 Anniversary Update (1607)
- App-V for Windows 10 Creators Update (1703)

Exact details and tests may differ between these versions. This documentation provides only a general overview of items and problems tested by RayQC Advanced for the App-V 5.x family.

VA001 - Missing Shortcuts

Description: The Windows Installer database is scanned for the presence of at least one shortcut.

Background: At least one shortcut should be present in the package as it is necessary to act as entry point for the virtualized application.

More Information: None available.

Manual Remediation: A shortcut can be created to an existing or dummy file in the package. The users have to be made aware that they will have to start the application through this shortcut to activate it.

VA002 - Drivers

Description: The Windows Installer database is scanned for the presence of drivers.

Background: Most drivers cannot be virtualized and will not work in the virtualized application.

More Information: None available.

Manual Remediation: The driver should be removed from the virtual packaage and be installed physically on the machine.

VA003 - Fonts

Description: The Windows Installer database is scanned for the presence of fonts in the File, Registry, and Font table.

Background: Fonts that are installed with a virtual application will only be available for that software. Issues may occur in case the font should also be available for other (physically installed) software.

More Information: None available.

Manual Remediation: The font should be removed from the virtual package and be installed physically on the machine.

VA004 - Custom Actions

Description: The Windows Installer database is scanned for the presence of Custom Actions.

Background: Custom Actions may contain operations that alter existing or add new resources (not being part of the standard MSI tables) to the system. As Custom Actions are discarded when converting the package into a virtual format, all changes made by them will not be part of the virtualized application which will cause the package to be incomplete.

More Information: None available.

Manual Remediation: None available.

VA005 - Conditions on Components

Description: The Windows Installer database is scanned for the presence of Conditions on Components.

Background: Components can contain a conditional statement that controls whether or not a component is installed. As Component Conditions are discarded when converting a package into a virtual format, the content of all components will be part of the virtualized application which may result in undesired content.

More Information: None available.

Manual Remediation: None available.

VA006 - Hardcoded shortcuts

Description: The Windows Installer database is scanned for the presence of hardcoded shortcuts.

Background: Shortcuts are used as entry points for the virtualized application. As the installation folder for virtual software may vary, these shortcuts should contain relative paths to the target, working directory, and arguments.

More Information: None available.

Manual Remediation: All hardcoded paths in the properties of the shortcut should be changed to relative paths.

VA007 - Shell extensions

Description: The Windows Installer database is scanned for the presence of shell extensions.

Background: If application contains shell extensions cannot be convert to virtual format.

More information: None available.

Manual Remediation: Please note that for App-V this rule can be ignored from version 5.0 SP2 onwards.

VA010 - Office Add-ins

Description: Scan the Registry table for existence of Office Add-ins

Background: Office add-ins are not supported and they will not work in virtual applications. To work properly, add-ins should be installed physically on the machine.

More Information: https://msdn.microsoft.com/en-us/library/aa371168%28v=vs.85%29.aspx

Manual Remediation: The Office Add-ins should be removed from the virtual package and be installed physically on the machine.

VA011 - Services

Description: The Windows Installer database is scanned for the presence of services with automatic Startup Type.

Background: Services with **Startup Type** equal to **Automatic** (boot services) are not supported for virtualization.

More Information: None available.

Manual Remediation: The Startup Type for each service should be changed from **Automatic** to **Manual**.

VA012 - RELS files

Description: Scan the file table for the existence of files with extension `.rels`.

Background: If an application contains an OPC relationship part (`.rels`) file, the Microsoft App-V 5.0 sequencer fails to package the application.

More Information: https://support.microsoft.com/en-us/kb/2843030

Manual Remediation: To work around the limitation, manually delete all relationship files from the package source folder prior to saving the package.

VA013 - Hosts file

Description: The Windows Installer database is scanned for the presence of hosts file.

Background: The packages that update the hosts file cannot be virtualized.

More Information: None available.

Manual Remediation: None available.

VA014 - Hard-coded Paths

Description: The Windows Installer database is scanned for the presence of hard-coded paths.

Background: Paths should be relative...

More Information: None available.

Manual Remediation: All hard-coded paths should be changed to relative paths.

ThinApp 4.x

VA001 - Missing Shortcuts

Description: The Windows Installer database is scanned for the presence of at least one shortcut.

Background: At least one shortcut should be present in the package as it is necessary to act as entry point for the virtualized application.

More Information: None available.

Manual Remediation: A shortcut can be created to an existing or dummy file in the package. The users have to be made aware that they will have to start the application through this shortcut to activate it.

VA002 - Drivers

Description: The Windows Installer database is scanned for the presence of drivers.

Background: Most drivers cannot be virtualized and will not work in the virtualized application.

More Information: None available.

Manual Remediation: The driver should be removed from the virtual packaage and be installed physically on the machine.

VA004 - Custom Actions

Description: The Windows Installer database is scanned for the presence of Custom Actions.

Background: **Custom Actions** may contain operations that alter existing or add new resources (not being part of the standard MSI tables) to the system. As **Custom Actions** are discarded when converting the package into a virtual format, all changes made by them will not be part of the virtualized application which will cause the package to be incomplete.

More Information: None available.

Manual Remediation: None available.

VA005 – Conditions on Components

Description: The Windows Installer database is scanned for the presence of **Conditions** on **Components**.

Background: Components can contain a conditional statement that controls whether or not a **Component** is installed. As **Component Conditions** are discarded when converting a package into a virtual format, the content of all components will be part of the virtualized application which may result in undesired content.

More Information: None available.

Manual Remediation: None available.

VA006 – Hardcoded shortcuts

Description: The Windows Installer database is scanned for the presence of hardcoded shortcuts.

Background: Shortcuts are used as entry points for the virtualized application. As the installation folder for virtual software may vary, these shortcuts should contain relative paths to the target, working directory, and arguments.

More Information: None available.

Manual Remediation: All hardcoded paths in the properties of the shortcut should be changed to relative paths.

VA007 – Shell extensions

Description: The Windows Installer database is scanned for the presence of shell extensions.

Background: If application contains shell extensions cannot be convert to virtual format.

More Information: None available.

Manual Remediation: Please note that for App-V this rule can be ignored from version 5.0 SP2 onwards.

VA010 – Office Add-ins

Description: Scan the `Registry` table for existence of Office Add-ins

Background: Office add-ins are not supported and they will not work in virtual applications. To work properly, add-ins should be installed physically on the machine.

More information: https://msdn.microsoft.com/en-us/library/aa371168%28v=vs.85%29.aspx

Manual Remediation: The Office Add-ins should be removed from the virtual package and be installed physically on the machine.

VA014 – Hard-coded Paths

Description: The Windows Installer database is scanned for the presence of hard-coded paths.

Background: Paths should be relative...

More Information: None available.

Manual Remediation: The name of the Windows Installer database file should be limited to

56 characters.

ThinApp 5.x

VA001 - Missing Shortcuts

Description: The Windows Installer database is scanned for the presence of at least one shortcut.

Background: At least one shortcut should be present in the package as it is necessary to act as entry point for the virtualized application.

More Information: None available.

Manual Remediation: A shortcut can be created to an existing or dummy file in the package. The users have to be made aware that they will have to start the application through this shortcut to activate it.

VA002 - Drivers

Description: The Windows Installer database is scanned for the presence of drivers.

Background: Most drivers cannot be virtualized and will not work in the virtualized application.

More Information: None available.

Manual Remediation: The driver should be removed from the virtual packaage and be installed physically on the machine.

VA004 - Custom Actions

Description: The Windows Installer database is scanned for the presence of **Custom Actions**.

Background: **Custom Actions** may contain operations that alter existing or add new resources (not being part of the standard MSI tables) to the system. As **Custom Actions** are discarded when converting the package into a virtual format, all changes made by them will not be part of the virtualized application which will cause the package to be incomplete.

More Information: None available.

Manual Remediation: None available.

VA005 - Conditions on Components

Description: The Windows Installer database is scanned for the presence of **Conditions** on **Components**.

Background: Components can contain a conditional statement that controls whether or not a component is installed. As **Component Conditions** are discarded when converting a package into a virtual format, the content of all components will be part of the virtualized application which may result in undesired content.

More Information: None available.

Manual Remediation: None available.

VA006 - Hardcoded shortcuts

Description: The Windows Installer database is scanned for the presence of hardcoded

shortcuts.

Background: Shortcuts are used as entry points for the virtualized application. As the installation folder for virtual software may vary, these shortcuts should contain relative paths to the target, working directory, and arguments.

More Information: None available.

Manual Remediation: All hardcoded paths in the properties of the shortcut should be changed to relative paths.

VA007 - Shell extensions

Description: The Windows Installer database is scanned for the presence of shell extensions.

Background: If application contains shell extensions cannot be convert to virtual format.

More Information: None available.

Manual Remediation: Please note that for App-V this rule can be ignored from version 5.0 SP2 onwards.

VA010 - Office Add-ins

Description: Scan the `Registry` table for existence of Office Add-ins

Background: Office add-ins are not supported and they will not work in virtual applications. To work properly, add-ins should be installed physically on the machine.

More information: https://msdn.microsoft.com/en-us/library/aa371168%28v=vs.85%29.aspx

Manual Remediation: The Office Add-ins should be removed from the virtual package and be installed physically on the machine.

VA014 - Hard-coded Paths

Description: The Windows Installer database is scanned for the presence of hard-coded paths.

Background: Paths should be relative...

More Information: None available.

Manual Remediation: The name of the Windows Installer database file should be limited to 56 characters.

System Readiness Test

Tests a package for deployment on a selected operating system.

Windows 7 32-bit

Below are the set of rules which can be used to test a package for deployment on Windows 7 32-bit

T001 - Known Compatibility Issues at Startup (AppHelp)

Description: RayQC Advanced scans the package for the presence of applications that may

trigger Application Help Dialog (AppHelp) when the program is being installed or run for the first time.

Background: Certain applications are known to cause issues or not even starting on modern operating systems. Windows contains a predefined list of software known to have compatibility issues and warns or prevents user from starting the application. The list of such applications is stored in a central compatibility database, and the dialog shown to the user is known as Application Help (AppHelp).

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/bb756937.aspx

Manual Remediation: Contact the manufacturer to obtain compatible software.

T002 - Deprecated Windows Features

Description: RayQC Advanced scans the MSI package for the presence of deprecated features: embedded installations of another MSI packages (Custom Actions type 7, 23, 39), NETDDE-dependencies in registry, deprecated proxy configuration component ProxyCfg.exe.

Background: Certain features present in previous versions of Windows systems are officially deprecated by Microsoft. This means they are provided as-is. These features may be still working, but there is no guarantee they will function correctly or at all after any update or security patch. Usually, there is a replacement technology that should be used in favor of deprecated features.

More Information: http://msdn.microsoft.com/en-us/library/aa368010%28v=VS.85%29.aspx
http://msdn.microsoft.com/en-us/library/bb756977.aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/aa384069(v=vs.85).aspx

Manual Remediation: Do not use use Custom Actions type 7, 23 and 39 anymore. Dependencies and prerequisites have to be installed and managed by the deployment tool or external setup wrapper. The deprecated components have to be replaced. Contact the manufacturer to obtain compatible software.

T003 - Obsolete Windows Features

Description: RayQC Advanced scans the MSI package for a presence of deprecated MSGina technology, as well as for a presence of file extensions, for which the handling application has been obsoleted.

Background: Certain features present in previous versions of Windows systems are officially marked as obsolete by Microsoft. This means they are not supported anymore and any functionality relying on them is likely to fail to operate. Usually, there is a replacement technology that should be used in favor of deprecated features.

More Information: http://msdn.microsoft.com/en-us/library/bb756900.aspx
http://technet.microsoft.com/en-en/library/ee681703(v=ws.10).aspx

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software using the MSGina.dll should be re-enginered and use the Credential Providers model. Obsolete extensions should not be used in MSI installer packages.

T004 - Windows Shell and User Experience Changes

Description: RayQC Advanced scans the MSI package for a presence of shortcuts created in

Quick Launch and subfolders of the SendTo folder.

Background: Each version of Microsoft Windows system introduces enhancements and changes of the user experience in the way Windows Shell is working and organizing files, shortcuts, context menu actions etc. Certain aspects of the user experience vary between newer version of Windows. There is a different handling for certain behaviors that were possible before. For example, shortcuts placed in subfolders of the SendTo folder are not displayed anymore. Finally, Quick Launch Bar feature is not present anymore.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/cc144179(v=vs.85).aspx

http://msdn.microsoft.com/en-us/library/windows/desktop/jj584985(v=vs.85).aspx

Manual Remediation: Avoid deploying shortcuts to Quick Launch location and to subfolders of SendTo folder.

T005 - Unsupported Windows Components

Description: RayQC Advanced scans the MSI package for a presence of applications using DHTML control and for the presence of 32-bit `.hlp` files.

Background: Certain functionalities and components present in Windows XP and previous systems are not anymore part of the standard OS image. Since then Microsoft offers them as downloadable add-ons which restore the missing functionality. On a standard system however, missing handlers/opening applications may cause runtime exceptions or other warnings. Typical examples of such components are viewers for 32-bit .hlp files, missing DHTLM editor controls and so on.

More Information: http://support.microsoft.com/kb/917607

http://msdn.microsoft.com/en-us/library/aa663363.aspx

Manual Remediation: Contact the manufacturer to obtain compatible software. You may also install the missing components - the update KB917607 restores the ability to view 32-bit `.hlp` files, and the redistributable installer `DHTMLEd.msi` from Microsoft installs the missing DHTML control.

T006 - .NET Framework Compatibility

Description: RayQC Advanced scans the MSI package for a presence of applications using .NET Framework 1.0 or 1.1.

Background: Since Windows 7, .NET Framework 1.0 and 1.1 are not supported. Although it may be possible to deploy deprecated .NET components, there is no support for these configurations provided by Microsoft.

More Information: http://support.microsoft.com/kb/2489698

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should be converted to .NET Framework 4.5.

T007 - Conditional Installation and Execution

Description: RayQC Advanced scans the MSI package for a presence of conditions that vary based on the value of properties: VersionNT, VersionNT64, WindowsBuild and ServicePackLevel. Additionally, the content of the package is scanned for the usage of AdminUser and Privilleged properties in Launch Conditions and components condition to

verify they will not cause issues with permission elevation. Merge modules, 16-bit components and certain conditions may neutralize otherwise failing conditions.

Background: Number of MSI properties like VersionNT, VersionNT64, ServicePackLevel etc. can be used to conditionally control the flow of installation and set of features/components/ policies to be installed. Software vendors use them frequently in critical places like LaunchConditions, conditions for components and Custom Actions, conditional security policies and many more. When a new version of Operating System is introduced, these conditions have to be reviewed, because they may generate false warnings even though the software is functioning correctly. Another source of issues are two distinctive MSI properties Privileged and AdminUser. Because of late elevation, since Windows Vista values of these properties are spoofed when evaluating LaunchConditions. This may produce unexpected results with packages designed for previous operating systems.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/ aa370556(v=vs.85).aspx

http://msdn.microsoft.com/en-us/library/windows/desktop/ aa369752(v=vs.85).aspx

Manual Remediation: Review all rows containing conditions that exclude the current operating system. Should the given component/action be required and function correctly on Windows 7, rewrite the condition so that it evaluates to true or remove it to always install the questionable resource. Do not use AdminUser property, because it may impact installation flows that elevate at some later point of installation. Legacy distinction between Provileged and AdminUser property can be restored by using the MSIREALADMINDETECTION property.

T008 - Deprecated and Obsolete API Calls

Description: RayQC Advanced scans the MSI package for a presence of API calls that are deprecated or obsolete. Internal database is used to assess each API call being used.

Background: Certain APIs present in previous versions of Microsoft Windows are now officially deprecated or obsoleted by Microsoft. Obsolete APIs may not work anymore, or their behavior may be different leading to unexpected results. The deprecated APIs may be still working, but there is no guarantee they will function correctly or at all after any update or security patch. Usually, there is a replacement API that should be used in favor of deprecated or obsolete API call.

More Information: None available.

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should not use obsolete functions anymore and switch to replacements as described by Microsoft in Microsoft SDK Updates.

T009 - Hard-Coded Resources and System Paths

Description: RayQC Advanced scans the MSI package for a usage of changed or obsolete junction points in INI files, registry entries, services, shortcuts, environment variables and custom actions.

Background: Since Microsoft Windows Vista, standard locations where user and system data are stored have been changed. For example, the root folder for user data was called "Documents and Settings" in Windows XP, but since Windows Vista its name is "Users". To provide a backward compatibility, junction points are used to reroute the calls from old, incorrect locations to the new, proper ones. A package that runs on various target systems

should not rely on hard-coded paths, because they may be not valid anymore or for a given system language.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/bb968829(v=vs.85).aspx

http://msdn.microsoft.com/en-us/library/windows/desktop/aa368977(v=vs.85).aspx

Manual Remediation: Hardcoded paths should not be used. Replace them with MSI properties using formatted syntax. If no predefined property exists, the path should be exposed via custom MSI property so that it can be adjusted on demand from command-line / MST transform.

T010 - Mismatched Target Architecture

Description: RayQC Advanced scans the MSI package for the presence of executables (16/32/64-bit) that are not compatible with Windows 7 32-bit platform.

Background: Some software is intended to run only in 32-bit or 64-bit operating systems. 16-bit executables are not supported on modern platforms, and 64-bit Microsoft Windows can correctly emulate 32-bit applications. If the MSI package is missing a correct Launch Condition it may try to install executables that are not designed for the current platform architecture. Attempting to launch such executable might result in an error message that the file is not a valid Win32 application. Additionally, attempting to run 16-bit code may result in a warning message informing that an extra Windows Feature is required.

More Information: http://support.microsoft.com/kb/282423/en-us

Manual Remediation: Contact the manufacturer to obtain compatible software. Reenginer self-developed software by replacing 16-bit executables with appropriate 32- or 64-bit code. Use Launch Conditions and component conditions to control to which platform software and its parts are deployed.

T011 - Driver Issues

Description: RayQC Advanced scans the MSI package for the presence of drivers containing no valid signature or not matching the target platform.

Background: Since Windows Vista 64-bit, all drivers have to be signed. Signed driver contains an extra digital signature used to validate the source and content of the driver package. Any unauthorized change in the driver package invalidates the signature. If an unsigned driver or a driver with invalid signature is attempted to be installed, Windows refuses the installation. Likewise, each driver has to match the target platform, which means that 64-bit systems require 64-bit drivers.

More Information: http://msdn.microsoft.com/en-us/library/bb756937.aspx

Manual Remediation: Contact the manufacturer to obtain compatible driver. Use WDK (Windows Driver Kit) to sign self-developed driver packages.

T012 - Installation Package Design Issues

Description: RayQC Advanced scans the MSI package for the presence of common installation design issues that may cause troubles during installation or using of software. The context of Custom Actions is scanned for the presence of deferred custom actions running in user-context, as well as system-wide actions running in immediate mode. The presence of conflicting permissions tables preventing the installation is detected as well. Additionally,

invalid combinations of user- and machine-data in a single component and invalid identifiers are reported.

Background: Microsoft recommends several best-practice approaches for MSI setup designers. They ensure that the package is deployed correctly in various scenarios and various operating systems. By following the guidelines many compatibility issues introduced by a new security model in Windows Vista can be avoided.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/aa368268%28v=vs.85%29.aspx

http://msdn.microsoft.com/en-us/library/windows/desktop/aa368268(v=vs.85).aspx

http://msdn.microsoft.com/en-us/library/windows/desktop/dd408053(v=vs.85).aspx

http://msdn.microsoft.com/en-us/library/6397xx85(v=vs.80).aspx

http://msdn.microsoft.com/en-us/library/windows/desktop/aa368994%28v=vs.85%29.aspx

Manual Remediation: Adjust the package content so that it complies to the best practises of Windows Installer. Do not mix per-machine and per-user data in a single component. Use valid identifiers for components. Make sure all custom actions are running in a valid context - all actions making system changes must be deferred in execution. Do not use both `LockPermissions` and `MsiLockPermissionsEx` tables at once.

T013 - Conflicts with Protected Windows Resources (WRP)

Description: RayQC Advanced scans the MSI package for the presence of files and registry keys that belong to the Windows Resource Protection list.

Background: Windows Resource Protection (WRP) prevents the modification of essential system resources (files, folders and registry keys). Windows Installer silently ignores any attempt to update or modify them, any other software trying to do it may fail. These kinds of resources may be only updated by Microsoft-provided redistributable packages. During the installation, if Windows Installer logging is enabled, a warning may be shown for each operation that was ignored because of the WRP protection.

More Information: http://msdn.microsoft.com/en-us/library/bb756998.aspx

Manual Remediation: Assess whether the conflicting resources are actually needed, and if not remove them from the MSI package. If a given resource is needed and the original system one cannot be used, consider reenginering the application or use any virtualization technique to override the resource.

T014 - Missing or Invalid Signatures

Description: RayQC Advanced scans the MSI package for the presence of unsigned executable files (.exe, .dll, .ocx). Additionally, the package itself and CAB files are also scanned.

Background: According to the set of best practices by Microsoft, all exercutable files deployed by an installation package and the installation package itself should be digitally signed with a certificate issued by a Trusted Publisher. When attempting to run an unsigned executable, Windows prompts the user for authorization. Similarly, attempting to install an unsigned MSI package also shows the Windows prompt.

More Information: http://technet.microsoft.com/en-us/library/cc962053.aspx

Manual Remediation: Contact the manufacturer to obtain signed executables and installers. Use WDK (Windows Driver Kit) to sign self-developed executables and packages.

T015 - Security and User Access Control Issues

Description: RayQC Advanced scans the MSI package for the presence of issues that may fail to work due to the security features. The executable files are scanned for the presence of correct manifestation. Direct calls to rundll32 are reported, because the UAC prompt hides the actual calling module when rundll32 is executed. Interactive sevices running in session 0 are detected, as well as MMC snap-ins that are not DEP-aware. Finally, setups, updaters and uninstallers are detected and checked for the presence of their UAC awareness.

Background: Session 0 isolation and Data Execution Prevention (DEP) are examples of security improvements introduced to prevent malcious software from compromising the security of the operating systems. They provide a separation between interactive user sessions and non-interactive session 0 devoted for services, and prevent execution of code from non-executable memory region. Modern software has to comply to these restrictions in order to function correctly on Windows 10. Another security issue present in Windows operating system is User Account Control (UAC). When an executable file requires additional non-standard permissions, the UAC elevation dialog prompts for confirmation or for correct credentials. The UAC prompt contains information about calling application, manufacturer and the source. Certain applications, like self-updaters, setups and other requiring higher privileges must be aware of the elevation, and use manifests to correctly inform the system about required execution permissions.

More Information: http://msdn.microsoft.com/en-us/windows/hardware/gg463353
http://msdn.microsoft.com/en-us/library/bb963893.aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/aa366553(v=vs.85).aspx
http://technet.microsoft.com/en-us/library/cc709628%28WS.10%29.aspx
http://technet.microsoft.com/en-us/library/cc709628%28WS.10%29.aspx

Manual Remediation: Contact the manufacturer to obtain software that complies to the security features of Microsoft Windows. For each unmanifested executable file, create a manifest, and set the required privileges to "`asInvoker`" for applications not requiring them, and "`requireAdministrator`" or "`highestAvailable`" for others. If the manifest cannot be corrected, a shim database has to be used to specify the desired privilege level.

T016 - Missing Application Manifest or Insufficient Execution Policy

Description: RayQC Advanced scans the MSI package for the presence of executabl files (`.exe`, `.cpl`) that do not contain the manifest, or that are not aware of Windows 10 in the list of supported operating systems in their manifest files.

Background: Since Windows Vista, all applications run by default with standard user privileges. This is also true when the current user is a member of Administrators group. Application that used to work on previous versions of Windows may fail to work, as no elevation will take place. In order to require higher permissions, each executable or control panel applications has to contain a manifest file - a simple `.XML` file informing the operating system how to handle the given program.

More Information: http://msdn.microsoft.com/en-us/library/Aa480152%23appcomp_topic30.com#appcomp_topic4
http://msdn.microsoft.com/en-us/library/hh848036%28v=vs.85%29.aspx

Manual Remediation: Create a manifest file for each executable. To manifest a control panel application (`.cpl`) create an executable wrapper with embedded manifest. Use the SupportedOS section in the manifest to define the list of supported operating systems.

T017 - Incomplete Reboot Handling

Description: RayQC Advanced scans the MSI package for the absence of a proper launch condition preventing the installation if a reboot is pending. Additionally, absence of "Files in use" dialog is detected. Presence of `ForceReboot` action is also detected and reported.

Background: Windows Installer supports natively various set of features and actions related to the reboot handling. They include for example the ability to show list of used/locked files, forcing or skipping the reboot and determining the installation state by the related MSI properties. Several aspects have to be considered so that the reboot handling works as expected.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/aa368607(v=vs.85).aspx

http://msdn.microsoft.com/en-us/library/windows/desktop/aa370492(v=vs.85).aspx

http://msdn.microsoft.com/en-us/library/windows/desktop/aa370379(v=vs.85).aspx

Manual Remediation: Add the `MSIRMFilesInUse` dialog to the dialog sequence if it is missing. Remove ForceReboot action from the sequence, reboots are handled automatically by MSI. In order to ensure the package is not installed when any reboot is pending, append the "`NOT MsiSystemRebootPending`" condition to the Launch Condition list.

T018 - Protected Mode (Internet Explorer)

Description: RayQC Advanced scans the MSI package for the presence of registry entries that disable Protected Mode.

Background: As a result of security changes introduced in Windows Vista, Internet Explorer runs now in a isolated mode called "Protected mode" by default. While it limits potential damages malware application can cause, it also prevents web-applications running in Internet Explorer from writing directly to disk while in Internet or Intranet zone. Internet Explorer warns when web-application tries to run certain software programs or write to protected areas.

More Information: http://msdn.microsoft.com/en-us/library/bb756991.aspx

Manual Remediation: Contact the manufacturer to obtain compatible software. Re-engineer self-developed software so that it runs correctly under Protected Mode, or add the required website(s) to the list of trusted sites.

Windows 7 64-bit

Below are the set of rules which can be used to test a package for deployment on Windows 7 64-bit

T101 - Known Compatibility Issues at Startup (AppHelp)

Description: RayQC Advanced scans the package for the presence of applications that may

trigger Application Help Dialog (AppHelp) when the program is being installed or run for the first time.

Background: Certain applications are known to cause issues or not even starting on modern operating systems. Windows contains a predefined list of software known to have compatibility issues and warns or prevents user from starting the application. The list of such applications is stored in a central compatibility database, and the dialog shown to the user is known as Application Help (AppHelp).

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/bb756937.aspx

Manual Remediation: Contact the manufacturer to obtain compatible software.

T102 - Deprecated Windows Features

Description: RayQC Advanced scans the MSI package for the presence of deprecated features: embedded installations of another MSI packages (Custom Actions type 7, 23, 39), NETDDE-dependencies in registry, deprecated proxy configuration component `ProxyCfg.exe.`

Background: Certain features present in previous versions of Windows systems are officially deprecated by Microsoft. This means they are provided as-is. These features may be still working, but there is no guarantee they will function correctly or at all after any update or security patch. Usually, there is a replacement technology that should be used in favor of deprecated features.

More Information: http://msdn.microsoft.com/en-us/library/aa368010%28v=VS.85%29.aspx
http://msdn.microsoft.com/en-us/library/bb756977.aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/aa384069(v=vs.85).aspx

Manual Remediation: Do not use use Custom Actions type 7, 23 and 39 anymore. Dependencies and prerequisites have to be installed and managed by the deployment tool or external setup wrapper. The deprecated components have to be replaced. Contact the manufacturer to obtain compatible software.

T103 - Obsolete Windows Features

Description: RayQC Advanced scans the MSI package for a presence of deprecated MSGina technology, as well as for a presence of file extensions, for which the handling application has been obsoleted.

Background: Certain features present in previous versions of Windows systems are officially marked as obsolete by Microsoft. This means they are not supported anymore and any functionality relying on them is likely to fail to operate. Usually, there is a replacement technology that should be used in favor of deprecated features.

More Information: http://msdn.microsoft.com/en-us/library/bb756900.aspx
http://technet.microsoft.com/en-en/library/ee681703(v=ws.10).aspx

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software using the `MSGina.dll` should be re-enginered and use the Credential Providers model. Obsolete extensions should not be used in MSI installer packages.

T104 - Windows Shell and User Experience Changes

Description: RayQC Advanced scans the MSI package for a presence of shortcuts created in

Quick Launch and subfolders of the SendTo folder.

Background: Each version of Microsoft Windows system introduces enhancements and changes of the user experience in the way Windows Shell is working and organizing files, shortcuts, context menu actions etc. Certain aspects of the user experience vary between newer version of Windows. There is a different handling for certain behaviors that were possible before. For example, shortcuts placed in subfolders of the SendTo folder are not displayed anymore. Finally, Quick Launch Bar feature is not present anymore.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/cc144179(v=vs.85).aspx

http://msdn.microsoft.com/en-us/library/windows/desktop/jj584985(v=vs.85).aspx

Manual Remediation: Avoid deploying shortcuts to Quick Launch location and to subfolders of SendTo folder.

T105 - Unsupported Windows Components

Description: RayQC Advanced scans the MSI package for a presence of applications using DHTML control and for the presence of 32-bit `.hlp` files.

Background: Certain functionalities and components present in Windows XP and previous systems are not anymore part of the standard OS image. Since then Microsoft offers them as downloadable add-ons which restore the missing functionality. On a standard system however, missing handlers/opening applications may cause runtime exceptions or other warnings. Typical examples of such components are viewers for 32-bit .hlp files, missing DHTLM editor controls and so on.

More Information: http://support.microsoft.com/kb/917607 http://msdn.microsoft.com/en-us/library/aa663363.aspx

Manual Remediation: Contact the manufacturer to obtain compatible software. You may also install the missing components - the update KB917607 restores the ability to view 32-bit `.hlp` files, and the redistributable installer `DHTMLEd.msi` from Microsoft installs the missing DHTML control.

T106 - .NET Framework Compatibility

Description: RayQC Advanced scans the MSI package for a presence of applications using .NET Framework 1.0 or 1.1.

Background: Since Windows 7, .NET Framework 1.0 and 1.1 are not supported. Although it may be possible to deploy deprecated .NET components, there is no support for these configurations provided by Microsoft.

More Information: http://support.microsoft.com/kb/2489698

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should be converted to .NET Framework 4.5.

T107 - Conditional Installation and Execution

Description: RayQC Advanced scans the MSI package for a presence of conditions that vary based on the value of properties: VersionNT, VersionNT64, WindowsBuild and ServicePackLevel. Additionally, the content of the package is scanned for the usage of AdminUser and Privilleged properties in Launch Conditions and components condition to

verify they will not cause issues with permission elevation. Merge modules, 16-bit components and certain conditions may neutralize otherwise failing conditions.

Background: Number of MSI properties like VersionNT, VersionNT64, ServicePackLevel etc. can be used to conditionally control the flow of installation and set of features/components/policies to be installed. Software vendors use them frequently in critical places like LaunchConditions, conditions for components and Custom Actions, conditional security policies and many more. When a new version of Operating System is introduced, these conditions have to be reviewed, because they may generate false warnings even though the software is functioning correctly. Another source of issues are two distinctive MSI properties Privileged and AdminUser. Because of late elevation, since Windows Vista values of these properties are spoofed when evaluating LaunchConditions. This may produce unexpected results with packages designed for previous operating systems.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/aa370556(v=vs.85).aspx

http://msdn.microsoft.com/en-us/library/windows/desktop/aa369752(v=vs.85).aspx

Manual Remediation: Review all rows containing conditions that exclude the current operating system. Should the given component/action be required and function correctly on Windows 7, rewrite the condition so that it evaluates to true or remove it to always install the questionable resource. Do not use AdminUser property, because it may impact installation flows that elevate at some later point of installation. Legacy distinction between Provileged and AdminUser property can be restored by using the MSIREALADMINDETECTION property.

T108 - Deprecated and Obsolete API Calls

Description: RayQC Advanced scans the MSI package for a presence of API calls that are deprecated or obsolete. Internal database is used to assess each API call being used.

Background: Certain APIs present in previous versions of Microsoft Windows are now officially deprecated or obsoleted by Microsoft. Obsolete APIs may not work anymore, or their behavior may be different leading to unexpected results. The deprecated APIs may be still working, but there is no guarantee they will function correctly or at all after any update or security patch. Usually, there is a replacement API that should be used in favor of deprecated or obsolete API call.

More Information: None available.

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should not use obsolete functions anymore and switch to replacements as described by Microsoft in Microsoft SDK Updates.

T109 - Hard-Coded Resources and System Paths

Description: RayQC Advanced scans the MSI package for a usage of changed or obsolete junction points in INI files, registry entries, services, shortcuts, environment variables and custom actions.

Background: Since Microsoft Windows Vista, standard locations where user and system data are stored have been changed. For example, the root folder for user data was called "Documents and Settings" in Windows XP, but since Windows Vista its name is "Users". To provide a backward compatibility, junction points are used to reroute the calls from old, incorrect locations to the new, proper ones. A package that runs on various target systems

should not rely on hard-coded paths, because they may be not valid anymore or for a given system language.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/ bb968829(v=vs.85).aspx

http://msdn.microsoft.com/en-us/library/windows/desktop/ aa368977(v=vs.85).aspx

Manual Remediation: Hard-coded paths should not be used. Replace them with MSI properties using formatted syntax. If no predefined property exists, the path should be exposed via custom MSI property so that it can be adjusted on demand from command-line / MST transform.

T110 - Mismatched Target Architecture

Description: RayQC Advanced scans the MSI package for the presence of executables (16/32/64-bit) that are not compatible with Windows 10 32-bit platform.

Background: Some software is intended to run only in 32-bit or 64-bit operating systems. 16-bit executables are not supported on modern platforms, and 64-bit Microsoft Windows can correctly emulate 32-bit applications. If the MSI package is missing a correct Launch Condition it may try to install executables that are not designed for the current platform architecture. Attempting to launch such executable might result in an error message that the file is not a valid Win32 application. Additionally, attempting to run 16-bit code may result in a warning message informing that an extra Windows Feature is required.

More Information: http://support.microsoft.com/kb/282423/en-us

Manual Remediation: Contact the manufacturer to obtain compatible software. Reenginer self-developed software by replacing 16-bit executables with appropriate 32- or 64-bit code. Use Launch Conditions and component conditions to control to which platform software and its parts are deployed.

T111 - Driver Issues

Description: RayQC Advanced scans the MSI package for the presence of drivers containing no valid signature or not matching the target platform.

Background: Since Windows Vista 64-bit, all drivers have to be signed. Signed driver contains an extra digital signature used to validate the source and content of the driver package. Any unauthorized change in the driver package invalidates the signature. If an unsigned driver or a driver with invalid signature is attempted to be installed, Windows refuses the installation. Likewise, each driver has to match the target platform, which means that 64-bit systems require 64-bit drivers.

More Information: http://msdn.microsoft.com/en-us/library/bb756937.aspx

Manual Remediation: Contact the manufacturer to obtain compatible driver. Use WDK (Windows Driver Kit) to sign self-developed driver packages.

T112 - Installation Package Design Issues

Description: RayQC Advanced scans the MSI package for the presence of common installation design issues that may cause troubles during installation or using of software. The context of Custom Actions is scanned for the presence of deferred custom actions running in user-context, as well as system-wide actions running in immediate mode. The presence of conflicting permissions tables preventing the installation is detected as well. Additionally,

invalid combinations of user- and machine-data in a single component and invalid identifiers are reported.

Background: Microsoft recommends several best-practises approaches for MSI setup designers. They ensure that the package is deployed correctly in various scenarios and various operating systems. By following the guidelines many compatibility issues introduced by a new security model in Windows Vista can be avoided.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/aa368268%28v=vs.85%29.aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/aa368268(v=vs.85).aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/dd408053(v=vs.85).aspx
http://msdn.microsoft.com/en-us/library/6397xx85(v=vs.80).aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/aa368994%28v=vs.85%29.aspx

Manual Remediation: Adjust the package content so that it complies to the best practises of Windows Installer. Do not mix per-machine and per-user data in a single component. Use valid identifiers for components. Make sure all custom actions are running in a valid context - all actions making system changes must be deferred in execution. Do not use both `LockPermissions` and `MsiLockPermissionsEx` tables at once.

T113 - Conflicts with Protected Windows Resources (WRP)

Description: RayQC Advanced scans the MSI package for the presence of files and registry keys that belong to the Windows Resource Protection list.

Background: Windows Resource Protection (WRP) prevents the modification of essential system resources (files, folders and registry keys). Windows Installer silently ignores any attempt to update or modify them, any other software trying to do it may fail. These kinds of resources may be only updated by Microsoft-provided redistributable packages. During the installation, if Windows Installer logging is enabled, a warning may be shown for each operation that was ignored because of the WRP protection.

More Information: http://msdn.microsoft.com/en-us/library/bb756998.aspx

Manual Remediation: Assess whether the conflicting resources are actually needed, and if not remove them from the MSI package. If a given resource is needed and the original system one cannot be used, consider re-engineering the application or use any virtualization technique to override the resource.

T114 - Missing or Invalid Signatures

Description: RayQC Advanced scans the MSI package for the presence of unsigned executable files (.exe, .dll, .ocx). Additionally, the package itself and CAB files are also scanned.

Background: According to the set of best practices by Microsoft, all exercutable files deployed by an installation package and the installation package itself should be digitally signed with a certificate issued by a Trusted Publisher. When attempting to run an unsigned executable, Windows prompts the user for authorization. Similarly, attempting to install an unsigned MSI package also shows the Windows prompt.

More Information: http://technet.microsoft.com/en-us/library/cc962053.aspx

Manual Remediation: Contact the manufacturer to obtain signed executables and installers. Use WDK (Windows Driver Kit) to sign self-developed executables and packages.

T115 - Security and User Access Control Issues

Description: RayQC Advanced scans the MSI package for the presence of issues that may fail to work due to the security features. The executable files are scanned for the presence of correct manifestation. Direct calls to rundll32 are reported, because the UAC prompt hides the actual calling module when rundll32 is executed. Interactive sevices running in session 0 are detected, as well as MMC snap-ins that are not DEP-aware. Finally, setups, updaters and uninstallers are detecteded and checked for the presence of their UAC awareness.

Background: Session 0 isolation and Data Execution Prevention (DEP) are examples of security improvements introduced to prevent malcious software from compromising the security of the operating systems. They provide a separation between interactive user sessions and non-interactive session 0 devoted for services, and prevent execution of code from non-executable memory region. Modern software has to comply to these restrictions in order to function correctly on Windows 10. Another security issue present in Windows operating system is User Account Control (UAC). When an executable file requires additional non-standard permissions, the UAC elevation dialog prompts for confirmation or for correct credentials. The UAC prompt contains information about calling application, manufacturer and the source. Certain applications, like self-updaters, setups and other requiring higher privileges must be aware of the elevation, and use manifests to correctly inform the system about required execution permissions.

More Information: http://msdn.microsoft.com/en-us/windows/hardware/gg463353
http://msdn.microsoft.com/en-us/library/bb963893.aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/aa366553(v=vs.85).aspx
http://technet.microsoft.com/en-us/library/cc709628%28WS.10%29.aspx
http://technet.microsoft.com/en-us/library/cc709628%28WS.10%29.aspx

Manual Remediation: Contact the manufacturer to obtain software that complies to the security features of Microsoft Windows. For each unmanifested executable file, create a manifest, and set the required privileges to "`asInvoker`" for applications not requiring them, and "`requireAdministrator`" or "`highestAvailable`" for others. If the manifest cannot be corrected, a shim database has to be used to specify the desired privilege level.

T116 - Missing Application Manifest or Insufficient Execution Policy

Description: RayQC Advanced scans the MSI package for the presence of executabl files (`.exe`, `.cpl`) that do not contain the manifest, or that are not aware of Windows 10 in the list of supported operating systems in their manifest files.

Background: Since Windows Vista, all applications run by default with standard user privileges. This is also true when the current user is a member of Administrators group. Application that used to work on previous versions of Windows may fail to work, as no elevation will take place. In order to require higher permissions, each executable or control panel applications has to contain a manifest file - a simple `.XML` file informing the operating system how to handle the given program.

More Information: http://msdn.microsoft.com/en-us/library/Aa480152%23appcomp_topic30.com#appcomp_topic4
http://msdn.microsoft.com/en-us/library/hh848036%28v=vs.85%29.aspx

Manual Remediation: Create a manifest file for each executable. To manifest a control panel application (.cpl) create an executable wrapper with embedded manifest. Use the SupportedOS section in the manifest to define the list of supported operating systems.

T117 - Incomplete Reboot Handling

Description: RayQC Advanced scans the MSI package for the absence of a proper launch condition preventing the installation if a reboot is pending. Additionally, absence of "Files in use" dialog is detected. Presence of `ForceReboot` action is also detected and reported.

Background: Windows Installer supports natively various set of features and actions related to the reboot handling. They include for example the ability to show list of used/locked files, forcing or skipping the reboot and determining the installation state by the related MSI properties. Several aspects have to be considered so that the reboot handling works as expected.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/aa368607(v=vs.85).aspx

http://msdn.microsoft.com/en-us/library/windows/desktop/aa370492(v=vs.85).aspx

http://msdn.microsoft.com/en-us/library/windows/desktop/aa370379(v=vs.85).aspx

Manual Remediation: Add the `MSIRMFilesInUse` dialog to the dialog sequence if it is missing. Remove `ForceReboot` action from the sequence, reboots are handled automatically by MSI. In order to ensure the package is not installed when any reboot is pending, append the "`NOT MsiSystemRebootPending`" condition to the Launch Condition list.

T118 - Protected Mode (Internet Explorer)

Description: RayQC Advanced scans the MSI package for the presence of registry entries that disable Protected Mode.

Background: As a result of security changes introduced in Windows Vista, Internet Explorer runs now in a isolated mode called "Protected mode" by default. While it limits potential damages malware application can cause, it also prevents web-applications running in Internet Explorer from writing directly to disk while in Internet or Intranet zone. Internet Explorer warns when web-application tries to run certain software programs or write to protected areas.

More Information: http://msdn.microsoft.com/en-us/library/bb756991.aspx

Manual Remediation: Contact the manufacturer to obtain compatible software. Re-engineer self-developed software so that it runs correctly under Protected Mode, or add the required website(s) to the list of trusted sites.

Windows 8 32-bit

Below are the set of rules which can be used to test a package for deployment on Windows 8 32-bit

T001 - Known Compatibility Issues at Startup (AppHelp)

Description: RayQC Advanced scans the package for the presence of applications that may

trigger Application Help Dialog (AppHelp) when the program is being installed or run for the first time.

Background: Certain applications are known to cause issues or not even starting on modern operating systems. Windows contains a predefined list of software known to have compatibility issues and warns or prevents user from starting the application. The list of such applications is stored in a central compatibility database, and the dialog shown to the user is known as Application Help (AppHelp).

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/bb756937.aspx

Manual Remediation: Contact the manufacturer to obtain compatible software.

T002 - Deprecated Windows Features

Description: RayQC Advanced scans the MSI package for the presence of deprecated features: embedded installations of another MSI packages (Custom Actions type 7, 23, 39), NETDDE-dependencies in registry, deprecated proxy configuration component `ProxyCfg.exe` and Windows Library files.

Background: Certain features present in previous versions of Windows systems are officially deprecated by Microsoft. This means they are provided as-is. These features may be still working, but there is no guarantee they will function correctly or at all after any update or security patch. Usually, there is a replacement technology that should be used in favor of deprecated features.

More Information: http://msdn.microsoft.com/en-us/library/aa368010%28v=VS.85%29.aspx
http://msdn.microsoft.com/en-us/library/bb756977.aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/aa384069(v=vs.85).aspx

Manual Remediation: Do not use use Custom Actions type 7, 23 and 39 anymore. Dependencies and prerequisites have to be installed and managed by the deployment tool or external setup wrapper. The deprecated components have to be replaced. Contact the manufacturer to obtain compatible software.

T003 - Obsolete Windows Features

Description: RayQC Advanced scans the MSI package for a presence of deprecated MSGina technology, as well as for a presence of file extensions, for which the handling application has been obsoleted.

Background: Certain features present in previous versions of Windows systems are officially marked as obsolete by Microsoft. This means they are not supported anymore and any functionality relying on them is likely to fail to operate. Usually, there is a replacement technology that should be used in favor of deprecated features.

More Information: http://msdn.microsoft.com/en-us/library/bb756900.aspx
http://technet.microsoft.com/en-en/library/ee681703(v=ws.10).aspx

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software using the `MSGina.dll` should be re-engineered and use the Credential Providers model. Obsolete extensions should not be used in MSI installer packages.

T004 - Windows Shell and User Experience Changes

Description: RayQC Advanced scans the MSI package for a presence of shortcuts created in Quick Launch and subfolders of the SendTo folder. Additionally, start menu shortcuts pointing to non-executable files will be detected. Finally, RayQC Advanced scans the MSI package for a presence of Windows Gadgets.

Background: Each version of Microsoft Windows system introduces enhancements and changes of the user experience in the way Windows Shell is working and organizing files, shortcuts, context menu actions etc. Certain aspects of the user experience vary between newer version of Windows, with the introduction of Modern Start Screen being a notable example. There is a different handling for certain behaviors that were possible before. For example, the new Start Screen does not pin non-executable files by default, and due to the deprecated tree-like structure certain shortcuts names may be duplicated and thus confusing. Another example are shortcuts placed in subfolders of the SendTo folder, which are not displayed anymore. Finally, features like Quick Launch Bar and Windows Desktop Gadgets layer are not present anymore.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/cc144179(v=vs.85).aspx

http://msdn.microsoft.com/en-us/library/windows/desktop/jj584985(v=vs.85).aspx

Manual Remediation: Avoid deploying shortcuts to Quick Launch location and to subfolders of SendTo folder. Migrate to the Modern application to allow pinning ups and running them in a gadget-mode. Rename Start menu shortcuts to unequivocally express their purpose and associated action, instead of using generic names like "Readme" or "Help". Non-executable files should be manually pinned by the logged on user.

T005 - Unsupported Windows Components

Description: RayQC Advanced scans the MSI package for a presence of applications using DHTML control and for the presence of 32-bit `.hlp` files.

Background: Certain functionalities and components present in Windows XP and previous systems are not anymore part of the standard OS image. Since then Microsoft offers them as downloadable add-ons wich restore the missing functionality. On a standard system however, missing handlers/opening applications may cause runtime exceptions or other warnings. Typical examples of such components are viewers for 32-bit .hlp files, missing DHTLM editor controls and so on.

More Information: http://support.microsoft.com/kb/917607

http://msdn.microsoft.com/en-us/library/aa663363.aspx

Manual Remediation: Contact the manufacturer to obtain compatible software. You may also install the missing components - the update KB917607 restores the ability to view 32-bit `.hlp` files, and the redistributable installer `DHTMLEd.msi` from Microsoft installs the missing DHTML control.

T006 - .NET Framework Compatibility

Description: RayQC Advanced scans the MSI package for a presence of applications using .NET Framework 1.0, 1.1, 2.0, 3.0 or 3.5.

Background: Since Windows 7, .NET Framework 1.0 and 1.1 are not supported. Although it may be possible to deploy deprecated .NET components, there is no support for these configurations provided by Microsoft. Additionally .NET Framework 2.0, 3.0 and 3.5 is not

included in the default configuration of Windows 8 and later operating systems, so applications that require one of these frameworks might trigger a request for installing the necessary files.

More Information: http://support.microsoft.com/kb/2489698

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should be converted to .NET Framework 4.5.

T007 - Conditional Installation and Execution

Description: RayQC Advanced scans the MSI package for a presence of conditions that vary based on the value of properties: VersionNT, VersionNT64, WindowsBuild and ServicePackLevel. Additionally, the content of the package is scanned for the usage of `AdminUser` and `Privileged` properties in Launch Conditions and components condition to verify they will not cause issues with permission elevation. Merge modules, 16-bit components and certain conditions may neutralize otherwise failing conditions.

Background: Number of MSI properties like VersionNT, VersionNT64, ServicePackLevel etc. can be used to conditionally control the flow of installation and set of features/components/policies to be installed. Software vendors use them frequently in critical places like LaunchConditions, conditions for components and Custom Actions, conditional security policies and many more. When a new version of Operating System is introduced, these conditions have to be reviewed, because they may generate false warnings even though the software is functioning correctly. Another source of issues are two distinctive MSI properties `Privileged` and `AdminUser`. Because of late elevation, since Windows Vista values of these properties are spoofed when evaluating LaunchConditions. This may produce unexpected results with packages designed for previous operating systems.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/aa370556(v=vs.85).aspx

http://msdn.microsoft.com/en-us/library/windows/desktop/aa369752(v=vs.85).aspx

Manual Remediation: Review all rows containing conditions that exclude the current operating system. Should the given component/action be required and function correctly on Windows 8, rewrite the condition so that it evaluates to true or remove it to always install the questionable resource. Do not use `AdminUser` property, because it may impact installation flows that elevate at some later point of installation. Legacy distinction between `Privileged` and `AdminUser` property can be restored by using the `MSIREALADMINDETECTION` property.

T008 - Deprecated and Obsolete API Calls

Description: RayQC Advanced scans the MSI package for a presence of API calls that are deprecated or obsolete. Internal database is used to assess each API call being used.

Background: Certain APIs present in previous versions of Microsoft Windows are now officially deprecated or obsoleted by Microsoft. Obsolete APIs may not work anymore, or their behavior may be different leading to unexpected results. The deprecated APIs may be still working, but there is no guarantee they will function correctly or at all after any update or security patch. Usually, there is a replacement API that should be used in favor of deprecated or obsolete API call.

More Information: None available.

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should not use obsolete functions anymore and switch to replacements as

described by Microsoft in Microsoft SDK Updates.

T009 - Hard-Coded Resource and System Paths

Description: RayQC Advanced scans the MSI package for a usage of changed or obsolete junction points in INI files, registry entries, services, shortcuts, environment variables and custom actions.

Background: Since Microsoft Windows Vista, standard locations where user and system data are stored have been changed. For example, the root folder for user data was called "Documents and Settings" in Windows XP, but since Windows Vista its name is "Users". To provide a backward compatibility, junction points are used to reroute the calls from old, incorrect locations to the new, proper ones. A package that runs on various target systems should not rely on hardcoded paths, because they may be not valid anymore or for a given system language.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/bb968829(v=vs.85).aspx

http://msdn.microsoft.com/en-us/library/windows/desktop/aa368977(v=vs.85).aspx

Manual Remediation: Hard-coded paths should not be used. Replace them with MSI properties using formatted syntax. If no predefined property exists, the path should be exposed via custom MSI property so that it can be adjusted on demand from command-line / MST transform.

T010 - Mismatched Target Architecture

Description: RayQC Advanced scans the MSI package for the presence of executables (16/32/64-bit) that are not compatible with Windows 8 32-bit platform.

Background: Some software is intended to run only in 32-bit or 64-bit operating systems. 16-bit executables are not supported on modern platforms, and 64-bit Microsoft Windows can correctly emulate 32-bit applications. If the MSI package is missing a correct Launch Condition it may try to install executables that are not designed for the current platform architecture. Attempting to launch such executable might result in an error message that the file is not a valid Win32 application. Additionally, attempting to run 16-bit code may result in a warning message informing that an extra Windows Feature is required.

More Information: http://support.microsoft.com/kb/282423/en-us

Manual Remediation: Contact the manufacturer to obtain compatible software. Re-engineer self-developed software by replacing 16-bit executables with appropriate 32- or 64-bit code. Use Launch Conditions and component conditions to control to which platform software and its parts are deployed.

T011 - Driver Issues

Description: RayQC Advanced scans the MSI package for the presence of drivers containing no valid signature or not matching the target platform.

Background: Since Windows Vista 64-bit, all drivers have to be signed. Signed driver contains an extra digital signature used to validate the source and content of the driver package. Any unauthorized change in the driver package invalidates the signature. If an unsigned driver or a driver with invalid signature is attempted to be installed, Windows refuses the installation. Likewise, each driver has to match the target platform, which means that 64-bit systems

require 64-bit drivers.

More Information: http://msdn.microsoft.com/en-us/library/bb756937.aspx

Manual Remediation: Contact the manufacturer to obtain compatible driver. Use WDK (Windows Driver Kit) to sign self-developed driver packages.

T012 - Installation Package Design Issues

Description: RayQC Advanced scans the MSI package for the presence of common installation design issues that may cause troubles during installation or using of software. The context of Custom Actions is scanned for the presence of deferred custom actions running in user-context, as well as system-wide actions running in immediate mode. The presence of conflicting permissions tables preventing the installation is detected as well. Additionally, invalid combinations of user- and machine-data in a single component and invalid identifiers are reported.

Background: Microsoft recommends several best-practises approaches for MSI setup designers. They ensure that the package is deployed correctly in various scenarios and various operating systems. By following the guidelines many compatibility issues introduced by a new security model in Windows Vista can be avoided.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/aa368268%28v=vs.85%29.aspx

http://msdn.microsoft.com/en-us/library/windows/desktop/aa368268(v=vs.85).aspx

http://msdn.microsoft.com/en-us/library/windows/desktop/dd408053(v=vs.85).aspx

http://msdn.microsoft.com/en-us/library/6397xx85(v=vs.80).aspx

http://msdn.microsoft.com/en-us/library/windows/desktop/aa368994%28v=vs.85%29.aspx

Manual Remediation: Adjust the package content so that it complies to the best practises of Windows Installer. Do not mix per-machine and per-user data in a single component. Use valid identifiers for components. Make sure all custom actions are running in a valid context - all actions making system changes must be deferred in execution. Do not use both `LockPermissions` and `MsiLockPermissionsEx` tables at once.

T013 - Conflicts with Protected Windows Resources (WRP)

Description: RayQC Advanced scans the MSI package for the presence of files and registry keys that belong to the Windows Resource Protection list.

Background: Windows Resource Protection (WRP) prevents the modification of essential system resources (files, folders and registry keys). Windows Installer silently ignores any attempt to update or modify them, any other software trying to do it may fail. These kinds of resources may be only updated by Microsoft-provided redistributable packages. During the installation, if Windows Installer logging is enabled, a warning may be shown for each operation that was ignored because of the WRP protection.

More Information: http://msdn.microsoft.com/en-us/library/bb756998.aspx

Manual Remediation: Assess whether the conflicting resources are actually needed, and if not remove them from the MSI package. If a given resource is needed and the original system one cannot be used, consider re-engineering the application or use any virtualization technique to

override the resource.

T014 - Missing or Invalid Signatures

Description: RayQC Advanced scans the MSI package for the presence of unsigned executable files (`.exe`, `.dll`, `.ocx`). Additionally, the package itself and CAB files are also scanned.

Background: According to the set of best practices by Microsoft, all exercutable files deployed by an installation package and the installation package itself should be digitally signed with a certificate issued by a Trusted Publisher. When attempting to run an unsigned executable, Windows prompts the user for authorization. Similarly, attempting to install an unsigned MSI package also shows the Windows prompt.

More Information: http://technet.microsoft.com/en-us/library/cc962053.aspx

Manual Remediation: Contact the manufacturer to obtain signed executables and installers. Use WDK (Windows Driver Kit) to sign self-developed executables and packages.

T015 - Security and User Access Control Issues

Description: RayQC Advanced scans the MSI package for the presence of issues that may fail to work due to the security features. The executable files are scanned for the presence of correct manifestation. Direct calls to rundll32 are reported, because the UAC prompt hides the actual calling module when rundll32 is executed. Interactive sevices running in session 0 are detected, as well as MMC snap-ins that are not DEP-aware. Finally, setups, updaters and uninstallers are detecteded and checked for the presence of their UAC awareness.

Background: Session 0 isolation and Data Execution Prevention (DEP) are examples of security improvements introduced to prevent malcious software from compromising the security of the operating systems. They provide a separation between interactive user sessions and non-interactive session 0 devoted for services, and prevent execution of code from non-executable memory region. Modern software has to comply to these restrictions in order to function correctly on Windows 8. Another security issue present in Windows operating system is User Account Control (UAC). When an executable file requires additional non-standard permissions, the UAC elevation dialog prompts for confirmation or for correct credentials. The UAC prompt contains information about calling application, manufacturer and the source. Certain applications, like self-updaters, setups and other requiring higher privileges must be aware of the elevation, and use manifests to correctly inform the system about required execution permissions.

More Information: http://msdn.microsoft.com/en-us/windows/hardware/gg463353
http://msdn.microsoft.com/en-us/library/bb963893.aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/aa366553(v=vs.85).aspx
http://technet.microsoft.com/en-us/library/cc709628%28WS.10%29.aspx
http://technet.microsoft.com/en-us/library/cc709628%28WS.10%29.aspx

Manual Remediation: Contact the manufacturer to obtain software that complies to the security features of Microsoft Windows. For each unmanifested executable file, create a manifest, and set the required privileges to "`asInvoker`" for applications not requiring them, and "`requireAdministrator`" or "`highestAvailable`" for others. If the manifest cannot be corrected, a shim database has to be used to specify the desired privilege level.

T016 - Missing Application Manifest or Insufficient Execution Policy

Description: RayQC Advanced scans the MSI package for the presence of executabl files (`.exe`, `.cpl`) that do not contain the manifest, or that are not aware of Windows 8 in the list of supported operating systems in their manifest files.

Background: Since Windows Vista, all applications run by default with standard user privileges. This is also true when the current user is a member of Administrators group. Application that used to work on previous versions of Windows may fail to work, as no elevation will take place. In order to require higher permissions, each executable or control panel applications has to contain a manifest file - a simple `.XML` file informing the operating system how to handle the given program.

More Information: http://msdn.microsoft.com/en-us/library/Aa480152%
23appcomp_topic30.com#appcomp_topic4
http://msdn.microsoft.com/en-us/library/hh848036%28v=vs.85%29.aspx

Manual Remediation: Create a manifest file for each executable. To manifest a control panel application (.cpl) create an executable wrapper with embedded manifest. Use the SupportedOS section in the manifest to define the list of supported operating systems.

T017 - Incomplete Reboot Handling

Description: RayQC Advanced scans the MSI package for the absence of a proper launch condition preventing the installation if a reboot is pending. Additionally, absence of "Files in use" dialog is detected. Presence of ForceReboot action is also detected and reported.

Background: Windows Installer supports natively various set of features and actions related to the reboot handling. They include for example the ability to show list of used/locked files, forcing or skipping the reboot and determining the installation state by the related MSI properties. Several aspects have to be considered so that the reboot handling works as expected.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/
aa368607(v=vs.85).aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/
aa370492(v=vs.85).aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/
aa370379(v=vs.85).aspx

Manual Remediation: Add the `MSIRMFilesInUse` dialog to the dialog sequence if it is missing. Remove ForceReboot action from the sequence, reboots are handled automatically by MSI. In order to ensure the package is not installed when any reboot is pending, append the `"NOT MsiSystemRebootPending"` condition to the Launch Condition list.

T018 - Protected Mode (Internet Explorer)

Description: RayQC Advanced scans the MSI package for the presence of registry entries that disable Protected Mode.

Background: As a result of security changes introduced in Windows Vista, Internet Explorer runs now in a isolated mode called "Protected mode" by default. While it limits potential damages malware application can cause, it also prevents web-applications running in Internet Explorer from writing directly to disk while in Internet or Intranet zone. Internet Explorer warns when web-application tries to run certain software programs or write to protected areas.

More Information: http://msdn.microsoft.com/en-us/library/bb756991.aspx

> **Manual Remediation:** Contact the manufacturer to obtain compatible software. Reengineer self-developed software so that it runs correctly under Protected Mode, or add the required website(s) to the list of trusted sites.

Windows 8 64-bit

Below are the set of rules which can be used to test a package for deployment on Windows 8 64-bit

T101 - Known Compatibility Issues at Startup (AppHelp)

Description: RayQC Advanced scans the package for the presence of applications that may trigger Application Help Dialog (AppHelp) when the program is being installed or run for the first time.

Background: Certain applications are known to cause issues or not even starting on modern operating systems. Windows contains a predefined list of software known to have compatibility issues and warns or prevents user from starting the application. The list of such applications is stored in a central compatibility database, and the dialog shown to the user is known as Application Help (AppHelp).

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/bb756937.aspx

Manual Remediation: Contact the manufacturer to obtain compatible software

T102 - Deprecated Windows Features

Description: RayQC Advanced scans the MSI package for the presence of deprecated features: embedded installations of another MSI packages (Custom Actions type 7, 23, 39), NETDDE-dependencies in registry, deprecated proxy configuration component `ProxyCfg.exe` and Windows Library files.

Background: Certain features present in previous versions of Windows systems are officially deprecated by Microsoft. This means they are provided as-is. These features may be still working, but there is no guarantee they will function correctly or at all after any update or security patch. Usually, there is a replacement technology that should be used in favor of deprecated features.

More Information: http://msdn.microsoft.com/en-us/library/aa368010%28v=VS.85%29.aspx
http://msdn.microsoft.com/en-us/library/bb756977.aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/aa384069(v=vs.85).aspx

Manual Remediation: Do not use use Custom Actions type 7, 23 and 39 anymore. Dependencies and prerequisites have to be installed and managed by the deployment tool or external setup wrapper. The deprecated components have to be replaced. Contact the manufacturer to obtain compatible software.

T103 - Obsolete Windows Features

Description: RayQC Advanced scans the MSI package for a presence of deprecated MSGina technology, as well as for a presence of file extensions, for which the handling application has

been obsoleted.

Background: Certain features present in previous versions of Windows systems are officially marked as obsolete by Microsoft. This means they are not supported anymore and any functionality relying on them is likely to fail to operate. Usually, there is a replacement technology that should be used in favor of deprecated features.

More Information: http://msdn.microsoft.com/en-us/library/bb756900.aspx
http://technet.microsoft.com/en-en/library/ee681703(v=ws.10).aspx

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software using the `MSGina.dll` should be re-enginered and use the Credential Providers model. Obsolete extensions should not be used in MSI installer packages.

T104 - Windows Shell and User Experience Changes

Description: RayQC Advanced scans the MSI package for a presence of shortcuts created in Quick Launch and subfolders of the SendTo folder. Additionally, start menu shortcuts pointing to non-executable files will be detected. Finally, RayQC Advanced scans the MSI package for a presence of Windows Gadgets.

Background: Each version of Microsoft Windows system introduces enhancements and changes of the user experience in the way Windows Shell is working and organizing files, shortcuts, context menu actions etc. Certain aspects of the user experience vary between newer version of Windows, with the introduction of Modern Start Screen being a notable example. There is a different handling for certain behaviors that were possible before. For example, the new Start Screen does not pin non-executable files by default, and due to the deprecated tree-like structure certain shortcuts names may be duplicated and thus confusing. Another example are shortcuts placed in subfolders of the SendTo folder, which are not displayed anymore. Finally, features like Quick Launch Bar and Windows Deskop Gadgets layer are not present anymore.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/
cc144179(v=vs.85).aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/
jj584985(v=vs.85).aspx

Manual Remediation: Avoid deploying shortcuts to Quick Launch location and to subfolders of SendTo folder. Migrate to the Modern application to allow pinning ups and running them in a gadget-mode. Rename Start menu shortcuts to unequivocally express their purpose and associated action, instead of using generic names like "Readme" or "Help". Non-executable files should be manually pinned by the logged on user.

T105 - Unsupported Windows Components

Description: RayQC Advanced scans the MSI package for a presence of applications using DHTML control and for the presence of 32-bit `.hlp` files.

Background: Certain functionalities and components present in Windows XP and previous systems are not anymore part of the standard OS image. Since then Microsoft offers them as downloadable add-ons wich restore the missing functionality. On a standard system however, missing handlers/opening applications may cause runtime exceptions or other warnings. Typical examples of such components are viewers for 32-bit `.hlp` files, missing DHTLM editor controls and so on.

More Information: http://support.microsoft.com/kb/917607

http://msdn.microsoft.com/en-us/library/aa663363.aspx

Manual Remediation: Contact the manufacturer to obtain compatible software. You may also install the missing components - the update KB917607 restores the ability to view 32-bit `.hlp` files, and the redistributable installer `DHTMLEd.msi` from Microsoft installs the missing DHTML control.

T106 - .NET Framework Compatibility

Description: RayQC Advanced scans the MSI package for a presence of applications using .NET Framework 1.0, 1.1, 2.0, 3.0 or 3.5.

Background: Since Windows 7, .NET Framework 1.0 and 1.1 are not supported. Although it may be possible to deploy deprecated .NET components, there is no support for these configurations provided by Microsoft. Additionally .NET Framework 2.0, 3.0 and 3.5 is not included in the default configuration of Windows 8 and later operating systems, so applications that require one of these frameworks might trigger a request for installing the necessary files.

More Information: http://support.microsoft.com/kb/2489698

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should be converted to .NET Framework 4.5.

T107 - Conditional Installation and Execution

Description: RayQC Advanced scans the MSI package for a presence of conditions that vary based on the value of properties: VersionNT, VersionNT64, WindowsBuild and ServicePackLevel. Additionally, the content of the package is scanned for the usage of `AdminUser` and `Privileged` properties in Launch Conditions and components condition to verify they will not cause issues with permission elevation. Merge modules, 16-bit components and certain conditions may neutralize otherwise failing conditions.

Background: Number of MSI properties like VersionNT, VersionNT64, ServicePackLevel etc. can be used to conditionally control the flow of installation and set of features/components/policies to be installed. Software vendors use them frequently in critical places like LaunchConditions, conditions for components and Custom Actions, conditional security policies and many more. When a new version of Operating System is introduced, these conditions have to be reviewed, because they may generate false warnings even though the software is functioning correctly. Another source of issues are two distinctive MSI properties `Privileged` and `AdminUser`. Because of late elevation, since Windows Vista values of these properties are spoofed when evaluating LaunchConditions. This may produce unexpected results with packages designed for previous operating systems.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/aa370556(v=vs.85).aspx

http://msdn.microsoft.com/en-us/library/windows/desktop/aa369752(v=vs.85).aspx

Manual Remediation: Review all rows containing conditions that exclude the current operating system. Should the given component/action be required and function correctly on Windows 8, rewrite the condition so that it evaluates to true or remove it to always install the questionable resource. Do not use `AdminUser` property, because it may impact installation flows that elevate at some later point of installation. Legacy distinction between `Privileged` and `AdminUser` property can be restored by using the `MSIREALADMINDETECTION` property.

T108 - Deprecated and Obsolete API Calls

Description: RayQC Advanced scans the MSI package for a presence of API calls that are deprecated or obsolete. Internal database is used to assess each API call being used.

Background: Certain APIs present in previous versions of Microsoft Windows are now officially deprecated or obsoleted by Microsoft. Obsolete APIs may not work anymore, or their behavior may be different leading to unexpected results. The deprecated APIs may be still working, but there is no guarantee they will function correctly or at all after any update or security patch. Usually, there is a replacement API that should be used in favor of deprecated or obsolete API call.

More Information: None available.

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should not use obsolete functions anymore and switch to replacements as described by Microsoft in Microsoft SDK Updates.

T109 - Hard-Coded Resources and System Paths

Description: RayQC Advanced scans the MSI package for a usage of changed or obsolete junction points in INI files, registry entries, services, shortcuts, environment variables and custom actions.

Background: Since Microsoft Windows Vista, standard locations where user and system data are stored have been changed. For example, the root folder for user data was called "Documents and Settings" in Windows XP, but since Windows Vista its name is "Users". To provide a backward compatibility, junction points are used to reroute the calls from old, incorrect locations to the new, proper ones. A package that runs on various target systems should not rely on hardcoded paths, because they may be not valid anymore or for a given system language.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/bb968829(v=vs.85).aspx

http://msdn.microsoft.com/en-us/library/windows/desktop/aa368977(v=vs.85).aspx

Manual Remediation: Hard-coded paths should not be used. Replace them with MSI properties using formatted syntax. If no predefined property exists, the path should be exposed via custom MSI property so that it can be adjusted on demand from command-line / MST transform.

T110 - Mismatched Target Architecture

Description: RayQC Advanced scans the MSI package for the presence of executables (16/32/64-bit) that are not compatible with Windows 8 62-bit platform.

Background: Some software is intended to run only in 32-bit or 64-bit operating systems. 16-bit executables are not supported on modern platforms, and 64-bit Microsoft Windows can correctly emulate 32-bit applications. If the MSI package is missing a correct Launch Condition it may try to install executables that are not designed for the current platform architecture. Attempting to launch such executable might result in an error message that the file is not a valid Win32 application. Additionally, attempting to run 16-bit code may result in a warning message informing that an extra Windows Feature is required.

More Information: http://support.microsoft.com/kb/282423/en-us

Manual Remediation: Contact the manufacturer to obtain compatible software. Reenginer self-developed software by replacing 16-bit executables with appropriate 32- or 64-bit code. Use Launch Conditions and component conditions to control to which platform software and its parts are deployed.

T111 - Driver Issues

Description: RayQC Advanced scans the MSI package for the presence of drivers containing no valid signature or not matching the target platform.

Background: Since Windows Vista 64-bit, all drivers have to be signed. Signed driver contains an extra digital signature used to validate the source and content of the driver package. Any unauthorized change in the driver package invalidates the signature. If an unsigned driver or a driver with invalid signature is attempted to be installed, Windows refuses the installation. Likewise, each driver has to match the target platform, which means that 64-bit systems require 64-bit drivers.

More Information: http://msdn.microsoft.com/en-us/library/bb756937.aspx

Manual Remediation: Contact the manufacturer to obtain compatible driver. Use WDK (Windows Driver Kit) to sign self-developed driver packages.

T112 - Installation Package Design Issues

Description: RayQC Advanced scans the MSI package for the presence of common installation design issues that may cause troubles during installation or using of software. The context of Custom Actions is scanned for the presence of deferred custom actions running in user-context, as well as system-wide actions running in immediate mode. The presence of conflicting permissions tables preventing the installation is detected as well. Additionally, invalid combinations of user- and machine-data in a single component and invalid identifiers are reported.

Background: Microsoft recommends several best-practices approaches for MSI setup designers. They ensure that the package is deployed correctly in various scenarios and various operating systems. By following the guidelines many compatibility issues introduced by a new security model in Windows Vista can be avoided.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/aa368268%28v=vs.85%29.aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/aa368268(v=vs.85).aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/dd408053(v=vs.85).aspx
http://msdn.microsoft.com/en-us/library/6397xx85(v=vs.80).aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/aa368994%28v=vs.85%29.aspx

Manual Remediation: Adjust the package content so that it complies to the best practises of Windows Installer. Do not mix per-machine and per-user data in a single component. Use valid identifiers for components. Make sure all custom actions are running in a valid context - all actions making system changes must be deferred in execution. Do not use both `LockPermissions` and `MsiLockPermissionsEx` tables at once

T113 - Conflicts with Protected Windows Resources (WRP)

Description: RayQC Advanced scans the MSI package for the presence of unsigned executable files (`.exe`, `.dll`, `.ocx`). Additionally, the package itself and CAB files are also scanned.

Background: Windows Resource Protection (WRP) prevents the modification of essential system resources (files, folders and registry keys). Windows Installer silently ignores any attempt to update or modify them, any other software trying to do it may fail. These kinds of resources may be only updated by Microsoft-provided redistributable packages. During the installation, if Windows Installer logging is enabled, a warning may be shown for each operation that was ignored because of the WRP protection.

More Information: http://msdn.microsoft.com/en-us/library/bb756998.aspx

Manual Remediation: Assess whether the conflicting resources are actually needed, and if not remove them from the MSI package. If a given resource is needed and the original system one cannot be used, consider re-engineering the application or use any virtualization technique to override the resource.

T114 - Missing or Invalid Signatures

Description: RayQC Advanced scans the MSI package for the presence of unsigned executable files (.exe, .dll, .ocx). Additionally, the package itself and CAB files are also scanned.

Background: According to the set of best practices by Microsoft, all exerrcutable files deployed by an installation package and the installation package itself should be digitally signed with a certificate issued by a Trusted Publisher. When attempting to run an unsigned executable, Windows prompts the user for authorization. Similarly, attempting to install an unsigned MSI package also shows the Windows prompt.

More Information: http://technet.microsoft.com/en-us/library/cc962053.aspx

Manual Remediation: Contact the manufacturer to obtain signed executables and installers. Use WDK (Windows Driver Kit) to sign self-developed executables and packages.

T115 - Security and User Access Control Issues

Description: RayQC Advanced scans the MSI package for the presence of issues that may fail to work due to the security features. The executable files are scanned for the presence of correct manifestation. Direct calls to rundll32 are reported, because the UAC prompt hides the actual calling module when rundll32 is executed. Interactive sevices running in session 0 are detected, as well as MMC snap-ins that are not DEP-aware. Finally, setups, updaters and uninstallers are detecteded and checked for the presence of their UAC awareness.

Background: Session 0 isolation and Data Execution Prevention (DEP) are examples of security improvements introduced to prevent malcious software from compromising the security of the operating systems. They provide a separation between interactive user sessions and non-interactive session 0 devoted for services, and prevent execution of code from non-executable memory region. Modern software has to comply to these restrictions in order to function correctly on Windows 8. Another security issue present in Windows operating system is User Account Control (UAC). When an executable file requires additional non-standard permissions, the UAC elevation dialog prompts for confirmation or for correct credentials. The UAC prompt contains information about calling application, manufacturer and the source. Certain applications, like self-updaters, setups and other requiring higher privileges must be aware of the elevation, and use manifests to correctly inform the system about required execution permissions.

More Information: http://msdn.microsoft.com/en-us/windows/hardware/gg463353

http://msdn.microsoft.com/en-us/library/bb963893.aspx

http://msdn.microsoft.com/en-us/library/windows/desktop/
aa366553(v=vs.85).aspx

http://technet.microsoft.com/en-us/library/cc709628%28WS.10%29.aspx

http://technet.microsoft.com/en-us/library/cc709628%28WS.10%29.aspx

Manual Remediation: Contact the manufacturer to obtain software that complies to the security features of Microsoft Windows. For each unmanifested executable file, create a manifest, and set the required privileges to "`asInvoker`" for applications not requiring them, and "`requireAdministrator`" or "`highestAvailable`" for others. If the manifest cannot be corrected, a shim database has to be used to specify the desired privilege level.

T116 - Missing Application Manifest or Insufficient Execution Policy

Description: RayQC Advanced scans the MSI package for the absence of a proper launch condition preventing the installation if a reboot is pending. Additionally, absence of "Files in use" dialog is detected. Presence of `ForceReboot` action is also detected and reported.

Background: Since Windows Vista, all applications run by default with standard user privileges. This is also true when the current user is a member of Administrators group. Application that used to work on previous versions of Windows may fail to work, as no elevation will take place. In order to require higher permissions, each executable or control panel applications has to contain a manifest file - a simple `.XML` file informing the operating system how to handle the given program.

More Information: http://msdn.microsoft.com/en-us/library/Aa480152%
23appcomp_topic30.com#appcomp_topic4

http://msdn.microsoft.com/en-us/library/hh848036%28v=vs.85%29.aspx

Manual Remediation: Create a manifest file for each executable. To manifest a control panel application (`.cpl`) create an executable wrapper with embedded manifest. Use the SupportedOS section in the manifest to define the list of supported operating systems.

T117 - Incomplete Reboot Handling

Description: RayQC Advanced scans the MSI package for the absence of a proper launch condition preventing the installation if a reboot is pending. Additionally, absence of "Files in use" dialog is detected. Presence of `ForceReboot` action is also detected and reported.

Background: Windows Installer supports natively various set of features and actions related to the reboot handling. They include for example the ability to show list of used/locked files, forcing or skipping the reboot and determining the installation state by the related MSI properties. Several aspects have to be considered so that the reboot handling works as expected.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/
aa368607(v=vs.85).aspx

http://msdn.microsoft.com/en-us/library/windows/desktop/
aa370492(v=vs.85).aspx

http://msdn.microsoft.com/en-us/library/windows/desktop/
aa370379(v=vs.85).aspx

Manual Remediation: Add the `MSIRMFilesInUse` dialog to the dialog sequence if it is missing. Remove ForceReboot action from the sequence, reboots are handled automatically by MSI. In order to ensure the package is not installed when any reboot is pending, append the

"NOT `MsiSystemRebootPending`" condition to the Launch Condition list.

T118 - Protected Mode (Internet Explorer)

Description: RayQC Advanced scans the MSI package for the presence of registry entries that disable Protected Mode.

Background: As a result of security changes introduced in Windows Vista, Internet Explorer runs now in a isolated mode called "Protected mode" by default. While it limits potential damages malware application can cause, it also prevents web-applications running in Internet Explorer from writing directly to disk while in Internet or Intranet zone. Internet Explorer warns when web-application tries to run certain software programs or write to protected areas.

More Information: http://msdn.microsoft.com/en-us/library/bb756991.aspx

Manual Remediation: Contact the manufacturer to obtain compatible software. Reengineer self-developed software so that it runs correctly under Protected Mode, or add the required website(s) to the list of trusted sites.

Windows 8.1 32-bit

Below are the set of rules which can be used to test a package for deployment on Windows 8.1 32-bit

T001 - Known Compatibility Issues at Startup (AppHelp)

Description: RayQC Advanced scans the package for the presence of applications that may trigger Application Help Dialog (AppHelp) when the program is being installed or run for the first time.

Background: Certain applications are known to cause issues or not even starting on modern operating systems. Windows contains a predefined list of software known to have compatibility issues and warns or prevents user from starting the application. The list of such applications is stored in a central compatibility database, and the dialog shown to the user is known as Application Help (AppHelp).

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/bb756937.aspx

Manual Remediation: Contact the manufacturer to obtain compatible software.

T002 - Deprecated Windows Features

Description: RayQC Advanced scans the MSI package for the presence of deprecated features: embedded installations of another MSI packages (Custom Actions type 7, 23, 39), NETDDE-dependencies in registry, deprecated proxy configuration component `ProxyCfg.exe` and Windows Library files.

Background: Certain features present in previous versions of Windows systems are officially deprecated by Microsoft. This means they are provided as-is. These features may be still working, but there is no guarantee they will function correctly or at all after any update or security patch. Usually, there is a replacement technology that should be used in favor of deprecated features.

More Information: http://msdn.microsoft.com/en-us/library/aa368010%28v=VS.85%29.aspx
http://msdn.microsoft.com/en-us/library/bb756977.aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/
aa384069(v=vs.85).aspx

Manual Remediation: Do not use use Custom Actions type 7, 23 and 39 anymore. Dependencies and prerequisites have to be installed and managed by the deployment tool or external setup wrapper. The deprecated components have to be replaced. Contact the manufacturer to obtain compatible software.

T003 - Obsolete Windows Features

Description: RayQC Advanced scans the MSI package for a presence of deprecated MSGina technology, as well as for a presence of file extensions, for which the handling application has been obsoleted.

Background: Certain features present in previous versions of Windows systems are officially marked as obsolete by Microsoft. This means they are not supported anymore and any functionality relying on them is likely to fail to operate. Usually, there is a replacement technology that should be used in favor of deprecated features.

More Information: http://msdn.microsoft.com/en-us/library/bb756900.aspx
http://technet.microsoft.com/en-en/library/ee681703(v=ws.10).aspx

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software using the `MSGina.dll` should be re-engineered and use the Credential Providers model. Obsolete extensions should not be used in MSI installer packages.

T004 - Windows Shell and User Experience Changes

Description: RayQC Advanced scans the MSI package for a presence of shortcuts created in Quick Launch and subfolders of the SendTo folder. Additionally, start menu shortcuts pointing to non-executable files will be detected. Finally, RayQC Advanced scans the MSI package for a presence of Windows Gadgets.

Background: Each version of Microsoft Windows system introduces enhancements and changes of the user experience in the way Windows Shell is working and organizing files, shortcuts, context menu actions etc. Certain aspects of the user experience vary between newer version of Windows, with the introduction of Modern Start Screen being a notable example. There is a different handling for certain behaviors that were possible before. For example, the new Start Screen does not pin non-executable files by default, and due to the deprecated tree-like structure certain shortcuts names may be duplicated and thus confusing. Another example are shortcuts placed in subfolders of the SendTo folder, which are not displayed anymore. Finally, features like Quick Launch Bar and Windows Deskop Gadgets layer are not present anymore.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/
cc144179(v=vs.85).aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/
jj584985(v=vs.85).aspx

Manual Remediation: Avoid deploying shortcuts to Quick Launch location and to subfolders of SendTo folder. Migrate to the Modern application to allow pinning ups and running them in a gadget-mode. Rename Start menu shortcuts to unequivocally express their purpose and associated action, instead of using generic names like "Readme" or "Help". Non-executable

files should be manually pinned by the logged on user.

T005 - Unsupported Windows Components

Description: RayQC Advanced scans the MSI package for a presence of applications using DHTML control and for the presence of 32-bit `.hlp` files.

Background: Certain functionalities and components present in Windows XP and previous systems are not anymore part of the standard OS image. Since then Microsoft offers them as downloadable add-ons wich restore the missing functionality. On a standard system however, missing handlers/opening applications may cause runtime exceptions or other warnings. Typical examples of such components are viewers for 32-bit `.hlp` files, missing DHTLM editor controls and so on.

More Information: http://support.microsoft.com/kb/917607
http://msdn.microsoft.com/en-us/library/aa663363.aspx

Manual Remediation: Contact the manufacturer to obtain compatible software. You may also install the missing components - the update KB917607 restores the ability to view 32-bit `.hlp` files, and the redistributable installer `DHTMLEd.msi` from Microsoft installs the missing DHTML control.

T006 - .NET Framework Compatibility

Description: RayQC Advanced scans the MSI package for a presence of applications using .NET Framework 1.0, 1.1, 2.0, 3.0 or 3.5.

Background: Since Windows 7, .NET Framework 1.0 and 1.1 are not supported. Although it may be possible to deploy deprecated .NET components, there is no support for these configurations provided by Microsoft. Additionally .NET Framework 2.0, 3.0 and 3.5 is not included in the default configuration of Windows 8 and later operating systems, so applications that require one of these frameworks might trigger a request for installing the necessary files.

More Information: http://support.microsoft.com/kb/2489698

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should be converted to .NET Framework 4.5.

T007 - Conditional Installation and Execution

Description: RayQC Advanced scans the MSI package for a presence of conditions that vary based on the value of properties: `VersionNT`, `VersionNT64`, `WindowsBuild` and `ServicePackLevel`. Additionally, the content of the package is scanned for the usage of `AdminUser` and `Privileged` properties in Launch Conditions and components condition to verify they will not cause issues with permission elevation. Merge modules, 16-bit components and certain conditions may neutralize otherwise failing conditions.

Background: Number of MSI properties like `VersionNT`, `VersionNT64`, `ServicePackLevel` etc. can be used to conditionally control the flow of installation and set of features/components/policies to be installed. Software vendors use them frequently in critical places like LaunchConditions, conditions for components and Custom Actions, conditional security policies and many more. When a new version of Operating System is introduced, these conditions have to be reviewed, because they may generate false warnings even though the software is functioning correctly. Another source of issues are two distinctive MSI properties `Privileged` and `AdminUser`. Because of late elevation, since Windows Vista values of these properties are spoofed when evaluating LaunchConditions. This may produce unexpected

results with packages designed for previous operating systems.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/
aa370556(v=vs.85).aspx

> http://msdn.microsoft.com/en-us/library/windows/desktop/
> aa369752(v=vs.85).aspx

Manual Remediation: Review all rows containing conditions that exclude the current operating system. Should the given component/action be required and function correctly on Windows 8.1, rewrite the condition so that it evaluates to true or remove it to always install the questionable resource. Do not use `AdminUser` property, because it may impact installation flows that elevate at some later point of installation. Legacy distinction between `Privileged` and `AdminUser` property can be restored by using the `MSIREALADMINDETECTION` property.

T008 - Deprecated and Obsolete API Calls

Description: RayQC Advanced scans the MSI package for a presence of API calls that are deprecated or obsolete. Internal database is used to assess each API call being used.

Background: Certain APIs present in previous versions of Microsoft Windows are now officially deprecated or obsoleted by Microsoft. Obsolete APIs may not work anymore, or their behavior may be different leading to unexpected results. The deprecated APIs may be still working, but there is no guarantee they will function correctly or at all after any update or security patch. Usually, there is a replacement API that should be used in favor of deprecated or obsolete API call.

More Information: None available.

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should not use obsolete functions anymore and switch to replacements as described by Microsoft in Microsoft SDK Updates.

T009 - Hard-Coded Resources and System Paths

Description: RayQC Advanced scans the MSI package for a usage of changed or obsolete junction points in INI files, registry entries, services, shortcuts, environment variables and custom actions.

Background: Since Microsoft Windows Vista, standard locations where user and system data are stored have been changed. For example, the root folder for user data was called "Documents and Settings" in Windows XP, but since Windows Vista its name is "Users". To provide a backward compatibility, junction points are used to reroute the calls from old, incorrect locations to the new, proper ones. A package that runs on various target systems should not rely on hard-coded paths, because they may be not valid anymore or for a given system language.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/
bb968829(v=vs.85).aspx

> http://msdn.microsoft.com/en-us/library/windows/desktop/
> aa368977(v=vs.85).aspx

Manual Remediation: Hard-coded paths should not be used. Replace them with MSI properties using formatted syntax. If no predefined property exists, the path should be exposed via custom MSI property so that it can be adjusted on demand from command-line / MST transform.

T010 - Mismatched Target Architecture

Description: RayQC Advanced scans the MSI package for the presence of executables (16/32/64-bit) that are not compatible with Windows 8.1 32-bit platform.

Background: Some software is intended to run only in 32-bit or 64-bit operating systems. 16-bit executables are not supported on modern platforms, and 64-bit Microsoft Windows can correctly emulate 32-bit applications. If the MSI package is missing a correct Launch Condition it may try to install executables that are not designed for the current platform architecture. Attempting to launch such executable might result in an error message that the file is not a valid Win32 application. Additionally, attempting to run 16-bit code may result in a warning message informing that an extra Windows Feature is required.

More Information: http://support.microsoft.com/kb/282423/en-us

Manual Remediation: Contact the manufacturer to obtain compatible software. Re-engineer self-developed software by replacing 16-bit executables with appropriate 32- or 64-bit code. Use Launch Conditions and component conditions to control to which platform software and its parts are deployed.

T011 - Driver Issues

Description: RayQC Advanced scans the MSI package for the presence of drivers containing no valid signature or not matching the target platform.

Background: Since Windows Vista 64-bit, all drivers have to be signed. Signed driver contains an extra digital signature used to validate the source and content of the driver package. Any unauthorized change in the driver package invalidates the signature. If an unsigned driver or a driver with invalid signature is attempted to be installed, Windows refuses the installation. Likewise, each driver has to match the target platform, which means that 64-bit systems require 64-bit drivers.

More Information: http://msdn.microsoft.com/en-us/library/bb756937.aspx

Manual Remediation: Contact the manufacturer to obtain compatible driver. Use WDK (Windows Driver Kit) to sign self-developed driver packages.

T012 - Installation Package Design Issues

Description: RayQC Advanced scans the MSI package for the presence of common installation design issues that may cause troubles during installation or using of software. The context of Custom Actions is scanned for the presence of deferred custom actions running in user-context, as well as system-wide actions running in immediate mode. The presence of conflicting permissions tables preventing the installation is detected as well. Additionally, invalid combinations of user- and machine-data in a single component and invalid identifiers are reported.

Background: Microsoft recommends several best-practices approaches for MSI setup designers. They ensure that the package is deployed correctly in various scenarios and various operating systems. By following the guidelines many compatibility issues introduced by a new security model in Windows Vista can be avoided.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/aa368268%28v=vs.85%29.aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/aa368268(v=vs.85).aspx

http://msdn.microsoft.com/en-us/library/windows/desktop/
dd408053(v=vs.85).aspx

http://msdn.microsoft.com/en-us/library/6397xx85(v=vs.80).aspx

http://msdn.microsoft.com/en-us/library/windows/desktop/aa368994%
28v=vs.85%29.aspx

Manual Remediation: Adjust the package content so that it complies to the best practices of Windows Installer. Do not mix per-machine and per-user data in a single component. Use valid identifiers for components. Make sure all custom actions are running in a valid context - all actions making system changes must be deferred in execution. Do not use both `LockPermissions` and `MsiLockPermissionsEx` tables at once.

T013 - Conflicts with Protected Windows Resources (WRP)

Description: RayQC Advanced scans the MSI package for the presence of files and registry keys that belong to the Windows Resource Protection list.

Background: Windows Resource Protection (WRP) prevents the modification of essential system resources (files, folders and registry keys). Windows Installer silently ignores any attempt to update or modify them, any other software trying to do it may fail. These kinds of resources may be only updated by Microsoft-provided redistributable packages. During the installation, if Windows Installer logging is enabled, a warning may be shown for each operation that was ignored because of the WRP protection.

More Information: http://msdn.microsoft.com/en-us/library/bb756998.aspx

Manual Remediation: Assess whether the conflicting resources are actually needed, and if not remove them from the MSI package. If a given resource is needed and the original system one cannot be used, consider re-engineering the application or use any virtualization technique to override the resource.

T014 - Missing or Invalid Signatures

Description: RayQC Advanced scans the MSI package for the presence of unsigned executable files (`.exe`, `.dll`, `.ocx`). Additionally, the package itself and CAB files are also scanned.

Background: According to the set of best practices by Microsoft, all exercutable files deployed by an installation package and the installation package itself should be digitally signed with a certificate issued by a Trusted Publisher. When attempting to run an unsigned executable, Windows prompts the user for authorization. Similarly, attempting to install an unsigned MSI package also shows the Windows prompt.

More Information: http://technet.microsoft.com/en-us/library/cc962053.aspx

Manual Remediation: Contact the manufacturer to obtain signed executables and installers. Use WDK (Windows Driver Kit) to sign self-developed executables and packages.

T015 - Security and User Access Control Issues

Description: RayQC Advanced scans the MSI package for the presence of issues that may fail to work due to the security features. The executable files are scanned for the presence of correct manifestation. Direct calls to rundll32 are reported, because the UAC prompt hides the actual calling module when rundll32 is executed. Interactive sevices running in session 0 are detected, as well as MMC snap-ins that are not DEP-aware. Finally, setups, updaters and uninstallers are detected and checked for the presence of their UAC awareness.

Background: Session 0 isolation and Data Execution Prevention (DEP) are examples of security improvements introduced to prevent malicious software from compromising the security of the operating systems. They provide a separation between interactive user sessions and non-interactive session 0 devoted for services, and prevent execution of code from non-executable memory region. Modern software has to comply to these restrictions in order to function correctly on Windows 8.1. Another security issue present in Windows operating system is User Account Control (UAC). When an executable file requires additional non-standard permissions, the UAC elevation dialog prompts for confirmation or for correct credentials. The UAC prompt contains information about calling application, manufacturer and the source. Certain applications, like self-updaters, setups and other requiring higher privileges must be aware of the elevation, and use manifests to correctly inform the system about required execution permissions.

More Information: http://msdn.microsoft.com/en-us/windows/hardware/gg463353
http://msdn.microsoft.com/en-us/library/bb963893.aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/aa366553(v=vs.85).aspx
http://technet.microsoft.com/en-us/library/cc709628%28WS.10%29.aspx
http://technet.microsoft.com/en-us/library/cc709628%28WS.10%29.aspx

Manual Remediation: Contact the manufacturer to obtain software that complies to the security features of Microsoft Windows. For each unmanifested executable file, create a manifest, and set the required privileges to "asInvoker" for applications not requiring them, and `"requireAdministrator"` or `"highestAvailable"` for others. If the manifest cannot be corrected, a shim database has to be used to specify the desired privilege level.

T016 - Missing Application Manifest or Insufficient Execution Policy

Description: RayQC Advanced scans the MSI package for the presence of executable files (`.exe`, `.cpl`) that do not contain the manifest, or that are not aware of Windows 8.1 in the list of supported operating systems in their manifest files.

Background: Since Windows Vista, all applications run by default with standard user privileges. This is also true when the current user is a member of Administrators group. Application that used to work on previous versions of Windows may fail to work, as no elevation will take place. In order to require higher permissions, each executable or control panel applications has to contain a manifest file - a simple `.XML` file informing the operating system how to handle the given program.

More Information: http://msdn.microsoft.com/en-us/library/Aa480152%23appcomp_topic30.com#appcomp_topic4
http://msdn.microsoft.com/en-us/library/hh848036%28v=vs.85%29.aspx

Manual Remediation: Create a manifest file for each executable. To manifest a control panel application (`.cpl`) create an executable wrapper with embedded manifest. Use the SupportedOS section in the manifest to define the list of supported operating systems.

T017 - Incomplete Reboot Handling

Description: RayQC Advanced scans the MSI package for the absence of a proper launch condition preventing the installation if a reboot is pending. Additionally, absence of "Files in use" dialog is detected. Presence of `ForceReboot` action is also detected and reported.

Background: Windows Installer supports natively various set of features and actions related to

the reboot handling. They include for example the ability to show list of used/locked files, forcing or skipping the reboot and determining the installation state by the related MSI properties. Several aspects have to be considered so that the reboot handling works as expected.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/aa368607(v=vs.85).aspx

http://msdn.microsoft.com/en-us/library/windows/desktop/aa370492(v=vs.85).aspx

http://msdn.microsoft.com/en-us/library/windows/desktop/aa370379(v=vs.85).aspx

Manual Remediation: Add the `MSIRMFilesInUse` dialog to the dialog sequence if it is missing. Remove ForceReboot action from the sequence, reboots are handled automatically by MSI. In order to ensure the package is not installed when any reboot is pending, append the "`NOT MsiSystemRebootPending`" condition to the Launch Condition list.

T018 - Protected Mode (Internet Explorer)

Description: RayQC Advanced scans the MSI package for the presence of registry entries that disable Protected Mode.

Background: As a result of security changes introduced in Windows Vista, Internet Explorer runs now in a isolated mode called "Protected mode" by default. While it limits potential damages malware application can cause, it also prevents web-applications running in Internet Explorer from writing directly to disk while in Internet or Intranet zone. Internet Explorer warns when web-application tries to run certain software programs or write to protected areas.

More Information: http://msdn.microsoft.com/en-us/library/bb756991.aspx

Manual Remediation: Contact the manufacturer to obtain compatible software. Re-engineer self-developed software so that it runs correctly under Protected Mode, or add the required website(s) to the list of trusted sites.

Windows 8.1 64-bit

Below are the set of rules which can be used to test a package for deployment on Windows 8.1 64-bit

T101 - Known Compatibility Issues at Startup (AppHelp)

Description: RayQC Advanced scans the package for the presence of applications that may trigger Application Help Dialog (AppHelp) when the program is being installed or run for the first time.

Background: Certain applications are known to cause issues or not even starting on modern operating systems. Windows contains a predefined list of software known to have compatibility issues and warns or prevents user from starting the application. The list of such applications is stored in a central compatibility database, and the dialog shown to the user is known as Application Help (AppHelp).

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/bb756937.aspx

Manual Remediation: Contact the manufacturer to obtain compatible software.

T102 - Deprecated Windows Features

Description: RayQC Advanced scans the MSI package for the presence of deprecated features: embedded installations of another MSI packages (Custom Actions type 7, 23, 39), NETDDE-dependencies in registry, deprecated proxy configuration component `ProxyCfg.exe` and Windows Library files.

Background: Certain features present in previous versions of Windows systems are officially deprecated by Microsoft. This means they are provided as-is. These features may be still working, but there is no guarantee they will function correctly or at all after any update or security patch. Usually, there is a replacement technology that should be used in favor of deprecated features.

More Information: http://msdn.microsoft.com/en-us/library/aa368010%28v=VS.85%29.aspx
http://msdn.microsoft.com/en-us/library/bb756977.aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/
aa384069(v=vs.85).aspx

Manual Remediation: Do not use use Custom Actions type 7, 23 and 39 anymore. Dependencies and prerequisites have to be installed and managed by the deployment tool or external setup wrapper. The deprecated components have to be replaced. Contact the manufacturer to obtain compatible software.

T103 - Obsolete Windows Features

Description: RayQC Advanced scans the MSI package for a presence of shortcuts created in Quick Launch and subfolders of the SendTo folder. Additionally, start menu shortcuts pointing to non-executable files will be detected. Finally, RayQC Advanced scans the MSI package for a presence of Windows Gadgets.

Background: Each version of Microsoft Windows system introduces enhancements and changes of the user experience in the way Windows Shell is working and organizing files, shortcuts, context menu actions etc. Certain aspects of the user experience vary between newer version of Windows, with the introduction of Modern Start Screen being a notable example. There is a different handling for certain behaviors that were possible before. For example, the new Start Screen does not pin non-executable files by default, and due to the deprecated tree-like structure certain shortcuts names may be duplicated and thus confusing. Another example are shortcuts placed in subfolders of the SendTo folder, which are not displayed anymore. Finally, features like Quick Launch Bar and Windows Deskop Gadgets layer are not present anymore.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/
cc144179(v=vs.85).aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/
jj584985(v=vs.85).aspx

Manual Remediation: Avoid deploying shortcuts to Quick Launch location and to subfolders of SendTo folder. Migrate to the Modern application to allow pinning ups and running them in a gadget-mode. Rename Start menu shortcuts to unequivocally express their purpose and associated action, instead of using generic names like "Readme" or "Help". Non-executable files should be manually pinned by the logged on user.

T104 - Windows Shell and User Experience Changes

Description: RayQC Advanced scans the MSI package for a presence of shortcuts created in Quick Launch and subfolders of the SendTo folder. Additionally, start menu shortcuts pointing to non-executable files will be detected. Finally, RayQC Advanced scans the MSI package for a presence of Windows Gadgets.

Background: Each version of Microsoft Windows system introduces enhancements and changes of the user experience in the way Windows Shell is working and organizing files, shortcuts, context menu actions etc. Certain aspects of the user experience vary between newer version of Windows, with the introduction of Modern Start Screen being a notable example. There is a different handling for certain behaviors that were possible before. For example, the new Start Screen does not pin non-executable files by default, and due to the deprecated tree-like structure certain shortcuts names may be duplicated and thus confusing. Another example are shortcuts placed in subfolders of the SendTo folder, which are not displayed anymore. Finally, features like Quick Launch Bar and Windows Deskop Gadgets layer are not present anymore.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/cc144179(v=vs.85).aspx

http://msdn.microsoft.com/en-us/library/windows/desktop/jj584985(v=vs.85).aspx

Manual Remediation: Avoid deploying shortcuts to Quick Launch location and to subfolders of SendTo folder. Migrate to the Modern application to allow pinning ups and running them in a gadget-mode. Rename Start menu shortcuts to unequivocally express their purpose and associated action, instead of using generic names like "Readme" or "Help". Non-executable files should be manually pinned by the logged on user.

T105 - Unsupported Windows Components

Description: RayQC Advanced scans the MSI package for a presence of applications using DHTML control and for the presence of 32-bit .hlp files.

Background: Certain functionalities and components present in Windows XP and previous systems are not anymore part of the standard OS image. Since then Microsoft offers them as downloadable add-ons wich restore the missing functionality. On a standard system however, missing handlers/opening applications may cause runtime exceptions or other warnings. Typical examples of such components are viewers for 32-bit `.hlp` files, missing DHTLM editor controls and so on.

More Information: http://support.microsoft.com/kb/917607

http://msdn.microsoft.com/en-us/library/aa663363.aspx

Manual Remediation: Contact the manufacturer to obtain compatible software. You may also install the missing components - the update KB917607 restores the ability to view 32-bit `.hlp` files, and the redistributable installer `DHTMLEd.msi` from Microsoft installs the missing DHTML control.

T106 - .Net Framework Compatibility

Description: RayQC Advanced scans the MSI package for a presence of applications using .NET Framework 1.0, 1.1, 2.0, 3.0 or 3.5.

Background: Since Windows 7, .NET Framework 1.0 and 1.1 are not supported. Although it may be possible to deploy deprecated .NET components, there is no support for these configurations provided by Microsoft. Additionally .NET Framework 2.0, 3.0 and 3.5 is not

included in the default configuration of Windows 8 and later operating systems, so applications that require one of these frameworks might trigger a request for installing the necessary files.

More Information: http://support.microsoft.com/kb/2489698

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should be converted to .NET Framework 4.5.

T107 - Conditional Installation Execution

Description: RayQC Advanced scans the MSI package for a presence of conditions that vary based on the value of properties: `VersionNT`, `VersionNT64`, `WindowsBuild` and `ServicePackLevel`. Additionally, the content of the package is scanned for the usage of `AdminUser` and `Privileged` properties in Launch Conditions and components condition to verify they will not cause issues with permission elevation. Merge modules, 16-bit components and certain conditions may neutralize otherwise failing conditions.

Background: Number of MSI properties like `VersionNT`, `VersionNT64`, `ServicePackLevel` etc. can be used to conditionally control the flow of installation and set of features/ components/policies to be installed. Software vendors use them frequently in critical places like LaunchConditions, conditions for components and Custom Actions, conditional security policies and many more. When a new version of Operating System is introduced, these conditions have to be reviewed, because they may generate false warnings even though the software is functioning correctly. Another source of issues are two distinctive MSI properties `Privileged` and `AdminUser`. Because of late elevation, since Windows Vista values of these properties are spoofed when evaluating LaunchConditions. This may produce unexpected results with packages designed for previous operating systems.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/ aa370556(v=vs.85).aspx

> http://msdn.microsoft.com/en-us/library/windows/desktop/ aa369752(v=vs.85).aspx

Manual Remediation: Review all rows containing conditions that exclude the current operating system. Should the given component/action be required and function correctly on Windows 8.1, rewrite the condition so that it evaluates to true or remove it to always install the questionable resource. Do not use `AdminUser` property, because it may impact installation flows that elevate at some later point of installation. Legacy distinction between `Privileged` and `AdminUser` property can be restored by using the `MSIREALADMINDETECTION` property.

T108 - Deprecated and Obsolete API Calls

Description: RayQC Advanced scans the MSI package for a presence of API calls that are deprecated or obsolete. Internal database is used to assess each API call being used.

Background: Certain APIs present in previous versions of Microsoft Windows are now officially deprecated or obsoleted by Microsoft. Obsolete APIs may not work anymore, or their behavior may be different leading to unexpected results. The deprecated APIs may be still working, but there is no guarantee they will function correctly or at all after any update or security patch. Usually, there is a replacement API that should be used in favor of deprecated or obsolete API call.

More Information: None available.

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should not use obsolete functions anymore and switch to replacements as

described by Microsoft in Microsoft SDK Updates.

T109 - Hard-Coded Resources and System Paths

Description: RayQC Advanced scans the MSI package for a usage of changed or obsolete junction points in INI files, registry entries, services, shortcuts, environment variables and custom actions.

Background: Since Microsoft Windows Vista, standard locations where user and system data are stored have been changed. For example, the root folder for user data was called "Documents and Settings" in Windows XP, but since Windows Vista its name is "Users". To provide a backward compatibility, junction points are used to reroute the calls from old, incorrect locations to the new, proper ones. A package that runs on various target systems should not rely on hardcoded paths, because they may be not valid anymore or for a given system language.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/
bb968829(v=vs.85).aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/
aa368977(v=vs.85).aspx

Manual Remediation: Hard-coded paths should not be used. Replace them with MSI properties using formatted syntax. If no predefined property exists, the path should be exposed via custom MSI property so that it can be adjusted on demand from command-line / MST transform.

T110 - Mismatched Target Architecture

Description: RayQC Advanced scans the MSI package for the presence of executables (16/32/64-bit) that are not compatible with Windows 8.1 32-bit platform.

Background: Some software is intended to run only in 32-bit or 64-bit operating systems. 16-bit executables are not supported on modern platforms, and 64-bit Microsoft Windows can correctly emulate 32-bit applications. If the MSI package is missing a correct Launch Condition it may try to install executables that are not designed for the current platform architecture. Attempting to launch such executable might result in an error message that the file is not a valid Win32 application. Additionally, attempting to run 16-bit code may result in a warning message informing that an extra Windows Feature is required.

More Information: http://support.microsoft.com/kb/282423/en-us

Manual Remediation: Contact the manufacturer to obtain compatible software. Re-engineer self-developed software by replacing 16-bit executables with appropriate 32- or 64-bit code. Use Launch Conditions and component conditions to control to which platform software and its parts are deployed.

T111 - Driver Issues

Description: RayQC Advanced scans the MSI package for the presence of drivers containing no valid signature or not matching the target platform.

Background: Since Windows Vista 64-bit, all drivers have to be signed. Signed driver contains an extra digital signature used to validate the source and content of the driver package. Any unauthorized change in the driver package invalidates the signature. If an unsigned driver or a driver with invalid signature is attempted to be installed, Windows refuses the installation. Likewise, each driver has to match the target platform, which means that 64-bit systems

require 64-bit drivers.

More Information: http://msdn.microsoft.com/en-us/library/bb756937.aspx

Manual Remediation: Contact the manufacturer to obtain compatible driver. Use WDK (Windows Driver Kit) to sign self-developed driver packages.

T112 - Installation Package Design Issues

Description: RayQC Advanced scans the MSI package for the presence of common installation design issues that may cause troubles during installation or using of software. The context of Custom Actions is scanned for the presence of deferred custom actions running in user-context, as well as system-wide actions running in immediate mode. The presence of conflicting permissions tables preventing the installation is detected as well. Additionally, invalid combinations of user- and machine-data in a single component and invalid identifiers are reported.

Background: Microsoft recommends several best-practices approaches for MSI setup designers. They ensure that the package is deployed correctly in various scenarios and various operating systems. By following the guidelines many compatibility issues introduced by a new security model in Windows Vista can be avoided.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/aa368268%28v=vs.85%29.aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/aa368268(v=vs.85).aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/dd408053(v=vs.85).aspx
http://msdn.microsoft.com/en-us/library/6397xx85(v=vs.80).aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/aa368994%28v=vs.85%29.aspx

Manual Remediation: Adjust the package content so that it complies to the best practices of Windows Installer. Do not mix per-machine and per-user data in a single component. Use valid identifiers for components. Make sure all custom actions are running in a valid context - all actions making system changes must be deferred in execution. Do not use both `LockPermissions` and `MsiLockPermissionsEx` tables at once.

T113 - Conflicts with Protected Windows Resources (WRP)

Description: RayQC Advanced scans the MSI package for the presence of files and registry keys that belong to the Windows Resource Protection list.

Background: Windows Resource Protection (WRP) prevents the modification of essential system resources (files, folders and registry keys). Windows Installer silently ignores any attempt to update or modify them, any other software trying to do it may fail. These kinds of resources may be only updated by Microsoft-provided redistributable packages. During the installation, if Windows Installer logging is enabled, a warning may be shown for each operation that was ignored because of the WRP protection.

More Information: http://msdn.microsoft.com/en-us/library/bb756998.aspx

Manual Remediation: Assess whether the conflicting resources are actually needed, and if not remove them from the MSI package. If a given resource is needed and the original system one cannot be used, consider re-engineering the application or use any virtualization technique to

override the resource.

T114 - Missing or Invalid Signatures

Description: RayQC Advanced scans the MSI package for the presence of unsigned executable files (`.exe`, `.dll`, `.ocx`). Additionally, the package itself and CAB files are also scanned.

Background: According to the set of best practices by Microsoft, all executable files deployed by an installation package and the installation package itself should be digitally signed with a certificate issued by a Trusted Publisher. When attempting to run an unsigned executable, Windows prompts the user for authorization. Similarly, attempting to install an unsigned MSI package also shows the Windows prompt.

More Information: http://technet.microsoft.com/en-us/library/cc962053.aspx

Manual Remediation: Contact the manufacturer to obtain signed executables and installers. Use WDK (Windows Driver Kit) to sign self-developed executables and packages.

T115 - Security and User Access Control Issues

Description: RayQC Advanced scans the MSI package for the presence of issues that may fail to work due to the security features. The executable files are scanned for the presence of correct manifestation. Direct calls to rundll32 are reported, because the UAC prompt hides the actual calling module when rundll32 is executed. Interactive sevices running in session 0 are detected, as well as MMC snap-ins that are not DEP-aware. Finally, setups, updaters and uninstallers are detecteded and checked for the presence of their UAC awareness.

Background: Session 0 isolation and Data Execution Prevention (DEP) are examples of security improvements introduced to prevent malcious software from compromising the security of the operating systems. They provide a separation between interactive user sessions and non-interactive session 0 devoted for services, and prevent execution of code from non-executable memory region. Modern software has to comply to these restrictions in order to function correctly on Windows 8.1. Another security issue present in Windows operating system is User Account Control (UAC). When an executable file requires additional non-standard permissions, the UAC elevation dialog prompts for confirmation or for correct credentials. The UAC prompt contains information about calling application, manufacturer and the source. Certain applications, like self-updaters, setups and other requiring higher privileges must be aware of the elevation, and use manifests to correctly inform the system about required execution permissions.

More Information: http://msdn.microsoft.com/en-us/windows/hardware/gg463353
http://msdn.microsoft.com/en-us/library/bb963893.aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/aa366553(v=vs.85).aspx
http://technet.microsoft.com/en-us/library/cc709628%28WS.10%29.aspx
http://technet.microsoft.com/en-us/library/cc709628%28WS.10%29.aspx

Manual Remediation: Contact the manufacturer to obtain software that complies to the security features of Microsoft Windows. For each unmanifested executable file, create a manifest, and set the required privileges to "asInvoker" for applications not requiring them, and "**`requireAdministrator`**" or "`highestAvailable`" for others. If the manifest cannot be corrected, a shim database has to be used to specify the desired privilege level.

T116 - Missing Application Manifest or Insufficient Execution Policy

Description: RayQC Advanced scans the MSI package for the presence of executable files (`.exe`, `.cpl`) that do not contain the manifest, or that are not aware of Windows 8.1 in the list of supported operating systems in their manifest files.

Background: Since Windows Vista, all applications run by default with standard user privileges. This is also true when the current user is a member of Administrators group. Application that used to work on previous versions of Windows may fail to work, as no elevation will take place. In order to require higher permissions, each executable or control panel applications has to contain a manifest file - a simple `.XML` file informing the operating system how to handle the given program.

More Information: http://msdn.microsoft.com/en-us/library/Aa480152%
23appcomp_topic30.com#appcomp_topic4
http://msdn.microsoft.com/en-us/library/hh848036%28v=vs.85%29.aspx

Manual Remediation: Create a manifest file for each executable. To manifest a control panel application (`.cpl`) create an executable wrapper with embedded manifest. Use the SupportedOS section in the manifest to define the list of supported operating systems.

T117 - Incomplete Reboot Handling

Description: RayQC Advanced scans the MSI package for the absence of a proper launch condition preventing the installation if a reboot is pending. Additionally, absence of "Files in use" dialog is detected. Presence of ForceReboot action is also detected and reported.

Background: Windows Installer supports natively various set of features and actions related to the reboot handling. They include for example the ability to show list of used/locked files, forcing or skipping the reboot and determining the installation state by the related MSI properties. Several aspects have to be considered so that the reboot handling works as expected.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/
aa368607(v=vs.85).aspx

http://msdn.microsoft.com/en-us/library/windows/desktop/
aa370492(v=vs.85).aspx

http://msdn.microsoft.com/en-us/library/windows/desktop/
aa370379(v=vs.85).aspx

Manual Remediation: Add the `MSIRMFilesInUse` dialog to the dialog sequence if it is missing. Remove `ForceReboot` action from the sequence, reboots are handled automatically by MSI. In order to ensure the package is not installed when any reboot is pending, append the `"NOT MsiSystemRebootPending"` condition to the Launch Condition list.

T118 - Protected Mode (Internet Explorer)

Description: RayQC Advanced scans the MSI package for the presence of registry entries that disable Protected Mode.

Background: As a result of security changes introduced in Windows Vista, Internet Explorer runs now in a isolated mode called "Protected mode" by default. While it limits potential damages malware application can cause, it also prevents web-applications running in Internet Explorer from writing directly to disk while in Internet or Intranet zone. Internet Explorer warns when web-application tries to run certain software programs or write to protected areas.

More Information: http://msdn.microsoft.com/en-us/library/bb756991.aspx

> **Manual Remediation:** Contact the manufacturer to obtain compatible software. Reengineer self-developed software so that it runs correctly under Protected Mode, or add the required website(s) to the list of trusted sites.

Windows 10 32-bit

Below are the set of rules which can be used to test a package for deployment on Windows 10 32-bit

Windows 10 Ruleset has several subeditions:

- RTM Build (1507)
- November update (1511)
- Anniversary Update (1607)
- Creators Update (1703)
- Fall Creators Update (1709)
- April 2018 Update (1803)
- October 2018 Update (1809)
- May 2019 Update (1903)
- May 2020 Update (2004)
- October 2020 Update (20H2)

Exact details and tests may differ between these versions. This documentation provides only a general overview of items and problems tested by RayQC Advanced for Windows 10 Operating Systems family.

T001 - Known Compatibility Issues at Startup (AppHelp)

Description: RayQC Advanced scans the package for the presence of applications that may trigger Application Help Dialog (AppHelp) when the program is being installed or run for the first time.

Background: Certain application are known to cause issues or not even starting on modern operating systems. Windows contains a predefined list of software known to have compatibility issues and warns or prevents user from starting the application. The list of such applications is stored in the central compatibility database and the dialog shown to the user is known as Application Help (AppHelp).

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/bb756937.aspx

Manual Remediation: Contact the manufacturer to obtain compatible software.

T002 - Deprecated Windows Features

Description: RayQC Advanced scans the MSI package for the presence of deprecated features: embedded installations of another MSI packages (**Custom Actions** type 7, 23, 39), NETDDE dependencies in registry, deprecated proxy configuration component `ProxyCfg.exe` and

---

Windows Library files.

Background: Certain features present in previous versions of Windows systems are officially deprecated by Microsoft. This means they are provided as-is. These features may be still working, but there is no guarantee they will function correctly or at all after any update or security patch. Usually, there is a replacement technology that should be used in favor of deprecated features.

More Information: http://msdn.microsoft.com/en-us/library/aa368010%28v=VS.85%29.aspx http://msdn.microsoft.com/en-us/library/bb756977.aspx http://msdn.microsoft.com/en-us/library/windows/desktop/ aa384069(v=vs.85).aspx

Manual Remediation: Do not use use Custom Actions type 7, 23, and 39 anymore. Dependencies and prerequisites have to be installed and managed by the deployment tool or external setup wrapper. The deprecated components have to be replaced. Contact the manufacturer to obtain compatible software.

T003 - Obsolete Windows Features

Description: RayQC Advanced scans the MSI package for a presence of deprecated MSGina technology, as well as for a presence of file extensions, for which the handling has been obsoleted.

Background: Certain features present in previous versions of Windows systems are officially marked as obsolete by Microsoft. This means they are not supported anymore and any functionality relying on them is likely to fail to operate. Usually, there is a replacement technology that should be used in favor of deprecated features.

More Information: http://msdn.microsoft.com/en-us/library/bb756900.aspx http://technet.microsoft.com/en-en/library/ee681703(v=ws.10).aspx

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software using the `MSGina.dll` should be re-engineered and use the Credential Providers model. Obsolete extensions should not be used in MSI installer packages.

T004 - Windows Shell and User Experience Changes

Description: RayQC Advanced scans the MSI package for a presence of shortcuts created in `Quick Launch` and subfolders of the `SendTo` folder. Additionally, start menu shortcuts pointing to non-executable files will be detected. Finally, RayQC Advanced scans the MSI package for a presence of Windows Gadgets.

Background: Each version of Microsoft Windows system introduces enhancements and changes of the user experience in the way Windows Shell is working and organizing files, shortcuts, context menu actions etc. Certain aspects of the user experience vary between newer version of Windows, with the introduction of Modern Start Screen being a notable example. There is a different handling for certain behaviors that were possible before. For example, the new Start Screen does not pin non-executable files by default, and due to the deprecated tree-like structure certain shortcuts names may be duplicated and thus confusing. Another example are shortcuts placed in subfolders of the SendTo folder, which are not displayed anymore. Finally, features like Quick Launch Bar and Windows Deskop Gadgets layer are not present anymore.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/

[cc144179(v=vs.5).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/cc144179(v=vs.5).aspx)

http://msdn.microsoft.com/en-us/library/windows/desktop/jj584985(v=vs.85).aspx

Manual Remediation: Avoid deploying shortcuts to Quick Launch location and to subfolders of SendTo folder. Migrate to the Modern application to allow pinning ups and running them in a gadget mode. Rename Start menu shortcuts to unequivocally express their purpose and associated action, instead of using generic names like "Readme" or "Help". Non-executable ´files should be manually pinned by the logged on user.

T005 - Unsupported Windows Components

Description: RayQC Advanced scans the MSI package for a presence of applications using DHTML control and for the presence of 32-bit `.hlp` files.

Background: Certain functionalities and components present in Windows XP and previous systems are not anymore part of the standard OS image. Since then Microsoft offers them as downloadable add-ons which restore the missing functionality. On a standard system however, missing handlers/opening applications may causes runtime exceptions or other warnings. Typical examples of such components are viewers for 32-bit `.hlp` files, missing DHLTM editor controls and so on.

More Information: http://support.microsoft.com/kb/917607
http://msdn.microsoft.com/en-us/library/aa663363.aspx

Manual Remediation: Contact the manufacturer to obtain compatible software. You may also install missing components - the update KB917607 restores the ability to view 32-bit `.hlp` files and the redistributable installer `DHTMLEd.msi` from Microsoft installs the missing DHTML control.

T006 - .NET Framework Compatibility

Description: RayQC Advanced scans the MSI package for a presence of applications using .NET Framework 1.0, 1.1, 2.0, 3.0, or 3.5.

Background: Since Windows 7, .NET Framework 1.0, and 1.1 are not supported. Although it may be possible to deploy deprecated .NET components, there is no support for these configurations provided by Microsoft. Additionally .NET Framework 2.0, 3.0, and 3.5 is not included in the default configuration of Windows 8 and later operating systems, so applications that require one of these frameworks might trigger a request for installing the necessary files.

More Information: http://support.microsoft.com/kb/2489698

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should be converted to .NET Framework 4.5.

T007 - Conditional Installation and Execution

Description: RayQC Advanced scans the MSI package for a presence of conditions that vary based on the value of properties: VersionNT, VersionNT64, WindowsBuild, and ServicePackLevel. Additionally, the content of the package is scanned for the usage of `AdminUser` and `Privileged` properties in Launch Conditions and components condition to verify they will not cause issues with permission elevation. Merge modules, 16-bit components and certain conditions may neutralize otherwise failing conditions.

Background: Number of MSI properties like VersionNT, VersionNT64, ServicePackLevel etc.

can be used to conditionally control the flow of installation and set of features / components / policies to be installed. Software vendors use them frequently in critical places like LaunchConditions, conditions for components, and Custom Actions, conditional security policies, and many more. When a new version of Operating System is introduced, these conditions have to be reviewed, because they may generate false warnings even though the software is functioning correctly. Another source of issues are two distinctive MSI properties `Privileged` and `AdminUser`. Because of late elevation, since Windows Vista values of these properties are spoofed when evaluating Launch Conditions. This may produce unexpected results with packages designed for previous operating systems.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/aa370556(v=vs.85).aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/aa369752(v=vs.85).aspx

Manual Remediation: Review all rows containing conditions that exclude the current operating system. Should the given component / action be required and function correctly on Windows 10, rewrite the condition so that it evaluates to true or remove it to always install the questionable resource. Do not use AdminUser property, because it may impact installation flows that elevate at some later point of installation. Legacy distinction between `Privileged` and `AdminUser` property can be restored by using the `MSIREALADMINDETECTION` property.

T008 - Deprecated and Obsolete API Calls

Description: RayQC Advanced scans the MSI package for a presence of API calls that are deprecated or obsolete. Internal database is used to assess each API call being used.

Background: Certain APIs present in previous versions of Microsoft Windows are now officially deprecated or obsoleted by Microsoft. Obsolete APIs may not work anymore, or their behavior may be different leading to unexpected results. The deprecated APIs may be still working, but there is no guarantee they will function correctly or at all after any update or security patch. Usually, there is a replacement API that should be used in favor of deprecated or obsolete API call.

More Information: None available.

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should not use obsolete functions anymore and switch to replacements as described by Microsoft in Microsoft SDK Updates.

T009 - Hard-Coded Resources and System Paths

Description: RayQC Advanced scans the MSI package for a usage of changed or obsolete junction points in INI files, registry entries, services, shortcuts, environment variables, and custom actions.

Background: Since Microsoft Windows Vista, standard locations where user and system data are stored have been changed. For example, the root folder for user data was called `Documents and Settings` in Windows XP, but since Windows Vista its name is `Users`. To provide a backward compatibility, junction points are used to reroute the calls from old, incorrect locations to the new, proper ones. A package that runs on various target systems should not rely on hardcoded paths, because they may be not valid anymore or for a given system language.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/bb968829(v=vs.85).aspx

http://msdn.microsoft.com/en-us/library/windows/desktop/aa368977(v=vs.85).aspx

Manual Remediation: Hardcoded paths should not be used. Replace them with MSI properties using formatted syntax. If no predefined property exists, the path should be exposed via custom MSI property so that it can be adjusted on demand from command-line / MST transform.

T010 - Mismatched Target Architecture

Description: RayQC Advanced scans the MSI package for the presence of executables (16/32/64-bit) that are not compatible with Windows 10 32-bit platform.

Background: Some software is intended to run only in 32-bit or 64-bit operating systems. 16-bit executables are not supported on modern platforms and 64-bit Microsoft Windows can correctly emulate 32-bit applications. If the MSI package is missing a correct Launch Condition it may try to install executables that are not designed for the current platform architecture. Attempting to launch such executable might result in an error message that the file is not a valid Win32 application. Additionally, attempting to run 16-bit code may result in a warning message informing that an extra Windows Feature is required.

More Information: *http://support.microsoft.com/kb/282423/en-us*

Manual Remediation: Contact the manufacturer to obtain compatible software. Reengineer self-developed software by replacing 16-bit executables with appropriate 32- or 64-bit code. Use Launch Conditions and component conditions to control to which platform software and its parts are deployed.

T011 - Driver Issues

Description: RayQC Advanced scans the MSI package for the presence of drivers containing no valid signature or not matching the target platform.

Background: Since Windows Vista 64-bit, all drivers have to be signed. Signed driver contains an extra digital signature used to validate the source and content of the driver package. Any unauthorized change in the driver package invalidates the signature. If an unsigned driver or a driver with invalid signature is attempted to be installed, Windows refuses the installation. Likewise, each driver has to match the target platform, which means that 64-bit systems require 64-bit drivers.

More Information: http://msdn.microsoft.com/en-us/library/bb756937.aspx

Manual Remediation: Contact the manufacturer to obtain compatible driver. Use WDK (Windows Driver Kit) to sign self-developed driver packages.

T012 - Installation Package Design Issues

Description: RayQC Advanced scans the MSI package for the presence of common installation design issues that may cause troubles during installation or using of software. The context of **Custom Actions** is scanned for the presence of deferred custom actions running in user-context, as well as system wide actions running in immediate mode. The presence of conflicting permissions tables preventing the installation is detected as well. Additionally, invalid combinations of user- and machine-data in a single component and invalid identifiers are reported.

Background: Microsoft recommends several best-practices approaches for MSI setup designers. They ensure that the package is deployed correctly in various scenarios and various operating systems. By following the guidelines many compatibility issues introduced by a new security model in Windows Vista can be avoided.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/aa368268%28v=vs.85%29.aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/aa368268(v=vs.85).aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/dd408053(v=vs.85).aspx
http://msdn.microsoft.com/en-us/library/6397xx85(v=vs.80).aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/aa368994%28v=vs.85%29.aspx

Manual Remediation: Adjust the package content so that it complies to the best practises of Windows Installer. Do not mix permachine and peruser data in a single component. Use valid identifiers for components. Make sure all custom actions are running in a valid context - all actions making system changes must be deferred in execution. Do not use both `LockPermissions` and `MsiLockPermissionsEx` tables at once.

T013 - Conflicts with Protected Windows Resources (WRP)

Description: RayQC Advanced scans the MSI package for the presence of files and registry keys that belong to the Windows Resource Protection list.

Background: Windows Resource Protection (WRP) prevents the modification of essential system resources (files, folders, and registry keys). Windows Installer silently ignores any attempt to update or modify them, any other software trying to do it may fail. These kinds of resources may be only updated by Microsoft-provided redistributable packages. During the installation, if Windows Installer logging is enabled, a warning may be shown for each operation that was ignored because of the WRP protection.

More Information: http://msdn.microsoft.com/en-us/library/bb756998.aspx

Manual Remediation: Assess whether the conflicting resources are actually needed and, if not, remove them from the MSI package. If a given resource is needed and the original system one cannot be used, consider re-engineering the application or use any virtualization technique to override the resource.

T014 - Missing or Invalid Signatures

Description: RayQC Advanced scans the MSI package for the presence of unsigned executable files (`.exe`, `.dll`, `.ocx`). Additionally, the package itself and CAB files are also scanned.

Background: According to the set of best practices by Microsoft, all executable files deployed by an installation package and the installation package itself should be digitally signed with a certificate issued by a Trusted Publisher. when attempting to run an unsigned executable, Windows prompts the user for authorization. Similarly, attempting to install an unsigned MSI package also shows the Windows prompt.

More Information: http://technet.microsoft.com/en-us/library/cc962053.aspx

Manual Remediation: Contact the manufacturer to obtain signed executables and installers. Use WDK (Windows Driver Kit) to sign self-developed executables and packages.

T015 - Security and User Access Control Issues

Description: RayQC Advanced scans the MSI package for the presence of issues that may fail to work due to the security features. The executable files are scanned for the presence of correct manifestation. Direct calls to rundll32 are reported, because the UAC prompt hides the actual calling module when rundll32 is executed. Interactive services running in session 0 are detected, as well as MMC snapins that are not DEP-aware. Finally, setups, updaters and uninstallers are detected and checked for the presence of their UAC awareness.

Background: Session 0 isolation and Data Execution Prevention (DEP) are examples of security improvements introduced to prevent malicious software from compromising the security of the operating systems. They provide a separation between interactive user sessions and non-interactive session 0 devoted for services, and prevent execution of code from non-executable memory region. Modern software has to comply to these restrictions in order to function correctly on Windows 10. Another security issue present in Windows operating system is User Account Control (UAC). When an executable file requires additional nonstandard permissions, the UAC elevation dialog prompts for confirmation or for correct credentials. The UAC prompt contains information about calling application, manufacturer and the source. Certain applications, like selfupdaters, setups and other requiring higher privileges must be aware of the elevation, and use manifests to correctly inform the system about required execution permissions.

More Information: http://msdn.microsoft.com/en-us/windows/hardware/gg463353
http://msdn.microsoft.com/en-us/library/bb963893.aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/
aa366553(v=vs.85).asp
http://technet.microsoft.com/en-us/library/cc709628%28WS.10%29.aspx

Manual Remediation: Contact the manufacturer to obtain software that complies to the security features of Microsoft Windows. For each unmanifested executable file, create a manifest, and set the required privileges to "`asInvoker`" for applications not requiring them, and "`requireAdministrator`" or "`highestAvailable`" for others. If the manifest cannot be corrected, a shim database has to be used to specify the desired privilege level.

T016 - Missing Application Manifest or Insufficient Execution Policy

Description: RayQC Advanced scans the MSI package for the presence of executabl files (`.exe`, `.cpl`) that do not contain the manifest, or that are not aware of Windows 10 in the list of supported operating systems in their manifest files.

Background: Since Windows Vista, all applications run by default with standard user privileges. This is also true when the current user is a member of Administrators group. Application that used to work on previous versions of Windows may fail to work, as no elevation will take place. In order to require higher permissions, each executable or control panel applications has to contain a manifest file - a simple `.xml` file informing the operating system how to handle the given program.

More Information: http://msdn.microsoft.com/en-us/library/Aa480152%
23appcomp_topic30.com#appcomp_topic4
http://msdn.microsoft.com/en-us/library/hh848036%28v=vs.85%29.aspx

Manual Remediation: Create a manifest file for each executable. To manifest a control panel application (`.cpl`) create an executable wrapper with embedded manifest. Use the SupportedOS section in the manifest to define the list of supported operating systems.

T017 - Incomplete Reboot Handling

Description: RayQC Advanced scans the MSI package for the absence of a proper launch condition preventing the installation if a reboot is pending. Additionally, the absence of the **Files in use** dialog is detected. The presence of the `ForceReboot` action is also detected and reported.

Background: Windows Installer supports natively various set of features and actions related to the reboot handling. They include for example, the ability to show list of used/locked files, forcing or skipping the reboot and determining the installation state by the related MSI properties. Several aspects have to be considered so that the reboot handling works as expected.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/aa368607(v=vs.85).aspx
> http://msdn.microsoft.com/en-us/library/windows/desktop/aa370492(v=vs.85).aspx
> http://msdn.microsoft.com/en-us/library/windows/desktop/aa370379(v=vs.85).aspx

Manual Remediation: Add the `MSIRMFilesInUse` dialog to the dialog sequence if it is missing. Remove `ForceReboot` action from the sequence, reboots are handled automatically by MSI. In order to ensure the package is not installed when any reboot is pending, append the "`NOTMsiSystemRebootPending`" condition to Launch Condition list.

T018 - Protected Mode (Internet Explorer)

Description: RayQC Advanced scans the MSI package for the presence of registry entries that disable Protected Mode.

Background: As a result of security changes introduced in Windows Vista, Internet Explorer runs now in an isolated mode called **Protected mode** by default. While it limits potential damages malware applications can cause, it also prevents web-applications running in Internet Explorer from writing directly to disk while in Internet or Intranet zone. Internet Explorer warns when web application tries to run certain software programs or write to protected areas.

More Information: http://msdn.microsoft.com/en-us/library/bb756991.aspx

Manual Remediation: Contact the manufacturer to obtain compatible software. Reengineer self-developed software so that it runs correctly under **Protected mode**, or add the required website(s) to the list of trusted sites.

Windows 10 64-bit

Below are the set of rules which can be used to test a package for deployment on Windows 10 64-bit.

Windows 10 Ruleset has several sub-editions:

- RTM Build (1507)
- November update (1511)

- Anniversary Update (1607)
- Creators Update (1703)
- Fall Creators Update (1709)
- April 2018 Update (1803)
- October 2018 Update (1809)
- May 2019 Update (1903)
- November 2019 Update (1909)
- May 2020 Update (2004)
- October 2020 Update (20H2)

Exact details and tests may differ between these versions. This documentation provides only a general overview of items and problems tested by RayQC Advanced for Windows 10 Operating Systems family.

T101 – Known Compatibility Issues at Startup (AppHelp)

Description: RayQC Advanced scans the package for the presence of applications that may trigger Application Help Dialog (AppHelp) when the program is being installed or run for the first time.

Background: Certain applications are known to cause issues or not even starting on modern operating systems. Windows contains a predefined list of software known to have compatibility issues and warns or prevents user from starting the application. The list of such applications is stored in a central compatibility database, and the dialog shown to the user is known as Application Help (AppHelp).

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/bb756937.aspx

Manual Remediation: Contact the manufacturer to obtain compatible software.

T102 – Deprecated Windows Features

Description: RayQC Advanced scans the MSI package for the presence of deprecated features: embedded installations of another MSI packages (Custom Actions type 7, 23, 39), NETDDEdependencies in registry, deprecated proxy configuration component `ProxyCfg.exe` and Windows Library files.

Background: Certain features present in previous versions of Windows systems are officially deprecated by Microsoft. This means they are provided as-is. These features may be still working, but there is no guarantee they will function correctly or at all after any update or security patch. Usually, there is a replacement technology that should be used in favor of deprecated features.

More Information: http://msdn.microsoft.com/en-us/library/aa368010%28v=VS.85%29.aspx
http://msdn.microsoft.com/en-us/library/bb756977.aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/aa384069(v=vs.85).aspx

Manual Remediation: Do not use use Custom Actions type 7, 23 and 39 anymore. Dependencies and prerequisites have to be installed and managed by the deployment tool or external setup wrapper. The deprecated components have to be replaced. Contact the

manufacturer to obtain compatible software.

T103 - Obsolete Windows Features

Description: RayQC Advanced scans the MSI package for a presence of deprecated MSGina technology, as well as for a presence of file extensions, for which the handling application has been obsoleted.

Background: Certain features present in previous versions of Windows systems are officially marked as obsolete by Microsoft. This means they are not supported anymore and any functionality relying on them is likely to fail to operate. Usually, there is a replacement technology that should be used in favor of deprecated features.

More Information: http://msdn.microsoft.com/en-us/library/bb756900.aspx
http://technet.microsoft.com/en-en/library/ee681703(v=ws.10).aspx

Manual Remediation: Contact the manufacturer to obtain compatible software. Selfdeveloped software using the `MSGina.dll` should be reenginered and use the Credential Providers model. Obsolete extensions should not be used in MSI installer packages.

T104 - Windows Shell and User Experience Changes

Description: RayQC Advanced scans the MSI package for a presence of shortcuts created in `Quick Launch` and subfolders of the `SendTo` folder. Additionally, start menu shortcuts pointing to non-executable files will be detected. Finally, RayQC Advanced scans the MSI package for a presence of Windows Gadgets.

Background: Each version of Microsoft Windows system introduces enhancements and changes of the user experience in the way Windows Shell is working and organizing files, shortcuts, context menu actions etc. Certain aspects of the user experience vary between newer versions of Windows, with the introduction of Modern Start Screen being a notable example. There is a different handling for certain behaviors that were possible before. For example, the new Start Screen does not pin non-executable files by default, and due to the deprecated tree-like structure certain shortcut names may be duplicated and thus confusing. Another example are shortcuts placed in subfolders of the SendTo folder, which are not displayed anymore. Finally, features like Quick Launch Bar and Windows Desktop Gadgets layer are not present anymore.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/cc144179(v=vs.85).aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/jj584985(v=vs.85).aspx

Manual Remediation: Avoid deploying shortcuts to `Quick Launch` location and to subfolders of `SendTo` folder. Migrate to the Modern application to allow pinning ups and running them in a gadget-mode. Rename Start menu shortcuts to unequivocally express their purpose and associated action, instead of using generic names like "Readme" or "Help". Non-executable files should be manually pinned by the logged on user.

T105 - Unsupported Windows Components

Description: RayQC Advanced scans the MSI package for a presence of applications using DHTML control and for the presence of 32-bit `.hlp` files.

Background: Certain functionalities and components present in Windows XP and previous systems are not anymore part of the standard OS image. Since then Microsoft offers them as

downloadable addons wich restore the missing functionality. On a standard system however, missing handlers/opening applications may cause runtime exceptions or other warnings. Typical examples of such components are viewers for 32-bit `.hlp` files, missing DHTLM editor controls and so on.

More Information: http://support.microsoft.com/kb/917607
http://msdn.microsoft.com/en-us/library/aa663363.aspx

Manual Remediation: Contact the manufacturer to obtain compatible software. You may also install the missing components - the update KB917607 restores the ability to view 32-bit `.hlp` files, and the redistributable installer `DHTMLEd.msi` from Microsoft installs the missing DHTML control.

T106 - .NET Framework Compatibility

Description: RayQC Advanced scans the MSI package for a presence of applications using .NET Framework 1.0, 1.1, 2.0, 3.0 or 3.5.

Background: Since Windows 7, .NET Framework 1.0 and 1.1 are not supported. Although it may be possible to deploy deprecated .NET components, there is no support for these configurations provided by Microsoft. Additionally .NET Framework 2.0, 3.0 and 3.5 is not included in the default configuration of Windows 8 and later operating systems, so applications that require one of these frameworks might trigger a request for installing the necessary files.

More Information: http://support.microsoft.com/kb/2489698

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should be converted to .NET Framework 4.5.

T107 - Conditional Installation and Execution

Description: RayQC Advanced scans the MSI package for a presence of conditions that vary based on the value of properties: VersionNT, VersionNT64, WindowsBuild and ServicePackLevel. Additionally, the content of the package is scanned for the usage of AdminUser and Privileged properties in Launch Conditions and component conditions to verify they will not cause issues with permission elevation. Merge modules, 16-bit components and certain conditions may neutralize otherwise failing conditions.

Background: Number of MSI properties like VersionNT, VersionNT64, ServicePackLevel etc. can be used to conditionally control the flow of installation and set of features / components / policies to be installed. Software vendors use them frequently in critical places like `LaunchConditions`, conditions for components and **Custom Actions**, conditional security policies and many more. When a new version of Operating System is introduced, these conditions have to be reviewed, because they my generate false warnings even though the software is functioning correctly. Another source of issues are two distinctive MSI properties `Privileged` and `AdminUser`. Because of late elevation, since Windows Vista values of these properties are spoofed when evaluation `LaunchConditions`. This may produce unexpected results with packages designed for previous operating systems.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/aa370556(v=vs.85).aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/aa369752(v=vs.85).aspx

Manual Remediation: Review all rows containing conditions that exclude the current operating system. Should the given component/action be required and function correctly on

Windows 10, rewrite the condition so that it evaluates to true or remove it to always install the questionable resource. Do not use `AdminUser` property, because it may impact installation flows that elevate at some later point of installation. Legacy distinction between `Privileged` and AdminUser property can be restored by using the `MSIREALADMINDETECTION` property.

T108 - Deprecated and Obsolete API Calls

Description: RayQC Advanced scans the MSI package for a presence of API calls that are deprecated or obsolete. Internal database is used to assess each API call being used.

Background: Certain APIs present in previous versions of Microsoft Windows are now officially deprecated or obsoleted by Microsoft. Obsolete APIs may not work anymore, or their behavior may be different leading to unexpected results. The deprecated APIs may be still working, but there is no guarantee they will function correctly or at all after any update or security patch. Usually, there is a replacement API that should be used in favor of deprecated or obsolete API call.

More Information: None available.

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should not use obsolete functions anymore and switch to replacements as described by Microsoft in Microsoft SDK Updates.

T109 - Hard-Coded Resources and System Paths

Description: RayQC Advanced scans the MSI package for a usage of changed or obsolete junction points in INI files, registry entries, services, shortcuts, environment variables and custom actions.

Background: Since Microsoft Windows Vista, standard locations where user and system data are stored have been changed. For example, the root folder for user data was called "`Documents and Settings`" in Windows XP, but since Windows Vista its name is "Users". To provide a backward compatibility, junction points are used to reroute the calls from old, incorrect locations to the new, proper ones. A package that runs on various target systems should not rely on hard-coded paths, because they may be not valid anymore or for a given system language.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/bb968829(v=vs.85).aspx

http://msdn.microsoft.com/en-us/library/windows/desktop/aa368977(v=vs.85).aspx

Manual Remediation: Hard-coded paths should not be used. Replace them with MSI properties using formatted syntax. If no predefined property exists, the path should be exposed via custom MSI property so that it can be adjusted on demand from command-line / MST transform.

T110 - Mismatched Target Architecture

Description: RayQC Advanced scans the MSI package for the presence of executables (16 / 32 / 64-bit) that are not compatible with Windows 10 32-bit platform.

Background: Some software is intended to run only in 32-bit or 64-bit operating systems. 16-bit executables are not supported on modern platforms, and 64-bit Microsoft Windows can correctly emulate 32-bit applications. If the MSI package is missing a correct Launch Condition it may try to install executables that are not designed for the current platform architecture.

Attempting to launch such executable might result in an error message that the file is not a valid Win32 application. Additionally, attempting to run 16-bit code may result in a warning message informing that an extra Windows Feature is required.

More Information: http://support.microsoft.com/kb/282423/en-us

Manual Remediation: Contact the manufacturer to obtain compatible software. Reenginer self-developed software by replacing 16-bit executables with appropriate 32- or 64-bit code. Use Launch Conditions and component conditions to control to which platform software and its parts are deployed.

T111 - Drivers Issues

Description: RayQC Advanced scans the MSI package for the presence of drivers containing no valid signature or not matching the target platform.

Background: Since Windows Vista 64-bit, all drivers have to be signed. Signed driver contains an extra digital signature used to validate the source and content of the driver package. Any unauthorized change in the driver package invalidates the signature. If an unsigned driver or a driver with invalid signature is attempted to be installed, Windows refuses the installation. Likewise, each driver has to match the target platform, which means that 64-bit systems require 64-bit drivers.

More Information: http://msdn.microsoft.com/en-us/library/bb756937.aspx

Manual Remediation: Contact the manufacturer to obtain compatible driver. Use WDK (Windows Driver Kit) to sign self-developed driver packages.

T112 - Installation Package Design Issues

Description: RayQC Advanced scans the MSI package for the presence of common installation design issues that may cause troubles during installation or using of software. The context of **Custom Actions** is scanned for the presence of deferred **Custom Actions** running in user-context, as well as system-wide actions running in immediate mode. The presence of conflicting permissions tables preventing the installation is detected as well. Additionally, invalid combinations of user- and machine-data in a single component and invalid identifiers are reported.

Background: Microsoft recommends several best-practices approaches for MSI setup designers. They ensure that the package is deployed correctly in various scenarios and various operating systems. By following the guidelines many compatibility issues introduced by a new security model in Windows Vista can be avoided.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/aa368268%28v=vs.85%29.aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/aa368268(v=vs.85).aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/dd408053(v=vs.85).aspx
http://msdn.microsoft.com/en-us/library/6397xx85(v=vs.80).aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/aa368994%28v=vs.85%29.aspx

Manual Remediation: Adjust the package content so that it complies to the best practices of Windows Installer. Do not mix per-machine and per-user data in a single component. Use valid

identifiers for components. Make sure all custom actions are running in a valid context - all actions making system changes must be deferred in execution. Do not use both `LockPermissions` and `MsiLockPermissionsEx` tables at once.

T113 - Conflicts with Protected Windows Resources (WRP)

Description: RayQC Advanced scans the MSI package for the presence of files and registry keys that belong to the Windows Resource Protection list.

Background: Windows Resource Protection (WRP) prevents the modification of essential system resources (files, folders and registry keys). Windows Installer silently ignores any attempt to update or modify them, any other software trying to do it may fail. These kinds of resources may be only updated by Microsoft-provided redistributable packages. During the installation, if Windows Installer logging is enabled, a warning may be shown for each operation that was ignored because of the WRP protection.

More Information: http://msdn.microsoft.com/en-us/library/bb756998.aspx

Manual Remediation: Assess whether the conflicting resources are actually needed, and if not remove them from the MSI package. If a given resource is needed and the original system one cannot be used, consider reenginering the application or use any virtualization technique to override the resource.

T114 - Missing or Invalid Signatures

Description: RayQC Advanced scans the MSI package for the presence of unsigned executable files (`.exe`, `.dll`, `.ocx`). Additionally, the package itself and CAB files are also scanned.

Background: According to the set of best practices by Microsoft, all exerctuable files deployed by an installation package and the installation package itself should be digitally signed with a certificate issued by a Trusted Publisher. When attempting to run an unsigned executable, Windows prompts the user for authorization. Similarly, attempting to install an unsigned MSI package also shows the Windows prompt.

More Information: http://technet.microsoft.com/en-us/library/cc962053.aspx

Manual Remediation: Contact the manufacturer to obtain signed executables and installers. Use WDK (Windows Driver Kit) to sign self-developed executables and packages.

T115 - Security and User Access Control Issues

Description: RayQC Advanced scans the MSI package for the presence of issues that may fail to work due to the security features. The executable files are scanned for the presence of correct manifestation. Direct calls to rundll32 are reported, because the UAC prompt hides the actual calling module when rundll32 is executed. Interactive services running in session 0 are detected, as well as MMC snap-ins that are not DEP-aware. Finally, setups, updaters and uninstallers are detected and checked for the presence of their UAC awareness.

Background: Session 0 isolation and Data Execution Prevention (DEP) are examples of security improvements introduced to prevent malicious software from compromising the security of the operating systems. They provide a separation between interactive user sessions and non-interactive session 0 devoted for services, and prevent execution of code from non-executable memory region. Modern software has to comply to these restrictions in order to function correctly on Windows 10. Another security issue present in Windows operating system is User Account Control (UAC). When an executable file requires additional non-standard permissions, the UAC elevation dialog prompts for confirmation or for correct credentials. The UAC prompt

contains information about calling application, manufacturer and the source. Certain applications, like self-updaters, setups and other requiring higher privileges must be aware of the elevation, and use manifests to correctly inform the system about required execution permissions.

More Information: http://msdn.microsoft.com/en-us/windows/hardware/gg463353
http://msdn.microsoft.com/en-us/library/bb963893.aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/aa366553(v=vs.85).aspx
http://technet.microsoft.com/en-us/library/cc709628%28WS.10%29.aspx

Manual Remediation: Contact the manufacturer to obtain software that complies to the security features of Microsoft Windows. For each unmanifested executable file, create a manifest, and set the required privileges to "`asInvoker`" for applications not requiring them, and "`requireAdministrator`" or "`highestAvailable`" for others. If the manifest cannot be corrected, a shim database has to be used to specify the desired privilege level.

T116 - Missing Application Manifest or Insufficient Execution Policy

Description: RayQC Advanced scans the MSI package for the presence of executabl files (`.exe`, `.cpl`) that do not contain the manifest, or that are not aware of Windows 10 in the list of supported operating systems in their manifest files.

Background: Since Windows Vista, all applications run by default with standard user privileges. This is also true when the current user is a member of Administrators group. Application that used to work on previous versions of Windows may fail to work, as no elevation will take place. In order to require higher permissions, each executable or control panel applications has to contain a manifest file - a simple `.xml` file informing the operating system how to handle the given program.

More Information: http://msdn.microsoft.com/en-us/library/Aa480152%23appcomp_topic30.com#appcomp_topic4
http://msdn.microsoft.com/en-us/library/hh848036%28v=vs.85%29.aspx

Manual Remediation: Create a manifest file for each executable. To manifest a control panel application (`.cpl`) create an executable wrapper with embedded manifest. Use the SupportedOS section in the manifest to define the list of supported operating systems.

T117 - Incomplete Reboot Handling

Description: RayQC Advanced scans the MSI package for the absence of a proper launch condition preventing the installation if a reboot is pending. Additionally, the absence of the **Files in use** dialog is detected. The presence of the `ForceReboot` action is also detected and reported.

Background: Windows Installer supports natively various set of features and actions related to the reboot handling. They include for example the ability to show list of used/locked files, forcing or skipping the reboot and determining the installation state by the related MSI properties. Several aspects have to be considered so that the reboot handling works as expected.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/aa368607(v=vs.85).aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/aa370492(v=vs.85).aspx

> http://msdn.microsoft.com/en-us/library/windows/desktop/
> aa370379(v=vs.85).aspx

Manual Remediation: Add the `MSIRMFilesInUse` dialog to the dialog sequence if it is missing. Remove `ForceReboot` action from the sequence, reboots are handled automatically by MSI. In order to ensure the package is not installed when any reboot is pending, append the "`NOT MsiSystemRebootPending`" condition to the Launch Condition list

T118 - Protected Mode (Internet Explorer)

Description: RayQC Advanced scans the MSI package for the presence of registry entries that disable **Protected mode**.

Background: As a result of security changes introduced in Windows Vista, Internet Explorer runs now in a isolated mode called **Protected mode** by default. While it limits potential damages malware application can cause, it also prevents web-applications running in Internet Explorer from writing directly to disk while in Internet or Intranet zone. Internet Explorer warns when web-application tries to run certain software programs or write to protected areas.

More Information: http://msdn.microsoft.com/en-us/library/bb756991.aspx

Manual Remediation: Contact the manufacturer to obtain compatible software. Reengineer self-developed software so that it runs correctly under **Protected mode**, or add the required website(s) to the list of trusted sites.

Windows Server 2008

Below are the set of rules which can be used to test a package for deployment on Windows Server 2008

T101 - Known Compatibility Issues at Startup (AppHelp)

Description: RayQC Advanced scans the package for the presence of applications that may trigger Application Help Dialog (AppHelp) when the program is being installed or run for the first time.

Background: Certain applications are known to cause issues or not even starting on modern operating systems. Windows contains a predefined list of software known to have compatibility issues and warns or prevents user from starting the application. The list of such applications is stored in a central compatibility database, and the dialog shown to the user is known as Application Help (AppHelp).

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/
bb756937.aspx

Manual Remediation: Contact the manufacturer to obtain compatible software.

T102 - Deprecated Windows Features

Description: RayQC Advanced scans the MSI package for the presence of deprecated features: embedded installations of another MSI packages (Custom Actions type 7, 23, 39), NETDDE-dependencies in registry, deprecated proxy configuration component `ProxyCfg.exe`.

Background: Certain features present in previous versions of Windows systems are officially deprecated by Microsoft. This means they are provided as-is. These features may be still

working, but there is no guarantee they will function correctly or at all after any update or security patch. Usually, there is a replacement technology that should be used in favor of deprecated features.

More Information: http://msdn.microsoft.com/en-us/library/aa368010%28v=VS.85%29.aspx
http://msdn.microsoft.com/en-us/library/bb756977.aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/
aa384069(v=vs.85).aspx

Manual Remediation: Do not use use Custom Actions type 7, 23 and 39 anymore. Dependencies and prerequisites have to be installed and managed by the deployment tool or external setup wrapper. The deprecated components have to be replaced. Contact the manufacturer to obtain compatible software.

T103 - Obsolete Windows Features

Description: RayQC Advanced scans the MSI package for a presence of deprecated MSGina technology, as well as for a presence of file extensions, for which the handling application has been obsoleted.

Background: Certain features present in previous versions of Windows systems are officially marked as obsolete by Microsoft. This means they are not supported anymore and any functionality relying on them is likely to fail to operate. Usually, there is a replacement technology that should be used in favor of deprecated features.

More Information: http://msdn.microsoft.com/en-us/library/bb756900.aspx
http://technet.microsoft.com/en-en/library/ee681703(v=ws.10).aspx

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software using the `MSGina.dll` should be re-engineered and use the Credential Providers model. Obsolete extensions should not be used in MSI installer packages.

T104 - Windows Shell and User Experience Changes

Description: RayQC Advanced scans the MSI package for a presence of shortcuts created in Quick Launch and subfolders of the SendTo folder.

Background: Each version of Microsoft Windows system introduces enhancements and changes of the user experience in the way Windows Shell is working and organizing files, shortcuts, context menu actions etc. Certain aspects of the user experience vary between newer version of Windows. There is a different handling for certain behaviors that were possible before. For example, shortcuts placed in subfolders of the SendTo folder are not displayed anymore. Finally, Quick Launch Bar feature is not present anymore.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/
cc144179(v=vs.85).aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/
jj584985(v=vs.85).aspx

Manual Remediation: Avoid deploying shortcuts to Quick Launch location and to subfolders of SendTo folder.

T105 - Unsupported Windows Components

Description: RayQC Advanced scans the MSI package for a presence of applications using DHTML control and for the presence of 32-bit `.hlp` files.

Background: Certain functionalities and components present in Windows XP and previous systems are not anymore part of the standard OS image. Since then Microsoft offers them as downloadable add-ons wich restore the missing functionality. On a standard system however, missing handlers/opening applications may cause runtime exceptions or other warnings. Typical examples of such components are viewers for 32-bit `.hlp` files, missing DHTLM editor controls and so on.

More Information: http://support.microsoft.com/kb/917607
http://msdn.microsoft.com/en-us/library/aa663363.aspx

Manual Remediation: Contact the manufacturer to obtain compatible software. You may also install the missing components - the update KB917607 restores the ability to view 32-bit .hlp files, and the redistributable installer `DHTMLEd.msi` from Microsoft installs the missing DHTML control.

T106 - .NET Framework Compatibility

Description: RayQC Advanced scans the MSI package for a presence of applications using .NET Framework 1.0 or 1.1.

Background: Since Windows 7, .NET Framework 1.0 and 1.1 are not supported. Although it may be possible to deploy deprecated .NET components, there is no support for these configurations provided by Microsoft.

More Information: http://support.microsoft.com/kb/2489698

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should be converted to .NET Framework 4.5.

T107 - Conditional Installation and Execution

Description: RayQC Advanced scans the MSI package for a presence of conditions that vary based on the value of properties: `VersionNT`, `VersionNT64`, `WindowsBuild` and `ServicePackLevel`. Additionally, the content of the package is scanned for the usage of `AdminUser` and `Privileged` properties in Launch Conditions and components condition to verify they will not cause issues with permission elevation. Merge modules, 16-bit components and certain conditions may neutralize otherwise failing conditions.

Background: Number of MSI properties like `VersionNT`, `VersionNT64`, `ServicePackLevel` etc. can be used to conditionally control the flow of installation and set of features/components/policies to be installed. Software vendors use them frequently in critical places like LaunchConditions, conditions for components and Custom Actions, conditional security policies and many more. When a new version of Operating System is introduced, these conditions have to be reviewed, because they may generate false warnings even though the software is functioning correctly. Another source of issues are two distinctive MSI properties `Privileged` and `AdminUser`. Because of late elevation, since Windows Vista values of these properties are spoofed when evaluating LaunchConditions. This may produce unexpected results with packages designed for previous operating systems.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/aa370556(v=vs.85).aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/aa369752(v=vs.85).aspx

Manual Remediation: Review all rows containing conditions that exclude the current operating system. Should the given component/action be required and function correctly on

Windows Server 2008, rewrite the condition so that it evaluates to true or remove it to always install the questionable resource. Do not use `AdminUser` property, because it may impact installation flows that elevate at some later point of installation. Legacy distinction between Provileged and AdminUser property can be restored by using the `MSIREALADMINDETECTION` property.

T108 - Deprecated and Obsolete API Calls

Description: RayQC Advanced scans the MSI package for a presence of API calls that are deprecated or obsolete. Internal database is used to assess each API call being used.

Background: Certain APIs present in previous versions of Microsoft Windows are now officially deprecated or obsoleted by Microsoft. Obsolete APIs may not work anymore, or their behavior may be different leading to unexpected results. The deprecated APIs may be still working, but there is no guarantee they will function correctly or at all after any update or security patch. Usually, there is a replacement API that should be used in favor of deprecated or obsolete API call.

More Information: None available.

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should not use obsolete functions anymore and switch to replacements as described by Microsoft in Microsoft SDK Updates.

T109 - Hard-Coded Resources and System Paths

Description: RayQC Advanced scans the MSI package for a usage of changed or obsolete junction points in INI files, registry entries, services, shortcuts, environment variables and custom actions.

Background: Since Microsoft Windows Vista, standard locations where user and system data are stored have been changed. For example, the root folder for user data was called "Documents and Settings" in Windows XP, but since Windows Vista its name is "Users". To provide a backward compatibility, junction points are used to reroute the calls from old, incorrect locations to the new, proper ones. A package that runs on various target systems should not rely on hard-coded paths, because they may be not valid anymore or for a given system language.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/bb968829(v=vs.85).aspx

http://msdn.microsoft.com/en-us/library/windows/desktop/aa368977(v=vs.85).aspx

Manual Remediation: Hard-coded paths should not be used. Replace them with MSI properties using formatted syntax. If no predefined property exists, the path should be exposed via custom MSI property so that it can be adjusted on demand from command-line / MST transform.

T110 - Mismatched Target Architecture

Description: RayQC Advanced scans the MSI package for the presence of executables (16/32/64-bit) that are not compatible with Windows Server 2008.

Background: Some software is intended to run only in 32-bit or 64-bit operating systems. 16-bit executables are not supported on modern platforms, and 64-bit Microsoft Windows can correctly emulate 32-bit applications. If the MSI package is missing a correct Launch Condition

it may try to install executables that are not designed for the current platform architecture. Attempting to launch such executable might result in an error message that the file is not a valid Win32 application. Additionally, attempting to run 16-bit code may result in a warning message informing that an extra Windows Feature is required.

More Information: http://support.microsoft.com/kb/282423/en-us

Manual Remediation: Contact the manufacturer to obtain compatible software. Re-engineer self-developed software by replacing 16-bit executables with appropriate 32- or 64-bit code. Use Launch Conditions and component conditions to control to which platform software and its parts are deployed.

T111 - Installation Package Design Issues

Description: RayQC Advanced scans the MSI package for the presence of drivers containing no valid signature or not matching the target platform.

Background: Since Windows Vista 64-bit, all drivers have to be signed. Signed driver contains an extra digital signature used to validate the source and content of the driver package. Any unauthorized change in the driver package invalidates the signature. If an unsigned driver or a driver with invalid signature is attempted to be installed, Windows refuses the installation. Likewise, each driver has to match the target platform, which means that 64-bit systems require 64-bit drivers.

More Information: http://msdn.microsoft.com/en-us/library/bb756937.aspx

Manual Remediation: Contact the manufacturer to obtain compatible driver. Use WDK (Windows Driver Kit) to sign self-developed driver packages.

T112 - Installation Package Design Issues

Description: RayQC Advanced scans the MSI package for the presence of common installation design issues that may cause troubles during installation or using of software. The context of Custom Actions is scanned for the presence of deferred custom actions running in user-context, as well as system-wide actions running in immediate mode. The presence of conflicting permissions tables preventing the installation is detected as well. Additionally, invalid combinations of user- and machine-data in a single component and invalid identifiers are reported.

Background: Microsoft recommends several best-practices approaches for MSI setup designers. They ensure that the package is deployed correctly in various scenarios and various operating systems. By following the guidelines many compatibility issues introduced by a new security model in Windows Vista can be avoided.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/aa368268%28v=vs.85%29.aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/aa368268(v=vs.85).aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/dd408053(v=vs.85).aspx
http://msdn.microsoft.com/en-us/library/6397xx85(v=vs.80).aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/aa368994%28v=vs.85%29.aspx

Manual Remediation: Adjust the package content so that it complies to the best practices of

Windows Installer. Do not mix per-machine and per-user data in a single component. Use valid identifiers for components. Make sure all custom actions are running in a valid context - all actions making system changes must be deferred in execution. Do not use both `LockPermissions` and `MsiLockPermissionsEx` tables at once.

T113 - Conflicts with Protected Windows Resources (WRP)

Description: RayQC Advanced scans the MSI package for the presence of files and registry keys that belong to the Windows Resource Protection list.

Background: Windows Resource Protection (WRP) prevents the modification of essential system resources (files, folders and registry keys). Windows Installer silently ignores any attempt to update or modify them, any other software trying to do it may fail. These kinds of resources may be only updated by Microsoft-provided redistributable packages. During the installation, if Windows Installer logging is enabled, a warning may be shown for each operation that was ignored because of the WRP protection.

More Information: http://msdn.microsoft.com/en-us/library/bb756998.aspx

Manual Remediation: Assess whether the conflicting resources are actually needed, and if not remove them from the MSI package. If a given resource is needed and the original system one cannot be used, consider re-engineering the application or use any virtualization technique to override the resource.

T114 - Missing or Invalid Signatures

Description: RayQC Advanced scans the MSI package for the presence of unsigned executable files (`.exe`, `.dll`, `.ocx`). Additionally, the package itself and CAB files are also scanned.

Background: According to the set of best practices by Microsoft, all exercutable files deployed by an installation package and the installation package itself should be digitally signed with a certificate issued by a Trusted Publisher. When attempting to run an unsigned executable, Windows prompts the user for authorization. Similarly, attempting to install an unsigned MSI package also shows the Windows prompt.

More Information: http://technet.microsoft.com/en-us/library/cc962053.aspx

Manual Remediation: Contact the manufacturer to obtain signed executables and installers. Use WDK (Windows Driver Kit) to sign self-developed executables and packages.

T115 - Security and User Access Control Issues

Description: RayQC Advanced scans the MSI package for the presence of issues that may fail to work due to the security features. The executable files are scanned for the presence of correct manifestation. Direct calls to rundll32 are reported, because the UAC prompt hides the actual calling module when rundll32 is executed. Interactive sevices running in session 0 are detected, as well as MMC snap-ins that are not DEP-aware. Finally, setups, updaters and uninstallers are detecteded and checked for the presence of their UAC awareness.

Background: Session 0 isolation and Data Execution Prevention (DEP) are examples of security improvements introduced to prevent malcious software from compromising the security of the operating systems. They provide a separation between interactive user sessions and non-interactive session 0 devoted for services, and prevent execution of code from non-executable memory region. Modern software has to comply to these restrictions in order to function correctly on Windows Server 2008. Another security issue present in Windows operating system is User Account Control (UAC). When an executable file requires additional non-

standard permissions, the UAC elevation dialog prompts for confirmation or for correct credentials. The UAC prompt contains information about calling application, manufacturer and the source. Certain applications, like self-updaters, setups and other requiring higher privileges must be aware of the elevation, and use manifests to correctly inform the system about required execution permissions.

More Information: http://msdn.microsoft.com/en-us/windows/hardware/gg463353
http://msdn.microsoft.com/en-us/library/bb963893.aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/aa366553(v=vs.85).aspx
http://technet.microsoft.com/en-us/library/cc709628%28WS.10%29.aspx
http://technet.microsoft.com/en-us/library/cc709628%28WS.10%29.aspx

Manual Remediation: Contact the manufacturer to obtain software that complies to the security features of Microsoft Windows. For each unmanifested executable file, create a manifest, and set the required privileges to "`asInvoker`" for applications not requiring them, and "`requireAdministrator`" or "`highestAvailable`" for others. If the manifest cannot be corrected, a shim database has to be used to specify the desired privilege level.

T116 - Missing Application Manifest or Insufficient Execution Policy

Description: RayQC Advanced scans the MSI package for the presence of executable files (`.exe`, `.cpl`) that do not contain the manifest, or that are not aware of Windows Server 2008 in the list of supported operating systems in their manifest files.

Background: Since Windows Vista, all applications run by default with standard user privileges. This is also true when the current user is a member of Administrators group. Application that used to work on previous versions of Windows may fail to work, as no elevation will take place. In order to require higher permissions, each executable or control panel applications has to contain a manifest file - a simple `.XML` file informing the operating system how to handle the given program.

More Information: http://msdn.microsoft.com/en-us/library/Aa480152%23appcomp_topic30.com#appcomp_topic4
http://msdn.microsoft.com/en-us/library/hh848036%28v=vs.85%29.aspx

Manual Remediation: Create a manifest file for each executable. To manifest a control panel application (`.cpl`) create an executable wrapper with embedded manifest. Use the SupportedOS section in the manifest to define the list of supported operating systems.

T117 - Incomplete Reboot Handling

Description: RayQC Advanced scans the MSI package for the absence of a proper launch condition preventing the installation if a reboot is pending. Additionally, absence of "Files in use" dialog is detected. Presence of `ForceReboot` action is also detected and reported.

Background: Windows Installer supports natively various set of features and actions related to the reboot handling. They include for example the ability to show list of used/locked files, forcing or skipping the reboot and determining the installation state by the related MSI properties. Several aspects have to be considered so that the reboot handling works as expected.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/aa368607(v=vs.85).aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/

aa370492(v=vs.85).aspx

http://msdn.microsoft.com/en-us/library/windows/desktop/
aa370379(v=vs.85).aspx

Manual Remediation: Add the `MSIRMFilesInUse` dialog to the dialog sequence if it is missing. Remove ForceReboot action from the sequence, reboots are handled automatically by MSI. In order to ensure the package is not installed when any reboot is pending, append the "`NOT MsiSystemRebootPending`" condition to the Launch Condition list.

T118 - Protected Mode (internet Explorer)

Description: RayQC Advanced scans the MSI package for the presence of registry entries that disable Protected Mode.

Background: As a result of security changes introduced in Windows Vista, Internet Explorer runs now in a isolated mode called "Protected mode" by default. While it limits potential damages malware application can cause, it also prevents web-applications running in Internet Explorer from writing directly to disk while in Internet or Intranet zone. Internet Explorer warns when web-application tries to run certain software programs or write to protected areas.

More Information: http://msdn.microsoft.com/en-us/library/bb756991.aspx

Manual Remediation: Contact the manufacturer to obtain compatible software. Re-engineer self-developed software so that it runs correctly under Protected Mode, or add the required website(s) to the list of trusted sites

Windows Server 2008 R2

Below are the set of rules which can be used to test a package for deployment on Windows Server 2008 R2

T101 - Known Compatibility Issues at Startup (AppHelp)

Description: RayQC Advanced scans the package for the presence of applications that may trigger Application Help Dialog (AppHelp) when the program is being installed or run for the first time.

Background: Certain applications are known to cause issues or not even starting on modern operating systems. Windows contains a predefined list of software known to have compatibility issues and warns or prevents user from starting the application. The list of such applications is stored in a central compatibility database, and the dialog shown to the user is known as Application Help (AppHelp).

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/
bb756937.aspx

Manual Remediation: Contact the manufacturer to obtain compatible software.

T102 - Deprecated Windows Features

Description: RayQC Advanced scans the MSI package for the presence of deprecated features: embedded installations of another MSI packages (Custom Actions type 7, 23, 39), NETDDE-dependencies in registry, deprecated proxy configuration component `ProxyCfg.exe`.

Background: Certain features present in previous versions of Windows systems are officially deprecated by Microsoft. This means they are provided as-is. These features may be still working, but there is no guarantee they will function correctly or at all after any update or security patch. Usually, there is a replacement technology that should be used in favor of deprecated features.

More Information: http://msdn.microsoft.com/en-us/library/aa368010%28v=VS.85%29.aspx
http://msdn.microsoft.com/en-us/library/bb756977.aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/aa384069(v=vs.85).aspx

Manual Remediation: Do not use use Custom Actions type 7, 23 and 39 anymore. Dependencies and prerequisites have to be installed and managed by the deployment tool or external setup wrapper. The deprecated components have to be replaced. Contact the manufacturer to obtain compatible software.

T103 - Obsolete Windows Features

Description: RayQC Advanced scans the MSI package for a presence of deprecated MSGina technology, as well as for a presence of file extensions, for which the handling application has been obsoleted.

Background: Certain features present in previous versions of Windows systems are officially marked as obsolete by Microsoft. This means they are not supported anymore and any functionality relying on them is likely to fail to operate. Usually, there is a replacement technology that should be used in favor of deprecated features.

More Information: http://msdn.microsoft.com/en-us/library/bb756900.aspx
http://technet.microsoft.com/en-en/library/ee681703(v=ws.10).aspx

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software using the `MSGina.dll` should be re-engineered and use the Credential Providers model. Obsolete extensions should not be used in MSI installer packages.

T104 - Windows Shell and User Experience Changes

Description: RayQC Advanced scans the MSI package for a presence of shortcuts created in Quick Launch and subfolders of the SendTo folder.

Background: Each version of Microsoft Windows system introduces enhancements and changes of the user experience in the way Windows Shell is working and organizing files, shortcuts, context menu actions etc. Certain aspects of the user experience vary between newer version of Windows. There is a different handling for certain behaviors that were possible before. For example, shortcuts placed in subfolders of the SendTo folder are not displayed anymore. Finally, Quick Launch Bar feature is not present anymore.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/cc144179(v=vs.85).aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/jj584985(v=vs.85).aspx

Manual Remediation: Avoid deploying shortcuts to Quick Launch location and to subfolders of SendTo folder.

T105 - Unsupported Windows Components

Description: RayQC Advanced scans the MSI package for a presence of applications using DHTML control and for the presence of 32-bit `.hlp` files.

Background: Certain functionalities and components present in Windows XP and previous systems are not anymore part of the standard OS image. Since then Microsoft offers them as downloadable add-ons wich restore the missing functionality. On a standard system however, missing handlers/opening applications may cause runtime exceptions or other warnings. Typical examples of such components are viewers for 32-bit `.hlp` files, missing DHTLM editor controls and so on.

More Information: http://support.microsoft.com/kb/917607
http://msdn.microsoft.com/en-us/library/aa663363.aspx

Manual Remediation: Contact the manufacturer to obtain compatible software. You may also install the missing components - the update KB917607 restores the ability to view 32-bit .hlp files, and the redistributable installer `DHTMLEd.msi` from Microsoft installs the missing DHTML control.

T106 - .NET Framework Compatibility

Description: RayQC Advanced scans the MSI package for a presence of applications using .NET Framework 1.0 or 1.1.

Background: Since Windows 7, .NET Framework 1.0 and 1.1 are not supported. Although it may be possible to deploy deprecated .NET components, there is no support for these configurations provided by Microsoft.

More Information: http://support.microsoft.com/kb/2489698

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should be converted to .NET Framework 4.5.

T107 - Conditional Installation and Execution

Description: RayQC Advanced scans the MSI package for a presence of conditions that vary based on the value of properties: `VersionNT`, `VersionNT64`, `WindowsBuild` and `ServicePackLevel`. Additionally, the content of the package is scanned for the usage of `AdminUser` and `Privileged` properties in Launch Conditions and components condition to verify they will not cause issues with permission elevation. Merge modules, 16-bit components and certain conditions may neutralize otherwise failing conditions.

Background: Number of MSI properties like `VersionNT`, `VersionNT64`, `ServicePackLevel` etc. can be used to conditionally control the flow of installation and set of features/components/policies to be installed. Software vendors use them frequently in critical places like LaunchConditions, conditions for components and Custom Actions, conditional security policies and many more. When a new version of Operating System is introduced, these conditions have to be reviewed, because they may generate false warnings even though the software is functioning correctly. Another source of issues are two distinctive MSI properties `Privileged` and `AdminUser`. Because of late elevation, since Windows Vista values of these properties are spoofed when evaluating LaunchConditions. This may produce unexpected results with packages designed for previous operating systems.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/aa370556(v=vs.85).aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/aa369752(v=vs.85).aspx

Manual Remediation: Review all rows containing conditions that exclude the current operating system. Should the given component/action be required and function correctly on Windows Server 2008, rewrite the condition so that it evaluates to true or remove it to always install the questionable resource. Do not use `AdminUser` property, because it may impact installation flows that elevate at some later point of installation. Legacy distinction between Provileged and AdminUser property can be restored by using the `MSIREALADMINDETECTION` property.

T108 - Deprecated and Obsolete API Calls

Description: RayQC Advanced scans the MSI package for a presence of API calls that are deprecated or obsolete. Internal database is used to assess each API call being used.

Background: Certain APIs present in previous versions of Microsoft Windows are now officially deprecated or obsoleted by Microsoft. Obsolete APIs may not work anymore, or their behavior may be different leading to unexpected results. The deprecated APIs may be still working, but there is no guarantee they will function correctly or at all after any update or security patch. Usually, there is a replacement API that should be used in favor of deprecated or obsolete API call.

More Information: None available.

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should not use obsolete functions anymore and switch to replacements as described by Microsoft in Microsoft SDK Updates.

T109 - Hard-Coded Resources and System Paths

Description: RayQC Advanced scans the MSI package for a usage of changed or obsolete junction points in INI files, registry entries, services, shortcuts, environment variables and custom actions.

Background: Since Microsoft Windows Vista, standard locations where user and system data are stored have been changed. For example, the root folder for user data was called "Documents and Settings" in Windows XP, but since Windows Vista its name is "Users". To provide a backward compatibility, junction points are used to reroute the calls from old, incorrect locations to the new, proper ones. A package that runs on various target systems should not rely on hard-coded paths, because they may be not valid anymore or for a given system language.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/bb968829(v=vs.85).aspx

http://msdn.microsoft.com/en-us/library/windows/desktop/aa368977(v=vs.85).aspx

Manual Remediation: Hard-coded paths should not be used. Replace them with MSI properties using formatted syntax. If no predefined property exists, the path should be exposed via custom MSI property so that it can be adjusted on demand from command-line / MST transform.

T110 - Mismatched Target Architecture

Description: RayQC Advanced scans the MSI package for the presence of executables (16/32/64-bit) that are not compatible with Windows Server 2008.

Background: Some software is intended to run only in 32-bit or 64-bit operating systems. 16-

bit executables are not supported on modern platforms, and 64-bit Microsoft Windows can correctly emulate 32-bit applications. If the MSI package is missing a correct Launch Condition it may try to install executables that are not designed for the current platform architecture. Attempting to launch such executable might result in an error message that the file is not a valid Win32 application. Additionally, attempting to run 16-bit code may result in a warning message informing that an extra Windows Feature is required.

More Information: http://support.microsoft.com/kb/282423/en-us

Manual Remediation: Contact the manufacturer to obtain compatible software. Re-engineer self-developed software by replacing 16-bit executables with appropriate 32- or 64-bit code. Use Launch Conditions and component conditions to control to which platform software and its parts are deployed.

T111 - Installation Package Design Issues

Description: RayQC Advanced scans the MSI package for the presence of drivers containing no valid signature or not matching the target platform.

Background: Since Windows Vista 64-bit, all drivers have to be signed. Signed driver contains an extra digital signature used to validate the source and content of the driver package. Any unauthorized change in the driver package invalidates the signature. If an unsigned driver or a driver with invalid signature is attempted to be installed, Windows refuses the installation. Likewise, each driver has to match the target platform, which means that 64-bit systems require 64-bit drivers.

More Information: http://msdn.microsoft.com/en-us/library/bb756937.aspx

Manual Remediation: Contact the manufacturer to obtain compatible driver. Use WDK (Windows Driver Kit) to sign self-developed driver packages.

T112 - Installation Package Design Issues

Description: RayQC Advanced scans the MSI package for the presence of common installation design issues that may cause troubles during installation or using of software. The context of Custom Actions is scanned for the presence of deferred custom actions running in user-context, as well as system-wide actions running in immediate mode. The presence of conflicting permissions tables preventing the installation is detected as well. Additionally, invalid combinations of user- and machine-data in a single component and invalid identifiers are reported.

Background: Microsoft recommends several best-practices approaches for MSI setup designers. They ensure that the package is deployed correctly in various scenarios and various operating systems. By following the guidelines many compatibility issues introduced by a new security model in Windows Vista can be avoided.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/aa368268%28v=vs.85%29.aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/aa368268(v=vs.85).aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/dd408053(v=vs.85).aspx
http://msdn.microsoft.com/en-us/library/6397xx85(v=vs.80).aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/aa368994%28v=vs.85%29.aspx

Manual Remediation: Adjust the package content so that it complies to the best practices of Windows Installer. Do not mix per-machine and per-user data in a single component. Use valid identifiers for components. Make sure all custom actions are running in a valid context - all actions making system changes must be deferred in execution. Do not use both `LockPermissions` and `MsiLockPermissionsEx` tables at once.

T113 - Conflicts with Protected Windows Resources (WRP)

Description: RayQC Advanced scans the MSI package for the presence of files and registry keys that belong to the Windows Resource Protection list.

Background: Windows Resource Protection (WRP) prevents the modification of essential system resources (files, folders and registry keys). Windows Installer silently ignores any attempt to update or modify them, any other software trying to do it may fail. These kinds of resources may be only updated by Microsoft-provided redistributable packages. During the installation, if Windows Installer logging is enabled, a warning may be shown for each operation that was ignored because of the WRP protection.

More Information: http://msdn.microsoft.com/en-us/library/bb756998.aspx

Manual Remediation: Assess whether the conflicting resources are actually needed, and if not remove them from the MSI package. If a given resource is needed and the original system one cannot be used, consider re-engineering the application or use any virtualization technique to override the resource.

T114 - Missing or Invalid Signatures

Description: RayQC Advanced scans the MSI package for the presence of unsigned executable files (`.exe`, `.dll`, `.ocx`). Additionally, the package itself and CAB files are also scanned.

Background: According to the set of best practices by Microsoft, all exercutable files deployed by an installation package and the installation package itself should be digitally signed with a certificate issued by a Trusted Publisher. When attempting to run an unsigned executable, Windows prompts the user for authorization. Similarly, attempting to install an unsigned MSI package also shows the Windows prompt.

More Information: http://technet.microsoft.com/en-us/library/cc962053.aspx

Manual Remediation: Contact the manufacturer to obtain signed executables and installers. Use WDK (Windows Driver Kit) to sign self-developed executables and packages.

T115 - Security and User Access Control Issues

Description: RayQC Advanced scans the MSI package for the presence of issues that may fail to work due to the security features. The executable files are scanned for the presence of correct manifestation. Direct calls to rundll32 are reported, because the UAC prompt hides the actual calling module when rundll32 is executed. Interactive sevices running in session 0 are detected, as well as MMC snap-ins that are not DEP-aware. Finally, setups, updaters and uninstallers are detecteded and checked for the presence of their UAC awareness.

Background: Session 0 isolation and Data Execution Prevention (DEP) are examples of security improvements introduced to prevent malcious software from compromising the security of the operating systems. They provide a separation between interactive user sessions and non-interactive session 0 devoted for services, and prevent execution of code from non-executable memory region. Modern software has to comply to these restrictions in order to function correctly on Windows Server 2008. Another security issue present in Windows operating

system is User Account Control (UAC). When an executable file requires additional non-standard permissions, the UAC elevation dialog prompts for confirmation or for correct credentials. The UAC prompt contains information about calling application, manufacturer and the source. Certain applications, like self-updaters, setups and other requiring higher privileges must be aware of the elevation, and use manifests to correctly inform the system about required execution permissions.

More Information: http://msdn.microsoft.com/en-us/windows/hardware/gg463353
http://msdn.microsoft.com/en-us/library/bb963893.aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/
aa366553(v=vs.85).aspx
http://technet.microsoft.com/en-us/library/cc709628%28WS.10%29.aspx
http://technet.microsoft.com/en-us/library/cc709628%28WS.10%29.aspx

Manual Remediation: Contact the manufacturer to obtain software that complies to the security features of Microsoft Windows. For each unmanifested executable file, create a manifest, and set the required privileges to "`asInvoker`" for applications not requiring them, and "`requireAdministrator`" or "`highestAvailable`" for others. If the manifest cannot be corrected, a shim database has to be used to specify the desired privilege level.

T116 - Missing Application Manifest or Insufficient Execution Policy

Description: RayQC Advanced scans the MSI package for the presence of executable files (`.exe`, `.cpl`) that do not contain the manifest, or that are not aware of Windows Server 2008 in the list of supported operating systems in their manifest files.

Background: Since Windows Vista, all applications run by default with standard user privileges. This is also true when the current user is a member of Administrators group. Application that used to work on previous versions of Windows may fail to work, as no elevation will take place. In order to require higher permissions, each executable or control panel applications has to contain a manifest file - a simple `.XML` file informing the operating system how to handle the given program.

More Information: http://msdn.microsoft.com/en-us/library/Aa480152%
23appcomp_topic30.com#appcomp_topic4
http://msdn.microsoft.com/en-us/library/hh848036%28v=vs.85%29.aspx

Manual Remediation: Create a manifest file for each executable. To manifest a control panel application (`.cpl`) create an executable wrapper with embedded manifest. Use the SupportedOS section in the manifest to define the list of supported operating systems.

T117 - Incomplete Reboot Handling

Description: RayQC Advanced scans the MSI package for the absence of a proper launch condition preventing the installation if a reboot is pending. Additionally, absence of "Files in use" dialog is detected. Presence of `ForceReboot` action is also detected and reported.

Background: Windows Installer supports natively various set of features and actions related to the reboot handling. They include for example the ability to show list of used/locked files, forcing or skipping the reboot and determining the installation state by the related MSI properties. Several aspects have to be considered so that the reboot handling works as expected.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/
aa368607(v=vs.85).aspx

http://msdn.microsoft.com/en-us/library/windows/desktop/
aa370492(v=vs.85).aspx

http://msdn.microsoft.com/en-us/library/windows/desktop/
aa370379(v=vs.85).aspx

Manual Remediation: Add the `MSIRMFilesInUse` dialog to the dialog sequence if it is missing. Remove ForceReboot action from the sequence, reboots are handled automatically by MSI. In order to ensure the package is not installed when any reboot is pending, append the "`NOT MsiSystemRebootPending`" condition to the Launch Condition list.

T118 - Protected Mode (internet Explorer)

Description: RayQC Advanced scans the MSI package for the presence of registry entries that disable Protected Mode.

Background: As a result of security changes introduced in Windows Vista, Internet Explorer runs now in a isolated mode called "Protected mode" by default. While it limits potential damages malware application can cause, it also prevents web-applications running in Internet Explorer from writing directly to disk while in Internet or Intranet zone. Internet Explorer warns when web-application tries to run certain software programs or write to protected areas.

More Information: http://msdn.microsoft.com/en-us/library/bb756991.aspx

Manual Remediation: Contact the manufacturer to obtain compatible software. Re-engineer self-developed software so that it runs correctly under Protected Mode, or add the required website(s) to the list of trusted sites

Windows Server 2012

Below are the set of rules which can be used to test a package for deployment on Windows Server 2012

T101 - Known Compatibility Issues at Startup (AppHelp)

Description: RayQC Advanced scans the package for the presence of applications that may trigger Application Help Dialog (AppHelp) when the program is being installed or run for the first time.

Background: Certain applications are known to cause issues or not even starting on modern operating systems. Windows contains a predefined list of software known to have compatibility issues and warns or prevents user from starting the application. The list of such applications is stored in a central compatibility database, and the dialog shown to the user is known as Application Help (AppHelp).

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/
bb756937.aspx

Manual Remediation: Contact the manufacturer to obtain compatible software.

T102 - Deprecated Windows Features

Description: RayQC Advanced scans the MSI package for the presence of deprecated features: embedded installations of another MSI packages (Custom Actions type 7, 23, 39), NETDDE-dependencies in registry, deprecated proxy configuration component `ProxyCfg.exe` and

Windows Library files.

Background: Certain features present in previous versions of Windows systems are officially deprecated by Microsoft. This means they are provided as-is. These features may be still working, but there is no guarantee they will function correctly or at all after any update or security patch. Usually, there is a replacement technology that should be used in favor of deprecated features.

More Information: http://msdn.microsoft.com/en-us/library/aa368010%28v=VS.85%29.aspx
http://msdn.microsoft.com/en-us/library/bb756977.aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/
aa384069(v=vs.85).aspx

Manual Remediation: Do not use use Custom Actions type 7, 23 and 39 anymore. Dependencies and prerequisites have to be installed and managed by the deployment tool or external setup wrapper. The deprecated components have to be replaced. Contact the manufacturer to obtain compatible software.

T103 - Obsolete Windows Features

Description: RayQC Advanced scans the MSI package for a presence of deprecated MSGina technology, as well as for a presence of file extensions, for which the handling application has been obsoleted.

Background: Certain features present in previous versions of Windows systems are officially marked as obsolete by Microsoft. This means they are not supported anymore and any functionality relying on them is likely to fail to operate. Usually, there is a replacement technology that should be used in favor of deprecated features.

More Information: http://msdn.microsoft.com/en-us/library/bb756900.aspx
http://technet.microsoft.com/en-en/library/ee681703(v=ws.10).aspx

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software using the `MSGina.dll` should be re-engineered and use the Credential Providers model. Obsolete extensions should not be used in MSI installer packages.

T104 - Windows Shell and User Experience Changes

Description: RayQC Advanced scans the MSI package for a presence of shortcuts created in Quick Launch and subfolders of the SendTo folder. Additionally, start menu shortcuts pointing to non-executable files will be detected. Finally, RayQC Advanced scans the MSI package for a presence of Windows Gadgets.

Background: Each version of Microsoft Windows system introduces enhancements and changes of the user experience in the way Windows Shell is working and organizing files, shortcuts, context menu actions etc. Certain aspects of the user experience vary between newer version of Windows, with the introduction of Modern Start Screen being a notable example. There is a different handling for certain behaviors that were possible before. For example, the new Start Screen does not pin non-executable files by default, and due to the deprecated tree-like structure certain shortcuts names may be duplicated and thus confusing. Another example are shortcuts placed in subfolders of the SendTo folder, which are not displayed anymore. Finally, features like Quick Launch Bar and Windows Desktop Gadgets layer are not present anymore.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/

cc144179(v=vs.85).aspx

> http://msdn.microsoft.com/en-us/library/windows/desktop/
> jj584985(v=vs.85).aspx

Manual Remediation: Avoid deploying shortcuts to Quick Launch location and to subfolders of SendTo folder. Migrate to the Modern application to allow pinning ups and running them in a gadget-mode. Rename Start menu shortcuts to unequivocally express their purpose and associated action, instead of using generic names like "Readme" or "Help". Non-executable files should be manually pinned by the logged on user.

T105 - Unsupported Windows Components

Description: RayQC Advanced scans the MSI package for a presence of applications using DHTML control and for the presence of 32-bit `.hlp` files.

Background: Certain functionalities and components present in Windows XP and previous systems are not anymore part of the standard OS image. Since then Microsoft offers them as downloadable add-ons wich restore the missing functionality. On a standard system however, missing handlers/opening applications may cause runtime exceptions or other warnings. Typical examples of such components are viewers for 32-bit `.hlp` files, missing DHTLM editor controls and so on.

More Information: http://support.microsoft.com/kb/917607

> http://msdn.microsoft.com/en-us/library/aa663363.aspx

Manual Remediation: Contact the manufacturer to obtain compatible software. You may also install the missing components - the update KB917607 restores the ability to view 32-bit `.hlp` files, and the redistributable installer `DHTMLEd.msi` from Microsoft installs the missing DHTML control.

T106 - .NET Framework Compatibility

Description: RayQC Advanced scans the MSI package for a presence of applications using .NET Framework 1.0, 1.1, 2.0, 3.0 or 3.5.

Background: Since Windows 7, .NET Framework 1.0 and 1.1 are not supported. Although it may be possible to deploy deprecated .NET components, there is no support for these configurations provided by Microsoft. Additionally .NET Framework 2.0, 3.0 and 3.5 is not included in the default configuration of Windows 8 and later operating systems, so applications that require one of these frameworks might trigger a request for installing the necessary files.

More Information: http://support.microsoft.com/kb/2489698

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should be converted to .NET Framework 4.5.

T107 - Conditional Installation and Execution

Description: RayQC Advanced scans the MSI package for a presence of conditions that vary based on the value of properties: `VersionNT`, `VersionNT64`, `WindowsBuild` and `ServicePackLevel`. Additionally, the content of the package is scanned for the usage of `AdminUser` and `Privileged` properties in Launch Conditions and components condition to verify they will not cause issues with permission elevation. Merge modules, 16-bit components and certain conditions may neutralize otherwise failing conditions.

Background: Number of MSI properties like `VersionNT`, `VersionNT64`, `ServicePackLevel`

etc. can be used to conditionally control the flow of installation and set of features/ components/policies to be installed. Software vendors use them frequently in critical places like LaunchConditions, conditions for components and Custom Actions, conditional security policies and many more. When a new version of Operating System is introduced, these conditions have to be reviewed, because they may generate false warnings even though the software is functioning correctly. Another source of issues are two distinctive MSI properties `Privileged` and `AdminUser`. Because of late elevation, since Windows Vista values of these properties are spoofed when evaluating LaunchConditions. This may produce unexpected results with packages designed for previous operating systems.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/ aa370556(v=vs.85).aspx

> http://msdn.microsoft.com/en-us/library/windows/desktop/ aa369752(v=vs.85).aspx

Manual Remediation: Review all rows containing conditions that exclude the current operating system. Should the given component/action be required and function correctly on Windows Server 2012, rewrite the condition so that it evaluates to true or remove it to always install the questionable resource. Do not use `AdminUser` property, because it may impact installation flows that elevate at some later point of installation. Legacy distinction between `Privileged` and `AdminUser` property can be restored by using the `MSIREALADMINDETECTION` property.

T108 - Deprecated and Obsolete API Calls

Description: RayQC Advanced scans the MSI package for a usage of changed or obsolete junction points in INI files, registry entries, services, shortcuts, environment variables and custom actions.

Background: Certain APIs present in previous versions of Microsoft Windows are now officially deprecated or obsoleted by Microsoft. Obsolete APIs may not work anymore, or their behavior may be different leading to unexpected results. The deprecated APIs may be still working, but there is no guarantee they will function correctly or at all after any update or security patch. Usually, there is a replacement API that should be used in favor of deprecated or obsolete API call.

More Information: None available.

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should not use obsolete functions anymore and switch to replacements as described by Microsoft in Microsoft SDK Updates.

T109 - Hard-Coded Resources and System Paths

Description: RayQC Advanced scans the MSI package for a usage of changed or obsolete junction points in INI files, registry entries, services, shortcuts, environment variables and custom actions.

Background: Since Microsoft Windows Vista, standard locations where user and system data are stored have been changed. For example, the root folder for user data was called "Documents and Settings" in Windows XP, but since Windows Vista its name is "Users". To provide a backward compatibility, junction points are used to reroute the calls from old, incorrect locations to the new, proper ones. A package that runs on various target systems should not rely on hard-coded paths, because they may be not valid anymore or for a given system language.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/
bb968829(v=vs.85).aspx

> http://msdn.microsoft.com/en-us/library/windows/desktop/
> aa368977(v=vs.85).aspx

Manual Remediation: Hard-coded paths should not be used. Replace them with MSI properties using formatted syntax. If no predefined property exists, the path should be exposed via custom MSI property so that it can be adjusted on demand from command-line / MST transform.

T110 - Mismatched Target Architecture

Description: RayQC Advanced scans the MSI package for the presence of executables (16/32/64-bit) that are not compatible with Windows Server 2012 platform.

Background: Some software is intended to run only in 32-bit or 64-bit operating systems. 16-bit executables are not supported on modern platforms, and 64-bit Microsoft Windows can correctly emulate 32-bit applications. If the MSI package is missing a correct Launch Condition it may try to install executables that are not designed for the current platform architecture. Attempting to launch such executable might result in an error message that the file is not a valid Win32 application. Additionally, attempting to run 16-bit code may result in a warning message informing that an extra Windows Feature is required.

More Information: http://support.microsoft.com/kb/282423/en-us

Manual Remediation: Contact the manufacturer to obtain compatible software. Reenginer self-developed software by replacing 16-bit executables with appropriate 32- or 64-bit code. Use Launch Conditions and component conditions to control to which platform software and its parts are deployed.

T111 - Driver Issues

Description: RayQC Advanced scans the MSI package for the presence of drivers containing no valid signature or not matching the target platform.

Background: Since Windows Vista 64-bit, all drivers have to be signed. Signed driver contains an extra digital signature used to validate the source and content of the driver package. Any unauthorized change in the driver package invalidates the signature. If an unsigned driver or a driver with invalid signature is attempted to be installed, Windows refuses the installation. Likewise, each driver has to match the target platform, which means that 64-bit systems require 64-bit drivers.

More Information: http://msdn.microsoft.com/en-us/library/bb756937.aspx

Manual Remediation: Contact the manufacturer to obtain compatible driver. Use WDK (Windows Driver Kit) to sign self-developed driver packages.

T112 - Installation Package Design Issues

Description: RayQC Advanced scans the MSI package for the presence of common installation design issues that may cause troubles during installation or using of software. The context of Custom Actions is scanned for the presence of deferred custom actions running in user-context, as well as system-wide actions running in immediate mode. The presence of conflicting permissions tables preventing the installation is detected as well. Additionally, invalid combinations of user- and machine-data in a single component and invalid identifiers are reported.

Background: Microsoft recommends several best-practices approaches for MSI setup designers. They ensure that the package is deployed correctly in various scenarios and various operating systems. By following the guidelines many compatibility issues introduced by a new security model in Windows Vista can be avoided.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/aa368268%28v=vs.85%29.aspx

> http://msdn.microsoft.com/en-us/library/windows/desktop/aa368268(v=vs.85).aspx
> http://msdn.microsoft.com/en-us/library/windows/desktop/dd408053(v=vs.85).aspx
> http://msdn.microsoft.com/en-us/library/6397xx85(v=vs.80).aspx
> http://msdn.microsoft.com/en-us/library/windows/desktop/aa368994%28v=vs.85%29.aspx

Manual Remediation: Adjust the package content so that it complies to the best practices of Windows Installer. Do not mix per-machine and per-user data in a single component. Use valid identifiers for components. Make sure all custom actions are running in a valid context - all actions making system changes must be deferred in execution. Do not use both `LockPermissions` and `MsiLockPermissionsEx` tables at once.

T113 - Installation Package Design Issues

Description: RayQC Advanced scans the MSI package for the presence of files and registry keys that belong to the Windows Resource Protection list.

Background: Windows Resource Protection (WRP) prevents the modification of essential system resources (files, folders and registry keys). Windows Installer silently ignores any attempt to update or modify them, any other software trying to do it may fail. These kinds of resources may be only updated by Microsoft-provided redistributable packages. During the installation, if Windows Installer logging is enabled, a warning may be shown for each operation that was ignored because of the WRP protection.

More Information: http://msdn.microsoft.com/en-us/library/bb756998.aspx

Manual Remediation: Assess whether the conflicting resources are actually needed, and if not remove them from the MSI package. If a given resource is needed and the original system one cannot be used, consider re-engineering the application or use any virtualization technique to override the resource.

T114 - Missing or invalid Signatures

Description: RayQC Advanced scans the MSI package for the presence of unsigned executable files (`.exe`, `.dll`, `.ocx`). Additionally, the package itself and CAB files are also scanned.

Background: According to the set of best practices by Microsoft, all exerctuable files deployed by an installation package and the installation package itself should be digitally signed with a certificate issued by a Trusted Publisher. When attempting to run an unsigned executable, Windows prompts the user for authorization. Similarly, attempting to install an unsigned MSI package also shows the Windows prompt.

More Information: http://technet.microsoft.com/en-us/library/cc962053.aspx

Manual Remediation: Contact the manufacturer to obtain signed executables and installers. Use WDK (Windows Driver Kit) to sign self-developed executables and packages.

T115 - Security and User Access Control Issues

Description: RayQC Advanced scans the MSI package for the presence of issues that may fail to work due to the security features. The executable files are scanned for the presence of correct manifestation. Direct calls to rundll32 are reported, because the UAC prompt hides the actual calling module when rundll32 is executed. Interactive sevices running in session 0 are detected, as well as MMC snap-ins that are not DEP-aware. Finally, setups, updaters and uninstallers are detecteded and checked for the presence of their UAC awareness.

Background: Session 0 isolation and Data Execution Prevention (DEP) are examples of security improvements introduced to prevent malcious software from compromising the security of the operating systems. They provide a separation between interactive user sessions and non-interactive session 0 devoted for services, and prevent execution of code from non-executable memory region. Modern software has to comply to these restrictions in order to function correctly on Windows Server 2012. Another security issue present in Windows operating system is User Account Control (UAC). When an executable file requires additional non-standard permissions, the UAC elevation dialog prompts for confirmation or for correct credentials. The UAC prompt contains information about calling application, manufacturer and the source. Certain applications, like self-updaters, setups and other requiring higher privileges must be aware of the elevation, and use manifests to correctly inform the system about required execution permissions.

More Information: http://msdn.microsoft.com/en-us/windows/hardware/gg463353
http://msdn.microsoft.com/en-us/library/bb963893.aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/aa366553(v=vs.85).aspx
http://technet.microsoft.com/en-us/library/cc709628%28WS.10%29.aspx
http://technet.microsoft.com/en-us/library/cc709628%28WS.10%29.aspx

Manual Remediation: Contact the manufacturer to obtain software that complies to the security features of Microsoft Windows. For each unmanifested executable file, create a manifest, and set the required privileges to "`asInvoker`" for applications not requiring them, and "`requireAdministrator`" or "`highestAvailable`" for others. If the manifest cannot be corrected, a shim database has to be used to specify the desired privilege level.

T116 - Missing Application Manifest or Insufficient Execution Policy

Description: RayQC Advanced scans the MSI package for the presence of executable files (`.exe`, `.cpl`) that do not contain the manifest, or that are not aware of Windows Server 2012 in the list of supported operating systems in their manifest files.

Background: Since Windows Vista, all applications run by default with standard user privileges. This is also true when the current user is a member of Administrators group. Application that used to work on previous versions of Windows may fail to work, as no elevation will take place. In order to require higher permissions, each executable or control panel applications has to contain a manifest file - a simple `.XML` file informing the operating system how to handle the given program.

More Information: http://msdn.microsoft.com/en-us/library/Aa480152%23appcomp_topic30.com#appcomp_topic4
http://msdn.microsoft.com/en-us/library/hh848036%28v=vs.85%29.aspx

Manual Remediation: Create a manifest file for each executable. To manifest a control panel application (.cpl) create an executable wrapper with embedded manifest. Use the

SupportedOS section in the manifest to define the list of supported operating systems.

T117 - Incomplete Reboot Handling

Description: RayQC Advanced scans the MSI package for the absence of a proper launch condition preventing the installation if a reboot is pending. Additionally, absence of "Files in use" dialog is detected. Presence of `ForceReboot` action is also detected and reported.

Background: Windows Installer supports natively various set of features and actions related to the reboot handling. They i nclude for example the ability to show list of used/locked files, forcing or skipping the reboot and determining the installation state by the related MSI properties. Several aspects have to be considered so that the reboot handling works as expected.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/aa368607(v=vs.85).aspx

> http://msdn.microsoft.com/en-us/library/windows/desktop/aa370492(v=vs.85).aspx
> http://msdn.microsoft.com/en-us/library/windows/desktop/aa370379(v=vs.85).aspx

Manual Remediation: Add the MSIRMFilesInUse dialog to the dialog sequence if it is missing. Remove `ForceReboot` action from the sequence, reboots are handled automatically by MSI. In order to ensure the package is not installed when any reboot is pending, append the "`NOT MsiSystemRebootPending`" condition to the Launch Condition list.

T118 - Protected Mode (Internet Explorer)

Description: RayQC Advanced scans the MSI package for the presence of registry entries that disable Protected Mode.

Background: As a result of security changes introduced in Windows Vista, Internet Explorer runs now in a isolated mode called "Protected mode" by default. While it limits potential damages malware application can cause, it also prevents web-applications running in Internet Explorer from writing directly to disk while in Internet or Intranet zone. Internet Explorer warns when web-application tries to run certain software programs or write to protected areas.

More Information: http://msdn.microsoft.com/en-us/library/bb756991.aspx

Manual Remediation: Contact the manufacturer to obtain compatible software. Re-engineer self-developed software so that it runs correctly under Protected Mode, or add the required website(s) to the list of trusted sites.

Windows Server 2012 R2

Below are the set of rules which can be used to test a package for deployment on Windows Server 2012 R2

T101 - Known Compatibility Issues at Startup (AppHelp)

Description: RayQC Advanced scans the package for the presence of applications that may trigger Application Help Dialog (AppHelp) when the program is being installed or run for the first time.

Background: Certain applications are known to cause issues or not even starting on modern operating systems. Windows contains a predefined list of software known to have compatibility issues and warns or prevents user from starting the application. The list of such applications is stored in a central compatibility database, and the dialog shown to the user is known as Application Help (AppHelp).

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/bb756937.aspx

Manual Remediation: Contact the manufacturer to obtain compatible software.

T102 - Deprecated Windows Features

Description: RayQC Advanced scans the MSI package for the presence of deprecated features: embedded installations of another MSI packages (Custom Actions type 7, 23, 39), NETDDE-dependencies in registry, deprecated proxy configuration component `ProxyCfg.exe` and Windows Library files.

Background: Certain features present in previous versions of Windows systems are officially deprecated by Microsoft. This means they are provided as-is. These features may be still working, but there is no guarantee they will function correctly or at all after any update or security patch. Usually, there is a replacement technology that should be used in favor of deprecated features.

More Information: http://msdn.microsoft.com/en-us/library/aa368010%28v=VS.85%29.aspx
http://msdn.microsoft.com/en-us/library/bb756977.aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/aa384069(v=vs.85).aspx

Manual Remediation: Do not use use Custom Actions type 7, 23 and 39 anymore. Dependencies and prerequisites have to be installed and managed by the deployment tool or external setup wrapper. The deprecated components have to be replaced. Contact the manufacturer to obtain compatible software.

T103 - Obsolete Windows Features

Description: RayQC Advanced scans the MSI package for a presence of deprecated MSGina technology, as well as for a presence of file extensions, for which the handling application has been obsoleted.

Background: Certain features present in previous versions of Windows systems are officially marked as obsolete by Microsoft. This means they are not supported anymore and any functionality relying on them is likely to fail to operate. Usually, there is a replacement technology that should be used in favor of deprecated features.

More Information: http://msdn.microsoft.com/en-us/library/bb756900.aspx
http://technet.microsoft.com/en-en/library/ee681703(v=ws.10).aspx

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software using the `MSGina.dll` should be re-engineered and use the Credential Providers model. Obsolete extensions should not be used in MSI installer packages.

T104 - Windows Shell and User Experience Changes

Description: RayQC Advanced scans the MSI package for a presence of shortcuts created in Quick Launch and subfolders of the SendTo folder. Additionally, start menu shortcuts pointing

to non-executable files will be detected. Finally, RayQC Advanced scans the MSI package for a presence of Windows Gadgets.

Background: Each version of Microsoft Windows system introduces enhancements and changes of the user experience in the way Windows Shell is working and organizing files, shortcuts, context menu actions etc. Certain aspects of the user experience vary between newer version of Windows, with the introduction of Modern Start Screen being a notable example. There is a different handling for certain behaviors that were possible before. For example, the new Start Screen does not pin non-executable files by default, and due to the deprecated tree-like structure certain shortcuts names may be duplicated and thus confusing. Another example are shortcuts placed in subfolders of the SendTo folder, which are not displayed anymore. Finally, features like Quick Launch Bar and Windows Deskop Gadgets layer are not present anymore.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/cc144179(v=vs.85).aspx

> http://msdn.microsoft.com/en-us/library/windows/desktop/jj584985(v=vs.85).aspx

Manual Remediation: Avoid deploying shortcuts to Quick Launch location and to subfolders of SendTo folder. Migrate to the Modern application to allow pinning ups and running them in a gadget-mode. Rename Start menu shortcuts to unequivocally express their purpose and associated action, instead of using generic names like "Readme" or "Help". Non-executable files should be manually pinned by the logged on user.

T105 - Unsupported Windows Components

Description: RayQC Advanced scans the MSI package for a presence of applications using DHTML control and for the presence of 32-bit `.hlp` files.

Background: Certain functionalities and components present in Windows XP and previous systems are not anymore part of the standard OS image. Since then Microsoft offers them as downloadable add-ons wich restore the missing functionality. On a standard system however, missing handlers/opening applications may cause runtime exceptions or other warnings. Typical examples of such components are viewers for 32-bit `.hlp` files, missing DHTLM editor controls and so on.

More Information: http://support.microsoft.com/kb/917607 http://msdn.microsoft.com/en-us/library/aa663363.aspx

Manual Remediation: Contact the manufacturer to obtain compatible software. You may also install the missing components - the update KB917607 restores the ability to view 32-bit `.hlp` files, and the redistributable installer `DHTMLEd.msi` from Microsoft installs the missing DHTML control.

T106 - .NET Framework Compatibility

Description: RayQC Advanced scans the MSI package for a presence of applications using .NET Framework 1.0, 1.1, 2.0, 3.0 or 3.5.

Background: Since Windows 7, .NET Framework 1.0 and 1.1 are not supported. Although it may be possible to deploy deprecated .NET components, there is no support for these configurations provided by Microsoft. Additionally .NET Framework 2.0, 3.0 and 3.5 is not included in the default configuration of Windows 8 and later operating systems, so applications that require one of these frameworks might trigger a request for installing the necessary files.

More Information: http://support.microsoft.com/kb/2489698

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should be converted to .NET Framework 4.5.

T107 - Conditional Installation and Execution

Description: RayQC Advanced scans the MSI package for a presence of conditions that vary based on the value of properties: `VersionNT`, `VersionNT64`, `WindowsBuild` and `ServicePackLevel`. Additionally, the content of the package is scanned for the usage of `AdminUser` and `Privileged` properties in Launch Conditions and components condition to verify they will not cause issues with permission elevation. Merge modules, 16-bit components and certain conditions may neutralize otherwise failing conditions.

Background: Number of MSI properties like `VersionNT`, `VersionNT64`, `ServicePackLevel` etc. can be used to conditionally control the flow of installation and set of features/components/policies to be installed. Software vendors use them frequently in critical places like LaunchConditions, conditions for components and Custom Actions, conditional security policies and many more. When a new version of Operating System is introduced, these conditions have to be reviewed, because they may generate false warnings even though the software is functioning correctly. Another source of issues are two distinctive MSI properties `Privileged` and `AdminUser`. Because of late elevation, since Windows Vista values of these properties are spoofed when evaluating LaunchConditions. This may produce unexpected results with packages designed for previous operating systems.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/aa370556(v=vs.85).aspx

http://msdn.microsoft.com/en-us/library/windows/desktop/aa369752(v=vs.85).aspx

Manual Remediation: Review all rows containing conditions that exclude the current operating system. Should the given component/action be required and function correctly on Windows Server 2012 R2, rewrite the condition so that it evaluates to true or remove it to always install the questionable resource. Do not use AdminUser property, because it may impact installation flows that elevate at some later point of installation. Legacy distinction between `Privileged` and `AdminUser` property can be restored by using the `MSIREALADMINDETECTION` property.

T108 - Deprecated and Obsolete API Calls

Description: RayQC Advanced scans the MSI package for a presence of API calls that are deprecated or obsolete. Internal database is used to assess each API call being used.

Background: Certain APIs present in previous versions of Microsoft Windows are now officially deprecated or obsoleted by Microsoft. Obsolete APIs may not work anymore, or their behavior may be different leading to unexpected results. The deprecated APIs may be still working, but there is no guarantee they will function correctly or at all after any update or security patch. Usually, there is a replacement API that should be used in favor of deprecated or obsolete API call.

More Information: None available.

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should not use obsolete functions anymore and switch to replacements as described by Microsoft in Microsoft SDK Updates.

T109 - Hard-Coded Resources and System Paths

Description: RayQC Advanced scans the MSI package for a usage of changed or obsolete junction points in INI files, registry entries, services, shortcuts, environment variables and custom actions.

Background: Since Microsoft Windows Vista, standard locations where user and system data are stored have been changed. For example, the root folder for user data was called "Documents and Settings" in Windows XP, but since Windows Vista its name is "Users". To provide a backward compatibility, junction points are used to reroute the calls from old, incorrect locations to the new, proper ones. A package that runs on various target systems should not rely on hardcoded paths, because they may be not valid anymore or for a given system language.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/bb968829(v=vs.85).aspx

http://msdn.microsoft.com/en-us/library/windows/desktop/aa368977(v=vs.85).aspx

Manual Remediation: Hard-coded paths should not be used. Replace them with MSI properties using formatted syntax. If no predefined property exists, the path should be exposed via custom MSI property so that it can be adjusted on demand from command-line / MST transform.

T110 - Mismatched Target Architecture

Description: RayQC Advanced scans the MSI package for the presence of executables (16/32/64-bit) that are not compatible with Windows Server 2012 R2 32-bit platform

Background: Some software is intended to run only in 32-bit or 64-bit operating systems. 16-bit executables are not supported on modern platforms, and 64-bit Microsoft Windows can correctly emulate 32-bit applications. If the MSI package is missing a correct Launch Condition it may try to install executables that are not designed for the current platform architecture. Attempting to launch such executable might result in an error message that the file is not a valid Win32 application. Additionally, attempting to run 16-bit code may result in a warning message informing that an extra Windows Feature is required.

More Information: http://support.microsoft.com/kb/282423/en-us

Manual Remediation: Contact the manufacturer to obtain compatible software. Reenginer self-developed software by replacing 16-bit executables with appropriate 32- or 64-bit code. Use Launch Conditions and component conditions to control to which platform software and its parts are deployed.

T111 - Driver Issues

Description: RayQC Advanced scans the MSI package for the presence of drivers containing no valid signature or not matching the target platform.

Background: Since Windows Vista 64-bit, all drivers have to be signed. Signed driver contains an extra digital signature used to validate the source and content of the driver package. Any unauthorized change in the driver package invalidates the signature. If an unsigned driver or a driver with invalid signature is attempted to be installed, Windows refuses the installation. Likewise, each driver has to match the target platform, which means that 64-bit systems require 64-bit drivers.

More Information: http://msdn.microsoft.com/en-us/library/bb756937.aspx

Manual Remediation: Contact the manufacturer to obtain compatible driver. Use WDK (Windows Driver Kit) to sign self-developed driver packages.

T112 - Installation Package Design Issues

Description: RayQC Advanced scans the MSI package for the presence of common installation design issues that may cause troubles during installation or using of software. The context of Custom Actions is scanned for the presence of deferred custom actions running in user-context, as well as system-wide actions running in immediate mode. The presence of conflicting permissions tables preventing the installation is detected as well. Additionally, invalid combinations of user- and machine-data in a single component and invalid identifiers are reported.

Background: Microsoft recommends several best-practices approaches for MSI setup designers. They ensure that the package is deployed correctly in various scenarios and various operating systems. By following the guidelines many compatibility issues introduced by a new security model in Windows Vista can be avoided.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/aa368268%28v=vs.85%29.aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/aa368268(v=vs.85).aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/dd408053(v=vs.85).aspx
http://msdn.microsoft.com/en-us/library/6397xx85(v=vs.80).aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/aa368994%28v=vs.85%29.aspx

Manual Remediation: Adjust the package content so that it complies to the best practices of Windows Installer. Do not mix per-machine and per-user data in a single component. Use valid identifiers for components. Make sure all custom actions are running in a valid context - all actions making system changes must be deferred in execution. Do not use both `LockPermissions` and `MsiLockPermissionsEx` tables at once.

T113 - Conflicts with Protected Windows Resources (WRP)

Description: RayQC Advanced scans the MSI package for the presence of files and registry keys that belong to the Windows Resource Protection list.

Background: Windows Resource Protection (WRP) prevents the modification of essential system resources (files, folders and registry keys). Windows Installer silently ignores any attempt to update or modify them, any other software trying to do it may fail. These kinds of resources may be only updated by Microsoft-provided redistributable packages. During the installation, if Windows Installer logging is enabled, a warning may be shown for each operation that was ignored because of the WRP protection.

More Information: http://msdn.microsoft.com/en-us/library/bb756998.aspx

Manual Remediation: Assess whether the conflicting resources are actually needed, and if not remove them from the MSI package. If a given resource is needed and the original system one cannot be used, consider re-engineering the application or use any virtualization technique to override the resource.

T114 - Missing or Invalid Signatures

Description: RayQC Advanced scans the MSI package for the presence of unsigned executable files (`.exe`, `.dll`, `.ocx`). Additionally, the package itself and CAB files are also scanned.

Background: According to the set of best practices by Microsoft, all exercutable files deployed by an installation package and the installation package itself should be digitally signed with a certificate issued by a Trusted Publisher. When attempting to run an unsigned executable, Windows prompts the user for authorization. Similarly, attempting to install an unsigned MSI package also shows the Windows prompt.

More Information: http://technet.microsoft.com/en-us/library/cc962053.aspx

Manual Remediation: Contact the manufacturer to obtain signed executables and installers. Use WDK (Windows Driver Kit) to sign self-developed executables and packages.

T115 - Security and User Access Control Issues

Description: RayQC Advanced scans the MSI package for the presence of issues that may fail to work due to the security features. The executable files are scanned for the presence of correct manifestation. Direct calls to rundll32 are reported, because the UAC prompt hides the actual calling module when rundll32 is executed. Interactive sevices running in session 0 are detected, as well as MMC snap-ins that are not DEP-aware. Finally, setups, updaters and uninstallers are detecteded and checked for the presence of their UAC awareness.

Background: Session 0 isolation and Data Execution Prevention (DEP) are examples of security improvements introduced to prevent malicious software from compromising the security of the operating systems. They provide a separation between interactive user sessions and non-interactive session 0 devoted for services, and prevent execution of code from non-executable memory region. Modern software has to comply to these restrictions in order to function correctly on Windows Server 2012 R2. Another security issue present in Windows operating system is User Account Control (UAC). When an executable file requires additional non-standard permissions, the UAC elevation dialog prompts for confirmation or for correct credentials. The UAC prompt contains information about calling application, manufacturer and the source. Certain applications, like self-updaters, setups and other requiring higher privileges must be aware of the elevation, and use manifests to correctly inform the system about required execution permissions.

More Information: http://msdn.microsoft.com/en-us/windows/hardware/gg463353
http://msdn.microsoft.com/en-us/library/bb963893.aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/
aa366553(v=vs.85).aspx
http://technet.microsoft.com/en-us/library/cc709628%28WS.10%29.aspx
http://technet.microsoft.com/en-us/library/cc709628%28WS.10%29.aspx

Manual Remediation: Contact the manufacturer to obtain software that complies to the security features of Microsoft Windows. For each unmanifested executable file, create a manifest, and set the required privileges to "`asInvoker`" for applications not requiring them, and "`requireAdministrator`" or "`highestAvailable`" for others. If the manifest cannot be corrected, a shim database has to be used to specify the desired privilege level.

T116 - Missing Application Manifest or Insufficient Execution Policy

Description: RayQC Advanced scans the MSI package for the presence of executable files (`.exe`, `.cpl`) that do not contain the manifest, or that are not aware of Windows Server 2012 R2

in the list of supported operating systems in their manifest files.

Background: Since Windows Vista, all applications run by default with standard user privileges. This is also true when the current user is a member of Administrators group. Application that used to work on previous versions of Windows may fail to work, as no elevation will take place. In order to require higher permissions, each executable or control panel applications has to contain a manifest file - a simple `.XML` file informing the operating system how to handle the given program.

More Information: http://msdn.microsoft.com/en-us/library/Aa480152%
23appcomp_topic30.com#appcomp_topic4
http://msdn.microsoft.com/en-us/library/hh848036%28v=vs.85%29.aspx

Manual Remediation: Create a manifest file for each executable. To manifest a control panel application (.cpl) create an executable wrapper with embedded manifest. Use the SupportedOS section in the manifest to define the list of supported operating systems.

T117 - Incomplete Reboot Handling

Description: RayQC Advanced scans the MSI package for the absence of a proper launch condition preventing the installation if a reboot is pending. Additionally, absence of "Files in use" dialog is detected. Presence of `ForceReboot` action is also detected and reported.

Background: Windows Installer supports natively various set of features and actions related to the reboot handling. They include for example the ability to show list of used/locked files, forcing or skipping the reboot and determining the installation state by the related MSI properties. Several aspects have to be considered so that the reboot handling works as expected.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/
aa368607(v=vs.85).aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/
aa370492(v=vs.85).aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/
aa370379(v=vs.85).aspx

Manual Remediation: Add the `MSIRMFilesInUse` dialog to the dialog sequence if it is missing. Remove `ForceReboot` action from the sequence, reboots are handled automatically by MSI. In order to ensure the package is not installed when any reboot is pending, append the `"NOT MsiSystemRebootPending"` condition to the Launch Condition list.

T118 - Protected Mode (Internet Explorer)

Description: RayQC Advanced scans the MSI package for the presence of registry entries that disable Protected Mode.

Background: As a result of security changes introduced in Windows Vista, Internet Explorer runs now in a isolated mode called "Protected mode" by default. While it limits potential damages malware application can cause, it also prevents web-applications running in Internet Explorer from writing directly to disk while in Internet or Intranet zone. Internet Explorer warns when web-application tries to run certain software programs or write to protected areas.

More Information: http://msdn.microsoft.com/en-us/library/bb756991.aspx

Manual Remediation: Contact the manufacturer to obtain compatible software. Re-engineer self-developed software so that it runs correctly under Protected Mode, or add the required

website(s) to the list of trusted sites.

Windows Server 2016

Below are the set of rules which can be used to test a package for deployment on Windows Server 2016

T101 - Known Compatibility Issues at Startup (AppHelp)

Description: RayQC Advanced scans the package for the presence of applications that may trigger Application Help Dialog (AppHelp) when the program is being installed or run for the first time.

Background: Certain applications are known to cause issues or not even starting on modern operating systems. Windows contains a predefined list of software known to have compatibility issues and warns or prevents user from starting the application. The list of such applications is stored in a central compatibility database, and the dialog shown to the user is known as Application Help (AppHelp).

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/bb756937.aspx

Manual Remediation: Contact the manufacturer to obtain compatible software.

T102 - Deprecated Windows Features

Description: RayQC Advanced scans the MSI package for the presence of deprecated features: embedded installations of another MSI packages (Custom Actions type 7, 23, 39), NETDDE-dependencies in registry, deprecated proxy configuration component `ProxyCfg.exe` and Windows Library files.

Background: Certain features present in previous versions of Windows systems are officially deprecated by Microsoft. This means they are provided as-is. These features may be still working, but there is no guarantee they will function correctly or at all after any update or security patch. Usually, there is a replacement technology that should be used in favor of deprecated features.

More Information: http://msdn.microsoft.com/en-us/library/aa368010%28v=VS.85%29.aspx
http://msdn.microsoft.com/en-us/library/bb756977.aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/aa384069(v=vs.85).aspx

Manual Remediation: Do not use use Custom Actions type 7, 23 and 39 anymore. Dependencies and prerequisites have to be installed and managed by the deployment tool or external setup wrapper. The deprecated components have to be replaced. Contact the manufacturer to obtain compatible software.

T103 - Obsolete Windows Features

Description: RayQC Advanced scans the MSI package for a presence of deprecated MSGina technology, as well as for a presence of file extensions, for which the handling application has been obsoleted.

Background: Certain features present in previous versions of Windows systems are officially marked as obsolete by Microsoft. This means they are not supported anymore and any

---

functionality relying on them is likely to fail to operate. Usually, there is a replacement technology that should be used in favor of deprecated features.

More Information: http://msdn.microsoft.com/en-us/library/bb756900.aspx
http://technet.microsoft.com/en-en/library/ee681703(v=ws.10).aspx

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software using the `MSGina.dll` should be re-engineered and use the Credential Providers model. Obsolete extensions should not be used in MSI installer packages.

T104 - Windows Shell and User Experience Changes

Description: RayQC Advanced scans the MSI package for a presence of shortcuts created in Quick Launch and subfolders of the SendTo folder. Additionally, start menu shortcuts pointing to non-executable files will be detected. Finally, RayQC Advanced scans the MSI package for a presence of Windows Gadgets.

Background: Each version of Microsoft Windows system introduces enhancements and changes of the user experience in the way Windows Shell is working and organizing files, shortcuts, context menu actions etc. Certain aspects of the user experience vary between newer version of Windows, with the introduction of Modern Start Screen being a notable example. There is a different handling for certain behaviors that were possible before. For example, the new Start Screen does not pin non-executable files by default, and due to the deprecated tree-like structure certain shortcuts names may be duplicated and thus confusing. Another example are shortcuts placed in subfolders of the SendTo folder, which are not displayed anymore. Finally, features like Quick Launch Bar and Windows Deskop Gadgets layer are not present anymore.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/cc144179(v=vs.85).aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/jj584985(v=vs.85).aspx

Manual Remediation: Avoid deploying shortcuts to Quick Launch location and to subfolders of SendTo folder. Migrate to the Modern application to allow pinning ups and running them in a gadget-mode. Rename Start menu shortcuts to unequivocally express their purpose and associated action, instead of using generic names like "Readme" or "Help". Non-executable files should be manually pinned by the logged on user.

T105 - Unsupported Windows Components

Description: RayQC Advanced scans the MSI package for a presence of applications using DHTML control and for the presence of 32-bit `.hlp` files.

Background: Certain functionalities and components present in Windows XP and previous systems are not anymore part of the standard OS image. Since then Microsoft offers them as downloadable add-ons wich restore the missing functionality. On a standard system however, missing handlers/opening applications may cause runtime exceptions or other warnings. Typical examples of such components are viewers for 32-bit `.hlp` files, missing DHTLM editor controls and so on.

More Information: http://support.microsoft.com/kb/917607 http://msdn.microsoft.com/en-us/library/aa663363.aspx

Manual Remediation: Contact the manufacturer to obtain compatible software. You may also install the missing components - the update KB917607 restores the ability to view 32-bit `.hlp`

files, and the redistributable installer `DHTMLEd.msi` from Microsoft installs the missing DHTML control.

T106 - .NET Framework Compatibility

Description: RayQC Advanced scans the MSI package for a presence of applications using .NET Framework 1.0, 1.1, 2.0, 3.0 or 3.5.

Background: Since Windows 7, .NET Framework 1.0 and 1.1 are not supported. Although it may be possible to deploy deprecated .NET components, there is no support for these configurations provided by Microsoft. Additionally .NET Framework 2.0, 3.0 and 3.5 is not included in the default configuration of Windows 8 and later operating systems, so applications that require one of these frameworks might trigger a request for installing the necessary files.

More Information: http://support.microsoft.com/kb/2489698

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should be converted to .NET Framework 4.5.

T107 - Conditional Installation and Execution

Description: RayQC Advanced scans the MSI package for a presence of conditions that vary based on the value of properties: `VersionNT`, `VersionNT64`, `WindowsBuild` and `ServicePackLevel`. Additionally, the content of the package is scanned for the usage of `AdminUser` and `Privileged` properties in Launch Conditions and components condition to verify they will not cause issues with permission elevation. Merge modules, 16-bit components and certain conditions may neutralize otherwise failing conditions.

Background: Number of MSI properties like `VersionNT`, `VersionNT64`, `ServicePackLevel` etc. can be used to conditionally control the flow of installation and set of features/components/policies to be installed. Software vendors use them frequently in critical places like LaunchConditions, conditions for components and Custom Actions, conditional security policies and many more. When a new version of Operating System is introduced, these conditions have to be reviewed, because they may generate false warnings even though the software is functioning correctly. Another source of issues are two distinctive MSI properties `Privileged` and `AdminUser`. Because of late elevation, since Windows Vista values of these properties are spoofed when evaluating LaunchConditions. This may produce unexpected results with packages designed for previous operating systems.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/aa370556(v=vs.85).aspx

http://msdn.microsoft.com/en-us/library/windows/desktop/aa369752(v=vs.85).aspx

Manual Remediation: Review all rows containing conditions that exclude the current operating system. Should the given component/action be required and function correctly on Windows Server 2012 R2, rewrite the condition so that it evaluates to true or remove it to always install the questionable resource. Do not use AdminUser property, because it may impact installation flows that elevate at some later point of installation. Legacy distinction between `Privileged` and `AdminUser` property can be restored by using the `MSIREALADMINDETECTION` property.

T108 - Deprecated and Obsolete API Calls

Description: RayQC Advanced scans the MSI package for a presence of API calls that are deprecated or obsolete. Internal database is used to assess each API call being used.

Background: Certain APIs present in previous versions of Microsoft Windows are now officially deprecated or obsoleted by Microsoft. Obsolete APIs may not work anymore, or their behavior may be different leading to unexpected results. The deprecated APIs may be still working, but there is no guarantee they will function correctly or at all after any update or security patch. Usually, there is a replacement API that should be used in favor of deprecated or obsolete API call.

More Information: None available.

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should not use obsolete functions anymore and switch to replacements as described by Microsoft in Microsoft SDK Updates.

T109 - Hard-Coded Resources and System Paths

Description: RayQC Advanced scans the MSI package for a usage of changed or obsolete junction points in INI files, registry entries, services, shortcuts, environment variables and custom actions.

Background: Since Microsoft Windows Vista, standard locations where user and system data are stored have been changed. For example, the root folder for user data was called "Documents and Settings" in Windows XP, but since Windows Vista its name is "Users". To provide a backward compatibility, junction points are used to reroute the calls from old, incorrect locations to the new, proper ones. A package that runs on various target systems should not rely on hardcoded paths, because they may be not valid anymore or for a given system language.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/bb968829(v=vs.85).aspx

http://msdn.microsoft.com/en-us/library/windows/desktop/aa368977(v=vs.85).aspx

Manual Remediation: Hard-coded paths should not be used. Replace them with MSI properties using formatted syntax. If no predefined property exists, the path should be exposed via custom MSI property so that it can be adjusted on demand from command-line / MST transform.

T110 - Mismatched Target Architecture

Description: RayQC Advanced scans the MSI package for the presence of executables (16/32/64-bit) that are not compatible with Windows Server 2012 R2 32-bit platform

Background: Some software is intended to run only in 32-bit or 64-bit operating systems. 16-bit executables are not supported on modern platforms, and 64-bit Microsoft Windows can correctly emulate 32-bit applications. If the MSI package is missing a correct Launch Condition it may try to install executables that are not designed for the current platform architecture. Attempting to launch such executable might result in an error message that the file is not a valid Win32 application. Additionally, attempting to run 16-bit code may result in a warning message informing that an extra Windows Feature is required.

More Information: http://support.microsoft.com/kb/282423/en-us

Manual Remediation: Contact the manufacturer to obtain compatible software. Reenginer self-developed software by replacing 16-bit executables with appropriate 32- or 64-bit code. Use Launch Conditions and component conditions to control to which platform software and its parts are deployed.

T111 - Driver Issues

Description: RayQC Advanced scans the MSI package for the presence of drivers containing no valid signature or not matching the target platform.

Background: Since Windows Vista 64-bit, all drivers have to be signed. Signed driver contains an extra digital signature used to validate the source and content of the driver package. Any unauthorized change in the driver package invalidates the signature. If an unsigned driver or a driver with invalid signature is attempted to be installed, Windows refuses the installation. Likewise, each driver has to match the target platform, which means that 64-bit systems require 64-bit drivers.

More Information: http://msdn.microsoft.com/en-us/library/bb756937.aspx

Manual Remediation: Contact the manufacturer to obtain compatible driver. Use WDK (Windows Driver Kit) to sign self-developed driver packages.

T112 - Installation Package Design Issues

Description: RayQC Advanced scans the MSI package for the presence of common installation design issues that may cause troubles during installation or using of software. The context of Custom Actions is scanned for the presence of deferred custom actions running in user-context, as well as system-wide actions running in immediate mode. The presence of conflicting permissions tables preventing the installation is detected as well. Additionally, invalid combinations of user- and machine-data in a single component and invalid identifiers are reported.

Background: Microsoft recommends several best-practices approaches for MSI setup designers. They ensure that the package is deployed correctly in various scenarios and various operating systems. By following the guidelines many compatibility issues introduced by a new security model in Windows Vista can be avoided.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/aa368268%28v=vs.85%29.aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/aa368268(v=vs.85).aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/dd408053(v=vs.85).aspx
http://msdn.microsoft.com/en-us/library/6397xx85(v=vs.80).aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/aa368994%28v=vs.85%29.aspx

Manual Remediation: Adjust the package content so that it complies to the best practices of Windows Installer. Do not mix per-machine and per-user data in a single component. Use valid identifiers for components. Make sure all custom actions are running in a valid context - all actions making system changes must be deferred in execution. Do not use both `LockPermissions` and `MsiLockPermissionsEx` tables at once.

T113 - Conflicts with Protected Windows Resources (WRP)

Description: RayQC Advanced scans the MSI package for the presence of files and registry keys that belong to the Windows Resource Protection list.

Background: Windows Resource Protection (WRP) prevents the modification of essential system resources (files, folders and registry keys). Windows Installer silently ignores any

attempt to update or modify them, any other software trying to do it may fail. These kinds of resources may be only updated by Microsoft-provided redistributable packages. During the installation, if Windows Installer logging is enabled, a warning may be shown for each operation that was ignored because of the WRP protection.

More Information: http://msdn.microsoft.com/en-us/library/bb756998.aspx

Manual Remediation: Assess whether the conflicting resources are actually needed, and if not remove them from the MSI package. If a given resource is needed and the original system one cannot be used, consider re-engineering the application or use any virtualization technique to override the resource.

T114 - Missing or Invalid Signatures

Description: RayQC Advanced scans the MSI package for the presence of unsigned executable files (`.exe`, `.dll`, `.ocx`). Additionally, the package itself and CAB files are also scanned.

Background: According to the set of best practices by Microsoft, all exercutable files deployed by an installation package and the installation package itself should be digitally signed with a certificate issued by a Trusted Publisher. When attempting to run an unsigned executable, Windows prompts the user for authorization. Similarly, attempting to install an unsigned MSI package also shows the Windows prompt.

More Information: http://technet.microsoft.com/en-us/library/cc962053.aspx

Manual Remediation: Contact the manufacturer to obtain signed executables and installers. Use WDK (Windows Driver Kit) to sign self-developed executables and packages.

T115 - Security and User Access Control Issues

Description: RayQC Advanced scans the MSI package for the presence of issues that may fail to work due to the security features. The executable files are scanned for the presence of correct manifestation. Direct calls to rundll32 are reported, because the UAC prompt hides the actual calling module when rundll32 is executed. Interactive sevices running in session 0 are detected, as well as MMC snap-ins that are not DEP-aware. Finally, setups, updaters and uninstallers are detecteded and checked for the presence of their UAC awareness.

Background: Session 0 isolation and Data Execution Prevention (DEP) are examples of security improvements introduced to prevent malicious software from compromising the security of the operating systems. They provide a separation between interactive user sessions and non-interactive session 0 devoted for services, and prevent execution of code from non-executable memory region. Modern software has to comply to these restrictions in order to function correctly on Windows Server 2012 R2. Another security issue present in Windows operating system is User Account Control (UAC). When an executable file requires additional non-standard permissions, the UAC elevation dialog prompts for confirmation or for correct credentials. The UAC prompt contains information about calling application, manufacturer and the source. Certain applications, like self-updaters, setups and other requiring higher privileges must be aware of the elevation, and use manifests to correctly inform the system about required execution permissions.

More Information: http://msdn.microsoft.com/en-us/windows/hardware/gg463353
http://msdn.microsoft.com/en-us/library/bb963893.aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/aa366553(v=vs.85).aspx
http://technet.microsoft.com/en-us/library/cc709628%28WS.10%29.aspx

http://technet.microsoft.com/en-us/library/cc709628%28WS.10%29.aspx

Manual Remediation: Contact the manufacturer to obtain software that complies to the security features of Microsoft Windows. For each unmanifested executable file, create a manifest, and set the required privileges to "`asInvoker`" for applications not requiring them, and "`requireAdministrator`" or "`highestAvailable`" for others. If the manifest cannot be corrected, a shim database has to be used to specify the desired privilege level.

T116 - Missing Application Manifest or Insufficient Execution Policy

Description: RayQC Advanced scans the MSI package for the presence of executable files (`.exe`, `.cpl`) that do not contain the manifest, or that are not aware of Windows Server 2012 R2 in the list of supported operating systems in their manifest files.

Background: Since Windows Vista, all applications run by default with standard user privileges. This is also true when the current user is a member of Administrators group. Application that used to work on previous versions of Windows may fail to work, as no elevation will take place. In order to require higher permissions, each executable or control panel applications has to contain a manifest file - a simple `.XML` file informing the operating system how to handle the given program.

More Information: http://msdn.microsoft.com/en-us/library/Aa480152%
23appcomp_topic30.com#appcomp_topic4
http://msdn.microsoft.com/en-us/library/hh848036%28v=vs.85%29.aspx

Manual Remediation: Create a manifest file for each executable. To manifest a control panel application (.cpl) create an executable wrapper with embedded manifest. Use the SupportedOS section in the manifest to define the list of supported operating systems.

T117 - Incomplete Reboot Handling

Description: RayQC Advanced scans the MSI package for the absence of a proper launch condition preventing the installation if a reboot is pending. Additionally, absence of "Files in use" dialog is detected. Presence of `ForceReboot` action is also detected and reported.

Background: Windows Installer supports natively various set of features and actions related to the reboot handling. They include for example the ability to show list of used/locked files, forcing or skipping the reboot and determining the installation state by the related MSI properties. Several aspects have to be considered so that the reboot handling works as expected.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/
aa368607(v=vs.85).aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/
aa370492(v=vs.85).aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/
aa370379(v=vs.85).aspx

Manual Remediation: Add the `MSIRMFilesInUse` dialog to the dialog sequence if it is missing. Remove `ForceReboot` action from the sequence, reboots are handled automatically by MSI. In order to ensure the package is not installed when any reboot is pending, append the "`NOT MsiSystemRebootPending`" condition to the Launch Condition list.

T118 - Protected Mode (Internet Explorer)

Description: RayQC Advanced scans the MSI package for the presence of registry entries that

disable Protected Mode.

Background: As a result of security changes introduced in Windows Vista, Internet Explorer runs now in a isolated mode called "Protected mode" by default. While it limits potential damages malware application can cause, it also prevents web-applications running in Internet Explorer from writing directly to disk while in Internet or Intranet zone. Internet Explorer warns when web-application tries to run certain software programs or write to protected areas.

More Information: http://msdn.microsoft.com/en-us/library/bb756991.aspx

Manual Remediation: Contact the manufacturer to obtain compatible software. Re-engineer self-developed software so that it runs correctly under Protected Mode, or add the required website(s) to the list of trusted sites.

Windows Server 2019

Below are the set of rules which can be used to test a package for deployment on Windows Server 2016

T101 - Known Compatibility Issues at Startup (AppHelp)

Description: RayQC Advanced scans the package for the presence of applications that may trigger Application Help Dialog (AppHelp) when the program is being installed or run for the first time.

Background: Certain applications are known to cause issues or not even starting on modern operating systems. Windows contains a predefined list of software known to have compatibility issues and warns or prevents user from starting the application. The list of such applications is stored in a central compatibility database, and the dialog shown to the user is known as Application Help (AppHelp).

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/bb756937.aspx

Manual Remediation: Contact the manufacturer to obtain compatible software.

T102 - Deprecated Windows Features

Description: RayQC Advanced scans the MSI package for the presence of deprecated features: embedded installations of another MSI packages (Custom Actions type 7, 23, 39), NETDDE-dependencies in registry, deprecated proxy configuration component `ProxyCfg.exe` and Windows Library files.

Background: Certain features present in previous versions of Windows systems are officially deprecated by Microsoft. This means they are provided as-is. These features may be still working, but there is no guarantee they will function correctly or at all after any update or security patch. Usually, there is a replacement technology that should be used in favor of deprecated features.

More Information: http://msdn.microsoft.com/en-us/library/aa368010%28v=VS.85%29.aspx
http://msdn.microsoft.com/en-us/library/bb756977.aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/aa384069(v=vs.85).aspx

Manual Remediation: Do not use use Custom Actions type 7, 23 and 39 anymore.

Dependencies and prerequisites have to be installed and managed by the deployment tool or external setup wrapper. The deprecated components have to be replaced. Contact the manufacturer to obtain compatible software.

T103 - Obsolete Windows Features

Description: RayQC Advanced scans the MSI package for a presence of deprecated MSGina technology, as well as for a presence of file extensions, for which the handling application has been obsoleted.

Background: Certain features present in previous versions of Windows systems are officially marked as obsolete by Microsoft. This means they are not supported anymore and any functionality relying on them is likely to fail to operate. Usually, there is a replacement technology that should be used in favor of deprecated features.

More Information: http://msdn.microsoft.com/en-us/library/bb756900.aspx
http://technet.microsoft.com/en-en/library/ee681703(v=ws.10).aspx

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software using the `MSGina.dll` should be re-engineered and use the Credential Providers model. Obsolete extensions should not be used in MSI installer packages.

T104 - Windows Shell and User Experience Changes

Description: RayQC Advanced scans the MSI package for a presence of shortcuts created in Quick Launch and subfolders of the SendTo folder. Additionally, start menu shortcuts pointing to non-executable files will be detected. Finally, RayQC Advanced scans the MSI package for a presence of Windows Gadgets.

Background: Each version of Microsoft Windows system introduces enhancements and changes of the user experience in the way Windows Shell is working and organizing files, shortcuts, context menu actions etc. Certain aspects of the user experience vary between newer version of Windows, with the introduction of Modern Start Screen being a notable example. There is a different handling for certain behaviors that were possible before. For example, the new Start Screen does not pin non-executable files by default, and due to the deprecated tree-like structure certain shortcuts names may be duplicated and thus confusing. Another example are shortcuts placed in subfolders of the SendTo folder, which are not displayed anymore. Finally, features like Quick Launch Bar and Windows Deskop Gadgets layer are not present anymore.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/cc144179(v=vs.85).aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/jj584985(v=vs.85).aspx

Manual Remediation: Avoid deploying shortcuts to Quick Launch location and to subfolders of SendTo folder. Migrate to the Modern application to allow pinning ups and running them in a gadget-mode. Rename Start menu shortcuts to unequivocally express their purpose and associated action, instead of using generic names like "Readme" or "Help". Non-executable files should be manually pinned by the logged on user.

T105 - Unsupported Windows Components

Description: RayQC Advanced scans the MSI package for a presence of applications using DHTML control and for the presence of 32-bit `.hlp` files.

Background: Certain functionalities and components present in Windows XP and previous systems are not anymore part of the standard OS image. Since then Microsoft offers them as downloadable add-ons wich restore the missing functionality. On a standard system however, missing handlers/opening applications may cause runtime exceptions or other warnings. Typical examples of such components are viewers for 32-bit `.hlp` files, missing DHTLM editor controls and so on.

More Information: http://support.microsoft.com/kb/917607 http://msdn.microsoft.com/en-us/library/aa663363.aspx

Manual Remediation: Contact the manufacturer to obtain compatible software. You may also install the missing components - the update KB917607 restores the ability to view 32-bit `.hlp` files, and the redistributable installer `DHTMLEd.msi` from Microsoft installs the missing DHTML control.

T106 - .NET Framework Compatibility

Description: RayQC Advanced scans the MSI package for a presence of applications using .NET Framework 1.0, 1.1, 2.0, 3.0 or 3.5.

Background: Since Windows 7, .NET Framework 1.0 and 1.1 are not supported. Although it may be possible to deploy deprecated .NET components, there is no support for these configurations provided by Microsoft. Additionally .NET Framework 2.0, 3.0 and 3.5 is not included in the default configuration of Windows 8 and later operating systems, so applications that require one of these frameworks might trigger a request for installing the necessary files.

More Information: http://support.microsoft.com/kb/2489698

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should be converted to .NET Framework 4.5.

T107 - Conditional Installation and Execution

Description: RayQC Advanced scans the MSI package for a presence of conditions that vary based on the value of properties: `VersionNT`, `VersionNT64`, `WindowsBuild` and `ServicePackLevel`. Additionally, the content of the package is scanned for the usage of `AdminUser` and `Privileged` properties in Launch Conditions and components condition to verify they will not cause issues with permission elevation. Merge modules, 16-bit components and certain conditions may neutralize otherwise failing conditions.

Background: Number of MSI properties like `VersionNT`, `VersionNT64`, `ServicePackLevel` etc. can be used to conditionally control the flow of installation and set of features/components/policies to be installed. Software vendors use them frequently in critical places like LaunchConditions, conditions for components and Custom Actions, conditional security policies and many more. When a new version of Operating System is introduced, these conditions have to be reviewed, because they may generate false warnings even though the software is functioning correctly. Another source of issues are two distinctive MSI properties `Privileged` and `AdminUser`. Because of late elevation, since Windows Vista values of these properties are spoofed when evaluating LaunchConditions. This may produce unexpected results with packages designed for previous operating systems.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/aa370556(v=vs.85).aspx

http://msdn.microsoft.com/en-us/library/windows/desktop/aa369752(v=vs.85).aspx

Manual Remediation: Review all rows containing conditions that exclude the current operating system. Should the given component/action be required and function correctly on Windows Server 2012 R2, rewrite the condition so that it evaluates to true or remove it to always install the questionable resource. Do not use AdminUser property, because it may impact installation flows that elevate at some later point of installation. Legacy distinction between `Privileged` and `AdminUser` property can be restored by using the `MSIREALADMINDETECTION` property.

T108 - Deprecated and Obsolete API Calls

Description: RayQC Advanced scans the MSI package for a presence of API calls that are deprecated or obsolete. Internal database is used to assess each API call being used.

Background: Certain APIs present in previous versions of Microsoft Windows are now officially deprecated or obsoleted by Microsoft. Obsolete APIs may not work anymore, or their behavior may be different leading to unexpected results. The deprecated APIs may be still working, but there is no guarantee they will function correctly or at all after any update or security patch. Usually, there is a replacement API that should be used in favor of deprecated or obsolete API call.

More Information: None available.

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should not use obsolete functions anymore and switch to replacements as described by Microsoft in Microsoft SDK Updates.

T109 - Hard-Coded Resources and System Paths

Description: RayQC Advanced scans the MSI package for a usage of changed or obsolete junction points in INI files, registry entries, services, shortcuts, environment variables and custom actions.

Background: Since Microsoft Windows Vista, standard locations where user and system data are stored have been changed. For example, the root folder for user data was called "Documents and Settings" in Windows XP, but since Windows Vista its name is "Users". To provide a backward compatibility, junction points are used to reroute the calls from old, incorrect locations to the new, proper ones. A package that runs on various target systems should not rely on hardcoded paths, because they may be not valid anymore or for a given system language.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/bb968829(v=vs.85).aspx

http://msdn.microsoft.com/en-us/library/windows/desktop/aa368977(v=vs.85).aspx

Manual Remediation: Hard-coded paths should not be used. Replace them with MSI properties using formatted syntax. If no predefined property exists, the path should be exposed via custom MSI property so that it can be adjusted on demand from command-line / MST transform.

T110 - Mismatched Target Architecture

Description: RayQC Advanced scans the MSI package for the presence of executables (16/32/64-bit) that are not compatible with Windows Server 2012 R2 32-bit platform

Background: Some software is intended to run only in 32-bit or 64-bit operating systems. 16-

bit executables are not supported on modern platforms, and 64-bit Microsoft Windows can correctly emulate 32-bit applications. If the MSI package is missing a correct Launch Condition it may try to install executables that are not designed for the current platform architecture. Attempting to launch such executable might result in an error message that the file is not a valid Win32 application. Additionally, attempting to run 16-bit code may result in a warning message informing that an extra Windows Feature is required.

More Information: http://support.microsoft.com/kb/282423/en-us

Manual Remediation: Contact the manufacturer to obtain compatible software. Reenginer self-developed software by replacing 16-bit executables with appropriate 32- or 64-bit code. Use Launch Conditions and component conditions to control to which platform software and its parts are deployed.

T111 - Driver Issues

Description: RayQC Advanced scans the MSI package for the presence of drivers containing no valid signature or not matching the target platform.

Background: Since Windows Vista 64-bit, all drivers have to be signed. Signed driver contains an extra digital signature used to validate the source and content of the driver package. Any unauthorized change in the driver package invalidates the signature. If an unsigned driver or a driver with invalid signature is attempted to be installed, Windows refuses the installation. Likewise, each driver has to match the target platform, which means that 64-bit systems require 64-bit drivers.

More Information: http://msdn.microsoft.com/en-us/library/bb756937.aspx

Manual Remediation: Contact the manufacturer to obtain compatible driver. Use WDK (Windows Driver Kit) to sign self-developed driver packages.

T112 - Installation Package Design Issues

Description: RayQC Advanced scans the MSI package for the presence of common installation design issues that may cause troubles during installation or using of software. The context of Custom Actions is scanned for the presence of deferred custom actions running in user-context, as well as system-wide actions running in immediate mode. The presence of conflicting permissions tables preventing the installation is detected as well. Additionally, invalid combinations of user- and machine-data in a single component and invalid identifiers are reported.

Background: Microsoft recommends several best-practices approaches for MSI setup designers. They ensure that the package is deployed correctly in various scenarios and various operating systems. By following the guidelines many compatibility issues introduced by a new security model in Windows Vista can be avoided.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/aa368268%28v=vs.85%29.aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/aa368268(v=vs.85).aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/dd408053(v=vs.85).aspx
http://msdn.microsoft.com/en-us/library/6397xx85(v=vs.80).aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/aa368994%28v=vs.85%29.aspx

Manual Remediation: Adjust the package content so that it complies to the best practices of Windows Installer. Do not mix per-machine and per-user data in a single component. Use valid identifiers for components. Make sure all custom actions are running in a valid context - all actions making system changes must be deferred in execution. Do not use both `LockPermissions` and `MsiLockPermissionsEx` tables at once.

T113 - Conflicts with Protected Windows Resources (WRP)

Description: RayQC Advanced scans the MSI package for the presence of files and registry keys that belong to the Windows Resource Protection list.

Background: Windows Resource Protection (WRP) prevents the modification of essential system resources (files, folders and registry keys). Windows Installer silently ignores any attempt to update or modify them, any other software trying to do it may fail. These kinds of resources may be only updated by Microsoft-provided redistributable packages. During the installation, if Windows Installer logging is enabled, a warning may be shown for each operation that was ignored because of the WRP protection.

More Information: http://msdn.microsoft.com/en-us/library/bb756998.aspx

Manual Remediation: Assess whether the conflicting resources are actually needed, and if not remove them from the MSI package. If a given resource is needed and the original system one cannot be used, consider re-engineering the application or use any virtualization technique to override the resource.

T114 - Missing or Invalid Signatures

Description: RayQC Advanced scans the MSI package for the presence of unsigned executable files (`.exe`, `.dll`, `.ocx`). Additionally, the package itself and CAB files are also scanned.

Background: According to the set of best practices by Microsoft, all exercutable files deployed by an installation package and the installation package itself should be digitally signed with a certificate issued by a Trusted Publisher. When attempting to run an unsigned executable, Windows prompts the user for authorization. Similarly, attempting to install an unsigned MSI package also shows the Windows prompt.

More Information: http://technet.microsoft.com/en-us/library/cc962053.aspx

Manual Remediation: Contact the manufacturer to obtain signed executables and installers. Use WDK (Windows Driver Kit) to sign self-developed executables and packages.

T115 - Security and User Access Control Issues

Description: RayQC Advanced scans the MSI package for the presence of issues that may fail to work due to the security features. The executable files are scanned for the presence of correct manifestation. Direct calls to rundll32 are reported, because the UAC prompt hides the actual calling module when rundll32 is executed. Interactive sevices running in session 0 are detected, as well as MMC snap-ins that are not DEP-aware. Finally, setups, updaters and uninstallers are detecteded and checked for the presence of their UAC awareness.

Background: Session 0 isolation and Data Execution Prevention (DEP) are examples of security improvements introduced to prevent malicious software from compromising the security of the operating systems. They provide a separation between interactive user sessions and non-interactive session 0 devoted for services, and prevent execution of code from non-executable memory region. Modern software has to comply to these restrictions in order to function correctly on Windows Server 2012 R2. Another security issue present in Windows operating

system is User Account Control (UAC). When an executable file requires additional non-standard permissions, the UAC elevation dialog prompts for confirmation or for correct credentials. The UAC prompt contains information about calling application, manufacturer and the source. Certain applications, like self-updaters, setups and other requiring higher privileges must be aware of the elevation, and use manifests to correctly inform the system about required execution permissions.

More Information: http://msdn.microsoft.com/en-us/windows/hardware/gg463353
http://msdn.microsoft.com/en-us/library/bb963893.aspx
http://msdn.microsoft.com/en-us/library/windows/desktop/aa366553(v=vs.85).aspx
http://technet.microsoft.com/en-us/library/cc709628%28WS.10%29.aspx
http://technet.microsoft.com/en-us/library/cc709628%28WS.10%29.aspx

Manual Remediation: Contact the manufacturer to obtain software that complies to the security features of Microsoft Windows. For each unmanifested executable file, create a manifest, and set the required privileges to "`asInvoker`" for applications not requiring them, and "`requireAdministrator`" or "`highestAvailable`" for others. If the manifest cannot be corrected, a shim database has to be used to specify the desired privilege level.

T116 - Missing Application Manifest or Insufficient Execution Policy

Description: RayQC Advanced scans the MSI package for the presence of executable files (`.exe`, `.cpl`) that do not contain the manifest, or that are not aware of Windows Server 2012 R2 in the list of supported operating systems in their manifest files.

Background: Since Windows Vista, all applications run by default with standard user privileges. This is also true when the current user is a member of Administrators group. Application that used to work on previous versions of Windows may fail to work, as no elevation will take place. In order to require higher permissions, each executable or control panel applications has to contain a manifest file - a simple `.XML` file informing the operating system how to handle the given program.

More Information: http://msdn.microsoft.com/en-us/library/Aa480152%23appcomp_topic30.com#appcomp_topic4
http://msdn.microsoft.com/en-us/library/hh848036%28v=vs.85%29.aspx

Manual Remediation: Create a manifest file for each executable. To manifest a control panel application (.cpl) create an executable wrapper with embedded manifest. Use the SupportedOS section in the manifest to define the list of supported operating systems.

T117 - Incomplete Reboot Handling

Description: RayQC Advanced scans the MSI package for the absence of a proper launch condition preventing the installation if a reboot is pending. Additionally, absence of "Files in use" dialog is detected. Presence of `ForceReboot` action is also detected and reported.

Background: Windows Installer supports natively various set of features and actions related to the reboot handling. They include for example the ability to show list of used/locked files, forcing or skipping the reboot and determining the installation state by the related MSI properties. Several aspects have to be considered so that the reboot handling works as expected.

More Information: http://msdn.microsoft.com/en-us/library/windows/desktop/aa368607(v=vs.85).aspx

http://msdn.microsoft.com/en-us/library/windows/desktop/
aa370492(v=vs.85).aspx

http://msdn.microsoft.com/en-us/library/windows/desktop/
aa370379(v=vs.85).aspx

Manual Remediation: Add the `MSIRMFilesInUse` dialog to the dialog sequence if it is missing. Remove `ForceReboot` action from the sequence, reboots are handled automatically by MSI. In order to ensure the package is not installed when any reboot is pending, append the "`NOT MsiSystemRebootPending`" condition to the Launch Condition list.

T118 - Protected Mode (Internet Explorer)

Description: RayQC Advanced scans the MSI package for the presence of registry entries that disable Protected Mode.

Background: As a result of security changes introduced in Windows Vista, Internet Explorer runs now in a isolated mode called "Protected mode" by default. While it limits potential damages malware application can cause, it also prevents web-applications running in Internet Explorer from writing directly to disk while in Internet or Intranet zone. Internet Explorer warns when web-application tries to run certain software programs or write to protected areas.

More Information: http://msdn.microsoft.com/en-us/library/bb756991.aspx

Manual Remediation: Contact the manufacturer to obtain compatible software. Re-engineer self-developed software so that it runs correctly under Protected Mode, or add the required website(s) to the list of trusted sites.

Modern Apps

MSIX (Desktop Bridge)

UM001 - .NET Framework

Description: Scans for the presence of executables compiled with the older version of .NET Framework.

Background: Only .NET Framework in version 4.6.1 or higher is supported.

More Information: https://docs.microsoft.com/en-us/windows/uwp/porting/desktop-to-uwp-prepare

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should be retargeted to .NET Framework 4.6.1.

UM002 - Software Architecture

Description: Scans for the presence of mismatched software architecture.

Background: If jump list is used by the application it needs to be build to the specific architecture.

More Information: https://docs.microsoft.com/en-us/windows/uwp/porting/desktop-to-uwp-prepare

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should be retargeted to the specific architecture.

UM003 - COM Isolation

Description: Scans for the presence of COM registrations.

Background: COM objects registered from within the UWP application are not accessible from other applications.

More Information: https://docs.microsoft.com/en-us/windows/uwp/porting/desktop-to-uwp-prepare

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should be reengineered to not use COM objects.

UM004 - Services

Description: Scans for the presence of Windows Services in a Windows Installer Database.

Background: Services that are installed with Windows Installer database are ignored by the UWP Bridge Desktop App converters. If an application relies on such services it may not work properly.

More Information: https://docs.microsoft.com/en-us/windows/uwp/porting/desktop-to-uwp-prepare

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should be reengineered.

UM005 - Drivers

Description: Scans for the presence of unsupported drivers.

Background: Kernel-mode drivers are not supported.

More Information: https://docs.microsoft.com/en-us/windows/uwp/porting/desktop-to-uwp-prepare

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should be reengineered.

UM006 - Installation Directory Access

Description: Scans for the presence of attempts to set permissions on files, directories, and registry keys within the installation package.

Background: Setting permissions on the installation directory and registry keys is not supported within the UWP application.

More Information: https://docs.microsoft.com/en-us/windows/uwp/porting/desktop-to-uwp-prepare

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should be reengineered.

UM007 - File Associations

Description: Scans for the presence of registered file extensions that are not supported by the UWP applications.

Background: Some of the file associations cannot be registered by the UWP application.

More information: https://docs.microsoft.com/en-us/windows/uwp/porting/desktop-to-uwp-prepare

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should be reengineered.

UM008 – Windows Registry Limitations

Description: Scans for the presence of the usage of DDEEXEC.

Background: UWP applications should not use DDEEXEC registry subkeys to launch another application.

More Information: https://docs.microsoft.com/en-us/windows/uwp/porting/desktop-to-uwp-prepare

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should be reengineered.

UM009 – Administrative Privileges

Description: Scans for the presence of executables that require administrative privileges to launch.

Background: UWP application will not run correctly if it will be started by the user without administrative rights.

More Information: https://docs.microsoft.com/en-us/windows/uwp/porting/desktop-to-uwp-prepare

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should be reengineered.

UM010 – API Calls

Description: Scans for the presence of certain API calls that are not supported by the UWP platform.

Background: Some of the API calls are not supported in the UWP applications due to the isolation level.

More Information: https://docs.microsoft.com/en-us/windows/uwp/porting/desktop-to-uwp-prepare

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should be reengineered.

UM011 – GUI Limitations

Description: Scans for the presence of manifest files that use UIAccess elements.

Background: Usage of UIAccess elements within the manifest file is not supported in the UWP application.

More Information: https://docs.microsoft.com/en-us/windows/uwp/porting/desktop-to-uwp-prepare

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-

developed software should be reengineered.

UM012 - Shortcuts

Description: Scans for the presence of missing shortcuts or multiple shortcuts pointing to different execution files.

Background: There needs to be at least one entry point to run an UWP application. Additionally, multiple shortcuts might cause issues when converting an application to UWP Platform.

More Information: https://docs.microsoft.com/en-us/windows/uwp/porting/desktop-to-uwp-prepare

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should be reengineered.

UM013 - Naming Convention

Description: Scans for the presence of non-alphabetic characters at the beginning of the `ProductName` property and shortcut names.

Background: Most of the tools for UWP conversion are using ProductName and shortcut names as identifiers. this means that they must begin with characters from the ASCII alphabet.

More Information: https://docs.microsoft.com/de-de/uwp/schemas/appxpackage/appxmanifestschema/element-application

Manual Remediation: Incorrect names should be changed to fit the requirements.

UM014 - Entry Point File Extensions

Description: Scans for the presence of entry point paths which are having invalid extensions.

Background: The formal descriptor of MSIX files requires, that file paths for application entry points (for example shortcuts) are conform with the MSIX-specific syntax requirements. Failure to meet these conditions results in validation errors raised by the UWP converter.

More Information: https://docs.microsoft.com/de-de/uwp/schemas/appxpackage/appxmanifestschema/element-application

Manual Remediation: The entry point file extensions must be rewritten to be lowercase.

UM015 - Product Version

Description: Scans for the presence of invalid product versions.

Background: The formal descriptor of MSIX files requires, that the product versions are conform with the MSIX-specific syntax requirements. Failure to meet these conditions results in validation errors raised by the UWP converter.

More Information: https://docs.microsoft.com/de-de/uwp/schemas/appxpackage/appxmanifestschema/element-application

Manual Remediation: The product version must be rewritten to an accepted format.

APPX (Desktop Bridge)

UW001 - .NET Framework

Description: Scans for the presence of executables compiled with the older version of .NET Framework.

Background: Only .NET Framework in version 4.6.1 or higher is supported.

More Information: https://docs.microsoft.com/en-us/windows/uwp/porting/desktop-to-uwp-prepare

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should be retargeted to .NET Framework 4.6.1.

UW002 - Software Architecture

Description: Scans for the presence of mismatched software architecture.

Background: If jump list is used by the application it needs to be build to the specific architecture.

More Information: https://docs.microsoft.com/en-us/windows/uwp/porting/desktop-to-uwp-prepare

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should be retargeted to the specific architecture.

UW003 - COM Isolation

Description: Scans for the presence of COM registrations.

Background: COM objects registered from within the UWP application are not accessible from other applications.

More Information: https://docs.microsoft.com/en-us/windows/uwp/porting/desktop-to-uwp-prepare

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should be reengineered to not use COM objects.

UW004 - Services

Description: Scans for the presence of Windows Services in a Windows Installer Database.

Background: Services that are installed with Windows Installer database are ignored by the UWP Bridge Desktop App converters. If an application relies on such services it may not work properly.

More Information: https://docs.microsoft.com/en-us/windows/uwp/porting/desktop-to-uwp-prepare

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should be reengineered.

UW005 - Drivers

Description: Scans for the presence of unsupported drivers.

Background: Kernel-mode drivers are not supported.

More Information: https://docs.microsoft.com/en-us/windows/uwp/porting/desktop-to-uwp-prepare

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-

developed software should be reengineered.

UW006 - Installation Directory Access

Description: Scans for the presence of attempts to set permissions on files, directories, and registry keys within the installation package.

Background: Setting permissions on the installation directory and registry keys is not supported within the UWP application.

More Information: https://docs.microsoft.com/en-us/windows/uwp/porting/desktop-to-uwp-prepare

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should be reengineered.

UW007 - File Associations

Description: Scans for the presence of registered file extensions that are not supported by the UWP applications.

Background: Some of the file associations cannot be registered by the UWP application.

More information: https://docs.microsoft.com/en-us/windows/uwp/porting/desktop-to-uwp-prepare

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should be reengineered.

UW008 - Windows Registry Limitations

Description: Scans for the presence of the usage of DDEEXEC.

Background: UWP applications should not use DDEEXEC registry subkeys to launch another application.

More Information: https://docs.microsoft.com/en-us/windows/uwp/porting/desktop-to-uwp-prepare

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should be reengineered.

UW009 - Administrative Privileges

Description: Scans for the presence of executables that require administrative privileges to launch.

Background: UWP application will not run correctly if it will be started by the user without administrative rights.

More Information: https://docs.microsoft.com/en-us/windows/uwp/porting/desktop-to-uwp-prepare

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should be reengineered.

UW010 - API Calls

Description: Scans for the presence of certain API calls that are not supported by the UWP platform.

Background: Some of the API calls are not supported in the UWP applications due to the isolation level.

More Information: https://docs.microsoft.com/en-us/windows/uwp/porting/desktop-to-uwp-prepare

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should be reengineered.

UW011 - GUI Limitations

Description: Scans for the presence of manifest files that use UIAccess elements.

Background: Usage of UIAccess elements within the manifest file is not supported in the UWP application.

More Information: https://docs.microsoft.com/en-us/windows/uwp/porting/desktop-to-uwp-prepare

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should be reengineered.

UW012 - Shortcuts

Description: Scans for the presence of missing shortcuts or multiple shortcuts pointing to different execution files.

Background: There needs to be at least one entry point to run an UWP application. Additionally, multiple shortcuts might cause issues when converting an application to UWP Platform.

More Information: https://docs.microsoft.com/en-us/windows/uwp/porting/desktop-to-uwp-prepare

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should be reengineered.

UW013 - Naming Convention

Description: Scans for the presence of non-alphabetic characters at the beginning of the `ProductName` property and shortcut names.

Background: Most of the tools for UWP conversion are using ProductName and shortcut names as identifiers. this means that they must begin with characters from the ASCII alphabet.

More Information: https://docs.microsoft.com/de-de/uwp/schemas/appxpackage/appxmanifestschema/element-application

Manual Remediation: Incorrect names should be changed to fit the requirements.

UW014 - Entry Point File Extensions

Description: Scans for the presence of entry point paths which are having invalid extensions.

Background: The formal descriptor of APPX files requires, that file paths for application entry points (for example shortcuts) are conform with the APPX-specific syntax requirements. Failure to meet these conditions results in validation errors raised by the UWP converter.

More Information: https://docs.microsoft.com/de-de/uwp/schemas/appxpackage/appxmanifestschema/element-application

Manual Remediation: The entry point file extensions must be rewritten to be lowercase.

UW015 – Product Version

Description: Scans for the presence of invalid product versions.

Background: The formal descriptor of APPX files requires, that the product versions are conform with the APPX-specific syntax requirements. Failure to meet these conditions results in validation errors raised by the UWP converter.

More Information: https://docs.microsoft.com/de-de/uwp/schemas/appxpackage/ appxmanifestschema/element-application

Manual Remediation: The product version must be rewritten to an accepted format.

Windows Nano Server

UN001 – .NET Framework

Description: Scans for the presence of executables that are not compiled with .NET Core Framework.

Background: Only .NET Core is supported in Nano Server.

More Information: https://docs.microsoft.com/en-us/windows/uwp/porting/desktop-to-uwp-prepare

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should be retargeted to .NET Core.

UN002 – Software Architecture

Description: Scans for the presence of mismatched software architecture.

Background: 64-bit installers should not install 32-bit files. Additionally, if jump is used by the application it needs to be build to the specific architecture.

More Information: https://docs.microsoft.com/en-us/windows/uwp/porting/desktop-to-uwp-prepare

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should be retargeted to the specific architecture.

UN003 – COM Isolation

Description: Scans for the presence of COM registrations.

Background: COM objects registered from within the Nano Server application are not accessible from other applications.

More Information: https://docs.microsoft.com/en-us/windows/uwp/porting/desktop-to-uwp-prepare

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should be reengineered to not use COM objects.

UN005 – Drivers

Description: Scans for the presence of drivers.

Background: Kernel-mode drivers are not supported.

More Information: https://docs.microsoft.com/en-us/windows/uwp/porting/desktop-to-uwp-prepare

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should be reengineered.

UN007 - File Associations

Description: Scans for the presence of registered file extensions that are not supported by the Nano Server applications.

Background: Some of the file associations cannot be registered by the Nano Server application.

More Information: https://docs.microsoft.com/en-us/windows/uwp/porting/desktop-to-uwp-prepare

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should be reengineered.

UN010 - API Calls

Description: Scans for the presence of certain API calls that are not supported by the UWP platform.

Background: Some of the API calls are not supported in the Nano Server application due to the isolation level.

More Information: https://docs.microsoft.com/en-us/windows/uwp/porting/desktop-to-uwp-prepare

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should be reengineered.

UN011 - GUI Limitations

Description: Nano Server is a headless OS, therefore any GUI-based application has to refactored to follow a client-server model that allows for remote installation and for the GUI to be run on the client.

Background: Nano Server is a headless OS, any GUI-based application has to be refactored.

More Information: https://docs.microsoft.com/en-us/windows/uwp/porting/desktop-to-uwp-prepare

Manual Remediation: Contact the manufacturer to obtain compatible software. Self-developed software should be reengineered.

UN012 - Shortcuts

Description: Scans the Windows Installer database for the presence of shortcuts.

Background: Due to a missing User Interface in Nano Server, shortcut registrations are not supported.

More Information: https://docs.microsoft.com/en-us/windows/uwp/porting/desktop-to-uwp-prepare

> **Manual Remediation:** Contact the manufacturer to obtain compatible software. Self-developed software should be reengineered.

Browser Readiness Test

Tests a web application for readiness for a selected browser.

Internet Explorer 9

Below are the set of rules which can be used to test a web application for readiness for Internet Explorer 9.

> **WA001 - Obsolete HTML Tags**
>
> **Description:** RayQC Advanced scans the web application for the use of obsolete HTML tags and JavaScript methods.
>
> **Background:** There is a number of obsolete HTML tags and connected JavaScript methods in Windows Internet Explorer 9.
>
> **More Information:** http://msdn.microsoft.com/en-us/library/ff806183%28v=vs.94%29.aspx
>
> **Manual Remediation:** Re-engineer the web application not to use the obsolete HTML tags anymore. With CSS and JavaScript the same functionality can be achieved.

> **WA002 - DHTML Editing Control Compatibility**
>
> **Description:** RayQC Advanced scans the web application for the use of the ActiveX DHTML Editing Control.
>
> **Background:** Since Windows Internet Explorer 5, the DHTML Editing Control has been available for HTML, Active Server Pages (ASP), ASP.NET pages, and for other documents accessed with HTTP. Due to security reasons, the support for this control was dropped by Microsoft since Windows Vista, which was shipped with Windows Internet Explorer 7. Web applications might fail to load the control if they have the save-for-scripting DHTML Editing control implemented (`<Object ID="editor">`). If this is the case, an image placeholder will be displayed. Additionally, exceptions might be thrown by any script that refers to the control. Because the script evaluation is terminated by script exceptions, other functions which are controlled by the script might also stop working.
>
> **More Information:** http://msdn.microsoft.com/en-us/library/aa663363.aspx
>
> **Manual Remediation:** Re-engineer the web application not to use the DHTML Editing Control anymore. There is a downloadable original control in a signed Windows Installer package called `DHTMLEd.msi` provided by Microsoft, which could be used if re-engineering is not practicable. (Caution: This is a workaround! The security risks identified by Microsoft will remain since the application itself is left unchanged.)

> **WA003 - CreateElement() Method Compatibility**
>
> **Description:** RayQC Advanced scans the web application for angle brackets which are used in arguments passed to the `createElement()` method.
>
> **Background:** An element node in the Document Object Model (DOM) hierarchy is created by

the createElement() method. Since Windows Internet Explorer 9, the support for the use of angle brackets (< >) within the createElement() method has been dropped by Microsoft. If those characters are contained within the argument of the `createElement()` method, parts of the web application might fail to work.

More Information: http://msdn.microsoft.com/en-us/library/ff986077(v=VS.85).aspx

Manual Remediation: Re-engineer the web application not to use angle brackets in the `createElement()` method anymore. Pass the element name and use the `setAttribute()` method to set the values of the required attributes instead.

WA004 - Obsolete `arguments.caller`

Description: RayQC Advanced scans the web application for the `arguments.caller` property.

Background: Prior to Windows Internet Explorer 9, along with the creation of argument objects, a property named "caller" was created. The reference to the argument object of the function which originally called the argument object was stored inside the property. Since Windows Internet Explorer 9 the `arguments.caller` property is no longer supported by Microsoft. The script error "object is null or undefined" will occur if a script tries to use this property. Because of this, parts of the web application might fail to work.

More Information: http://msdn.microsoft.com/en-us/library/gg622933(v=VS.85).aspx

Manual Remediation: Re-engineer the web application not to use the arguments.caller property anymore. Use the Windows Internet Explorer 8 Compatibility View where this is not practicable. Trigger the view by using the meta attribute value "X-UA-Compatible".

WA005 - Obsolete Document Object Model (DOM) Event Features

Description: RayQC Advanced scans the web application for the following DOM event features: `attachEvent(), detachEvent(), createEventObject(),` and `fireEvent().`

Background: The following DOM event features are no longer supported by Microsoft since Windows Internet Explorer 9: `attachEvent(), detachEvent(), createEventObject(),` and `fireEvent().`

More Information: http://msdn.microsoft.com/en-us/library/ms537512(v=vs.85).aspx

Manual Remediation: Re-engineer the web application not to use the outdated DOM event features. There are W3C standard conform replacements which should be used instead.

WA006 - Conditional Comments Compatibilty

Description: RayQC Advanced scans the web application for conditional comments which are used to detect the version number of the Windows Internet Explorer. (Take care: This rule might detect false positives for web applications which use conditional comments to fix some well-known visual glitches for older Windows Internet Explorer versions!)

Background: There are non-standard conditional comments provided by the Windows Internet Explorer which are used to provide content which is optimized for a specific browser, for example, the use of specific HTML, CSS, or JavaScript code(`<!--[if IE 7]> <p>You are using Windows Internet Explorer 7.</p> <![endif]-->`). Web applications using conditional comments might serve incompatible content due to not recognizing Windows Internet Explorer 9 since the major version number has been changed in Windows Internet Explorer 9.

More Information: http://support.microsoft.com/kb/2489698

Manual Remediation: Re-engineer the web application not to use conditional comments. W3C proposals like JavaScript-based feature detection should be used instead.

WA007 - Changed User-Agent String

Description: RayQC Advanced scans the web application for the use of the user-agent string for browser or system detection. The common Javascript frameworks jQuery, jQuery UI, Prototype, MooTools, and Cufon will not be scanned. (Take Care: This rule might detect false positives for web applications which use the user-agent string for adjunct purposes like statistical data collection)

Background: The user-agent string submits browser details, such as name, version number, running platform, etc., to the hosting server when accessing a web application (User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0; SLCC1; .NET CLR 2.0.50727; .NET CLR 1.1.4322)). This information can be used to provide content which has been optimized for the specific browser. Some web applications might not recognize the user-agent string and therefore serve incompatible content, because the user-agent string has been changed in Windows Internet Explorer 9.

More Information: http://msdn.microsoft.com/en-us/library/cc848857%28v=vs.85%29.aspx

Manual Remediation: Re-engineer the web application not to use the user-agent string, but to use feature support detection instead. Use the Windows Internet Explorer 7 Compatibility View where this is not practicable. Trigger the view by using the meta attribute value "X-UA-Compatible".

WA008 - Use of "`onload`" and "`onreadystatechange`" Event

Description: RayQC Advanced scans the web application for the attachment of both events ("`onload`" and "`onreadystatechange`") to one script element.

Background: The standard-based and interoperable load event for script elements has been introduced in Windows Internet Explorer 9. Before the introduction of Windows Internet Explorer 9, the only event for script elements that was supported was the non-interoperable "`onreadystatechange`" event. This event is still supported in Windows Internet Explorer to make sure existing websites are still compatible. For sites which register for both, "`onload`" and "`onreadystatechange`" events, there may be two callbacks now. This might lead to the production of unexpected results or failure of a part of the web application.

More Information: http://msdn.microsoft.com/en-us/library/hh180173(v=VS.85).aspx

Manual Remediation: Re-engineer the web application to exclusively use the "`onload`" event for scripts that need a load event.

WA009 - JavaScript Framework Compatibility

Description: RayQC Advanced scans the web application for the use of older versions of JavaScript frameworks which are not compatible with Windows Internet Explorer 9. jQuery (prior to 1.5.1), jQuery UI (prior to 1.6.8), MooTools (prior to 1.3), Prototype (prior to 1.7), and Cufon (prior to 1.09i) are the frameworks that will be scanned.

Background: Features to improve the standards for compliance and interoperability with other web browsers were introduced and modified by Microsoft in Windows Internet Explorer 9. A lot of JavaScript frameworks have utilities which rely on functions of earlier versions of Windows Internet Explorer. In Windows Internet Explorer 9, some well-known JavaScript

frameworks might not work as they should. Most of these JavaScript frameworks already received updates to fix this. Nonetheless, there are still a lot of web applications where the older versions of these frameworks are still in use and have not yet been updated.

More Information: http://msdn.microsoft.com/en-us/library/hh180175(v=VS.85).aspx

Manual Remediation: Ask the manufacturer to deliver a framework which is compatible to Microsoft Internet Explorer 9. Use the Windows Internet Explorer 7 Compatibility View if there is no compatible framework. Trigger the view by using the meta attribute value "X-UA-Compatible".

WA010 - Unconventional Protocol Handlers

Description: RayQC Advanced scans the web application for the use of unconventional protocols in script redirections and hyperlinks.

Background: The prefix of the URL address refers to a protocol name (http://www.raynet.de for a HTTP protocol, `javascript:alert('Welcome')` for a JavaScript protocol). An application can be registered to a URL protocol. If this is the case, since Windows Internet Explorer 9, the Application Protocol Handler Dialog will be shown when the application is launched. This is a security feature which should protect users from executing an application containing dangerous or malicious content. The dialog will be shown with each execution of the request until the dialog for this protocol has been disabled. The information, that a program which is not installed is required for the launch of the web application, will be shown if no application is registered to a URL protocol.

More Information: http://msdn.microsoft.com/en-us/library/dd565637(VS.85).aspx

Manual Remediation: Uncheck the "Always ask before opening this type of address" checkbox after using a link to prevent further displays of the Application Protocol Handler Dialog by Windows Internet Explorer 9. Portions of a web application might not work if no application is configured to handle a non-standard protocol.

WA011 - Status Bar Text Changes

Description: RayQC Advanced scans the JavaScript properties `window.status` and `window.defaultStatus` for the use of scripts that change the status bar content.

Background: Since Windows Internet Explorer 7, web applications are no longer allowed to use scripts to configure the status bar in the internet or restricted zones. Because of this, calls to the JavaScript properties `window.status` or `window.defaultStatus` might silently fail. By this measure, attackers should no longer be able to spoof the status bar.

More Information: http://msdn.microsoft.com/en-us/ie/aa740486

Manual Remediation: Tick the "Allow status bar updates via script" checkbox which you will find in the custom security level in the Internet Options setting in Windows Internet Explorer 9 to allow the configuration of the status bar by scripts which use the `window.status` and `window.defaultStatus` methods.

WA012 - Obsolete Dynamic Properties

Description: RayQC Advanced scans the web application for obsolete dynamic properties in CSS or JavaScript code.

Background: Property values could be set as formulas, not only as constants, through the use of dynamic CSS properties since Windows Internet Explorer 5. Authors were provided with the

ability to reference property values from other values by using a dynamic property, and they were thereby offered an unparalleled flexibility when designing their webpages. But this also led to a damaging impact on standard compliance, performance, reliability, and security considerations. Dynamic properties are obsolete since Windows Internet Explorer 8, but there is still support for web applications which use dynamic properties and are displayed in Windows Internet Explorer 5 (Quirks) mode or Windows Internet Explorer 7 Standards mode.

More Information: http://msdn.microsoft.com/en-us/library/ms537634(v=vs.85).aspx

Manual Remediation: Replace the dynamic properties functionality with JavaScript event listeners.

WA013 - Conformity to the Request for Comments (RFC) Guidelines

Description: RayQC Advanced scans the web application for the use of URLs that do not meet the requirements of the RFC 3986 and 3987 guidelines.

Background: To prevent malformed URLs from fooling Windows Internet Explorer, the URL is parsed to assure that it meets the RFC guidelines after being entered into the address bar since Windows Internet Explorer 7. The web application will be allowed to appear with a restricted functionality if it fails to pass the verification process. This might lead to an unexpected behavior of the web application.

More Information: https://msdn.microsoft.com/en-us/library/dd565653(v=vs.85).aspx

Manual Remediation: Re-engineer the web application and make sure that all URLs used in the web application meet the requirements of the RFC 3986 and 3987 guidelines.

WA014 - CSS Compatibility

Description: RayQC Advanced scans the web application for the use of CSS features which are not supported by Windows Internet Explorer 9.

Background: The support for the W3C CSS standard has been improved with each new release of Windows Internet Explorer (:focus {sRules} is supported by Windows Internet Explorer 9, but it is not supported by Windows Internet Explorer 7). There is a full compliance with CSS 2.1 in Windows Internet Explorer 9. There are also many CSS 3 features which are supported.

More Information: http://msdn.microsoft.com/en-us/library/cc351024(v=vs.85).aspx

Manual Remediation: Re-engineer the web application to use only CSS features which are supported by Windows Explorer 9.

WA015 - XSLT (Extensible Stylesheet Language Transformations) Changes

Description: RayQC Advanced scans the web application for the use of unsupported XSLT elements. Legacy XSL namespaces, legacy stylesheets processing instructions, and XSLT output directives are the features that will be scanned.

Background: XSLT is used for the modification of XML documents and is a declarative language based on XML. The processing of XML and XSLT files has been modified for the improvement of conformation to the standards of other browsers and the compatibility to other browsers since Windows Internet Explorer 9. Chiefly, there have been changes to some of the non-standard behaviors relating to the processing of XSLT files. These might cause web applications to show unexpected behavior or a limited functionality.

More Information: http://msdn.microsoft.com/en-us/library/hh180178(v=vs.85).aspx

Manual Remediation: Re-engineer the web application by migrating to a compatible and standardized XSLT namespace. Microsoft has prepared some migration scenarios.

WA017 - Obsolete DirectX-based Filters and Transitions Reference

Description: RayQC Advanced scans the web application for the use of DirectX-based filters and transitions which are no longer supported in Windows Internet Explorer 9.

Background: Web developers were allowed to add multimedia-style effects to their webpages by the usage of a set of visual filters and transitions since Windows Internet Explorer 4.0. They are called DX filters because of their underlying implementation, DirectX, and their long-form syntax (`filter:progid:DXImageTransform.Microsoft.Alpha(opacity=75)`). There exists a standard-based alternative to common DX filters since Windows Internet Explorer 9. In Windows Internet Explorer 9, you can still use the legacy feature in the document modes 5, 7, and 8, though the performance will be inferior to their hardware-accelerated, standard-based replacements.

More Information: http://msdn.microsoft.com/en-us/library/ms532853%28v=vs.85%29.aspx

Manual Remediation: Re-engineer the web application to use standard-based technologies. Use the Windows Internet Explorer Compatibility View where this is not practicable. Trigger the view by using the meta attribute value "X-UA-Compatible".

WA021 - Missing Touch Detection

Description: RayQC Advanced scans the web application for JavaScript properties used to return the number of touch points.

Background: Feature detection as a method to determine the support of touch screens by a device is not supported in Windows Internet Explorer 9. The `msMaxTouchPoints` property which returns the maximum number of supported touch points will only return "undefined" in Windows Internet Explorer 9.

More Information: http://msdn.microsoft.com/en-us/library/ie/hh772144(v=vs.85).aspx

Manual Remediation: Re-engineer the web application not to use the `msMaxTouchPoints` property.

Internet Explorer 10

Below are the set of rules which can be used to test a web application for readiness for Internet Explorer 10.

WB001 - Obsolete HTML Tags

Description: RayQC Advanced scans the web application for the use of obsolete HTML tags and JavaScript methods.

Background: There is a number of obsolete HTML tags and connected JavaScript methods in Windows Internet Explorer 10.

More Information: http://msdn.microsoft.com/en-us/library/ff806183%28v=vs.94%29.aspx

Manual Remediation: Re-engineer the web application not to use the obsolete HTML tags anymore. With CSS and JavaScript the same functionality can be achieved.

WB002 - DHTML Editing Control Compatibility

Description: RayQC Advanced scans the web application for the use of the ActiveX DHTML Editing Control.

Background: Since Windows Internet Explorer 5, the DHTML Editing Control has been available for HTML, Active Server Pages (ASP), ASP.NET pages, and for other documents accessed with HTTP. Due to security reasons, the support for this control was dropped by Microsoft since Windows Vista, which was shipped with Windows Internet Explorer 7. Web applications might fail to load the control if they have the save-for-scripting DHTML Editing control implemented (`<Object ID="editor">`). If this is the case, an image placeholder will be displayed. Additionally, exceptions might be thrown by any script that refers to the control. Because the script evaluation is terminated by script exceptions, other functions which are controlled by the script might also stop working.

More Information: http://msdn.microsoft.com/en-us/library/aa663363.aspx

Manual Remediation: Re-engineer the web application not to use the DHTML Editing Control anymore. There is a downloadable original control in a signed Windows Installer package called `DHTMLEd.msi` provided by Microsoft, which could be used if re-engineering is not practicable. (Caution: This is a workaround! The security risks identified by Microsoft will remain since the application itself is left unchanged.)

WB003 - `CreateElement()` **Method Compatibility**

Description: RayQC Advanced scans the web application for angle brackets which are used in arguments passed to the `createElement()` method.

Background: An element node in the Document Object Model (DOM) hierarchy is created by the `createElement()` method. Since Windows Internet Explorer 9, the support for the use of angle brackets (< >) within the createElement() method has been dropped by Microsoft. If those characters are contained within the argument of the `createElement()` method, parts of the web application might fail to work.

More Information: http://msdn.microsoft.com/en-us/library/ff986077(v=VS.85).aspx

Manual Remediation: Re-engineer the web application not to use angle brackets in the `createElement()` method anymore. Pass the element name and use the `setAttribute()` method to set the values of the required attributes instead.

WB004 - Obsolete `arguments.caller`

Description: RayQC Advanced scans the web application for the `arguments.caller` property.

Background: Prior to Windows Internet Explorer 9, along with the creation of argument objects, a property named "caller" was created. The reference to the argument object of the function which originally called the argument object was stored inside the property. Since Windows Internet Explorer 9 the `arguments.caller` property is no longer supported by Microsoft. The script error "object is null or undefined" will occur if a script tries to use this property. Because of this, parts of the web application might fail to work.

More Information: http://msdn.microsoft.com/en-us/library/gg622933(v=VS.85).aspx

Manual Remediation: Re-engineer the web application not to use the `arguments.caller` property anymore. Use the Windows Internet Explorer 8 Compatibility View where this is not practicable. Trigger the view by using the meta attribute value "X-UA-Compatible".

WB005 - Obsolete Document Object Model (DOM) Event Features

Description: RayQC Advanced scans the web application for the following DOM event features: `attachEvent()`, `detachEvent()`, `createEventObject()`, and `fireEvent()`.

Background: The following DOM event features are no longer supported by Microsoft since Windows Internet Explorer 9: `attachEvent()`, `detachEvent()`, `createEventObject()`, and `fireEvent()`.

More Information: http://msdn.microsoft.com/en-us/library/ff986080(v=vs.85).aspx

Manual Remediation: Re-engineer the web application not to use the outdated DOM event features. There are W3C standard conform replacements which should be used instead.

WB006 - Conditional Comments Compatibility

Description: RayQC Advanced scans the web application for conditional comments which are used to detect the version number of the Windows Internet Explorer. (Take care: This rule might detect false positives for web applications which use conditional comments to fix some well-known visual glitches for older Windows Internet Explorer versions!)

Background: There are non-standard conditional comments provided by the Windows Internet Explorer which are used to provide content which is optimized for a specific browser, for example, the use of specific HTML, CSS, or JavaScript code(`<!--[if IE 7]> <p>You are using Windows Internet Explorer 7.</p> <![endif]-->`). Web applications using conditional comments might serve incompatible content due to not recognizing Windows Internet Explorer 10 since the major version number has been changed in Windows Internet Explorer 10.

More Information: http://msdn.microsoft.com/en-us/library/ms537512(v=vs.85).aspx

Manual Remediation: Re-engineer the web application not to use conditional comments. W3C proposals like JavaScript-based feature detection should be used instead.

WB007 - Changed User-Agent String

Description: RayQC Advanced scans the web application for the use of the user-agent string for browser or system detection. The common Javascript frameworks jQuery, jQuery UI, Prototype, MooTools, and Cufon will not be scanned. (Take Care: This rule might detect false positives for web applications which use the user-agent string for adjunct purposes like statistical data collection)

Background: The user-agent string submits browser details, such as name, version number, running platform, etc., to the hosting server when accessing a web application (User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0; SLCC1; .NET CLR 2.0.50727; .NET CLR 1.1.4322)). This information can be used to provide content which has been optimized for the specific browser. Some web applications might not recognize the user-agent string and therefore serve incompatible content, because the user-agent string has been changed in Windows Internet Explorer 10.

More Information: http://msdn.microsoft.com/en-us/library/cc848857%28v=vs.85%29.aspx

Manual Remediation: Re-engineer the web application not to use the user-agent string, but to use feature support detection instead. Use the Windows Internet Explorer 7 Compatibility View where this is not practicable. Trigger the view by using the meta attribute value "X-UA-Compatible".

WB008 - Use of "`onload`" and "`onreadystatechange`" Event

Description: RayQC Advanced scans the web application for the attachment of both events ("`onload`" and "`onreadystatechange`") to one script element.

Background: The standard-based and interoperable load event for script elements has been introduced since Windows Internet Explorer 9. Before the introduction of Windows Internet Explorer 9, the only event for script elements that was supported was the non-interoperable "`onreadystatechange`" event. This event is still supported in Windows Internet Explorer to make sure existing websites are still compatible. For sites which register for both, "`onload`" and "`onreadystatechange`", events, there might be two callbacks now. This might lead to the production of unexpected results or failure of a part of the web application.

More Information: http://msdn.microsoft.com/en-us/library/hh180173(v=VS.85).aspx

Manual Remediation: Re-engineer the web application to exclusively use the "onload" event for scripts that need a load event.

WB009 - JavaScript Framework Compatibility

Description: RayQC Advanced scans the web application for the use of older versions of JavaScript frameworks which are not compatible with Windows Internet Explorer 10. jQuery (prior to 1.5.1), jQuery UI (prior to 1.6.8), MooTools (prior to 1.3), Prototype (prior to 1.7), and Cufon (prior to 1.09i) are the frameworks that will be scanned.

Background: Features to improve the standards for compliance and interoperability with other web browser were introduced and modified by Microsoft since Windows Internet Explorer 9. A lot of JavaScript frameworks have functions which rely on functions of earlier versions of Windows Internet Explorer. In Windows Internet Explorer 10, some well-known JavaScript frameworks might not work as they should. Most of these JavaScript frameworks already received updates to fix this. Nonetheless, there are still a lot of web applications where the older versions of these frameworks are still in use and which have not yet been updated.

More Information: http://msdn.microsoft.com/en-us/library/hh180175(v=VS.85).aspx

Manual Remediation: Ask the manufacturer to deliver a framework which is compatible to Microsoft Internet Explorer 10. Use the Windows Internet Explorer 7 Compatibility View if there is no compatible framework. Trigger the view by using the meta attribute value "X-UA-Compatible".

WB010 - Unconventional Protocol Handlers

Description: RayQC Advanced scans the web application for the use of unconventional protocols in script redirections and hyperlinks.

Background: The prefix of the URL address refers to a protocol name (http://www.raynet.de for a HTTP protocol, `javascript:alert('Welcome')` for a JavaScript protocol). An application can be registered to a URL protocol. If this is the case, since Windows Internet Explorer 9, the Application Protocol Handler Dialog will be shown when the application is launched. This is a security feature which should protect users from executing an application containing dangerous or malicious content by accident. The dialog will be shown with each execution of the request until the dialog for this protocol has been disabled. The information, that a program which is not installed is required for the launch of the web application, will be shown if no application is registered to a URL protocol.

More Information: http://msdn.microsoft.com/en-us/library/dd565637(VS.85).aspx

Manual Remediation: Uncheck the **Always as before opening this type of address** checkbox after using a link to prevent further displays of the Application Protocol Handler Dialog by Windows Internet Explorer 10. Portions of a web application might not work if no application is configured to handle a non-standard protocol.

WB011 - Status Bar Text Changes

Description: RayQC Advanced scans the JavaScript properties `window.status` and `window.defaultStatus` for the use of scripts that change the status bar content.

Background: Since Windows Internet Explorer 7, web applications are no longer allowed to use scripts to configure the status bar in the internet or restricted zones. Because of this, calls to the JavaScript properties `window.status` or `window.defaultStatus` might silently fail. By this measure, attackers should no longer be able to spoof the status bar.

More Information: http://msdn.microsoft.com/en-us/ie/aa740486

Manual Remediation: Check the **Allow status bar updates via script** checkbox which you will find in the custom security level in the Internet Options setting in Windows Internet Explorer 10 to allow the configuration of the status bar by scripts which use the `window.status` and `window.defaultStatus` methods.

WB012 - Obsolete Dynamic Properties

Description: RayQC Advanced scans the web application for obsolete dynamic properties in CSS or JavaScript code.

Background: Property values could be set as formulas, not only as constants, through the use of dynamic CSS properties since Windows Internet Explorer 5. Authors were provided with the ability to reference property values from other values by using a dynamic property, and they were thereby offered an unparalleled flexibility when designing their webpages. But this also led to a damaging impact on standard compliance, performance, reliability, and security considerations. Dynamic properties are obsolete since Windows Internet Explorer 8, but there is still support for web applications which use dynamic properties and are displayed in Windows Internet Explorer 5 (Quirks) mode or Windows Internet Explorer 7 Standards mode.

More Information: http://msdn.microsoft.com/en-us/library/ms537634(v=vs.85).aspx

Manual Remediation: Replace the dynamic properties functionality with JavaScript event listeners.

WB013 - Conformity to the Request for Comments (RFC) Guidelines

Description: RayQC Advanced scans the web application for the use of URLs that do not meet the requirements of the RFC 3986 and 3987 guidelines.

Background: To prevent malformed URLs from fooling Windows Internet Explorer, the URL is parsed to assure that it meets the RFC guidelines after being entered into the address bar since Windows Internet Explorer 7. The web application will be allowed to appear with a restricted functionality if it fails to pass the verification process. This might lead to an unexpected behavior of the web application.

More Information: https://msdn.microsoft.com/en-us/library/dd565653(v=vs.85).aspx

Manual Remediation: Re-engineer the web application and make sure that all URLs used in the web application meet the requirements of the RFC 3986 and 3987 guidelines.

WB014 - CSS Compatibility

Description: RayQC Advanced scans the web application for the use of CSS features which are not supported by Windows Internet Explorer 10.

Background: The support for the W3C CSS standard has been improved with each new release of Windows Internet Explorer (`:focus {sRules}` is supported by Windows Internet Explorer 10, but it is not supported by Windows Internet Explorer 7). There is a full compliance with CSS 2.1 and many CSS 3 features are supported in Windows Internet Explorer 10.

More Information: http://msdn.microsoft.com/en-us/library/cc351024(v=vs.85).aspx

Manual Remediation: Re-engineer the web application to use only CSS features which are supported by Windows Explorer 10.

WB015 - XSLT (Extensible Stylesheet Language Transformations) Changes

Description: RayQC Advanced scans the web application for the use of unsupported XSLT elements. Legacy XSL namespaces, legacy stylesheets processing instructions, and XSLT output directives are the features that will be scanned.

Background: XSLT is used for the modification of XML documents and is a declarative language based on XML. The processing of XML and XSLT files has been modified for the improvement of conformation to the standards of other browsers and the compatibility to other browsers since Windows Internet Explorer 9. Chiefly, there have been changes to some of the non-standard behaviors relating to the processing of XSLT files. These might cause web applications to show unexpected behavior or a limited functionality.

More Information: http://msdn.microsoft.com/en-us/library/hh180178(v=vs.85).aspx

Manual Remediation: Re-engineer the web application by migrating to a compatible and standardized XSLT namespace. Microsoft has prepared some migration scenarios.

WB017 - Obsolete DirectX-based Filters and Transitions Reference

Description: RayQC Advanced scans the web application for the use of DirectX-based filters and transitions which are no longer supported in Windows Internet Explorer 10.

Background: Web developers were allowed to add multimedia-style effects to their webpages by the usage of a set of visual filters and transitions since Windows Internet Explorer 4.0. They are called DX filters because of their underlying implementation, DirectX, and their long-form syntax (`filter:progid:DXImageTransform.Microsoft.Alpha(opacity=75)`). There exists a standard-based alternative to common DX filters since Windows Internet Explorer 9. In Windows Internet Explorer 10, you can still use the legacy feature in the document modes 5, 7, and 8, though the performance will be inferior to their hardware-accelerated, standard-based replacements.

More Information: http://msdn.microsoft.com/en-us/library/ms532853%28v=vs.85%29.aspx

Manual Remediation: Re-engineer the web application to use standard-based technologies. Use the Windows Internet Explorer Compatibility View where this is not practicable. Trigger the view by using the meta attribute value "X-UA-Compatible".

WB018 - Obsolete Vector Markup Language (VML) Elements

Description: RayQC Advanced scans the web application for the use of obsolete VML elements.

Background: VML, which was used to create vector graphics that were displayed in web applications, is no longer supported by Microsoft since Windows Internet Explorer 10. In

Windows Internet Explorer 10 you can still use the legacy feature in the document modes 5, 7, 8, and 9, though the performance will be inferior to their hardware-accelerated, standard-based replacements.

More Information: http://msdn.microsoft.com/en-us/library/ie/hh801223%28v=vs.85%29.aspx

Manual Remediation: Re-engineer the web application to use standard-based technologies like e.g. Scalable Vector Graphics (SVG) format. Use the Windows Internet Explorer Compatibility View where this is not practicable. Trigger the view by using the meta attribute value "X-UA-Compatible".

WB019 - Microsoft Internet Explorer plug-in Compatibility in the Windows UI

Description: RayQC Advanced scans the web application for embedded content for which the use of external plug-ins is required.

Background: Windows Internet Explorer 10 offers two different ways of browsing. There is the Windows Internet Explorer in the Windows UI and there is the Windows Internet Explorer for the desktop, which are both using the same technology for the rendering of web applications. Even though, the behavior and feel might differ. For example, the Adobe Flash support is limited and other plug-ins, like Java applets, are not supported by the Windows Internet Explorer in the Windows UI. If using Windows Internet Explorer 10 in the Windows UI, web applications that rely on these technologies might not be able to work as anticipated.

More Information: https://msdn.microsoft.com/nl-be/library/hh920753(v=vs.85).aspx

Manual Remediation: Re-engineer the web application to use standard-based technologies, which includes supported HTML5 features, to work properly with Windows Internet Explorer 10 in the Windows UI.

WB020 - XML Data Islands Compatibility

Description: RayQC Advanced scans the web application for the use of obsolete XML data islands.

Background: The support for XML data islands has been dropped by Microsoft since Windows Internet Explorer 10. They are now parsed in HTML in order to improve compatibility and compliance with HTML5. Pages which are written for Windows Internet Explorer or pages that use browser sniffing to modify their behavior in Windows Internet Explorer will be influenced by this.

More Information: http://msdn.microsoft.com/en-us/library/ie/hh801224(v=vs.85).aspx

Manual Remediation: Re-engineer the web application not to use XML data islands anymore. Use other technologies or use meta tags that can define document compatibility with Microsoft Internet Explorer 10 instead.

Internet Explorer 11

Below are the set of rules which can be used to test a web application for readiness for Internet Explorer 11.

WC001 - Obsolete HTML Tags

Description: RayQC Advanced scans the web application for the use of obsolete HTML tags and JavaScript methods.

Background: There is a number of obsolete HTML tags and connected JavaScript methods in Windows Internet Explorer 11.

More Information: http://msdn.microsoft.com/en-us/library/ff806183%28v=vs.94%29.aspx

Manual Remediation: Re-engineer the web application not to use the obsolete HTML tags anymore. With CSS and JavaScript the same functionality can be achieved.

WC002 - DHTML Editing Control Compatibility

Description: RayQC Advanced scans the web application for the use of the ActiveX DHTML Editing Control.

Background: Since Windows Internet Explorer 5, the DHTML Editing Control has been available for HTML, Active Server Pages (ASP), ASP.NET pages, and for other documents accessed with HTTP. Due to security reasons, the support for this control was dropped by Microsoft since Windows Vista, which was shipped with Windows Internet Explorer 7. Web applications might fail to load the control if they have the save-for-scripting DHTML Editing control implemented (`<Object ID="editor">`). If this is the case, an image placeholder will be displayed. Additionally, exceptions might be thrown by any script that refers to the control. Because the script evaluation is terminated by script exceptions, other functions which are controlled by the script might also stop working.

More Information: http://msdn.microsoft.com/en-us/library/aa663363.aspx

Manual Remediation: Re-engineer the web application not to use the DHTML Editing Control anymore. There is a downloadable original control in a signed Windows Installer package called `DHTMLEd.msi` provided by Microsoft, which could be used if re-engineering is not practicable. (Caution: This is a workaround! The security risks identified by Microsoft will remain since the application itself is left unchanged.)

WC003 - `CreateElement()` Method Compatibility

Description: RayQC Advanced scans the web application for angle brackets which are used in arguments passed to the `createElement()` method.

Background: An element node in the Document Object Model (DOM) hierarchy is created by the `createElement()` method. Since Windows Internet Explorer 9, the support for the use of angle brackets (< >) within the `createElement()` method has been dropped by Microsoft. If those characters are contained within the argument of the `createElement()` method, parts of the web application might fail to work.

More Information: http://msdn.microsoft.com/en-us/library/ff986077(v=VS.85).aspx

Manual Remediation: Re-engineer the web application not to use angle brackets in the `createElement()` method anymore. Pass the element name and use the `setAttribute()` method to set the values of the required attributes instead.

WC004 - Obsolete `arguments.caller`

Description: RayQC Advanced scans the web application for the `arguments.caller` property.

Background: Prior to Windows Internet Explorer 9, along with the creation of argument objects, a property named "caller" was created. The reference to the argument object of the

function which originally called the argument object was stored inside the property. Since Windows Internet Explorer 9 the `arguments.caller` property is no longer supported by Microsoft. The script error "object is null or undefined" will occur if a script tries to use this property. Because of this, parts of the web application might fail to work.

More Information: http://msdn.microsoft.com/en-us/library/gg622933(v=VS.85).aspx

Manual Remediation: Re-engineer the web application not to use the arguments.caller property anymore. Use the Windows Internet Explorer 8 Compatibility View where this is not practicable. Trigger the view by using the meta attribute value "X-UA-Compatible".

WC005 - Obsolete Document Object Model (DOM) Event Features

Description: RayQC Advanced scans the web application for the following DOM event features: `attachEvent(),detachEvent(),createEventObject()`, and `fireEvent()`.

Background: The following DOM event features are no longer supported by Microsoft since Windows Internet Explorer 9: `attachEvent(),detachEvent(),createEventObject()`, and `fireEvent()`.

More Information: http://msdn.microsoft.com/en-us/library/ff986080(v=vs.85).aspx

Manual Remediation: Re-engineer the web application not to use the outdated DOM event features. There are W3C standard conform replacements which should be used instead.

WC006 - Conditional Comments Compatibility

Description: RayQC Advanced scans the web application for conditional comments which are used to detect the version number of the Windows Internet Explorer. (Take care: This rule might detect false positives for web applications which use conditional comments to fix some well-known visual glitches for older Windows Internet Explorer versions!)

Background: There are non-standard conditional comments provided by the Windows Internet Explorer which are used to provide content which is optimized for a specific browser, for example, the use of specific HTML, CSS, or JavaScript code(`<!--[if IE 7]> <p>You are using Windows Internet Explorer 7.</p> <![endif]-->`). Web applications using conditional comments might serve incompatible content due to not recognizing Windows Internet Explorer 11 since the major version number has been changed in Windows Internet Explorer 11.

More Information: http://msdn.microsoft.com/en-us/library/ms537512(v=vs.85).aspx

Manual Remediation: Re-engineer the web application not to use conditional comments. W3C proposals like JavaScript-based feature detection should be used instead.

WC007 - Changed User-Agent String

Description: RayQC Advanded scans the web application for the use of the user-agent string for browser or system detection. The common Javascript frameworks jQuery, jQuery UI, Prototype, MooTools, and Cufon will not be scanned. (Take Care: This rule might detect false positives for web applications which use the user-agent string for adjunct purposes like statistical data collection)

Background: The user-agent string submits browser details, such as name, version number, running platform, etc., to the hosting server when accessing a web application (User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0; SLCC1; .NET CLR 2.0.50727; .NET CLR 1.1.4322)). This information can be used to provide content which has been optimized for the

specific browser. Some web applications might not recognize the user-agent string and therefore serve incompatible content, because the user-agent string has been changed in Windows Internet Explorer 11.

More Information: http://msdn.microsoft.com/en-us/library/cc848857%28v=vs.85%29.aspx

Manual Remediation: Re-engineer the web application not to use the user-agent string, but to use feature support detection instead. Use the Windows Internet Explorer 7 Compatibility View where this is not practicable. Trigger the view by using the meta attribute value "X-UA-Compatible".

WC008 - Use of "`onload`" and "`onreadystatechange`" Event

Description: RayQC Advanced scans the web application for the attachment of both events ("`onload`" and "`onreadystatechange`") to one script element.

Background: The standard-based and interoperable load event for script elements has been introduced since Windows Internet Explorer 9. Before the introduction of Windows Internet Explorer 9, the only event for script elements that was supported was the non-interoperable "`onreadystatechange`" event. This event is still supported in Windows Internet Explorer to make sure existing websites are still compatible. For sites which register for both, "`onload`" and "`onreadystatechange`", events, there might be two callbacks now. This might lead to the production of unexpected results or failure of a part of the web application.

More Information http://msdn.microsoft.com/en-us/library/hh180173(v=VS.85).aspx

Manual Remediation: Re-engineer the web application to exclusively use the "`onload`" event for scripts that need a load event.

WC009 - JavaScript Framework Compatibility

Description: RayQC Advanced scans the web application for the use of older versions of JavaScript frameworks which are not compatible with Windows Internet Explorer 11. jQuery (prior to 1.5.1), jQuery UI (prior to 1.6.8), MooTools (prior to 1.3), Prototype (prior to 1.7), and Cufon (prior to 1.09i) are the frameworks that will be scanned.

Background: Features to improve the standards for compliance and interoperability with other web browser were introduced and modified by Microsoft since Windows Internet Explorer 9. A lot of JavaScript frameworks have functions which rely on functions of earlier versions of Windows Internet Explorer. In Windows Internet Explorer 11, some well-known JavaScript frameworks might not work as they should. Most of these JavaScript frameworks already received updates to fix this. Nonetheless, there are still a lot of web applications where the older versions of these frameworks are still in use and which have not yet been updated.

More Information: http://msdn.microsoft.com/en-us/library/hh180175(v=VS.85).aspx

Manual Remediation: Ask the manufacturer to deliver a framework which is compatible to Microsoft Internet Explorer 11.

WC010 - Unconventional Protocol Handlers

Description: RayQC Advanced scans the web application for the use of unconventional protocols in script redirections and hyperlinks.

Background: The prefix of the URL address refers to a protocol name (http://www.raynet.de for a HTTP protocol, `javascript:alert('Welcome')` for a JavaScript protocol). An application can be registered to a URL protocol. If this is the case, since Windows Internet Explorer 9, the

Application Protocol Handler Dialog will be shown when the application is launched. This is a security feature which should protect users from executing an application containing dangerous or malicious content by accident. The dialog will be shown with each execution of the request until the dialog for this protocol has been disabled. The information, that a program which is not installed is required for the launch of the web application, will be shown if no application is registered to a URL protocol.

More Information: http://msdn.microsoft.com/en-us/library/dd565637(VS.85).aspx

Manual Remediation: Uncheck the **Always ask before opening this type of address** checkbox after using a link to prevent further displays of the Application Protocol Handler Dialog by Windows Internet Explorer 11. Portions of a web application might not work if no application is configured to handle a non-standard protocol.

WC011 - Status Bar Text Changes

Description: RayQC Advanced scans the JavaScript properties `window.status` and `window.defaultStatus` for the use of scripts that change the status bar content.

Background: Since Windows Internet Explorer 7, web applications are no longer allowed to use scripts to configure the status bar in the internet or restricted zones. Because of this, calls to the JavaScript properties `window.status` or `window.defaultStatus` might silently fail. By this measure, attackers should no longer be able to spoof the status bar.

More Information: http://msdn.microsoft.com/en-us/ie/aa740486

Manual Remediation: Check the **Allow status bar updates via script** checkbox which you will find in the custom security level in the Internet Options setting in Windows Internet Explorer 11 to allow the configuration of the status bar by scripts which use the `window.status` and `window.defaultStatus` methods.

WC012 - Obsolete Dynamic Properties

Description: RayQC Advanced scans the web application for obsolete dynamic properties in CSS or JavaScript code.

Background: Property values could be set as formulas, not only as constants, through the use of dynamic CSS properties since Windows Internet Explorer 5. Authors were provided with the ability to reference property values from other values by using a dynamic property and thereby offered an unparalleled flexibility when designing their webpages. But this also led to a damaging impact on standard compliance, performance, reliability, and security considerations. Dynamic properties are obsolete since Windows Internet Explorer 8.

More Information: http://msdn.microsoft.com/en-us/library/ms537634(v=vs.85).aspx

Manual Remediation: Replace the dynamic properties functionality with JavaScript event listeners.

WC013 - Conformity to the Request for Comments (RFC) Guidelines

Description: RayQC Advanced scans the web application for the use of URLs that do not meet the requirements of the RFC 3986 and 3987 guidelines.

Background: To prevent malformed URLs from fooling Windows Internet Explorer, the URL is parsed to assure that it meets the RFC guidelines after being entered into the address bar since Windows Internet Explorer 7. The web application will be allowed to appear with a restricted functionality if it fails to pass the verification process. This might lead to an unexpected

behavior of the web application.

More Information: https://msdn.microsoft.com/en-us/library/dd565653(v=vs.85).aspx

Manual Remediation: Re-engineer the web application and make sure that all URLs used in the web application meet the requirements of the RFC 3986 and 3987 guidelines.

WC014 - CSS Compatibility

Description: RayQC Advanced scans the web application for the use of CSS features which are not supported by Windows Internet Explorer 11.

Background: The support for the W3C CSS standard has been improved with each new release of Windows Internet Explorer (:`focus {sRules}` is supported by Windows Internet Explorer 11, but it is not supported by Windows Internet Explorer 7). There is a full compliance with CSS 2.1 and many CSS 3 features are supported in Windows Internet Explorer 11.

More Information: http://msdn.microsoft.com/en-us/library/cc351024(v=vs.85).aspx

Manual Remediation: Re-engineer the web application to use only CSS features which are supported by Windows Explorer 11.

WC015 - XSLT (Extensible Stylesheet Language Transformations) Changes

Description: RayQC Advanced scans the web application for the use of unsupported XSLT elements. Legacy XSL namespaces, legacy stylesheets processing instructions, and XSLT output directives are the features that will be scanned.

Background: XSLT is used for the modification of XML documents and is a declarative language based on XML. The processing of XML and XSLT files has been modified for the improvement of conformation to the standards of other browsers and the compatibility to other browsers since Windows Internet Explorer 9. Chiefly, there have been changes to some of the non-standard behaviors relating to the processing of XSLT files. These might cause web applications to show unexpected behavior or a limited functionality.

More Information: http://msdn.microsoft.com/en-us/library/hh180178(v=vs.85).aspx

Manual Remediation: Re-engineer the web application by migrating to a compatible and standardized XSLT namespace. Microsoft has prepared some migration scenarios.

WC016 - Obsolete Document Modes

Description: RayQC Advanced scans the web application for the use of Document Compatibility Modes.

Background: With document modes, a tool to maintain features which were supported by earlier versions of the browser was provided by Microsoft since Windows Internet Explorer 8. The edge mode, representing the highest possible support for modern standards, is the preferred mode in Windows Internet Explorer 11. Therefore, document modes have become obsolete and they should not be used any longer.

More Information: http://msdn.microsoft.com/en-us/library/ie/dn384051(v=vs.85).aspx

Manual Remediation: Re-engineer the web application not to use Document Compatibility Modes.

WC017 - Obsolete DirectX- based Filters and Transitions Reference

Description: RayQC Advanced scans the web application for the use of DirectX-based filters

and transitions which are no longer supported in Windows Internet Explorer 11.

Background: Web developers were allowed to add multimedia-style effects to their webpages by the usage of a set of visual filters and transitions since Windows Internet Explorer 4.0. They are called DX filters because of their underlying implementation, DirectX, and their long-form syntax (`filter:progid:DXImageTransform.Microsoft.Alpha(opacity=75)`). There exists a standard-based alternative to common DX filters since Windows Internet Explorer 9.

More Information: http://msdn.microsoft.com/en-us/library/ms532853%28v=vs.85%29.aspx

Manual Remediation: Re-engineer the web application to use standard-based technologies.

WC018 - Obsolete Vector Markup Language (VML) Elements

Description: RayQC Advanced scans the web application for the use of obsolete VML elements.

Background: VML, which was used to create vector graphics that were displayed in web applications, is no longer supported by Microsoft since Windows Internet Explorer 11.

More Information: http://msdn.microsoft.com/en-us/library/ie/hh801223%28v=vs.85%29.aspx

Manual Remediation: Re-engineer the web application to use standard-based technologies like e.g. Scalable Vector Graphics (SVG) format.

WC019 - Microsoft Internet Explorer plug-in Compatibility in the Windows UI

Description: RayQC Advanced scans the web application for embedded content for which the use of external plug-ins is required.

Background: Windows Internet Explorer 11 offers two different ways of browsing. There is the Windows Internet Explorer in the Windows UI and there is the Windows Internet Explorer for the desktop, which are both using the same technology for the rendering of web applications. Even though, the behavior and feel might differ. For example, the Adobe Flash support is limited and other plug-ins, like Java applets, are not supported by the Windows Internet Explorer in the Windows UI. In the Windows internet Explorer 11 in the Windows UI web applications that use these technologies might not be able to work as anticipated.

More Information: https://msdn.microsoft.com/nl-be/library/hh920753(v=vs.85).aspx

Manual Remediation: Re-engineer the web application to use standard-based technologies, which include supported HTML5 features, to work properly in Windows Internet Explorer 11 in the Windows UI.

WC020 - XML Data Islands Compatibility

Description: RayQC Advanced scans the web application for the use of obsolete XML data islands.

Background: The support for XML data islands has been dropped by Microsoft since Windows Internet Explorer 10. They are now parsed in HTML in order to improve compatibility and compliance with HTML5. Pages which are written for Windows Internet Explorer or pages that use browser sniffing to modify their behavior in Windows Internet Explorer will be influenced by this.

More Information: http://msdn.microsoft.com/en-us/library/ie/hh801224(v=vs.85).aspx

Manual Remediation: Re-engineer the web application not to use XML data islands but to use other technologies instead.

WC021 - Obsolete VBScript Code

Description: RayQC Advanced scans the web application for the use of VBScript code.

Background: VBScript code is no longer supported as scripting language for Windows Internet Explorer since Windows Internet Explorer 11. If displayed in the edge mode, web applications will not execute VBScript code.

More Information: http://msdn.microsoft.com/en-us/library/ie/dn384057(v=vs.85).aspx

Manual Remediation: Re-engineer the web application to use JavaScript instead of VBScript.

WC022 - JavaScript API Features

Description: RayQC Advanced scans the web application for the use of removed JavaScript API features.

Background: Some JavaScript API features have been removed by Microsoft since Windows Internet Explorer 11 (`document.all`, `document.selection`, etc.). This might lead to incorrect display or crashes if unhandled exceptions occur for applications which still rely on the removed standards.

More Information: http://msdn.microsoft.com/en-us/library/ie/ bg182625(v=vs.85).aspx#legacyAPIs

Manual Remediation: Re-engineer the web application to use the replacements of the removed JavaScript features (Removed API feature: `document.all`; Replacement feature: `document.getElementByld`).

WC023 - Obsolete Prefixed Pointer Events

Description: RayQC Advanced scans the web application for JavaScript and CSS code using Microsoft pointer events.

Background: Pointer events with vendor prefixes (`MSPointerCancel` event, etc.) were introduced as a replacement of W3C Pointer Events since Windows Internet Explorer 10. The support for the prefixed versions of the pointer events and APIs was dropped by Microsoft since Windows Internet Explorer 11. The Microsoft prefixed version of the pointer events may be removed completely in future releases.

More Information: http://msdn.microsoft.com/en-us/library/ie/dn304886(v=vs.85).aspx

Manual Remediation: Re-engineer the web application to use the W3C Pointer Events instead of the obsolete prefixed versions of the pointer events (Prefixed pointer event: `MSPointerDown` event; W3C Pointer Event: `pointerdown` event).

WC024 - Flexible Box Changes in CSS Script

Description: RayQC Advanced scans the web application for obsolete vendor prefixes in CSS flexible boxes.

Background: Flexible boxes with vendor prefixes (The "`-ms-flex-wrap`" property, etc.) were introduced by Microsoft since Windows Internet Explorer 10. W3C CSS properties have replaced the vendor prefixes in the flexible boxes since Windows Internet Explorer 11 and the support for the prefixed version was dropped by Microsoft.

More Information: http://msdn.microsoft.com/en-us/library/ie/dn265027(v=vs.85)

Manual Remediation: Re-engineer the web application not to use the removed CSS properties anymore, but to use their replacements instead ("`-ms-flex-pack`" property use the "`justify-content`" property instead of the "`-ms-flex-pack`" property, etc.).

WC025 - Cross-browser plug-in Detection Compatibility

Description: RayQC Advanced scans the web application for the use of the `window.ActiveXObject` property.

Background: plug-ins and Internet media type properties (mimeTypes) are supported by the navigator object since Windows Internet Explorer 11. Likewise, it is not possible to find a plug-in if it is using the `window.ActiveXObject property`, because this property is hidden from the document Object Model (DOM).

More Information: http://msdn.microsoft.com/en-us/library/ie/dn423948(v=vs.85).aspx

Manual Remediation: Re-engineer the web application so that a replacement for the `window.ActiveXObject` property will be used.

RayQC Custom Rules

It is possible to create custom rules for RayQC. These custom rules offer an even greater flexibility and the possibility of expansion. Custom rules can be added by simply creating a RayQC checklist and importing it into the RayQC Advanced **Library** to use it for testing.

Import a Custom Rule

Open the **RULE BROWSER** by clicking on the **rules** tile on the RayQC **Dashboard**.

Open the context menu on the RayQC section.

Add a new ruleset underneath the RayQC section of the **RULE BROWSER**.

> **Note:**
> It is necessary to create a sub-ruleset to be able to import checklists into RayQC Advanced.
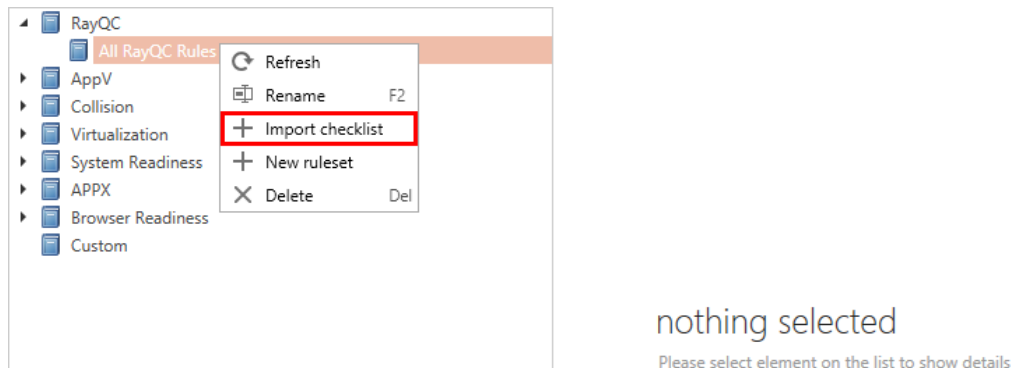
Right-click on the newly created ruleset and select the **Import checklist** item to open the **IMPORT RAYQC CHECKLIST WIZARD**. For information on how to create a checklist refer to the *RayQC User Guide*.

Import RayQC Checklist Wizard

Checklist selection section

Specify the path to the checklist file (`.rqct`) by using the Browse button [**...**].
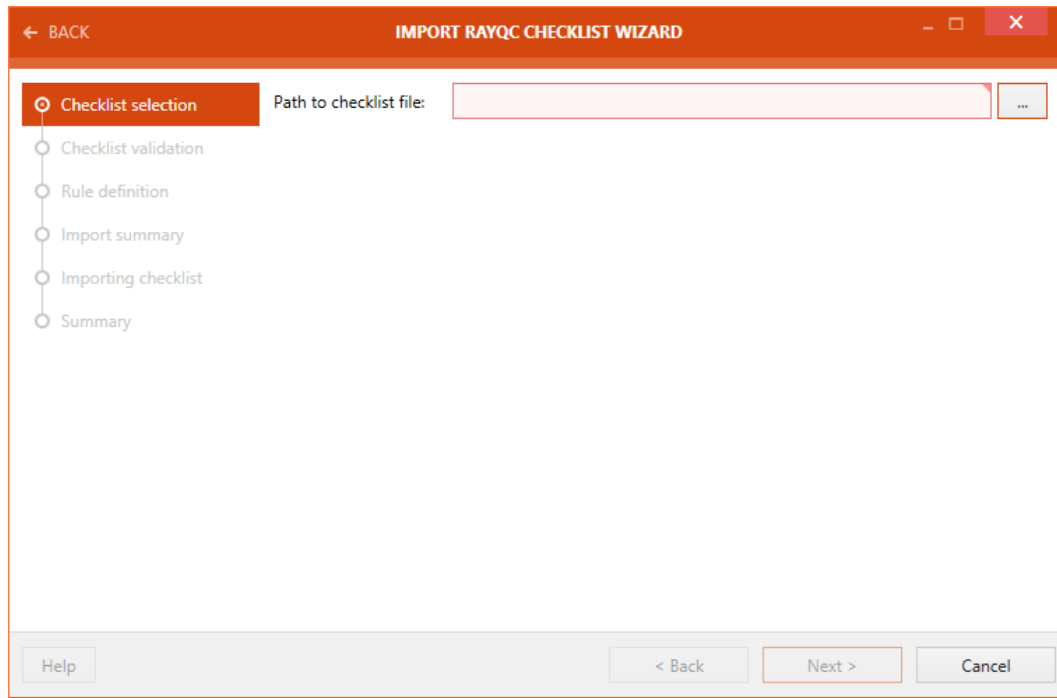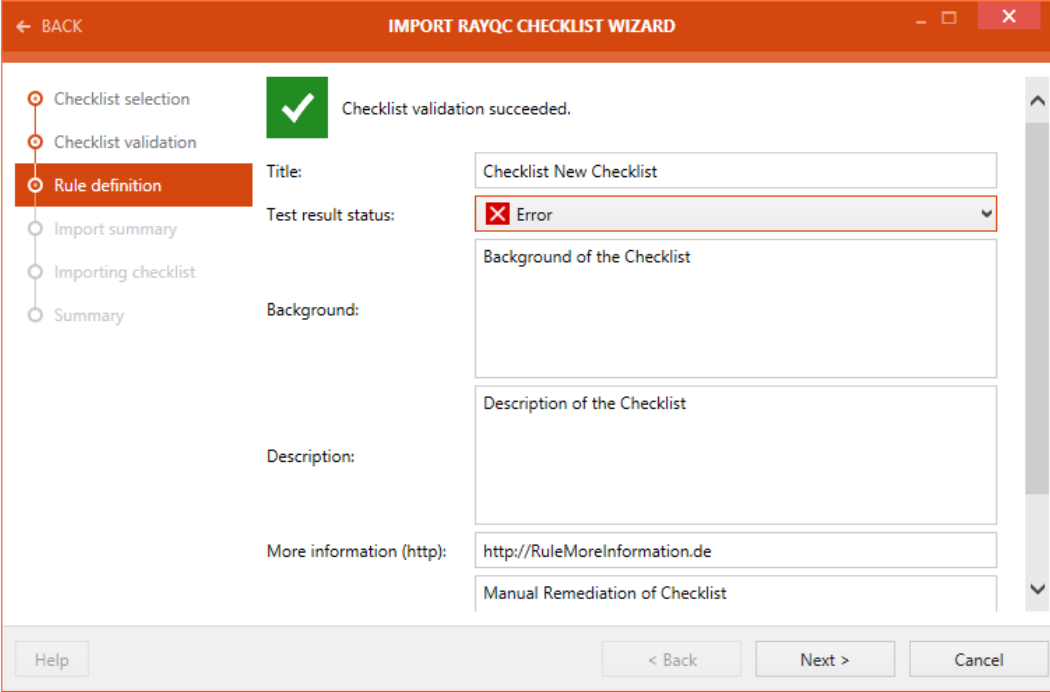
Click on the **Next > button** to proceed to the **Checklist validation**.

Checklist validation section

The checklist will be validated while this page is shown. The validation will pass if the specified checklist does not require any user interaction (The only plug-ins that need an interaction should be single `FileOpenDialog` plug-ins that require the specification of an MSI path). After the checklist has been validated, the wizard will automatically continue to the next section.

Rule definition section

This page contains the result of the validation of the checklist. If the checklist has been validated successfully, the basic rule information can be specified.

The basic rule information consist of **Title**, **Test result status**, **Background**, **Description**, **More information (http)**, and **Manual remediation**, similar to the basic information given for the predefined rules.

If all information have been specified, click on the **Next >** button to continue.

Import summary section

This section shows a summary of the import. Information given in this section include the path to the checklist, the ruleset, the title of the rule, background information on the issue, a description of what the rule is doing, a link where more information on the issue can be found, and a manual remediation for the issue if one exists.
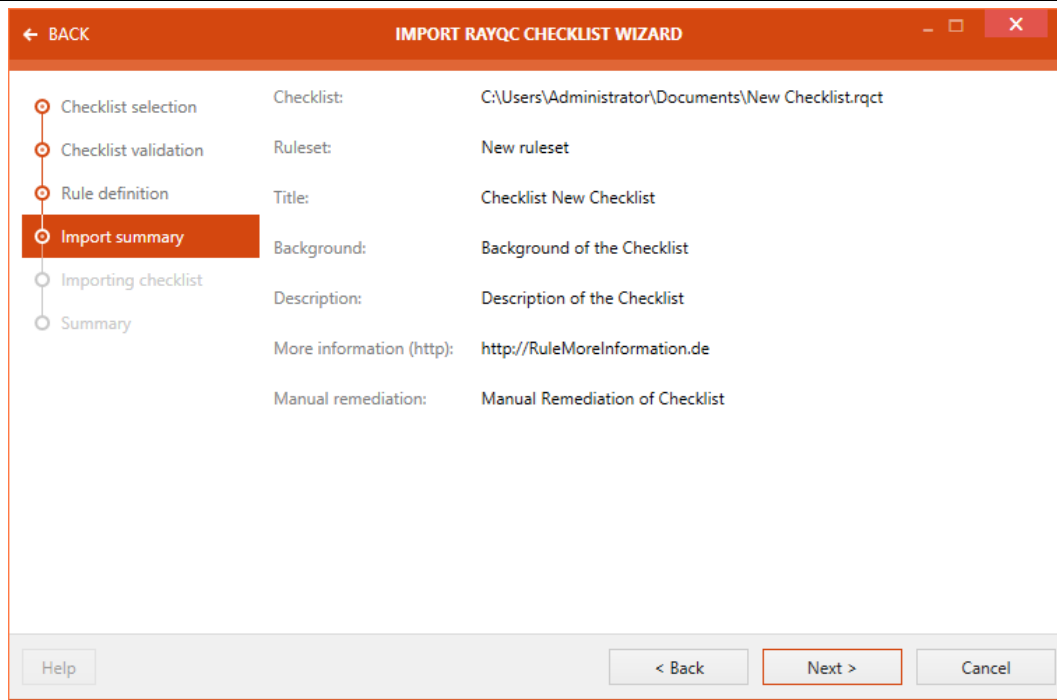
Click on the **Next >** button to continue.

The **Importing checklist** section will be shown while the checklist is being imported. On this page the progress of the import is shown. After the import has been completed successfully the page will automatically switch to the **SUMMARY** page.
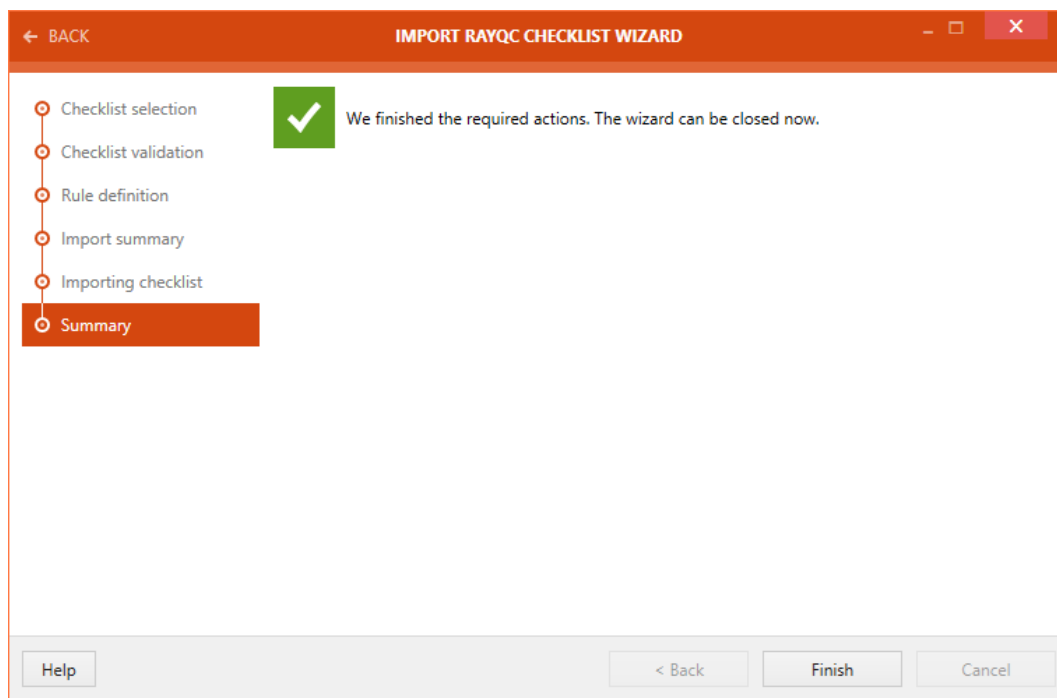
The import has been successfully finished. Click on the **Finish** button to close the **IMPORT**

RAYQC CHECKLIST WIZARD. The imported rule will now be visible in the **RULE BROWSER**.
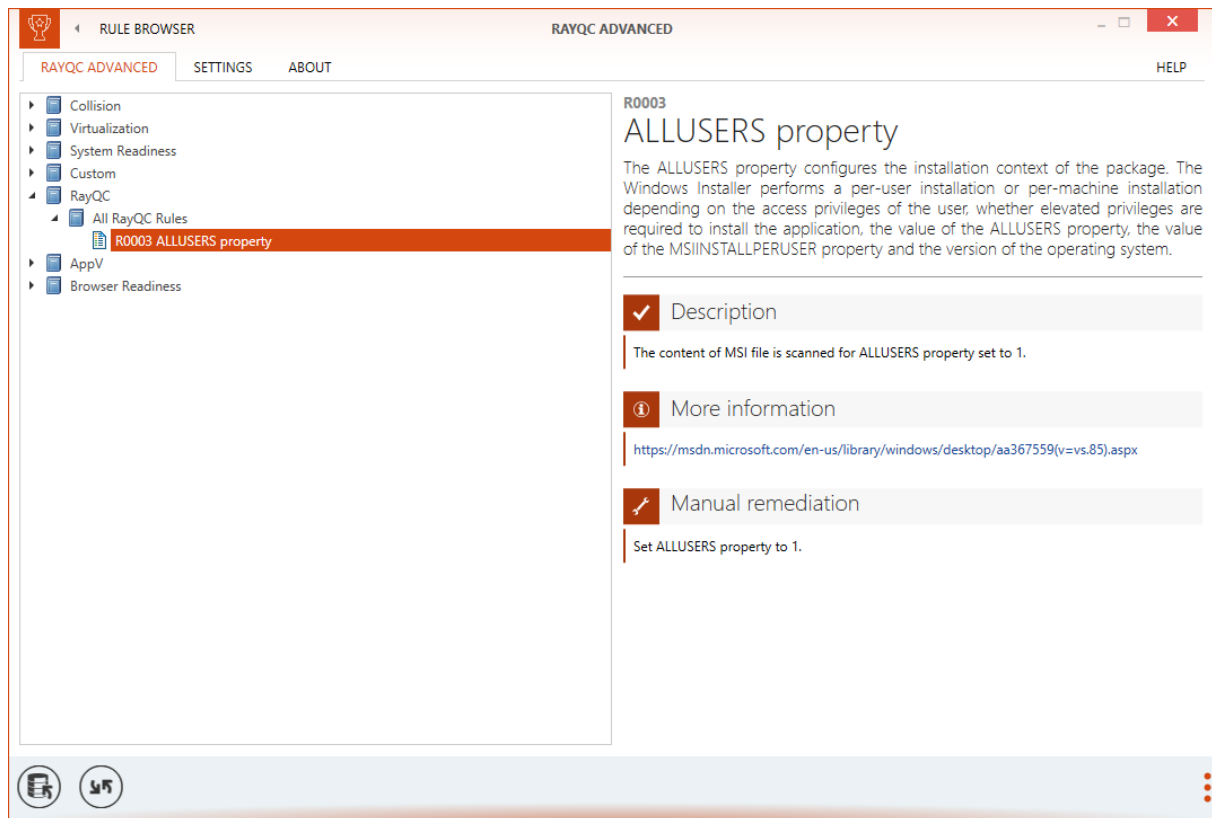
Once the checklist has been imported it can be used for testing in the RayQC Advanced **Test Wizard**. Select the **rayqc checklist** tile in the **Testing areas** section of the **TEST WIZARD** to perform tests using custom rules.
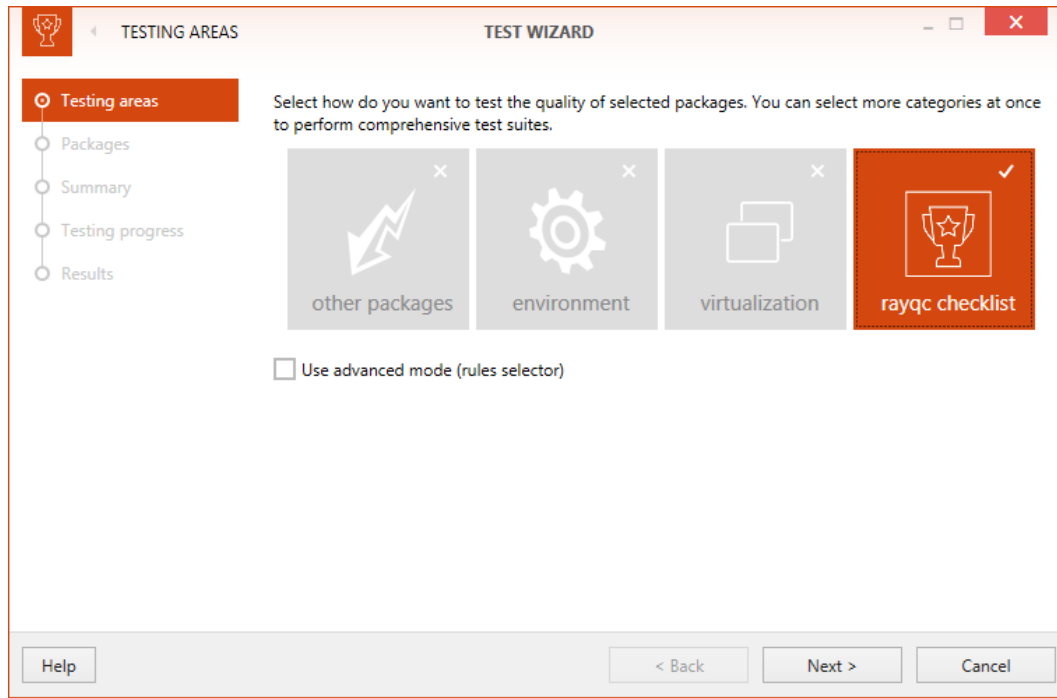
For more information on the **TEST WIZARD** refer to the *Test Wizard* chapter.

Rule Browser

Rule Browser is a UI component of RayQC Advanced, which allows a user to browser through the rules and view their related properties. The **Rule Browser** view can be accessed by selecting **Rules** tile from the RayQC Advanced **Dashboard** on the home screen. Within this interface, rules are cataloged categorically under different test types (called RuleSet), which includes **Collision**, **Virtualization**, **System Readiness**, **Browser Readiness**, and **Custom**.
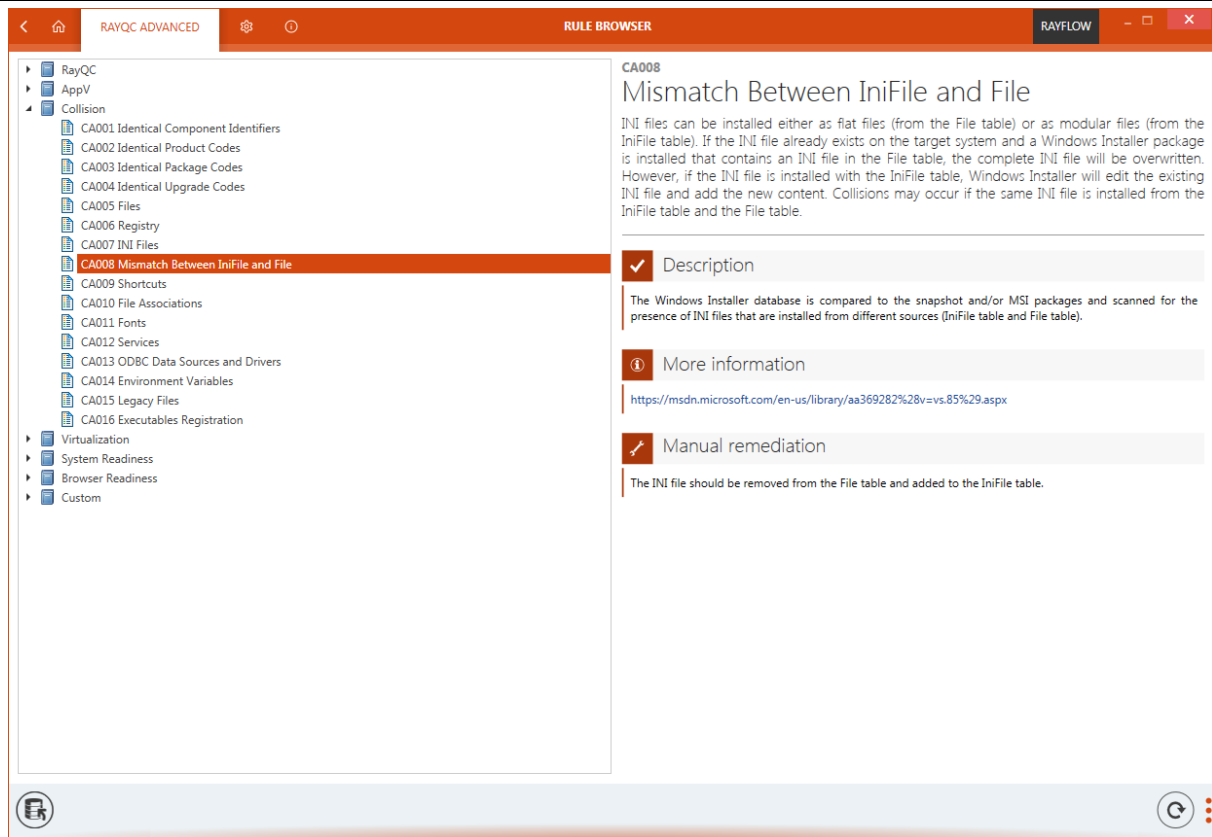
Rule Browser Interface

The **Rule Browser** view consist of two primary areas and a swipe-bar at the bottom. On the left side of the view, rule sets are shown. Each of these sets can be expanded to show rules belonging to it. Contrary to other rule sets, custom allows user to define new rule sets under it.
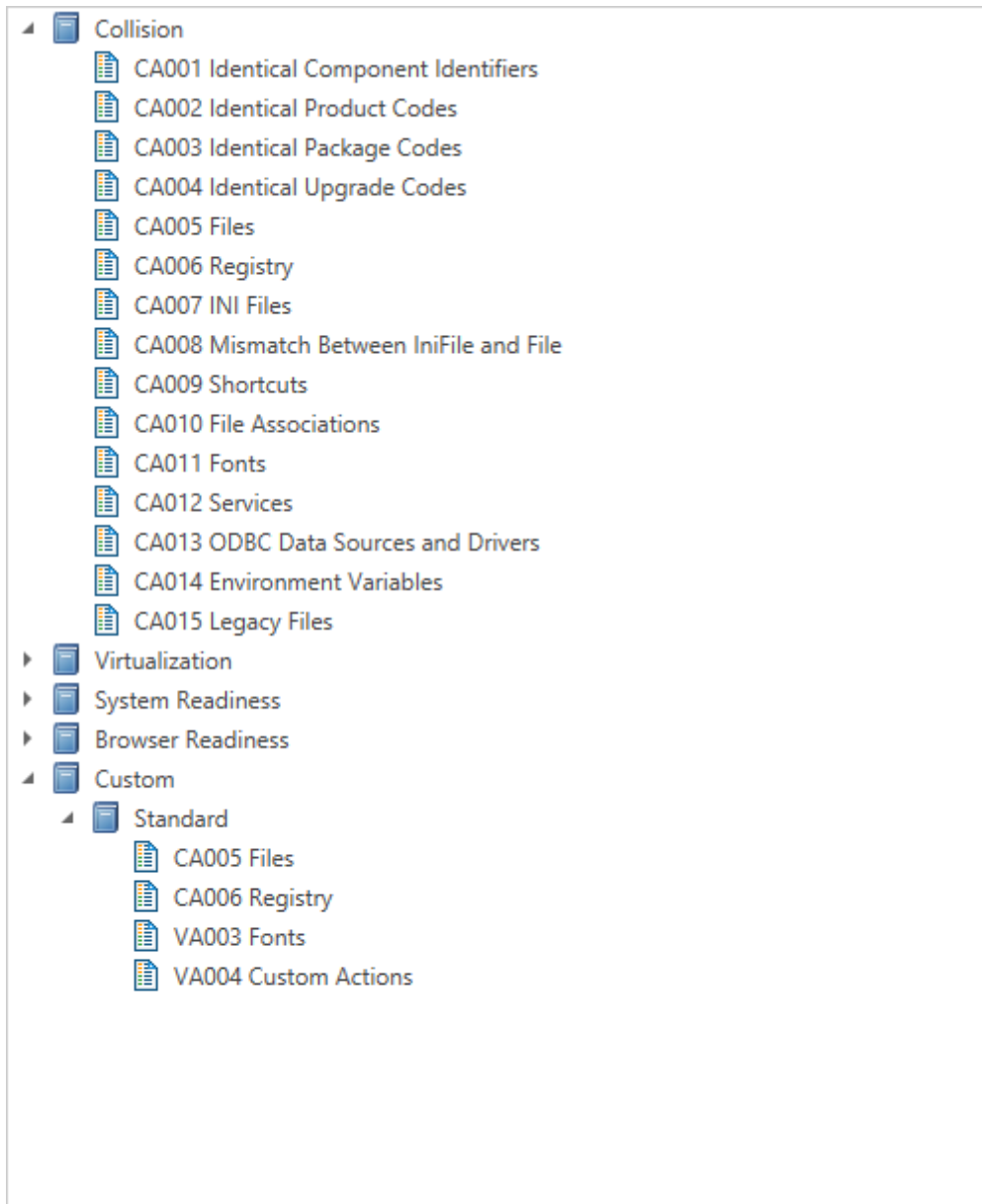
Properties Area

Information pertaining to selected Rule set and rule is shown in the right side-bar. When a particular rule set is selected, the right side bar shows the number of child rule sets and rules under it.

Image below shows the information available in the right side-bar when a user selects a rule set:
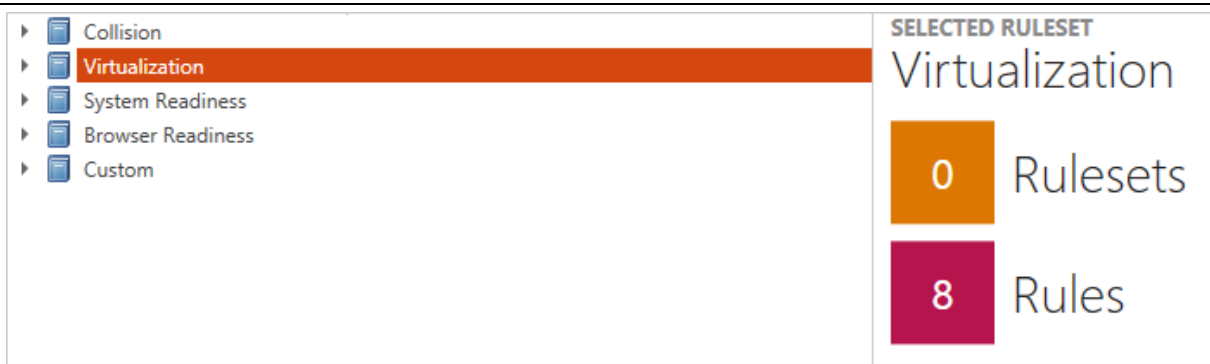
Image below shows the right side-bar when a user selects a rule:
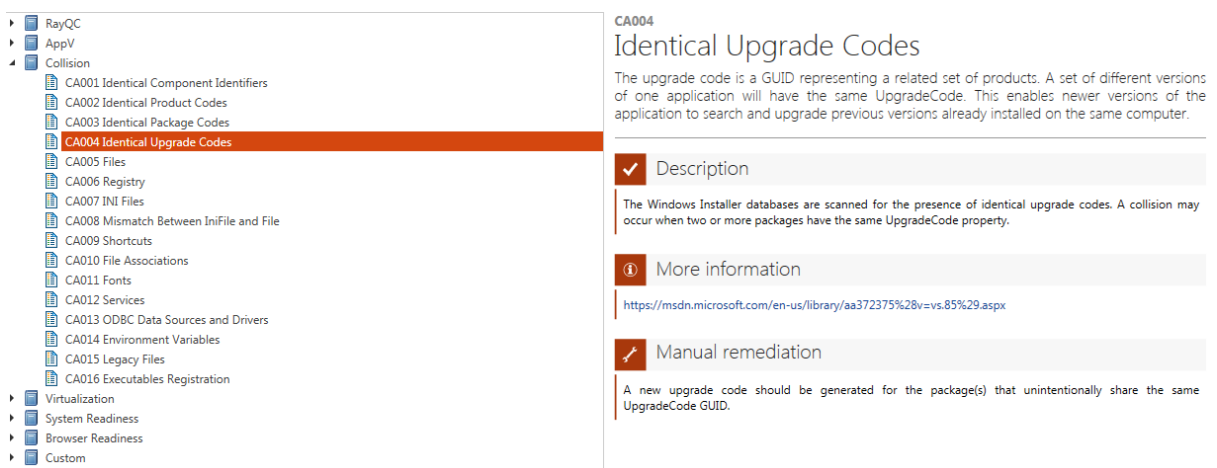
For a particular rule, properties shown in the right side-bar includes following information:

- ID and Name of the rule
- Title – Title of the selected rule
- Description – Description of the actions performed by this rule during test
- Background – Detailed description on what will be checked during the test
- External Reference- Web link to external reference pertaining to the rule

Swipe Bar

Swipe bar is present at the bottom of **Rule Browser** view.
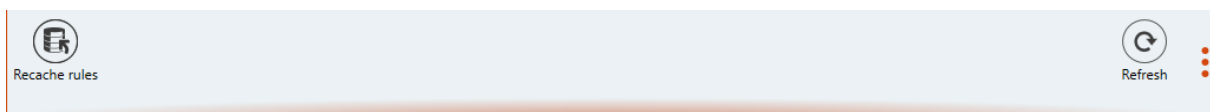
Following actions can be performed using this view:

- **Recache rules**: When a user selects to perform Recache rules action, then RayQC Advanced will import all rules from RayQC Advanced plug-ins catalog (`installation_folder`

`\RayQCAdvanced\Libs\plug-ins`) into database and will be available from all the other functionalities of the application.

- **Refresh:** Performing the refresh action will reload the rule browser view.

Creating Custom Rule Set

A user has an ability to define new rule sets under custom category. To create a new rule set:

1. Access the **Rule Browser** by selecting rules element on the home screen.
   The **Rules Browser** view is loaded.

2. From the left side of the view, right click on the Custom category and select **New RuleSet** option from the context menu.
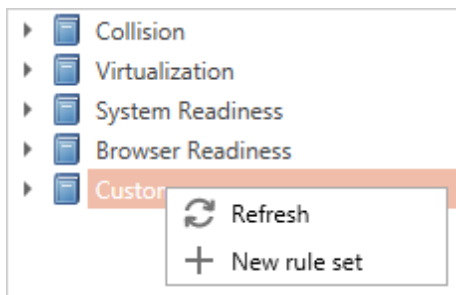
3. A New Rule Set is added, edit its name
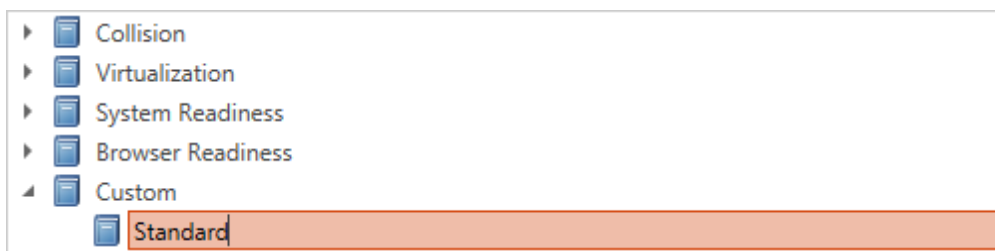
4. A user can either choose to add a sub-rule set or rules to it; or both. Functional options to accomplish these are available through the context menu.To access the context menu, right-click on the newly added rule set.
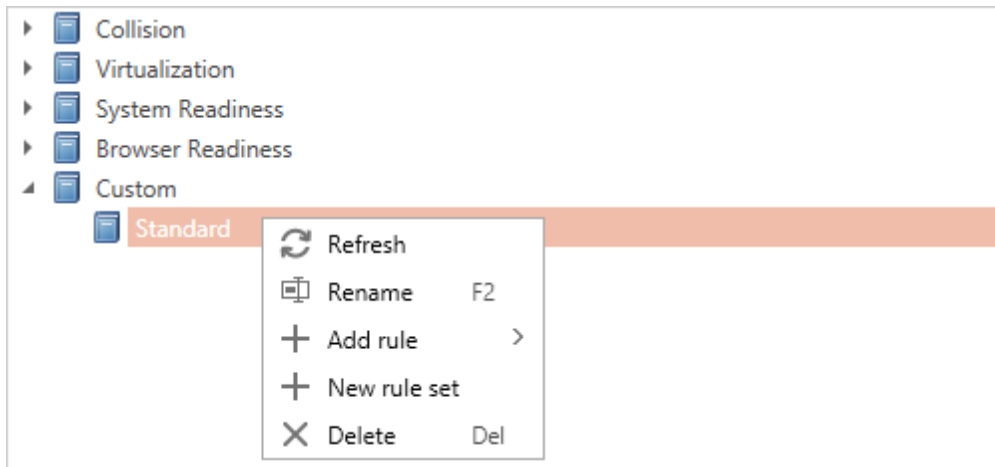
- **Refresh**: Select this option to reload the view.
- **Rename**: Rename the selected rule set. Can also be accessed via **F2** shortcut.
- **Add rule**: Select rules to be added to the rule set. When mouse is hovered over this option, it expands to show different categories of rules, which can further be extended to select rules for respective categories.
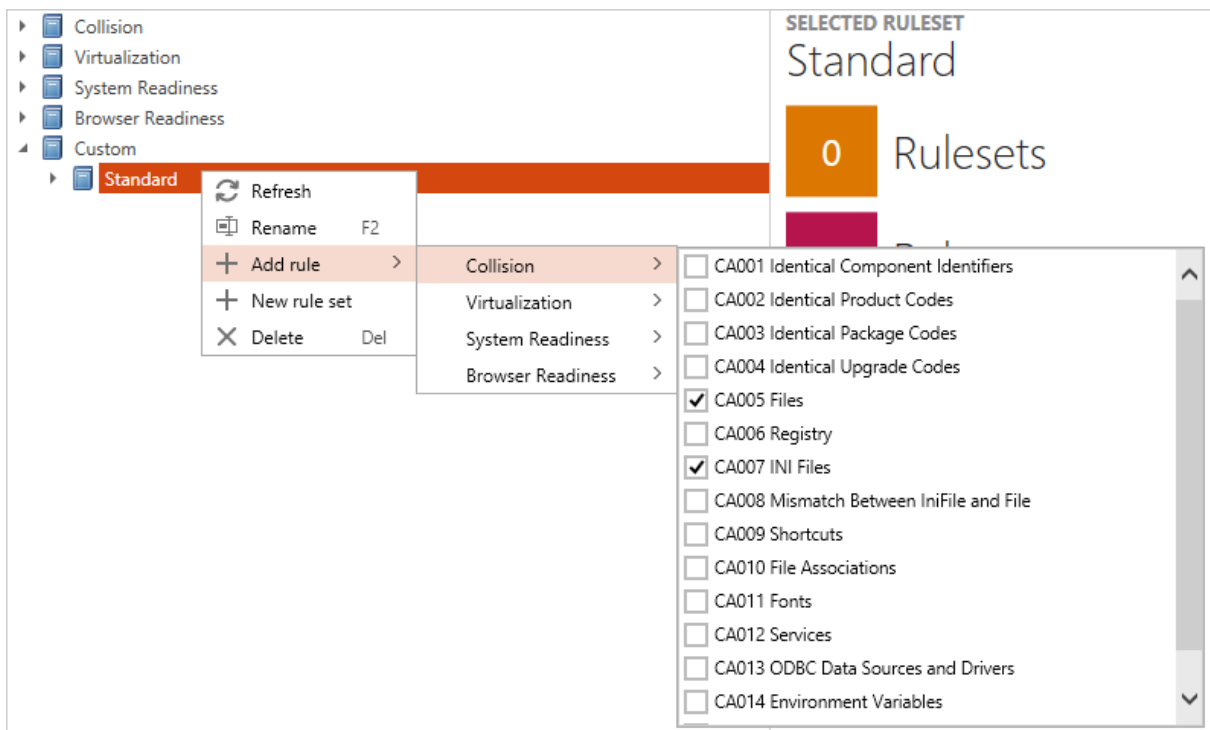
- **New rule set**: Select to add a child rule set to the selected set.
- **Delete**: Delete the selected custom rule set. Can also be accessed via **Del** shortcut.

Modifying a Custom Rule Set

Renaming a Custom Rule Set

A custom rule set can be renamed by first selecting the target rule set and then choosing **Rename** option from the context menu. This option can also be directly executed by using **F2** shortcut key.

Deleting a custom rule set

A custom rule set can be deleted by first selecting the target set and then choosing the **Delete** option from the context menu. This option can also be directly executed by using **Del** shortcut.

Adding or removing rules from a custom rule set

- To add or remove rule(s) to and from a custom rule set, right click on the target set to show the context menu.
- From the context menu select the option **Add rule**.
- This option is then expanded to the right to show different rule categories including **Collision**, **Virtualization**, and **System Readiness**. Each of these categories can be further selected and expanded to the right to show rules list.
- Select the rule (checkbox) to add it to the set.

Additionally a rule belonging to a custom set can be removed by selecting Delete option (shortcut Del) from its context menu.
- Removing a rule from the set will require deselecting an already selected rule.

Test Wizard

The **Test Wizard** is the test execution module of RayQC Advanced. A user can initialize this wizard either from the **Library** or by selecting the **quick test** element on the **Dashboard**. This wizard uses predefined sets of rules to execute collision, OS conformity, and virtualization tests on a package or a set of packages.This wizard also uses a predefined set of rules to execute browser conformity tests on a web application for different web browser.

These test types can briefly be described as:

- **Collision Test** (other packages): Collision tests are carried out to identify common conflicts between different applications, which hinder achieving required level of application isolation. This test can be executed between:

  - MSI (or EXE) and MSI (or EXE)
  - MSI (or EXE) and MSM (Merge Module file)
  - MSI and OS Snapshot

- **Virtualization Test**: Verifies application readiness for virtualization against frontline virtualization technologies

- **OS Conformity Test** (environment): Tests a package for deployment on a selected operating system. A user can execute this test either against predefined set of conformity rules or an OS snapshot, stored in the software library.

- **Environment tests on Virtualization packages**: Tests `.appv` packages against different operating systems.

- **Internet Explorer 9 Conformity Test**: Tests a web application for conformity on Internet Explorer 9.

- **Internet Explorer 10 Conformity Test**: Tests a web application for conformity on Internet Explorer 10.

- **Internet Explorer 11 Conformity Test**: Tests a web application for conformity on Internet Explorer 11.

Quick Test vs. Test via Software Library

If a user wants to execute a test either on an existing package in the **Library** or on a package located on the disk they can directly launch the **Test wizard** from the **quick test** element on the **Dashboard**. When compared to executing test via the **Library**, the **Test wizard** adds two additional steps to the process. In this steps a user has to specify whether to test a package or a

web application. The user also has to specify the target package against which a source package will be tested. The source and the target package can both either come directly from the **software library** or from the disk. If a web application is tested, the application can either come from the **software library** or directly from an URL. When a source package is directly taken from the disk or a web application directly from an URL, the result of the test is available to be stored locally but not in the database, hence the result is not shown in the reports viewer.

Executing Quick Test

To execute a quick test on a package or a web application, follow the steps mentioned below:

Select quick test element from the **Dashboard**. The **Test Wizard** is initialized.

Choose between testing a desktop package or a web application.
Click on the **Next >** button to proceed.

- If **Installer package** has been selected, continue with this *section.*
- If **Web application** has been selected, continue with this *section.*
- If **Virtualization packages** has been selected, continue with this *section.*
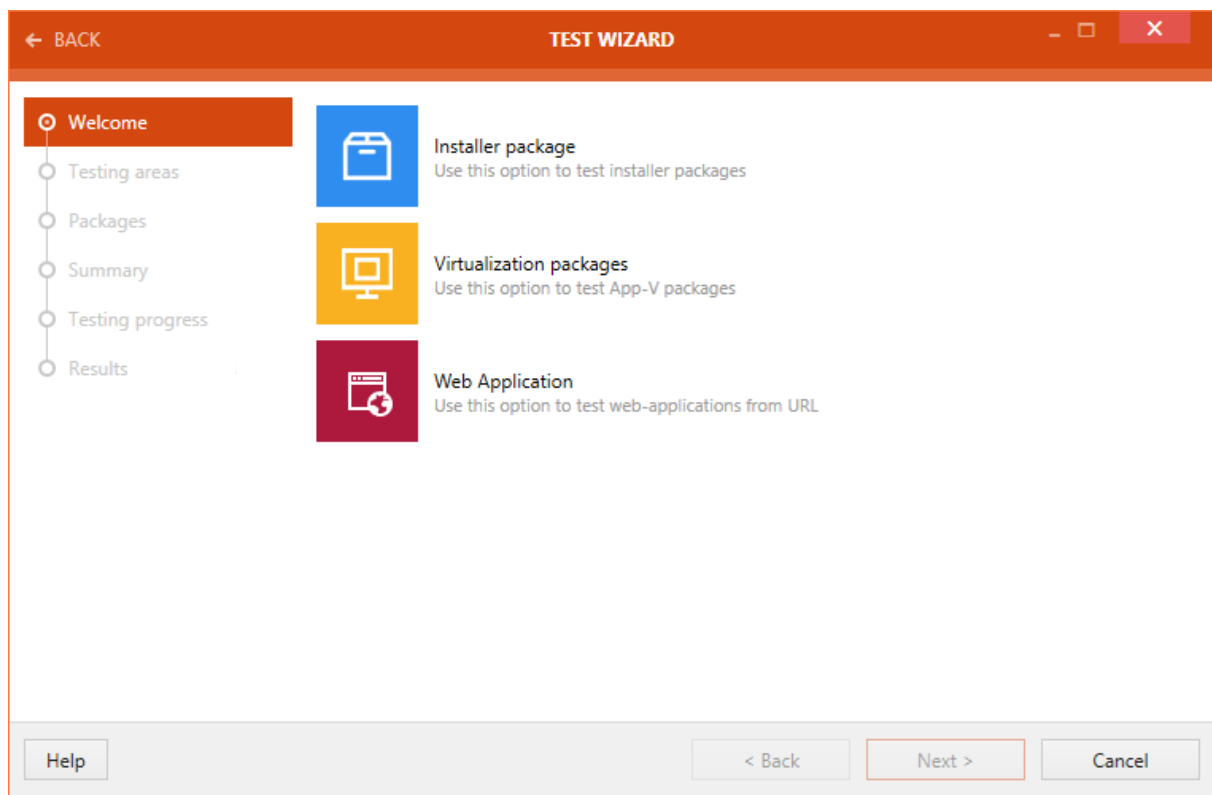
Test an Installer Package

The **Testing areas** are shown.

Within the **Testing areas**, five options are available to users: **other packages** (collision test), **environment** (conformity test), **virtualization**, **appx** and **rayqc checklist**. A user can either execute a test on a package for all the areas or in a mixed mode. Initially, all the testing areas are selected; a user can simply deselect any area by clicking on it.
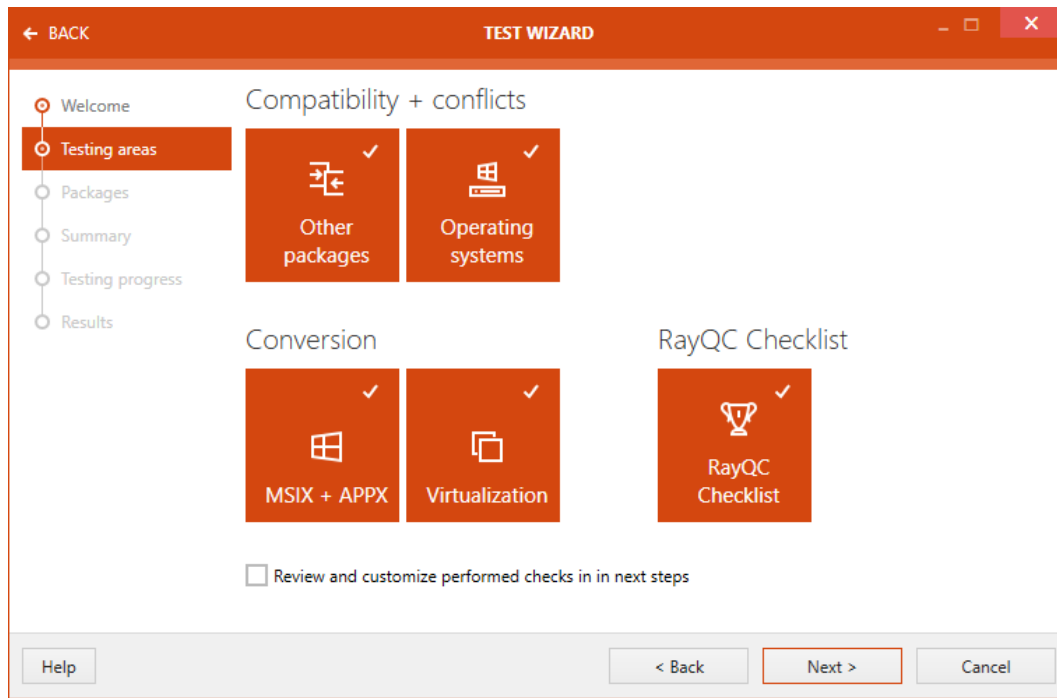
Show detailed rule selector in next step:
Activating the advanced mode provides users an ability to choose testing rules from the supported areas of testing. When this option is not activated, then a package is tested against all the rules from the areas of testing.

To execute collision tests on a package, it is required to select the target packages..

Select package to test. Two radio button options are available to users: **From library** and **From File**.

**From library**:

When this option is selected, then the packages in the **Library** are shown. Navigate and select the desired package(s) for testing.
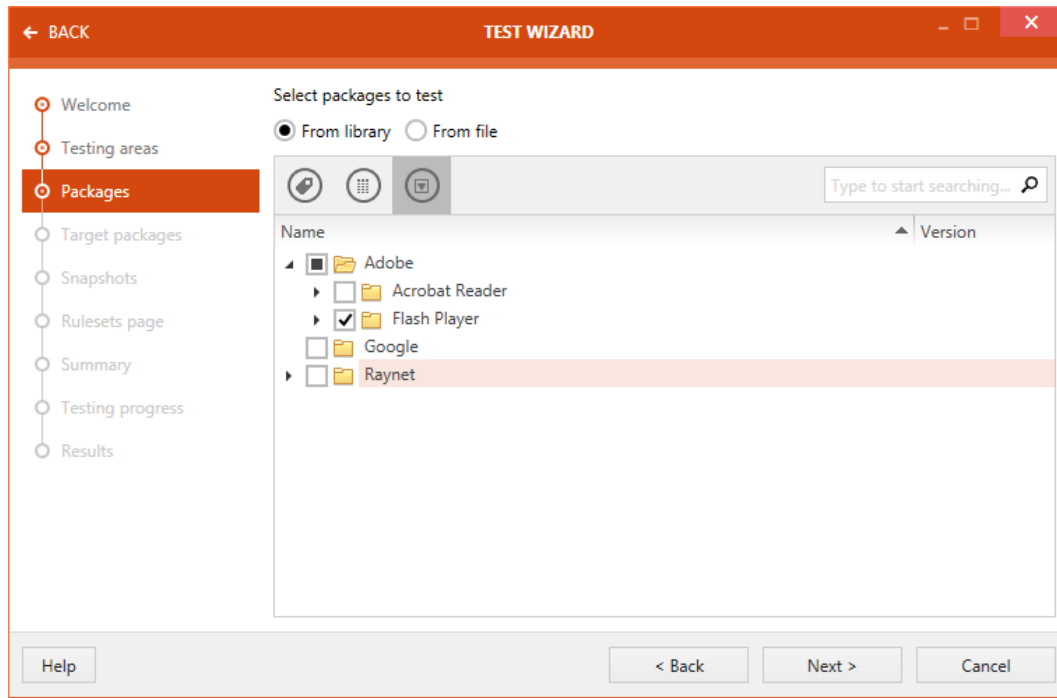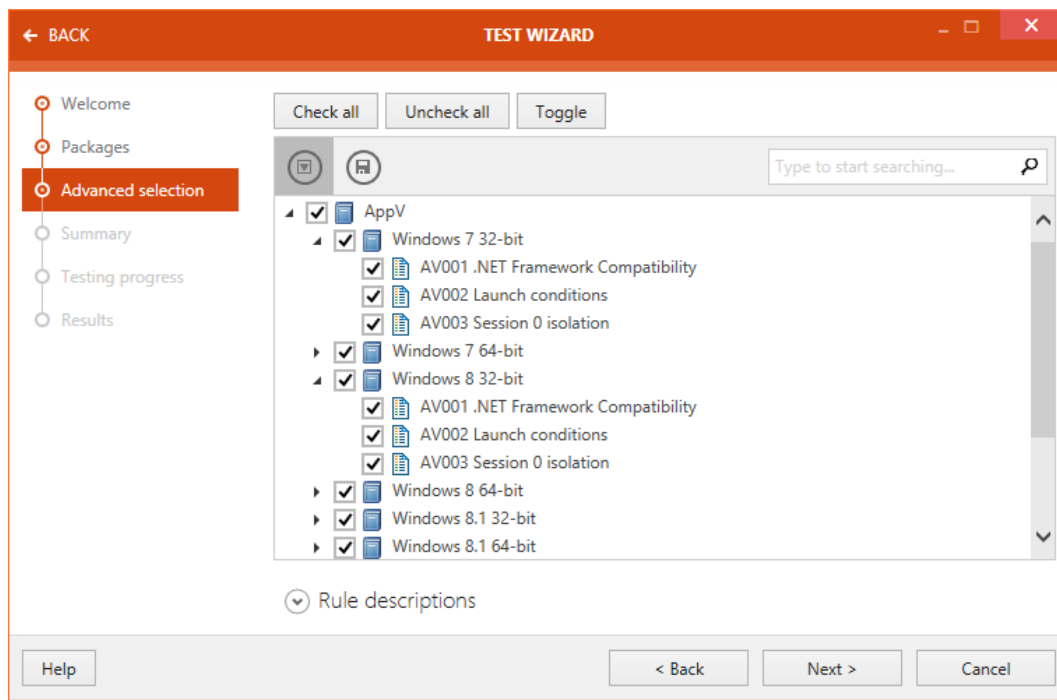
From file:

When this option is selected, three additional buttons are shown: **Add package**, **Add transform**, and **Remove**. The last two buttons are initially deactivated and are automatically activated when a package is added.
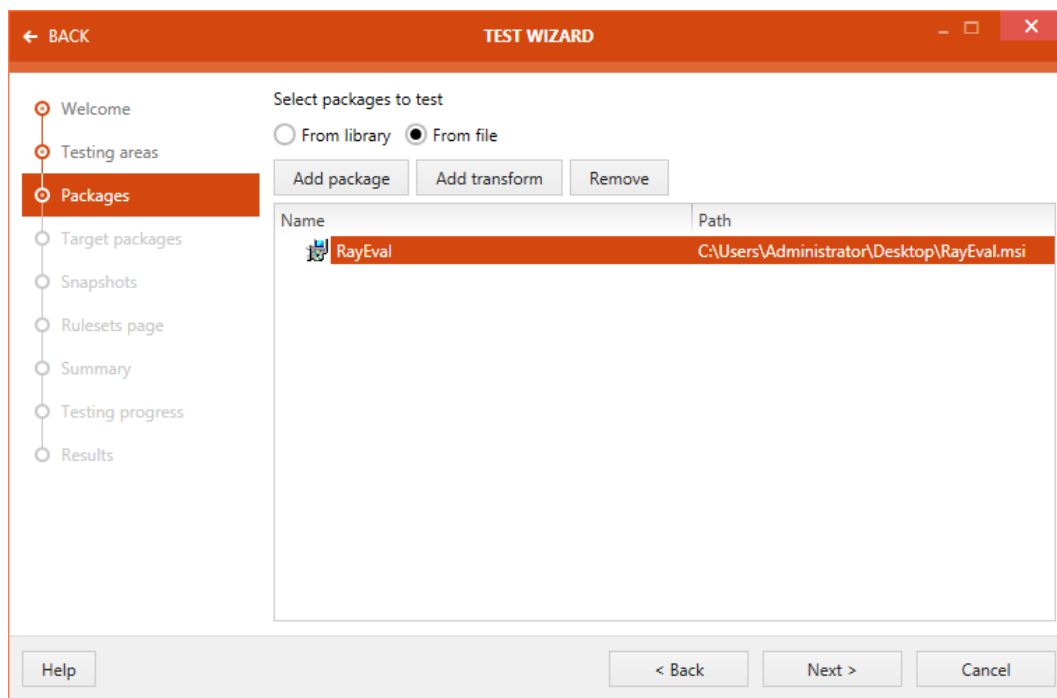
Local files can be imported to the **library** as well. To do this a user has to check the **Import local**

packages option in the **Summary** step.

Once the package(s) has been added, click upon the **Next >** button.

When **other packages** is chosen as the testing area, **Target packages** section is available to users after clicking on the **Next >** button in **Testing areas** section.
Target package can either be selected from database or directly from the disk.
- **From library**: Select that target package(s) and / or merge module(s)
- **From file**: Add package and / or transform from disk.
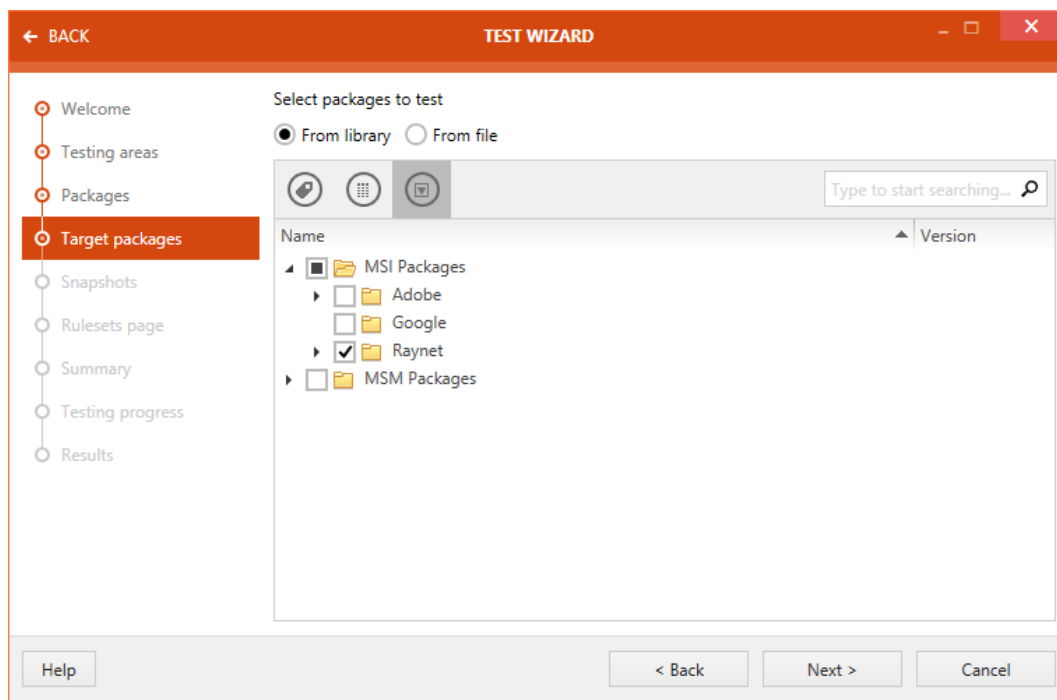
Click on the **Next >** button.

When environment test is selected as one of the testing areas, a user has options to either test the package against an OS snapshot (stored in the **software library**) or execute basic rule based testing.

Testing against an OS snapshot: To use this option for testing, select the option **Test selected packages against a specific snapshot from the library**. When this option is selected, the drop-down list is activated and user can select the target OS snapshot.

Additionally a user can select to perform extended quality assurance with this option. Activating this action will lead to additionally scanning of the package for potential issues that may affect the deployment to a selected operating system.

Testing for a given system: RayQC Advanced contains built-in rules to execute conformity test for a package against particular OS. To use this, select: **Test basic quality assurance for a given system**. After selecting this option, select the target OS from the drop down list.

Click on the **Next >** button.

When APPX, Nano Server, or a virtualization solution is selected as one of the testing areas the **Rulesets** page will be opened. The different rulesets for virtualization and for other fields can be selected.
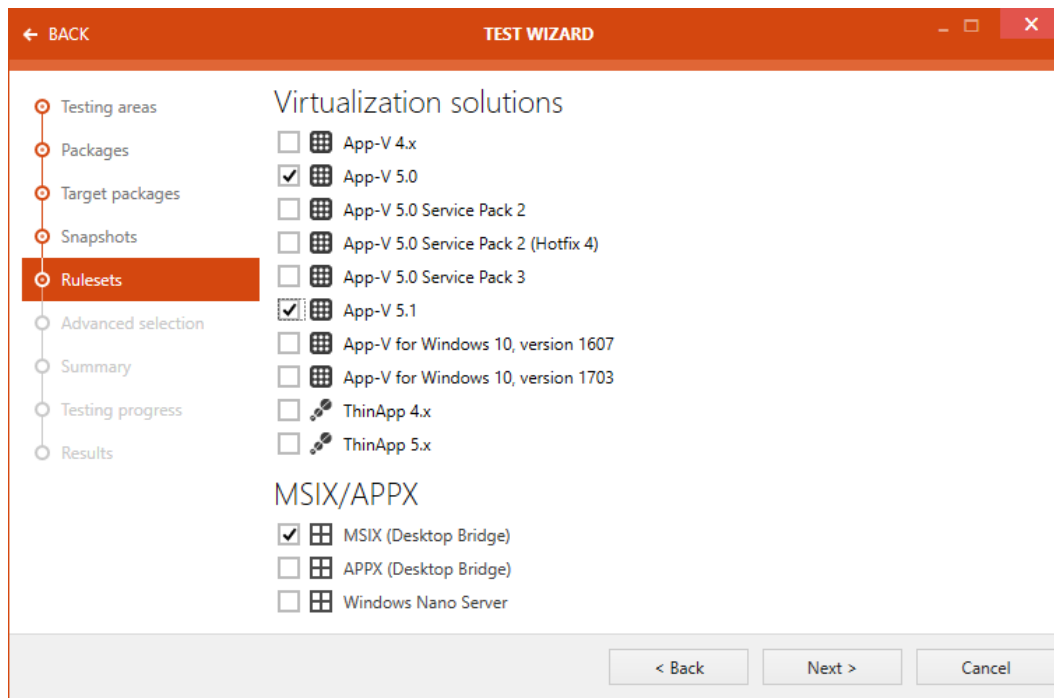
After all target rulesets have been selected click on the **Next >** button.

If advanced mode was selected, then advanced selection section is shown in the next step. Under advanced selection section, a user can select/de-select rules for executing different test types. Test types shown here are directly related to the testing areas chosen.

When a rule is selected, description of that rule is shown under the Rule descriptions.

On top of this section, three buttons are shown: **Check all**, **Uncheck all**, and **Toggle**.

- **Check all**: Selects all the rule, covered under different test areas.
- **Uncheck all**: Deselects all the selected rules, covered under different test areas.
- **Toggle**: Toggle the selection of rules.

Click on the **Next >** button. Summary section is now available. Test criteria are summarized under this section. This summary includes information on source and target package, and a list of test rules, against which the test will be carried out.
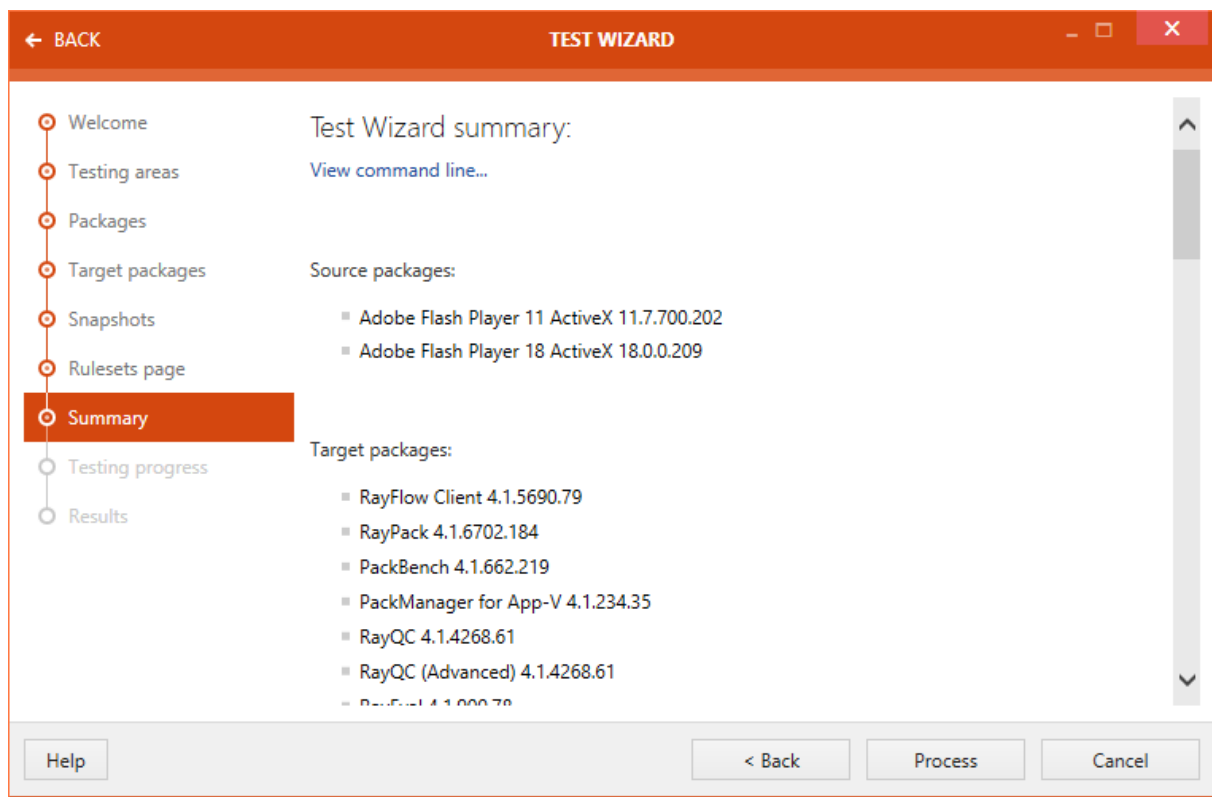
If a user checks the **Import local packages** option, all local files will be imported into the **library**.

Click on the **Process** button to start executing test.

Progress of the test is shown.

After the test are finished the **Issues and fixes** view will be displayed. The issues found in the test are listed here. Select the issues that are going to be displayed in the report by checking the checkbox next to the issue on the left.

If **environment** has been chosen as one of the testing areas, to some of the issues found, fixes can be directly applied.
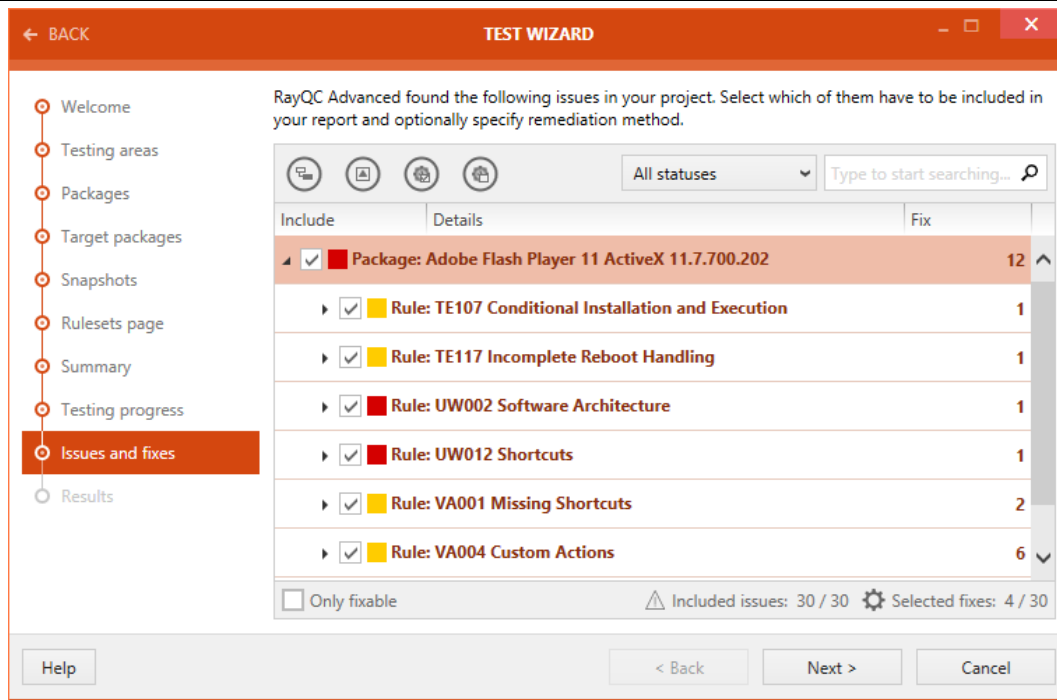
There are two different types of fixes available.

- **Light fix**: Make only minor changes to the package.
- **Power fix**: Which make huge changes to the package.

A fix can be chosen by using the dropdown menu next to the issue on the right. By executing fixes an `.mst`, and in some cases also a `.cab`, for the package will be created.

Select the fixes that should be applied to the package and the issues that will be displayed in the report and click on the **Next >** button.

> ⚠️ **Warning:**
> Since Power fixes can damage the package, only apply Power fixes if sufficient packaging experience and knowledge is at hand.

The progress of the fixing is shown in the **Fixing Progress** section.

After execution of the test, the test result is shown in the Results section.
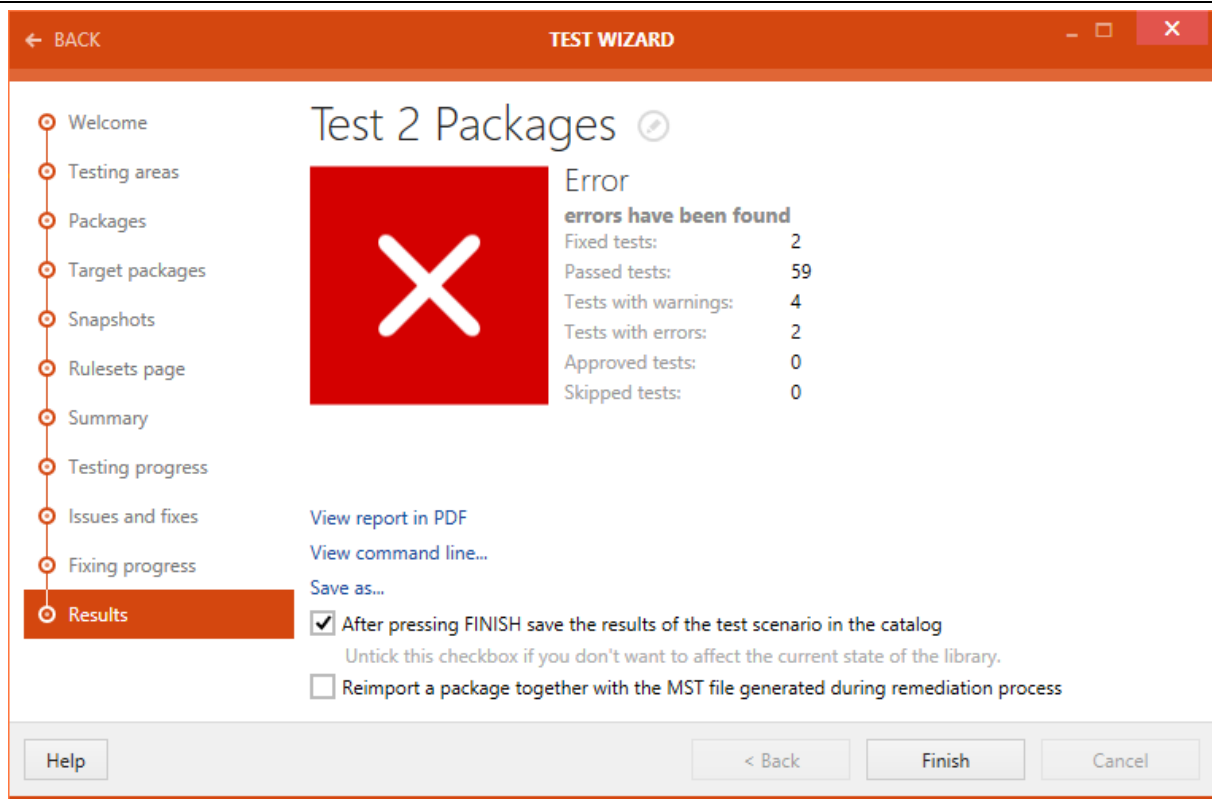
After the fixing is finished, the result will be shown in the **Results** section. There are different options available:

- **See the generated MST file**: Click on this option to open the directory which contains the generated `.mst` file.
- **View reports in PDF**: Click on this option to open the test result in `.pdf` format.
- **View command line...**: Click on this option to view the command line arguments for the current testing scenario.
- **Save as...**: Click on this option to export the test result in one of various available formats. Possible formats are: `.pdf`, `.docx`, `.doc`, `.html`, `.xps`, and `.xml`.

If the **After pressing FINISH save the results of the test scenario in the catalog** option is checked the results of test will be saved in the catalog after clicking on the **Finish** button. Untick the option if the result should not be saved in the library. By default the checkbox is ticked.

If the **After pressing FINISH save the report in RayFlow server** option is checked, the result of the test will be saved to the RayFlow instance after clicking on the **Finish** button. By default, the checkbox is unticked.

If the **Reimport a package together with the MST file generated during remediation process** option is checked, after clicking on the Finish button, the package will be reimported and the `.mst` that was generated when applying the fixes will be imported alongside the package.

Click on the **Finish** button to close the **TEST WIZARD**.

Test a Web Application

The **Web browser** section is shown.

Within the **Web browser** section, select the browsers the web application should be tested against. There are three browsers available for selection: **Internet Explorer 9**, **Internet Explorer 10**, and **Internet Explorer 11**. A user can either execute tests on a web application for all the browsers or in a mixed mode. Initially all the browsers are selected; users can simply deselect any browser by clicking on it.
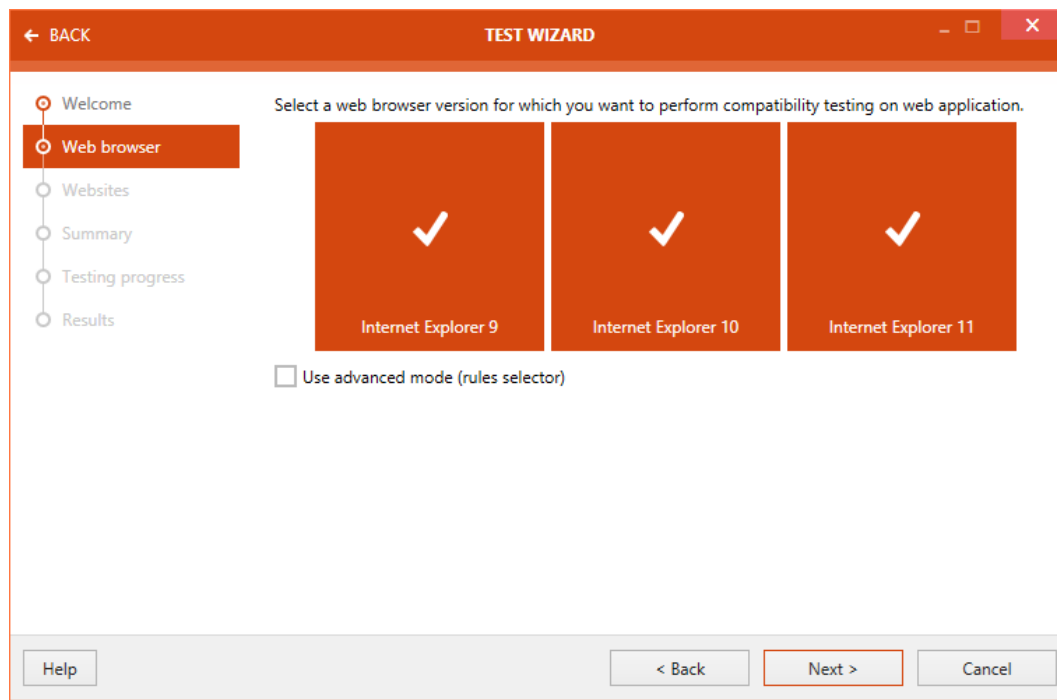
Use advanced mode (rules selector)
Activating the advanced mode, provides the user with an ability to choose testing rules from the supported areas of testing. When this option is not activated, then a package is tested against all the rules from the areas of testing.

Click on the **Next >** button to proceed.

Select package to test.
Two radio button options are available to users: **From library** and **From URL**.

From library:

When this option is selected, then the web applications in the software library are shown. Navigate and select the desired web application for testing.
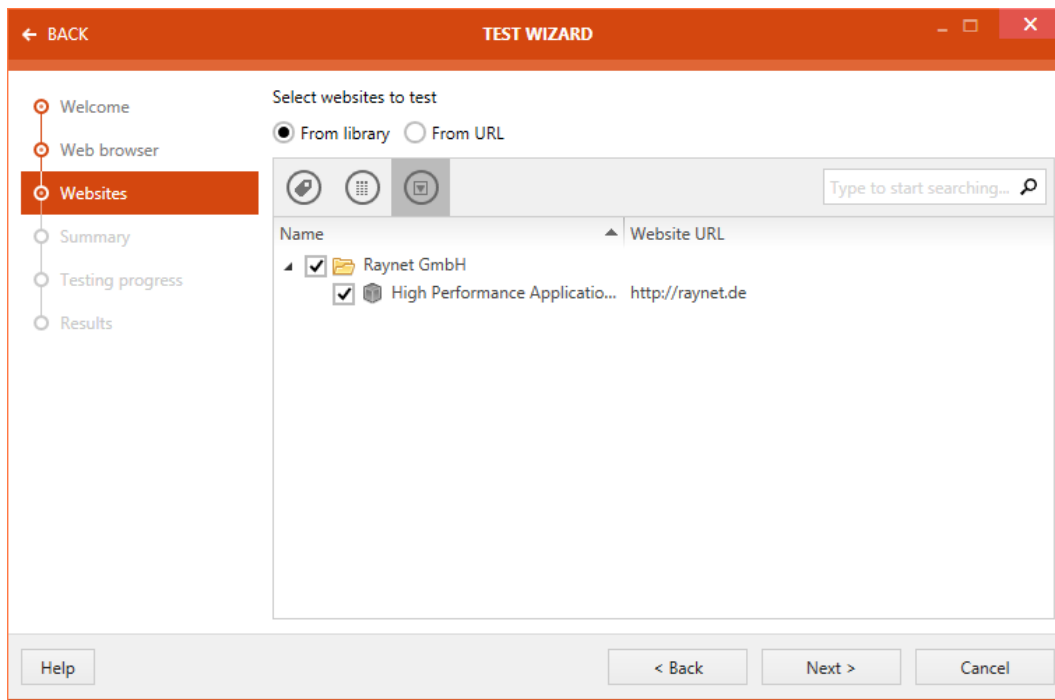
From URL:

a) When this option is selected, enter the URL of the website into the corresponding field. Then specify whether only the entry page should be tested or if crawling should be used.

If crawling is used, define the deepness and the maximum number of pages to crawl. It is also possible to set an URL filter.

> **Be aware:**
> If you try to test a web application from an URL and you have no internet connection, an error message will show when you try to continue.
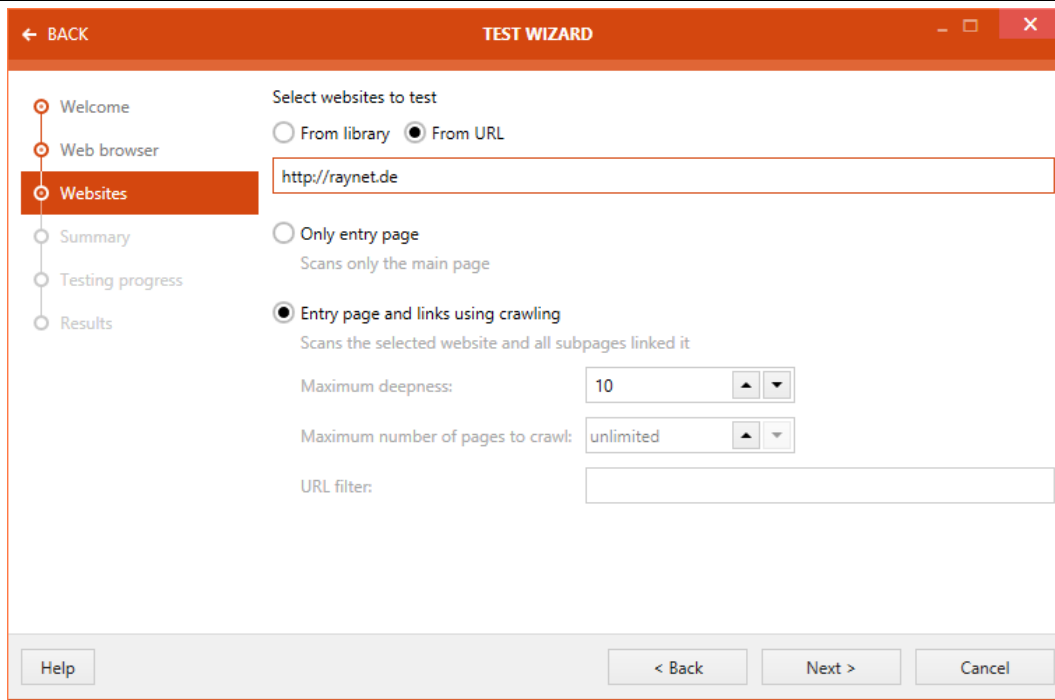
Once the web application has been configured click upon the **Next >** button.

The **Summary** section is now available. The test criteria are summarized under this section. This summary includes information on the web application and a list of test rules against which the test will be carried out.
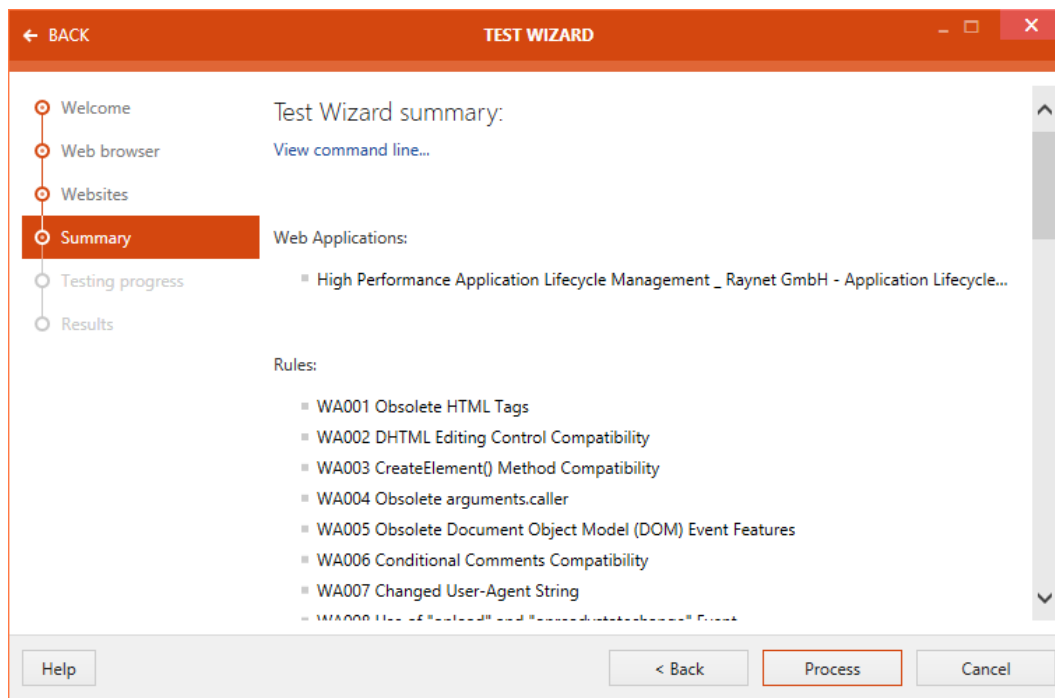
Click on the **Process** button to start executing test.
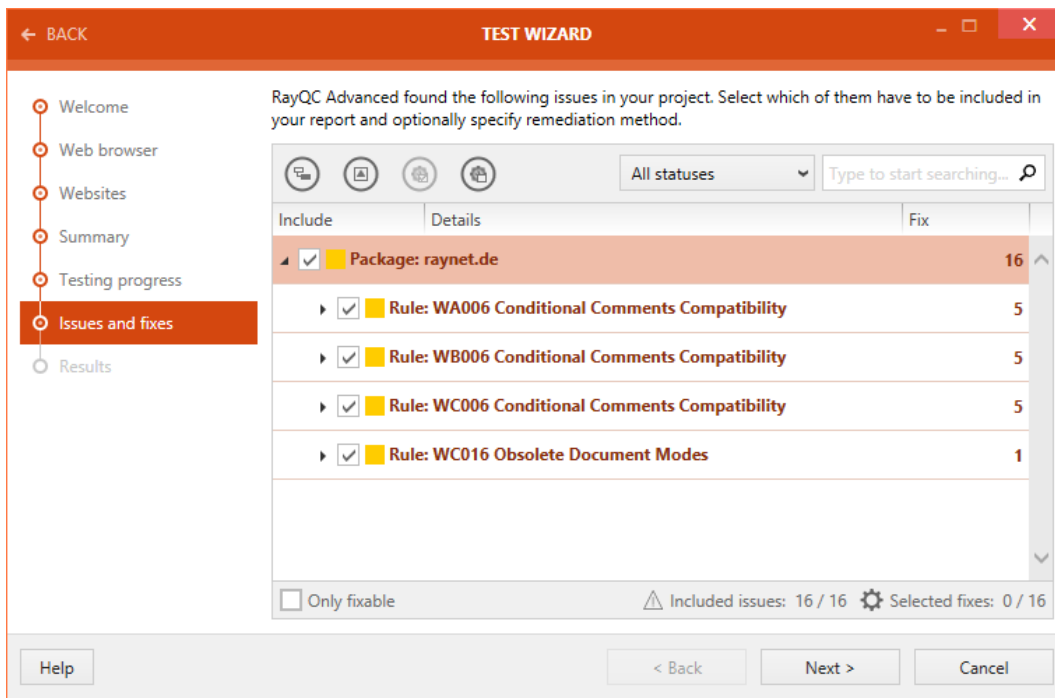
Be aware:
Because the files of the web application that is going to be tested will be fetched in the moment you perform the test, you need a connection to the URL of the target web application.
If you try to test a web application and you have no internet or intranet connection to the URL of the target web application, no tests will be performed and the Test Wizard will proceed to the Results screen.

The progress of the test is shown.

After the test are finished the **Issues and fixes** view will be displayed. The issues found in the web application are listed here. Select the issues that are going to be displayed in the report by checking the checkbox next to the issue.

Click on the **Next >** button to proceed.

After the test is finished, the result will be shown in the **Results** section. There are different options available:

- **View reports in PDF**: Click on this option to open the test result in `.pdf` format.
- **View command line...**: Click on this option to view the command line arguments for the current testing scenario.
- **View crawled links...**: Will show the specific links that have been crawled while testing the applicatoin
- **Save as...**: Click on this option to export the test result in one of various available formats. Possible formats are: `.pdf`, `.docx`, `.doc`, `.html`, `.xps`, and `.xml`.

If the **After pressing FINISH save the results of the test scenario in the catalog** option is checked the results of test will be saved in the library after clicking on the Finish button. Untick the option if the result should not be saved in the library. By default the checkbox is ticked.

Click on the **Finish** button to close the **TEST WIZARD**.

Test a Virtualization Package

Select package to test. Two radio button options are available to users: **From library** and **From File**.

From library:

When this option is selected, then the packages in the software library are shown. Navigate and select the desired package(s) for testing.
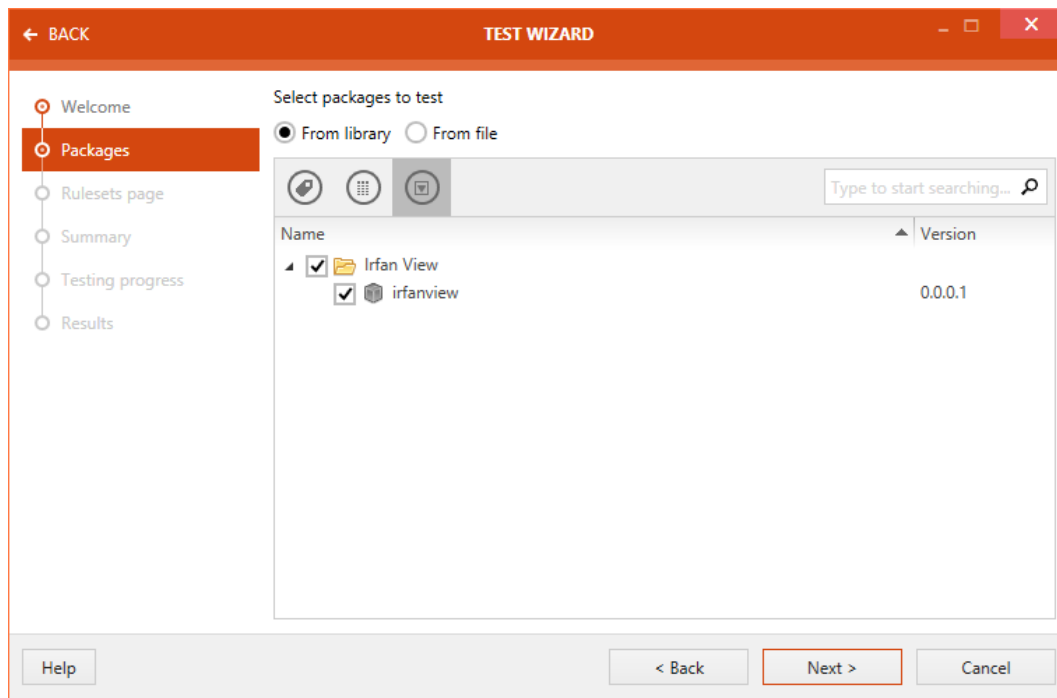
From file:

When this option is selected, two additional buttons are shown: **Add package**, and **Remove**. The last button is initially deactivated and are automatically activated when a package is added.
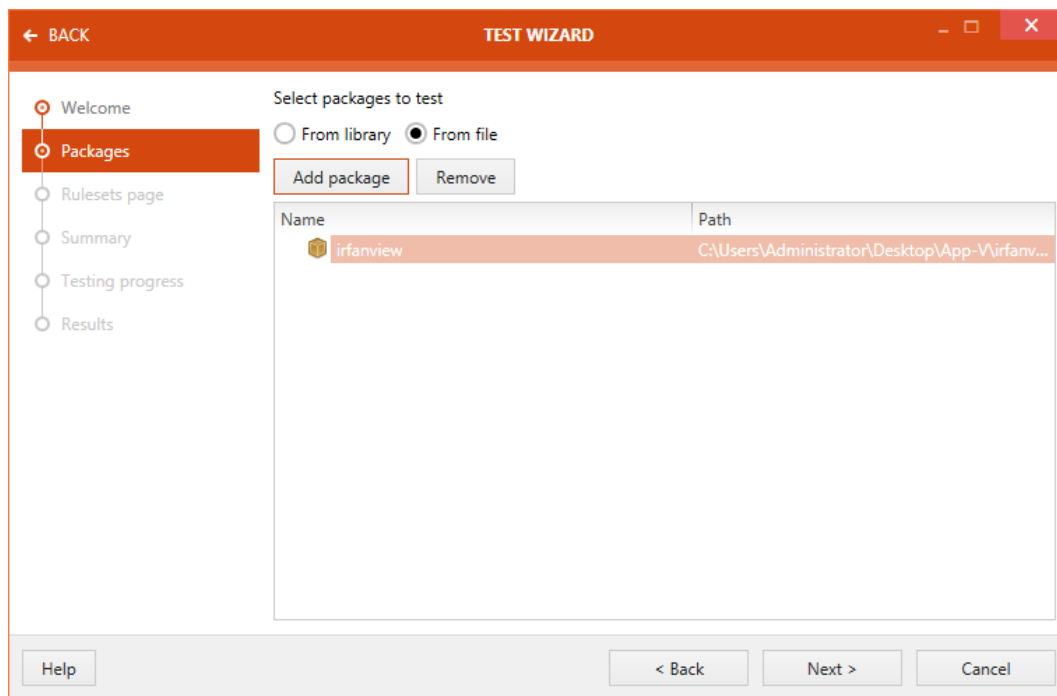
Once the package(s) has been added, click upon the **Next >** button.

The advanced selection section is shown in the next step. Under advanced selection section, a user can select / deselect rules for executing different test types. Test types shown here are directly related to the testing areas chosen.

When a rule is selected, description of that rule is shown under the Rule descriptions. On top of this section, three buttons are shown: **Check all**, **Uncheck all**, and **Toggle**.

- **Check all**: Selects all the rule, covered under different test areas.
- **Uncheck all**: Deselects all the selected rules, covered under different test areas.
- **Toggle**: Toggle the selection of rules.

Click on the **Next >** button. Summary section is now available. Test criteria are summarized under this section.

Click on the **Process** button to start executing test.

Progress of the test is shown.

After the testing is finished, the result will be shown in the **Results** section. There are different options available:

- **View reports in PDF**: Click on this option to open the test result in `.pdf` format.
- **View command line...**: Click on this option to view the command line arguments for the current testing scenario.
- **Save as...**: Click on this option to export the test result in one of various available formats. Possible formats are: `.pdf, .docx, .doc, .html, .xps,` and `.xml`.

If the **After pressing FINISH save the results of the test scenario in the catalog** option is checked the results of test will be saved in the catalog after clicking on the **Finish** button. Untick the option if the result should not be saved in the library. By default the checkbox is ticked.

Click on the **Finish** button to close the **TEST WIZARD**.

Migration Wizard
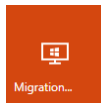
The **MIGRATION WIZARD** is designed to assist with the migration from one operating system to another. It can be launched by clicking the **migration** tile on the **Dashboard** of RayQC Advanced. The **MIGRATION WIZARD** enables users to easily perform collision and os readiness checks for all packages that are necessary for the migration to the new operating system. It is possible to quickly import a bunch of packages and test them against a default set of rules.

Testing areas section

In the **Testing areas** section users can decide if they want to perform either **collision** or **os readiness** checks or both. This can be done by simply selecting or deselecting the respective areas. If an area has been deselected, it is grayed out. By default, both areas are selected.
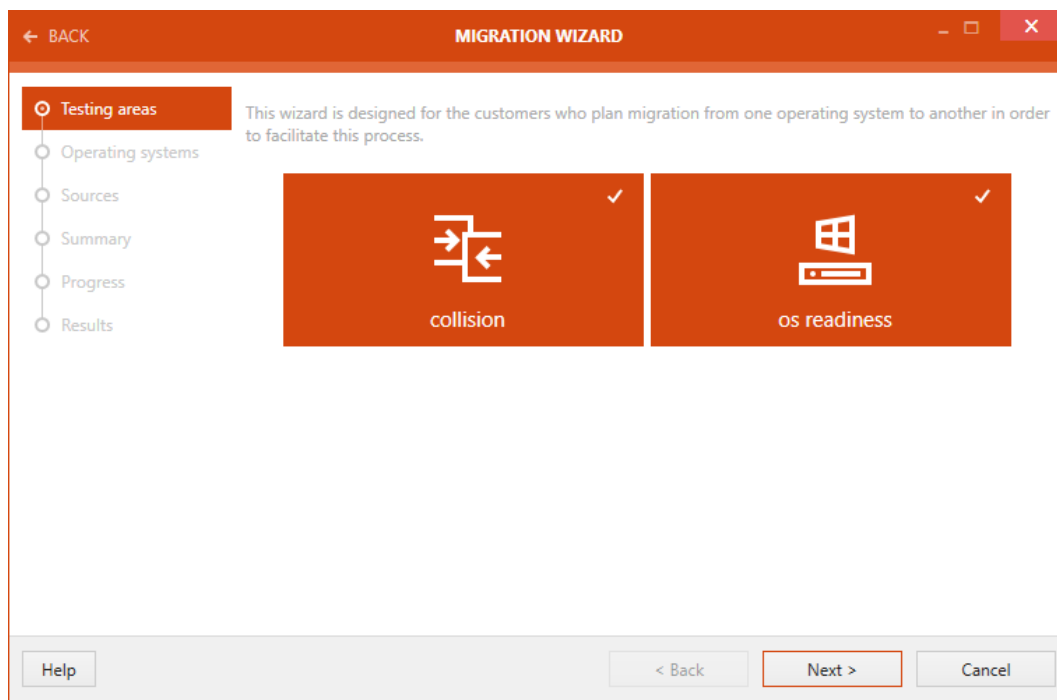
After the **Testing areas** have been selected, click on the **Next >** button to proceed.

Operating systems section

The **Operating systems** section will only be available if os readiness or both have been chosen as testing areas. If only collision has been chosen, this step will be skipped.

In this section select the target operating system. It is possible to select multiple operating systems. The operating systems are selected by clicking on them. The selected operating systems are highlighted like shown in the screenshot below.
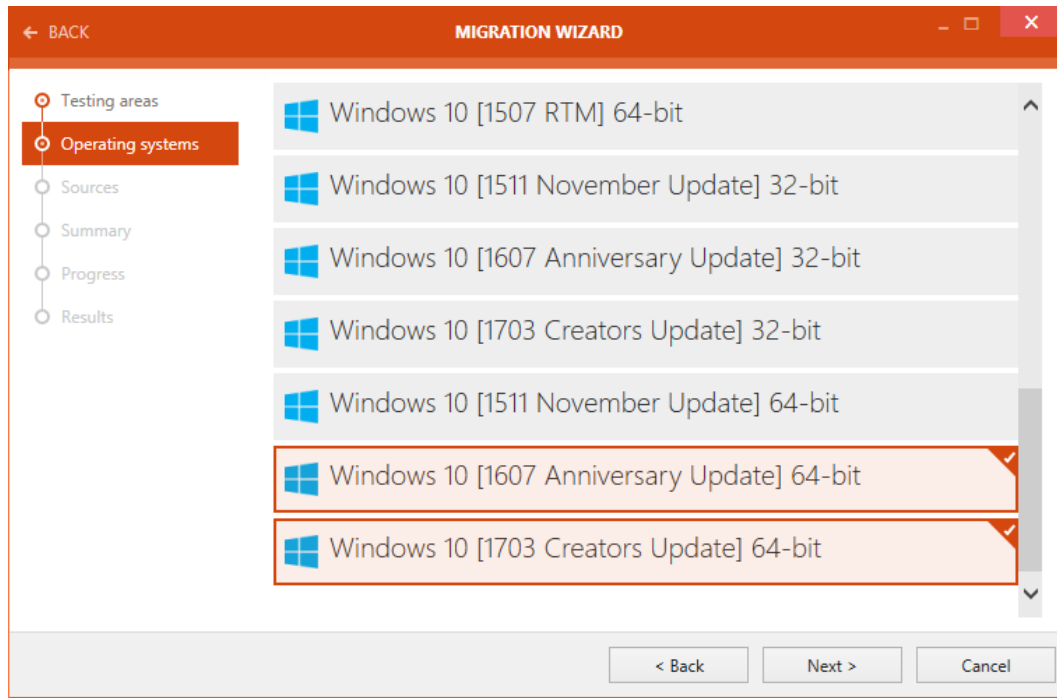
After all operating systems for testing have been selected, click on the **Next** > button to proceed.

Sources section

In the **Sources** section, the packages for testing are selected.

The **Select Folder** window is opened by clicking on the Browse button [**...**]. In the **Select Folder** window, browse to the folder that contains the packages for testing. Click on the **Select Folder** button.

All packages, including any transforms, contained in that folder are now available for testing. A package can be deselected by unchecking the checkbox next to it. Underneath the list of packages that are contained in the folder, there is a **Select all** and an **Unselect all** option.
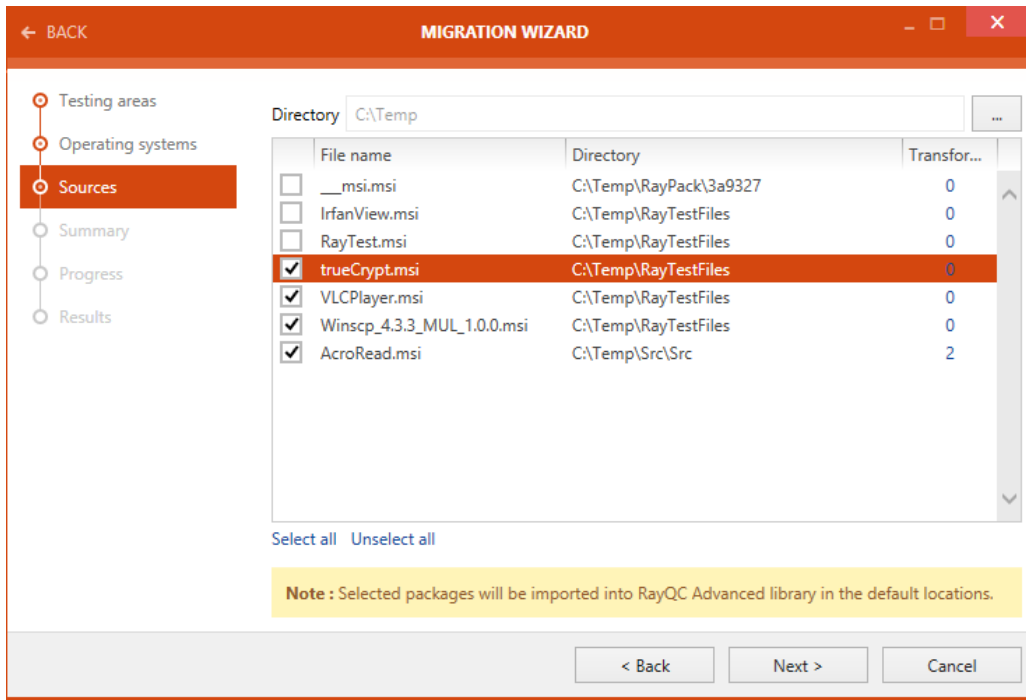
When all packages for testing have been selected, proceed by clicking on the **Next >** button.

> **Note:**
> In case of software collision tests, all software that has been imported into the RayQC Advanced **library** is chosen as target packages (including the newly imported packages from the **Source** screen).

> **Note:**
> All packages imported via the **MIGRATION WIZARD** are located in the migration folder in the **Software library** tab.

Summary Section

Summary section is now available. Test criteria are summarized under this section. This summary includes information on the testing areas, the directory and a list of the files against which the test will be carried out.
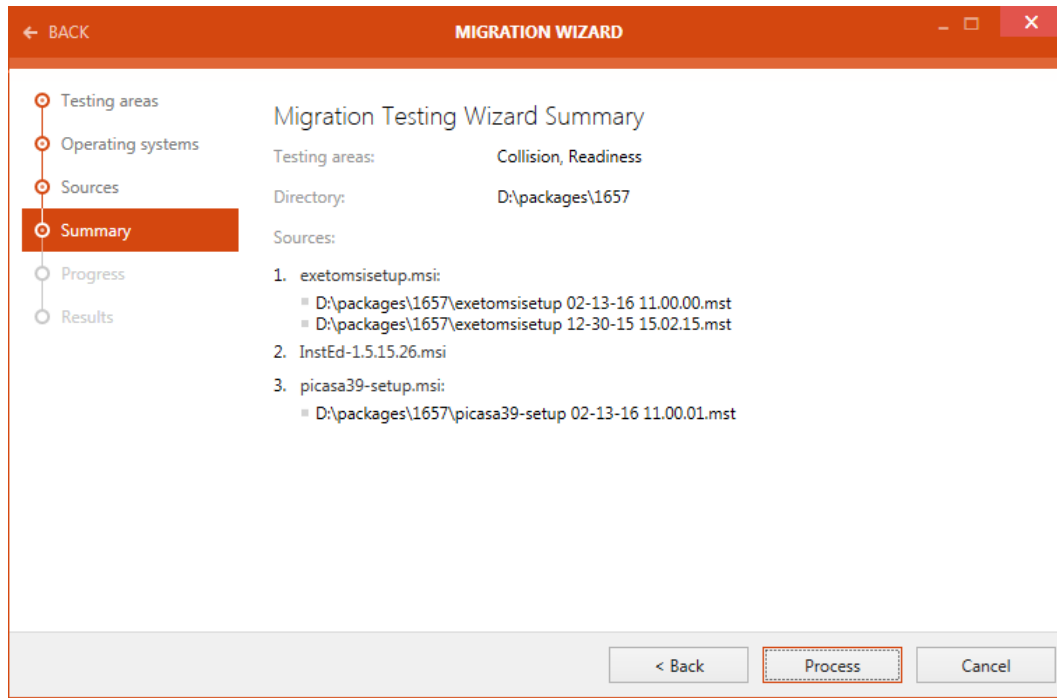
Click on the **Process** button to start executing test.

Progress section

The **Progress** section will be shown as long as the test is being executed. The progress of the test is shown.
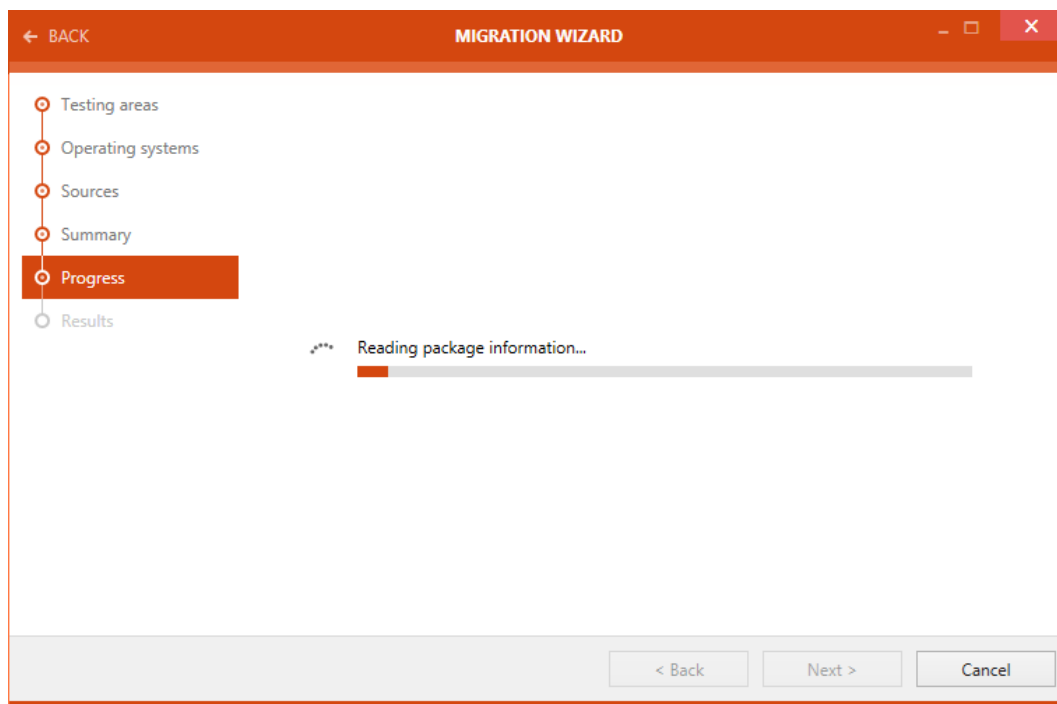
When the test has been finished the screen will automatically change from the **Progress** to the

Results section.

Results section
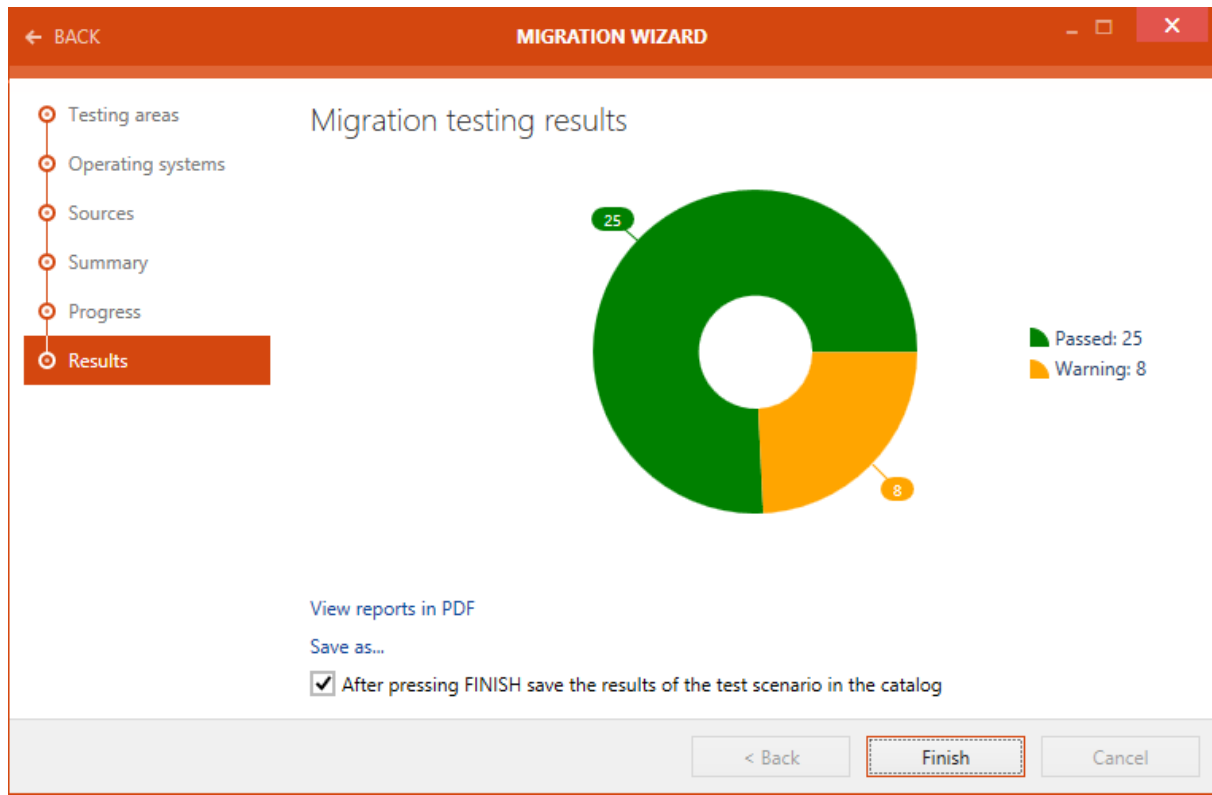
After the testing is finished, the result will be shown in the **Results** section. There are different options available:

- **View reports in PDF**: Click on this option to open the test result in `.pdf` format.
- **Save as...**: Click on this option to export the test result in one of various available formats. Possible formats are: `.pdf`, `.docx`, `.doc`, `.html`, `.xps`, and `.xml`.

If the **After pressing FINISH save the results of the test scenario in the catalog** option is checked the results of test will be saved in the catalog after clicking on the **Finish** button. Untick the option if the result should not be saved in the library. By default the checkbox is ticked.

Click on the **Finish** button to close the **MIGRATION WIZARD**.

> **Note:**
> After **Finish** has been clicked there will not be a redirection to any screen.

Deployment

This chapter describes the Deployment options that are available in RayQC Advanced. It is possible to use either SCCM or RayManageSoft to deploy packages from the RayQC Advanced Software Library.

The export can easily be started by opening the context menu on a target package in the RayQC Advanced library and then selecting either the **RMS** or the **SCCM** option which can be found under **Export**. If a deployment method is not configured in RayQC Advanced, the option in the context menu will be grayed out and cannot be selected.
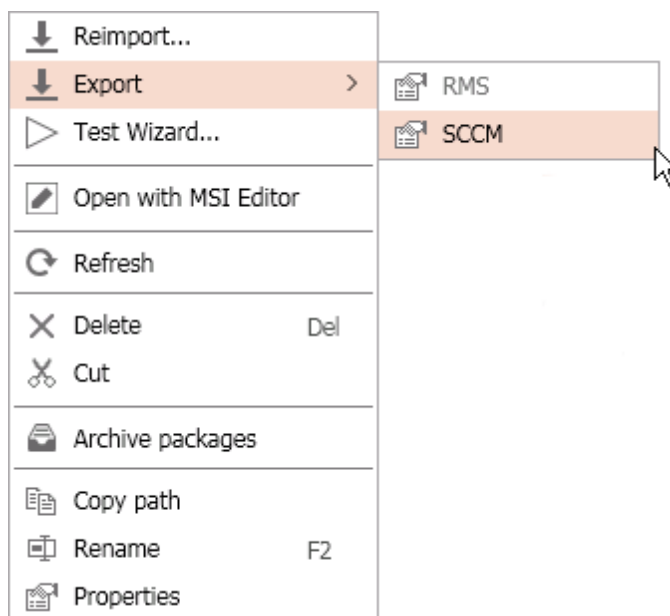
After selecting one of the options either the **Deployment Wizard** for SCCM or the Deployment Wizard for RayManageSoft will be opened.

For **SCCM** continue with the *Export Using SCCM* chapter.
For **RMS** continue with the *Export Using RMS* chapter.

Export Using SCCM

The Deployment Wizard for SCCM differs depending on the **Deploying Type** that has been selected in the **Deployment Tab** of the **Settings** section of RayQC Advanced.
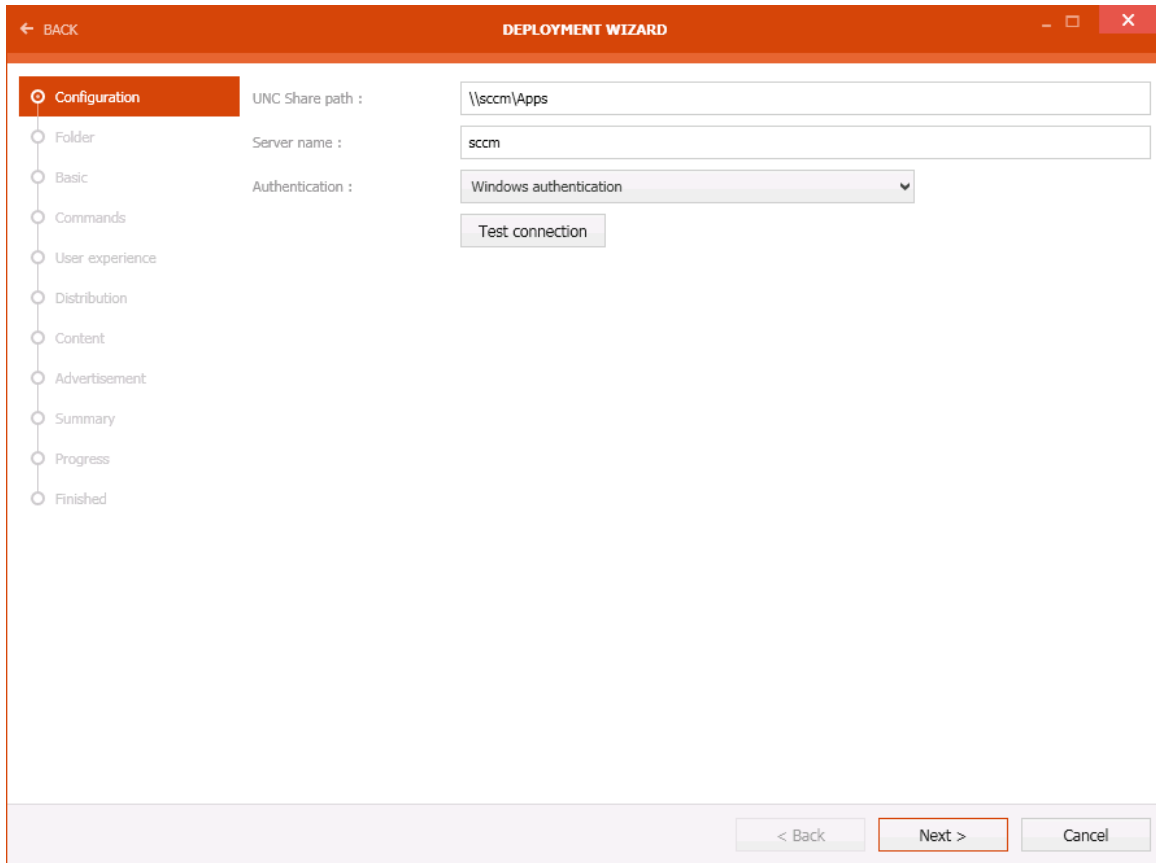
If **Application** has been selected as **Deploying Type** continue with the *Deployment Type Application* chapter.
If **Package** has been selected as **Deploying Type** continue with the *Deployment Type Package* chapter.

Deployment Type: Application

Configuration Page

On this page the connection to the server is configured.

- **UNC Share path**: The path to the UNC share.
- **Server name**: The name of the server.
- **Authentication**: The authentication method can be selected using the dropdown menu. Depending on the authentication method, the credentials for the method may be needed.
- **Test connection**: This button can be used to check if a connection can be established with the given information.

Click on the **Next >** button to continue.

Folder Page

The folder for the application can be selected on this page.

Click on the **Next >** button to continue.

Basic Page

The **Basic** page contains some general information about the package itself.

The following options are available on the **Basic** page.

- **Name**: This field contains the name of the application.
- **Product version**: This field contains the version of the application.
- **Manufacturer**: This field contains the name of the manufacturer of the application.
- **Package type**: The package type is shown in this field.

The **Restore data from answer file** link can be used to restore the data.

Click on the **Next >** button to continue.

Commands Page

On the Commands page, the exact install and uninstall commands can be configured.
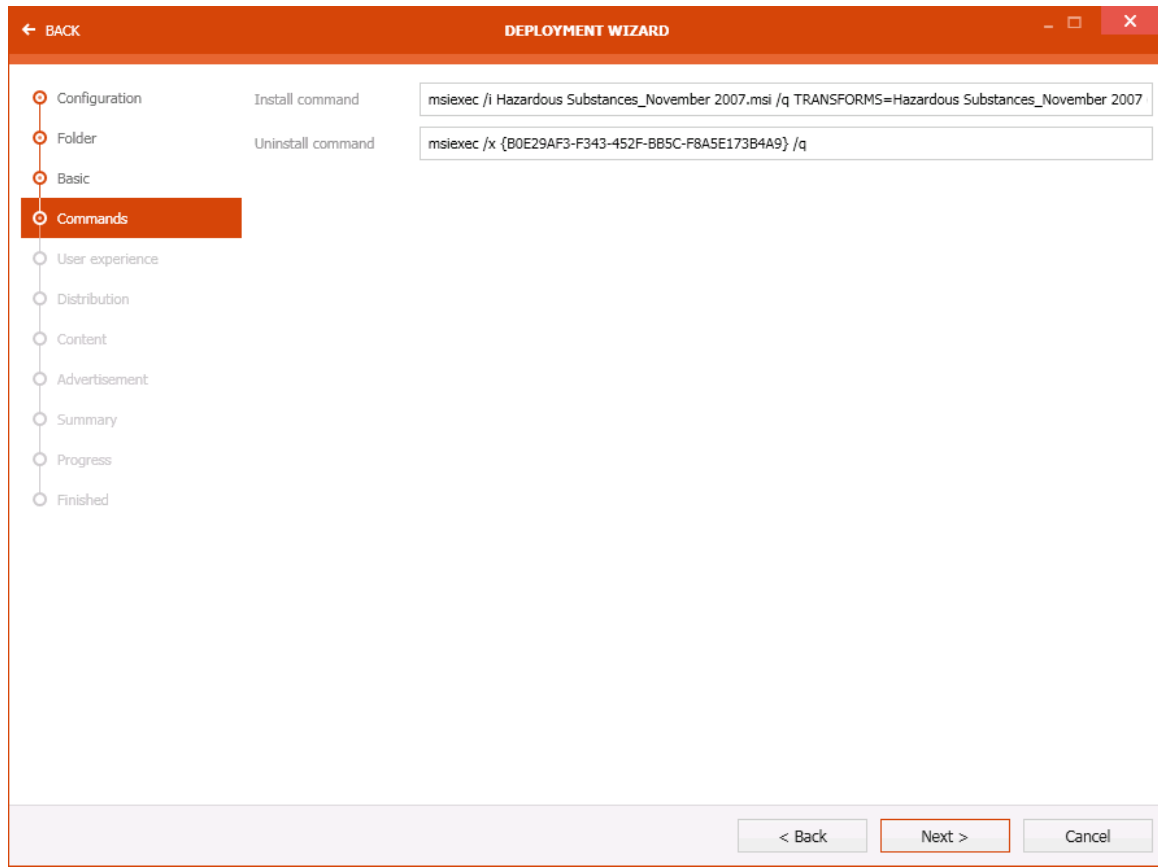
The following options are available:
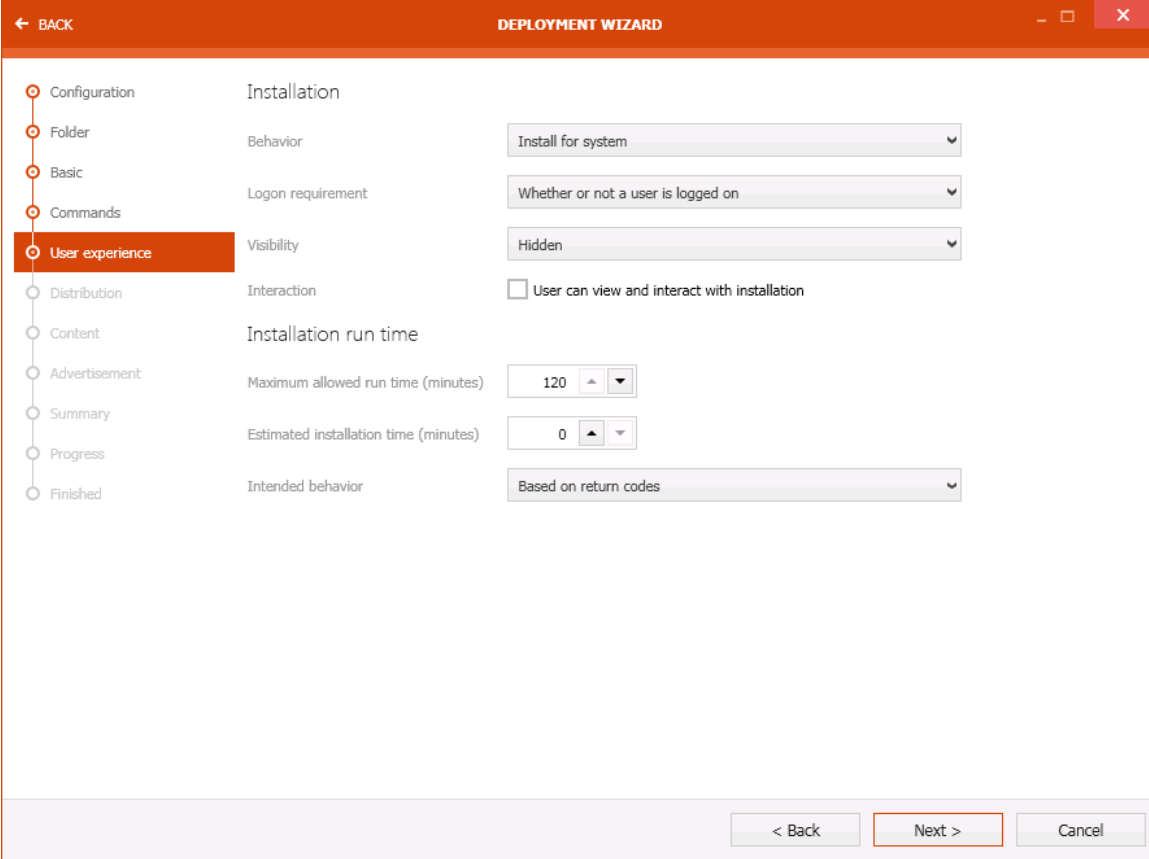
Install command:The exact command for the installation can be configured here. For example, any transforms that are to be applied.
Uninstall command: The exact command for the uninstallation can be configured here.

Click on the **Next >** button to continue.

User Experience Page

On this page the behavior that will be experienced by the user is configured. For example, if the user is logged out during installation, or if a log out is not needed.

The page is divided into the **Installation** section and the **Installation run time** section.

The following settings are available in the **Installation** section on this page:

- **Behavior**: The behavior of the installation, for example if the installation is for the user or for the system, can be chosen using this dropdown menu.
- **Logon requirement**: The logon requirements, for example if a user needs to be logged on or not, can be chosen using this dropdown menu.
- **Visibility**: This dropdown menu defines the visibility of the installation. For example, if **Hidden** is selected, the installation is hidden from the user.
- **Interaction**: Checkbox that controls whether the User can view and interact with the installation.

The following settings are available in the **Installation run time** section on this page:

- **Maximum allowed run time (minutes)**: This setting defines the maximum time that the installation is allowed to run. The time is in minutes and can be configured either by typing it or by using the arrow buttons.
- **Estimated installation time (minutes)**: This is an estimation of the time that the installation will run. The time is in minutes and can be configured either by typing it or by using the arrow buttons.
- **Intended behavior**: The intended behavior for the installation can be configured using the

dropdown menu.

Click on the **Next >** button to continue.

Distribution Page

This is where the distribution settings are configured.

The page is divided into the **Package distribution settings** and the **Prestaged distribution point**.

The following options are available for the **Package distribution settings**:

- **Distribution priority**: The priority for the distribution can be selected using the dropdown menu underneath this option.
- **Distribute to preferred distribution points**: Enable this checkbox to favor preferred distribution points.

The **Prestaged distribution point** can be configured using the dropdown menu that is located underneath this option.

Click on the **Next >** button to continue.

Content Page

Content and **Location** settings are available on this page.

The following options are available underneath the **Content** settings:

- **Location**: The full path to the location is shown in the text field.
- **Persist in the client cache**: Enable the checkbox to keep the data in the cache of the client.
- **Allow clients share content**: Enable the checkbox to allow clients to share content data.
- **Allow clients to use a fallback source location**: Enable the checkbox to allow clients to use a fallback source location.
- **Download content and run locally**: If this checkbox is enabled, the clients will download the content and execute it locally.

The following options are available underneath the **Location** settings:

- **Distribution points**: The available distribution points are shown here. Select the target distribution points.
- **Distrbution groups**: The available distribution groups are shown here. Select the target distribution groups.

Click on the **Next >** button to continue.

Advertisement Page

The **Advertisement** page is divided into two sections.

The first section contains the following options:

- **Deploy program**: The button can be set to either **Yes** or **No**.
- **Collection ID**: This field shows the ID of the the collection.
- **Comment**: A comment can be entered into this textfield.

The second section consists of five different tabs.

The COLLECTIONS Tab
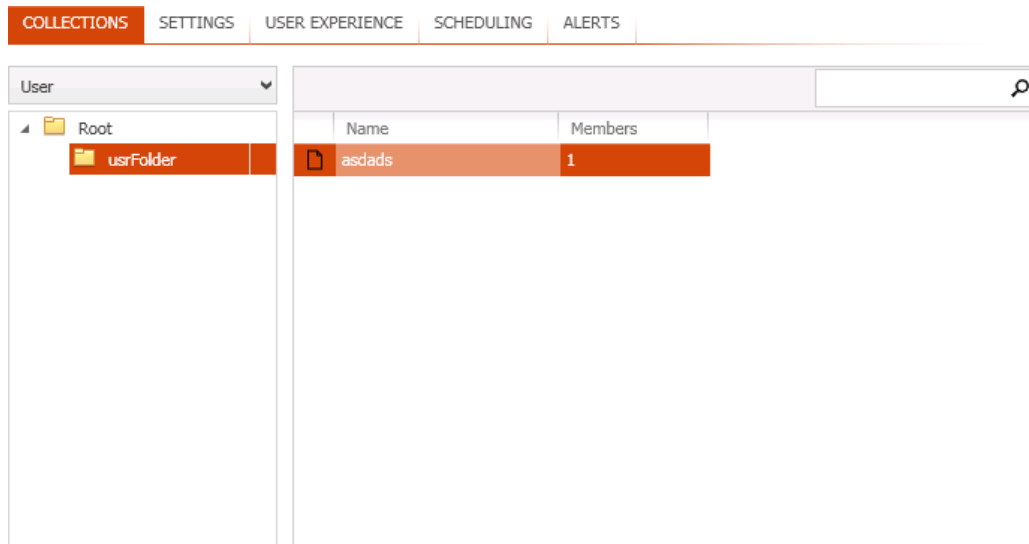
The path and the packages that are chosen for deployment are shown here.
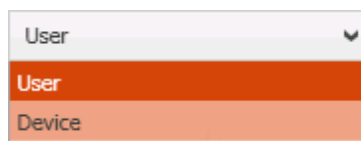
It is possible to switch between **User** and **Device** context by using the dropdown menu.

The SETTINGS Tab
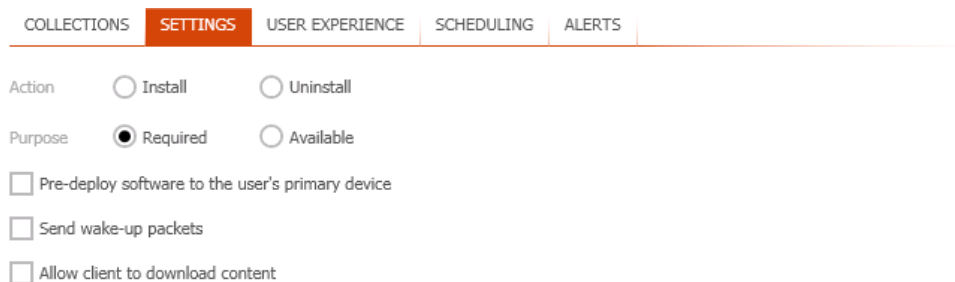
The following settings are available in this tab:

- **Action**: It is possible to select either **Install** or **Uninstall**.
- **Purpose**: Select either **Required** or **Available** as purpose.
- **Pre-deploy software to the user's primary device**: Enable this checkbox to allow pre-deployment for the primary devices.
- **Send wake-up packets**: Enable this checkbox to allow to send packets which are intended to wake a sleeping client.
- **Allow client to download content**: Enable this checkbox to allow clients to download the data.

The USER EXPERIENCE Tab

The following settings are available in this tab:

- **User notifications**: Which notifications are shown and where the notifications are shown can be configured using this dropdown menu.
- **Software Installation**: Enable this checkbox to make the software installation visible to the user.
- **System restart**: Enable this checkbox to allow a restart of the system.
- **Commit changes at deadline**: Enable this checkbox to commit changes at the deadline.

The SCHEDULING Tab

The schedule for the deployment can be configured in this tab. It is possible to schedule the availability of the application as well as the deadline for the installation.

Be aware:
The time of availability must be scheduled before the time for the installation.

The ALERTS Tab

The alerts are configured in this tab. Check the checkbox of those options that shall be enabled for this deployment.

Click on the **Next >** button to continue.

Summary Page

This page shows a summary of all configurations that have been made in the previous step.

Click on the **Process** button to start the deployment.

Progress Page

On the **Progress page** the progress of the export is shown.
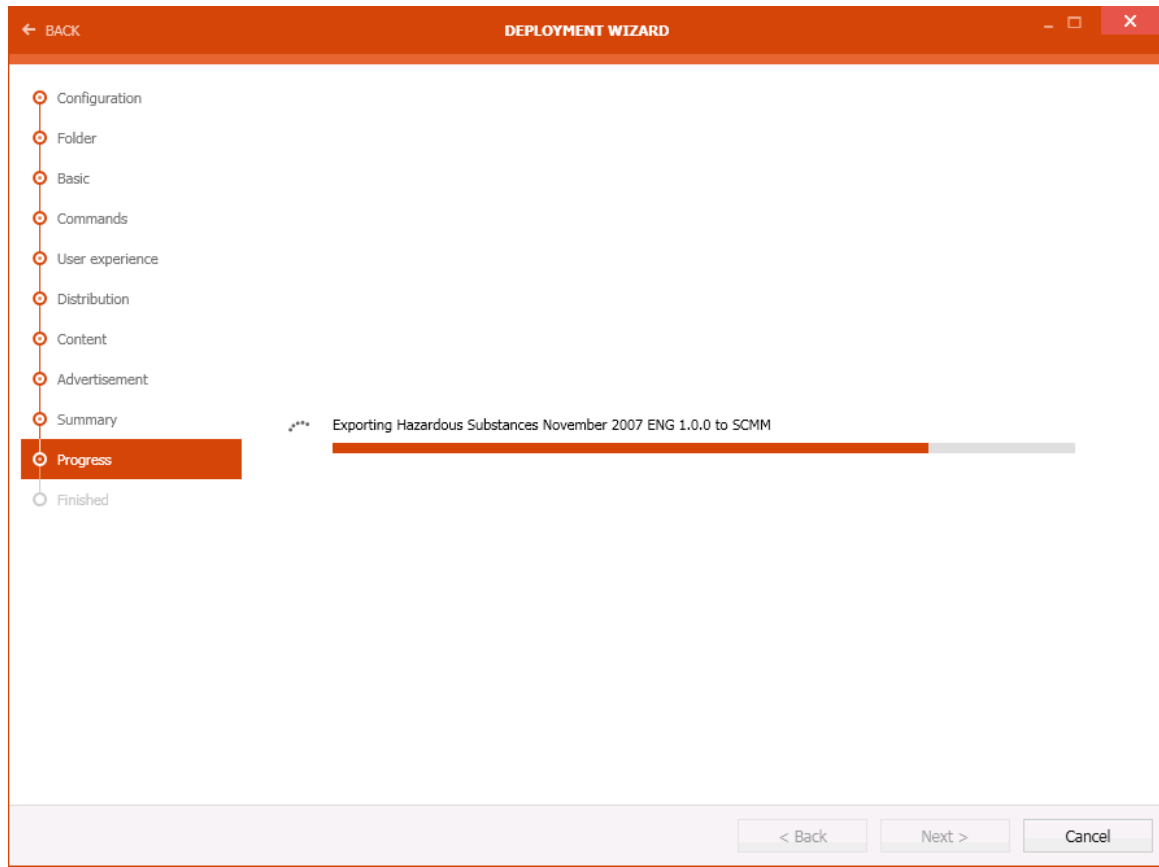
After the export has been finished the wizard will automatically continue to the next page.

Finished Page

The **Finished page** contains the information if the export has been successful.
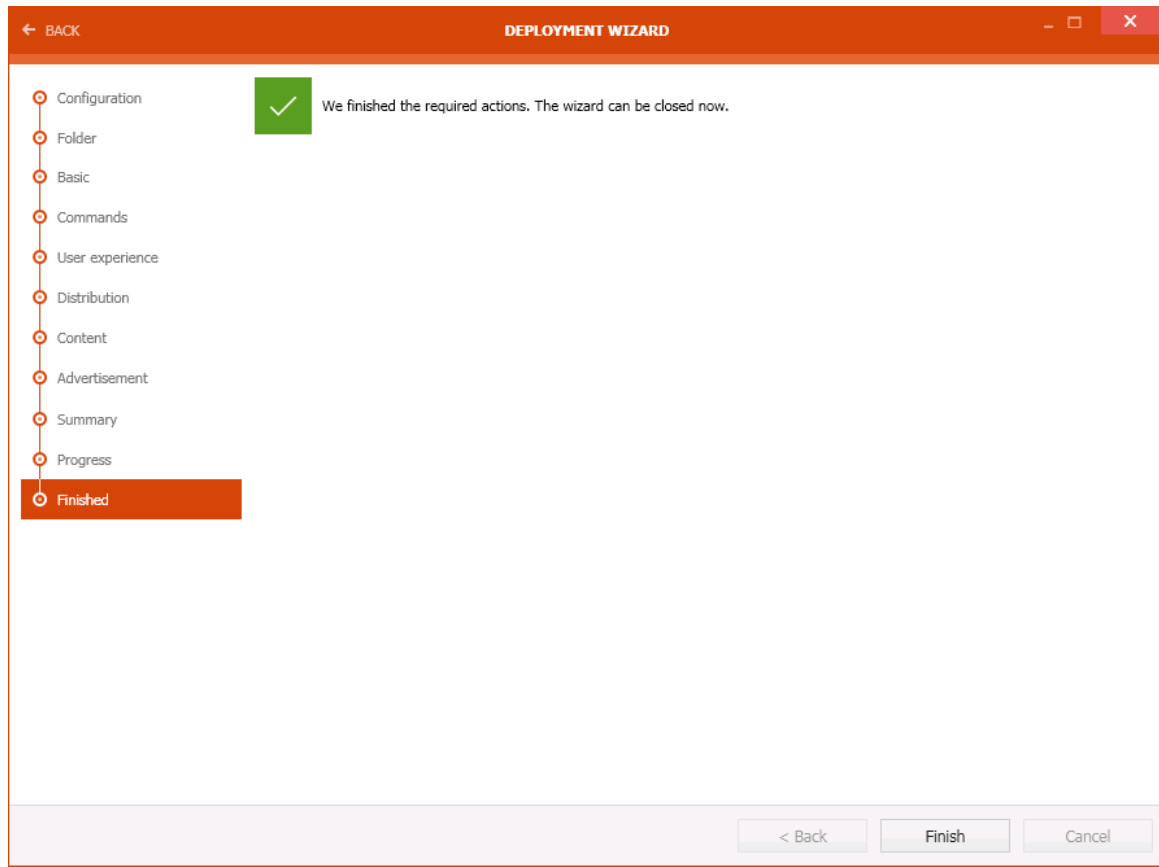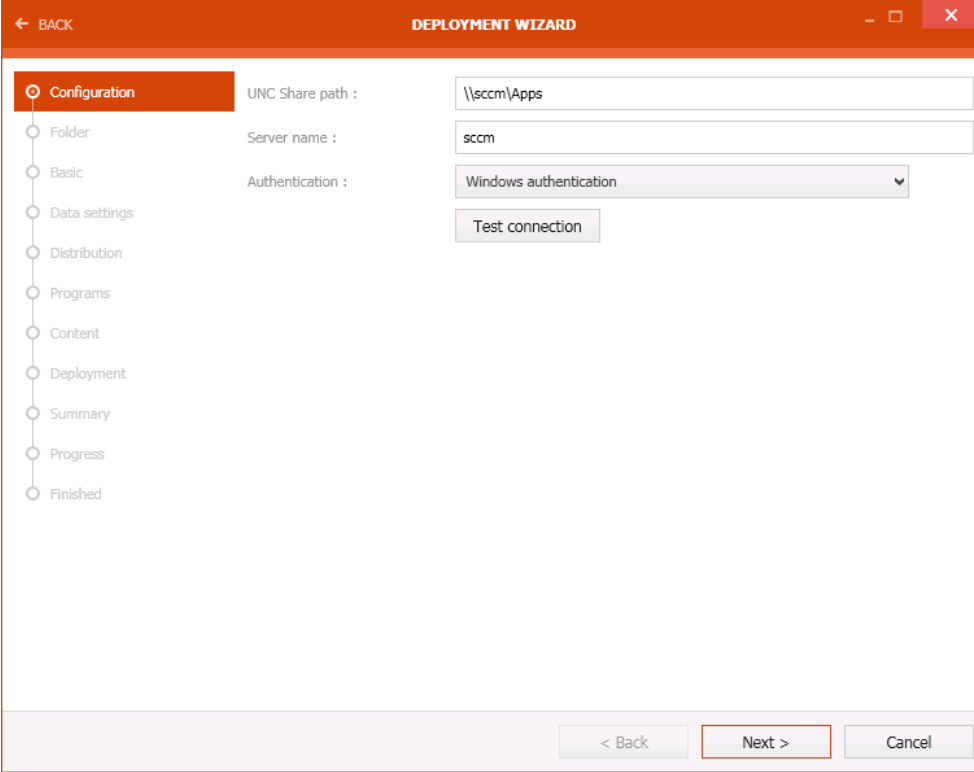
Click on the **Finished** button to close the wizard.

Deployment Type: Package

Configuration Page

On this page the connection to the server is configured.

- **UNC Share path**: The path to the UNC share.
- **Server name**: The name of the server.
- **Authentication**: The authentication method can be selected using the dropdown menu. Depending on the authentication method, the credentials for the method may be needed.
- **Test connection**: This button can be used to check if a connection can be established with the given information.

Click on the **Next >** button to continue.

Folder Page

The folder for the application can be selected on this page.

Click on the **Next >** button to continue.

Basic Page

The **Basic** page contains some general information about the package itself.

The following options are available on the **Basic** page.

• **Name**: This field contains the name of the application.
• **Product version**: This field contains the version of the application.
• **Manufacturer**: This field contains the name of the manufacturer of the application.
• **Package type**: The package type is shown in this field.

The **Restore data from answer file** link can be used to restore the data.
Click on the **Next >** button to continue.

Data Settings Page

On the **Data Settings** page the way how the data is accessed and the sources for the data are configured.
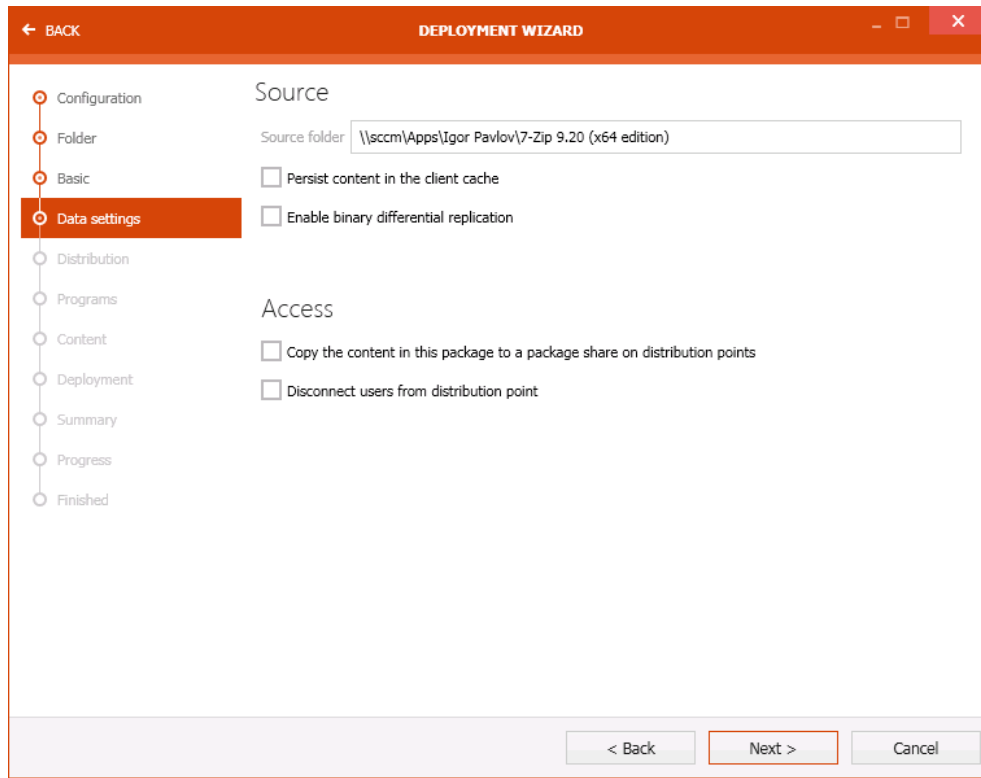
The page is divided into the Source area and the Access area.

The following options are available in the the **Source** area:

- **Source folder**: This field contains the full path to the source folder.
- **Persist content in the client cache**: This checkbox can be checked if the data should stay in the cache of the client.
- **Enable binary differential replication**: Enable this checkbox to activate the binary differential replication.

The following options are available in the **Access** area.

- **Copy the content in this package to a package share on distribution points**: This checkbox can be checked to copy the data to an existing package share on a distribution point.
- **Disconnect users from distribution point**: If this checkbox is checked, users will be disconnected from the distribution point.

Click on the **Next >** button to continue.

Distribution Page

This is where the distribution settings are configured.

The page is divided into the **Package distribution settings** and the **Prestaged distribution point**.

The following options are available for the **Package distribution settings**:

- **Distribution priority**: The priority for the distribution can be selected using the dropdown menu underneath this option.
- **Distribute to preferred distribution points**: Enable this checkbox to favor preferred distribution points.

The **Prestaged distribution point** can be configured using the dropdown menu that is located underneath this option.

Click on the **Next >** button to continue.

Programs Page

This section contains the list of programs. On this page, new programs can be added.
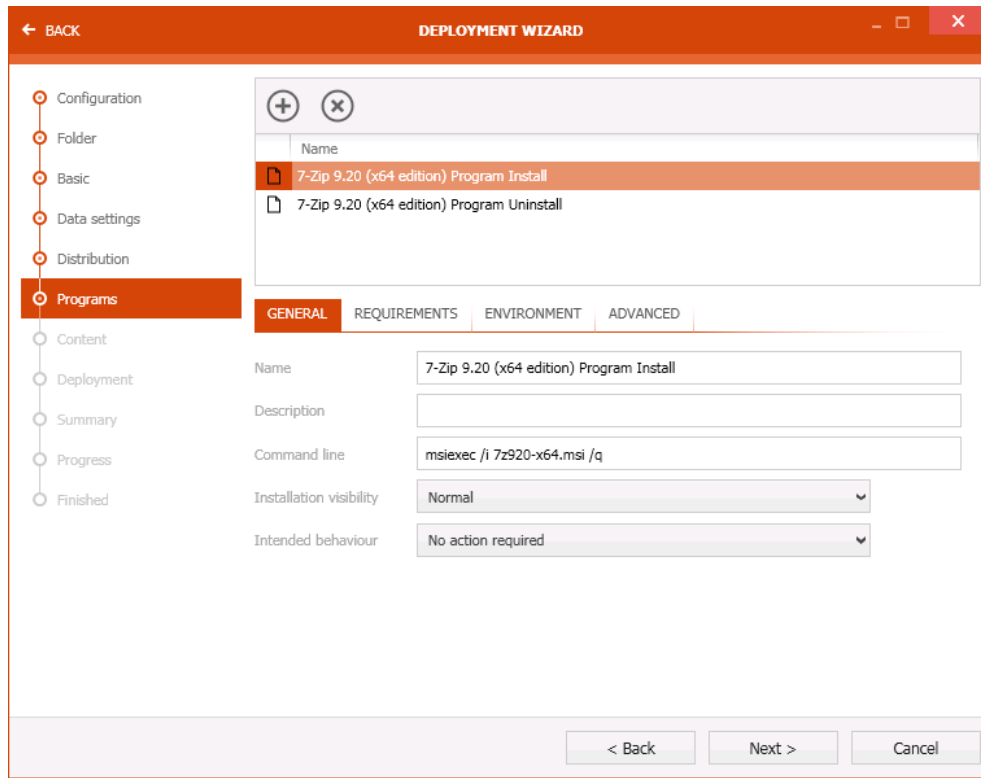
Program List: Select the package together with its intended action. Click on the **x** button to delete the selected program and on the **+** button to add a new one.

Clicking on the **+** button will open the Add program dialog.
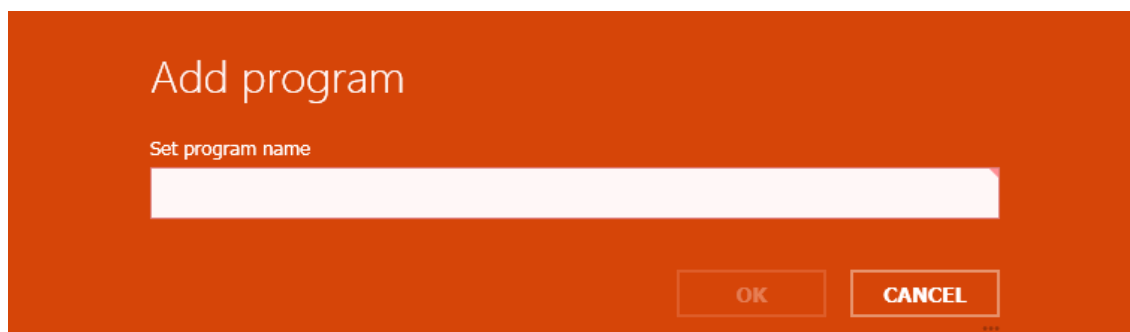
Enter the program name into the field and click the **OK** button to add the new program or the **CANCEL** button to abort the action.

Below the Progam List, four different tabs with the settings for the selected program are available.

The GENERAL Tab

- **Name**: The name of the program can be configured here.
- **Description**: A description can be entered into this textfield.
- **Command line**: The command line for the action can be configured here.
- **Installation visibility**: The visibility of the installation can be configured using this dropdown menu.
- **Intended behavior**: This is a dropdown menu that can be used to configure the behavior.

The REQUIREMENTS Tab

- **Disc space units**: Select either MB or GB as disk space units for the next option.
- **Estimated disk space**: This is the estimation of the disk space that is needed for the installation. It can be configured by either entering a number or using the arrow buttons.
- **Maximum allowed run time (minutes)**: This is the maximum time that is allowed for the installation. It is measured in minutes and can be configured by either entering a number or using the arrow buttons.
- **Supported client platforms**: The client platforms that are supported by the application can be selected from this list. Check the checkboxes of all supported platforms.

The ENVIRONMENT Tab

- **Allow user interaction**: Enable this checkbox to allow the user to interact with the installation.
- **Logon requirement**: Use this dropdown menu to select the logon requirements for the installation. For example, if the user needs to be logged out or not.
- **Run mode**: This dropdown box is used to configure the mode in which the installation is run. For example, if elevated rights are used.
- **Program drive mode**: The mode for the program drive can be selected using this dropdown menu.
- **Program drive letter**: The pogram drive letter used for the installation can be configured here.
- **Reconnect to distribution point**: Check this checkbox to reconnect to the distribution point.

The ADVANCED Tab

- **Program run behavior**: The behavior of the program (for example, if the installation is only run once for a device) can be set using the dropdown menu.
- **Suppress program notifications**: Enable this checkbox to suppress notifications from the program.
- **Disable program when deployed**: Enable this checkbox to disable the program after it has been deployed.
- **Allow task sequence installation**: Enable this checkbox to allow task sequence installation.

Click on the **Next >** button to continue.

Content Page

Content and **Location** settings are available on this page.

The following options are available underneath the **Content** settings:

- **Location**: The full path to the location is shown in the text field.
- **Persist in the client cache**: Enable the checkbox to keep the data in the cache of the client.
- **Allow clients share content**: Enable the checkbox to allow clients to share content data.
- **Allow clients to use a fallback source location**: Enable the checkbox to allow clients to use a fallback source location.
- **Download content and run locally**: If this checkbox is enabled, the clients will download the content and execute it locally.

The following options are available underneath the **Location** settings:

- **Distribution points**: The available distribution points are shown here. Select the target distribution points.
- **Distrbution groups**: The available distribution groups are shown here. Select the target distribution groups.

Click on the **Next >** button to continue.

Deployment Page

The Deployment Page is divided into to sections.
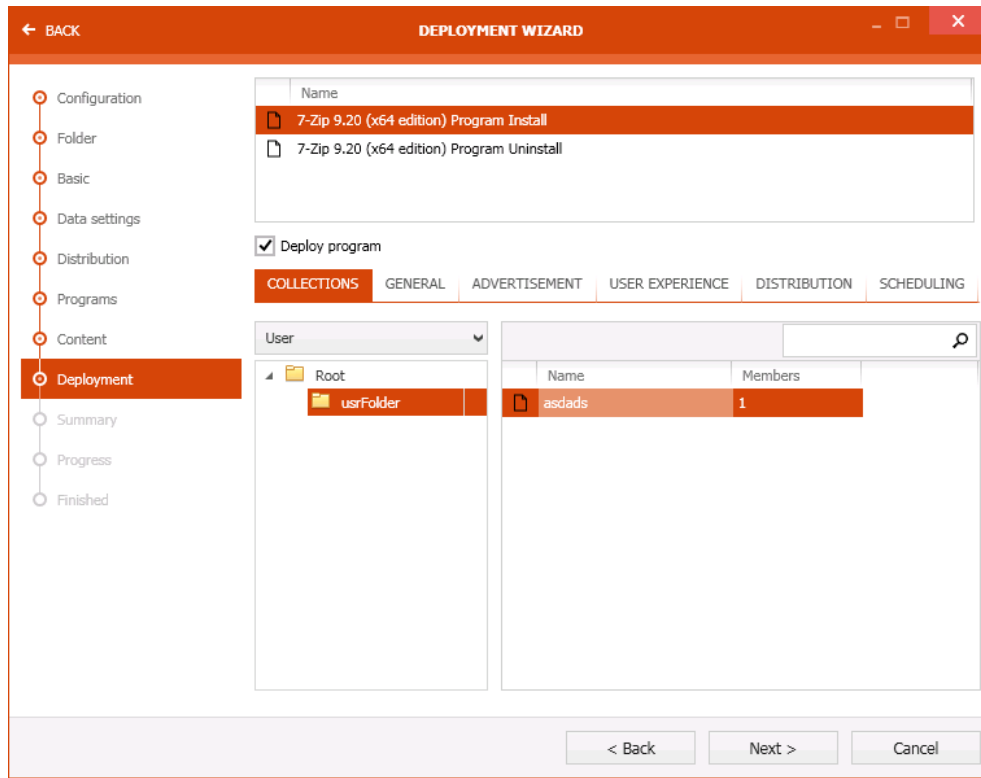
The first section contains the following options:

- **Program List**: Select the target program. The settings for the program will become available in the second section.
- **Deploy program**: This checkbox needs to be enabled in order to deploy the program.

The second section consists of six different tabs.

The COLLECTIONS Tab
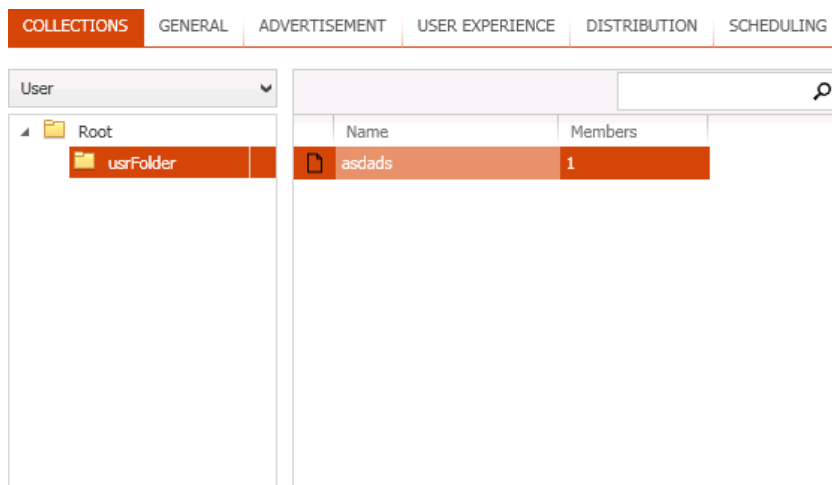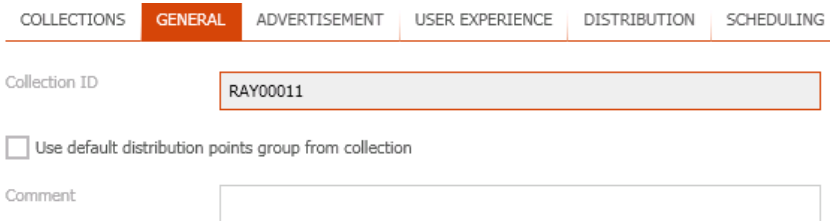
The path and the packages that are chosen for deployment are shown here.

It is possible to switch between **User** and **Device** context by using the dropdown menu.
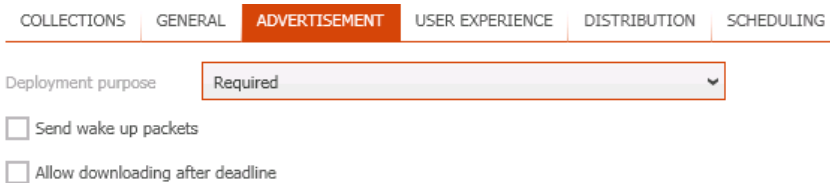
The GENERAL Tab

- **Collection ID**: The ID of the collection is shown here.
- **Use default distribution points group from collection**: Enable this checkbox to use the default distribution points group that is part of the collection.
- **Comment**: A comment can be entered into this textfield.
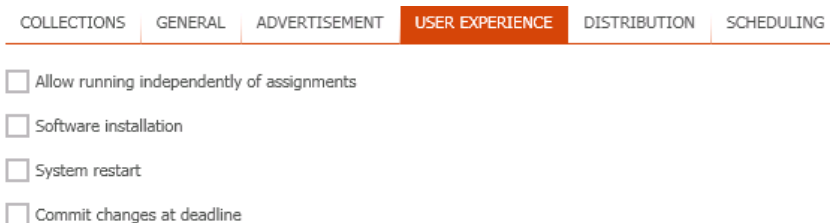
The ADVERTISEMENT Tab

- **Deployment purpose**: The purpose for the deployment (if it is required or not) can be configured using this dropdown menu.
- **Send wake up packets**: Enable this checkbox to allow to send packets to wake up sleeping clients.
- **Allow downloading after deadline**: Enable this checkbox to allow clients to download the packages after the deadline.

The USER EXPERIENCE Tab

The following settings are available in this tab:

- **User notifications**: Which notifications are shown and where the notifications are shown can be configured using this dropdown menu.
- **Software Installation**: Enable this checkbox to make the software installation visible to the user.
- **System restart**: Enable this checkbox to allow a restart of the system.
- **Commit changes at deadline**: Enable this checkbox to commit changes at the deadline.

The DISTRIBUTION Tab

- **Allow to share content with other clients**: If this checkbox is enabled, clients are allowed to share data with other clients.
- **Allow to use a fallback source for content**: If this checkbox is enabled, the clients are allowed to use a fallback source for content.
- **Connection with a fast network boundary**: The behavior for clients located in a fast network can be set using this dropdown menu.
- **Connection with a slow or unreliable network boundary**: The behavior for clients located in a slow or unreliable network can be set using this dropdown menu.

The SCHEDULING Tab

- **Schedule when this deployment will become available**: Enable this checkbox to schedule the time the deployment will become.
- **Schedule when this deployment will expire**: Enable this checbox to schedule the deadline for the deployment.
- **Rerun behavior**: This dropdown menu is used to define the rerun behavior for the application.

Beneath these options there is a list of schedules from which a fitting schedule can be selected. To delete a selected schedule the **x** button can be used. To add a new schedule the **+** button can be used. There are six different schedule item types available. A schedule will be added after clicking on the **Add** button. Clicking on **Cancel** will abort the action.
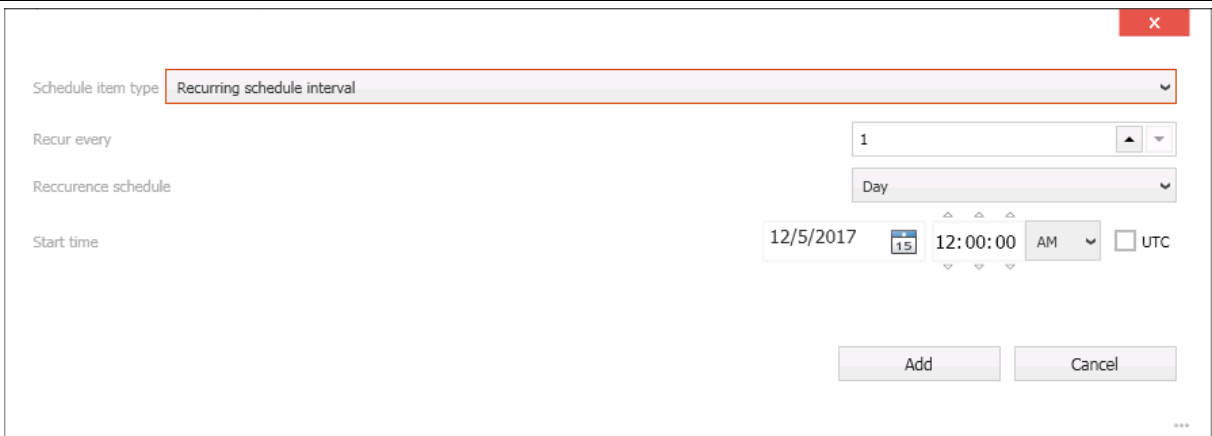
Schedule Event

This schedule will trigger on a specific event instead of a fixed date. The event can be selected from the dropdown menu.
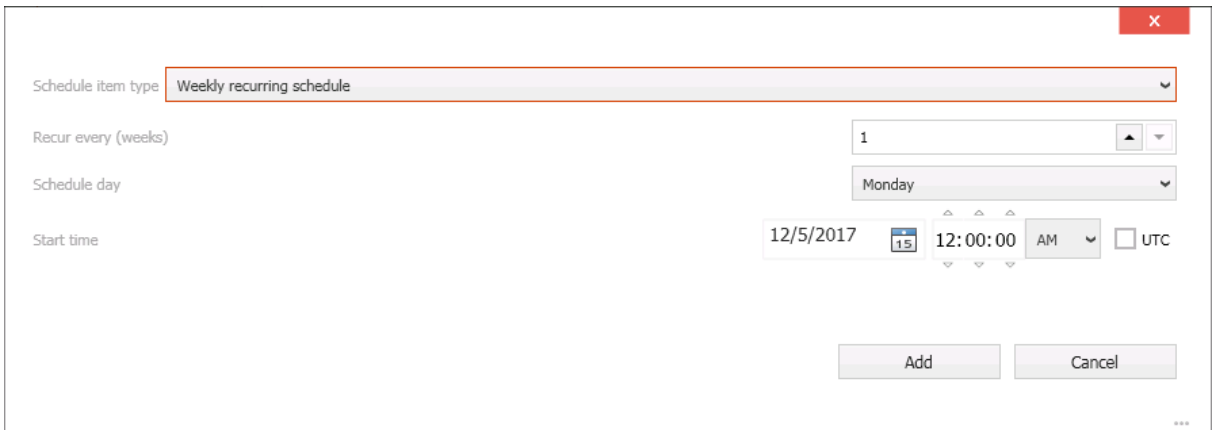
Non Recurring Schedule

This schedule will be triggered once at a specified time and date.
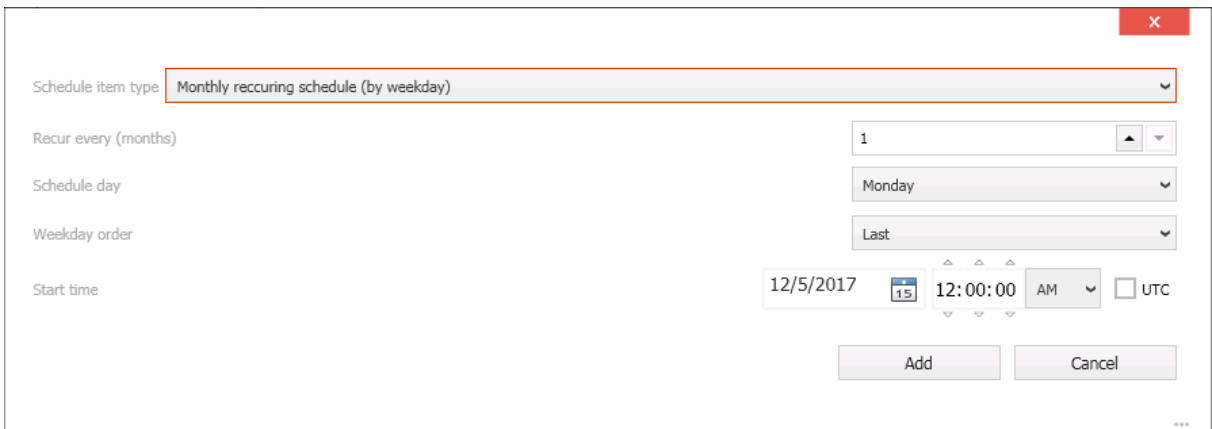
Recurring Schedule Interval

This schedule is triggered on a recurring interval. The interval of the schedule and the start time of the schedule can be configured.

Weekly Recurring Schedule

This schedule can be configured to trigger once a week or a given number of weeks. The day of the week and the start date can be configured.

Monthly Recurring Schedule (by weekday)

This schedule can be configured to trigger once a month or a given number of months. The weekday, the week and the start date can be configured.

Monthly Recurring Schedule (by date)

This schedule can be configured to trigger once a month or a given number of months. The day of the month and the start date can be configured.

Click on the **Next >** button to continue.

Summary Page

This page shows a summary of all configurations that have been made in the previous step.

Click on the **Process** button to start the deployment.

Progress Page

On the **Progress page** the progress of the export is shown.
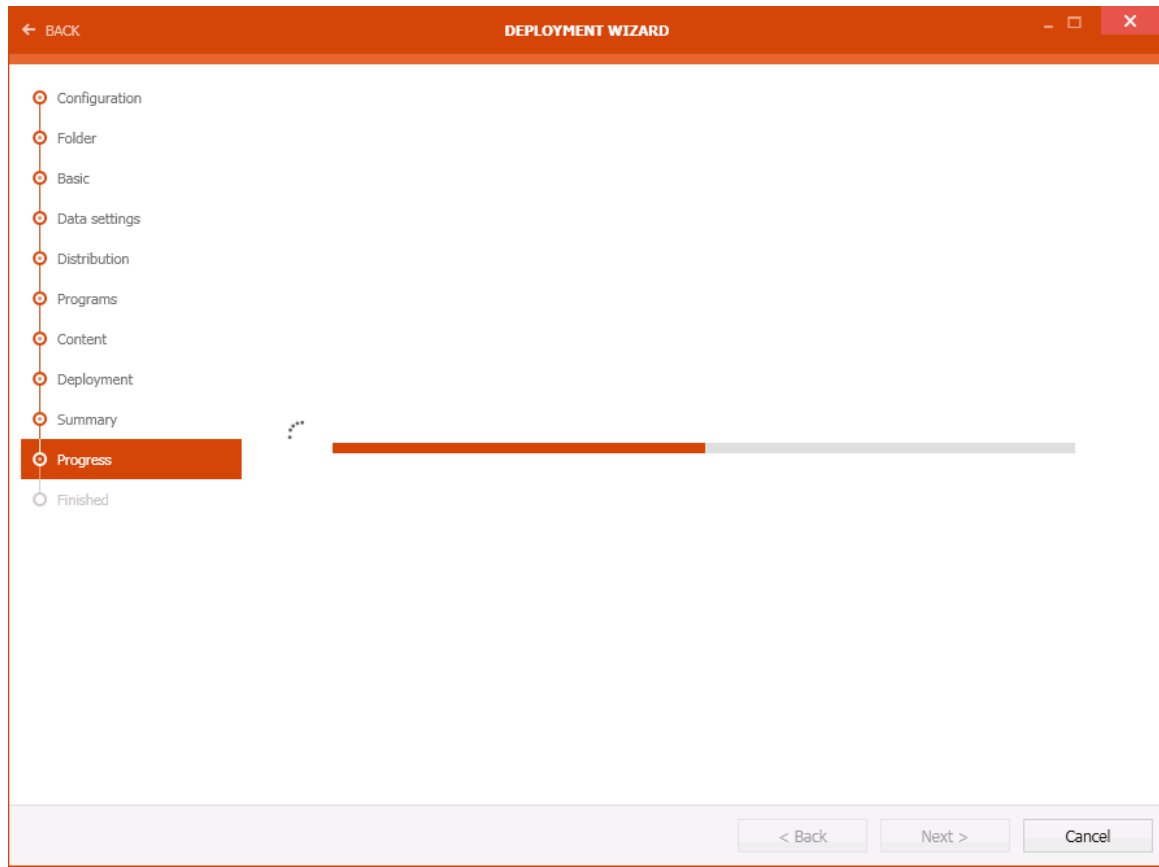
After the export has been finished the wizard will automatically continue to the next page.

Finished Page

The **Finished page** contains the information if the export has been successful.
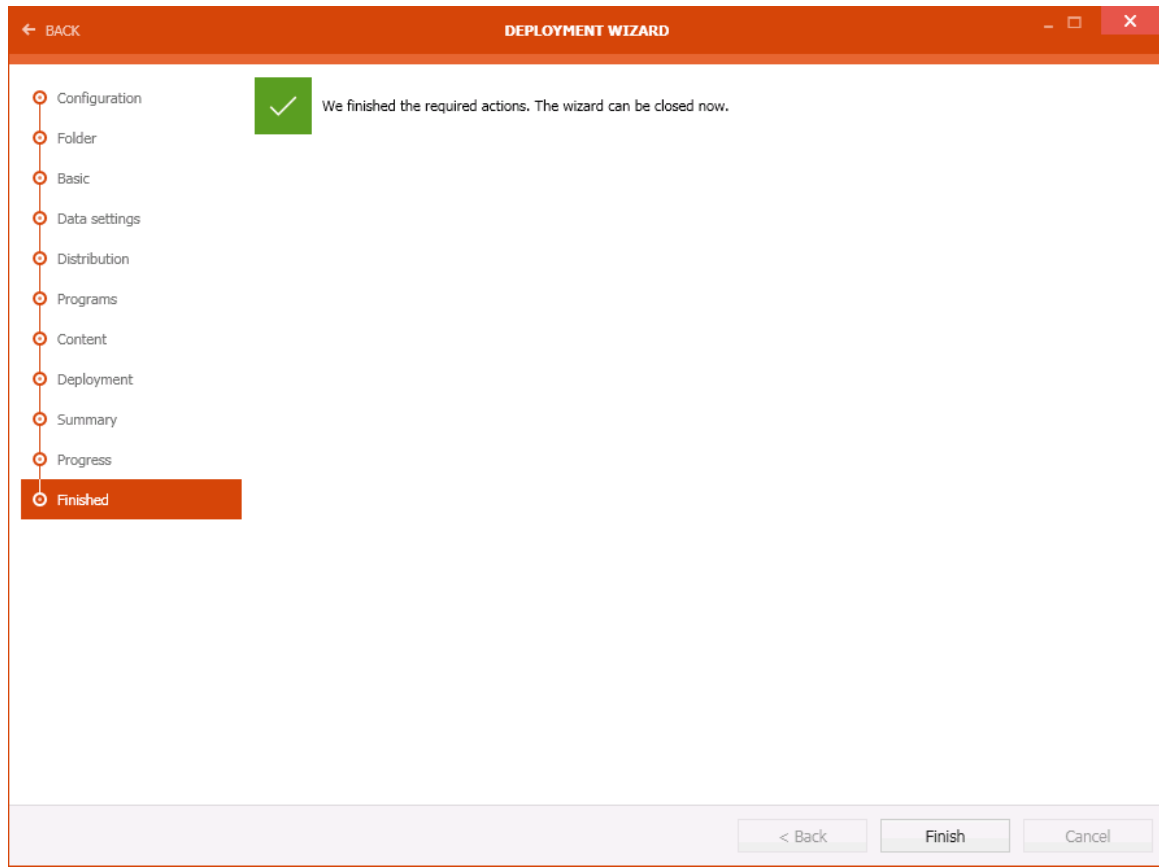
Click on the **Finished** button to close the wizard.

Export Using RMS

Folder Page
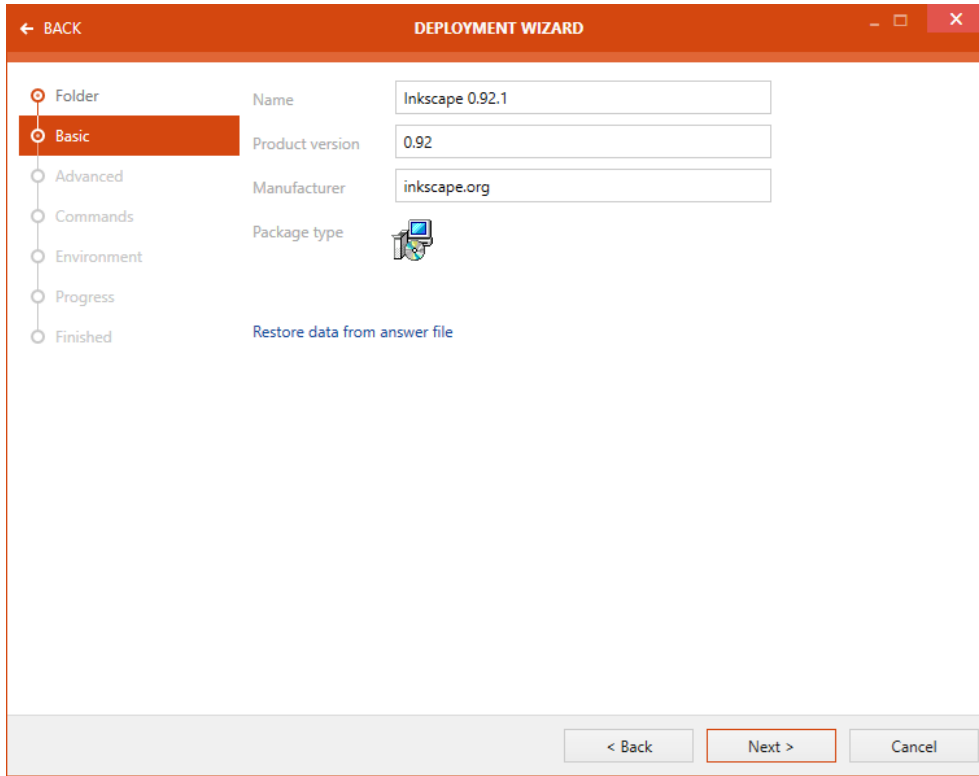
In the **Folder** page, select the folder to which to deploy the package.
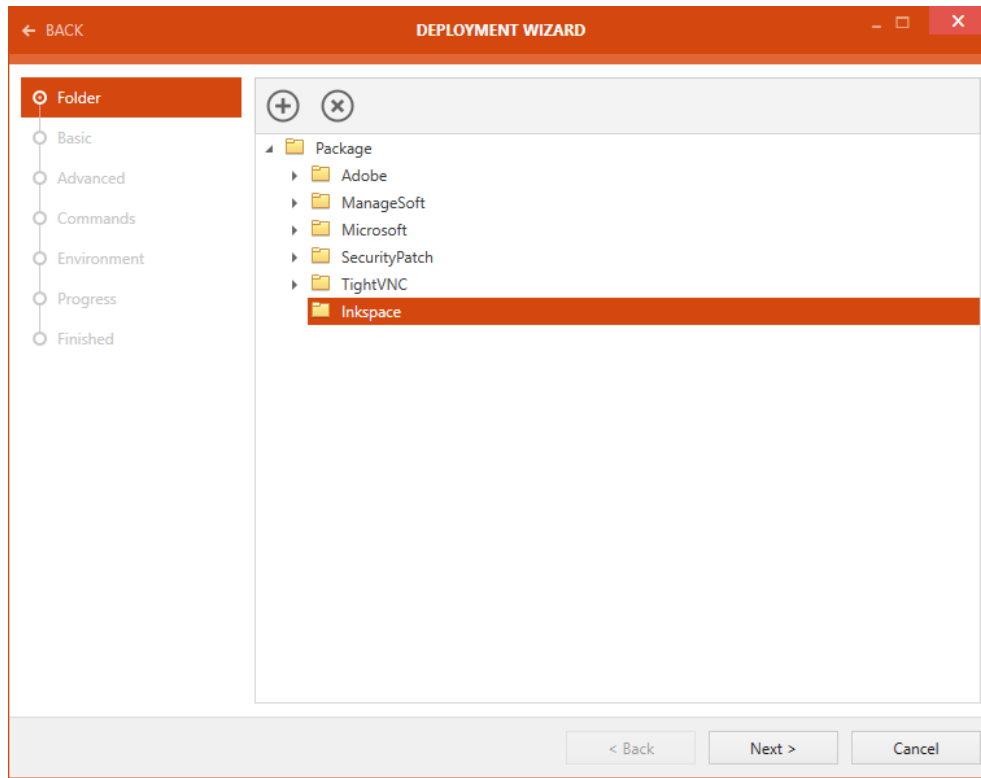
After the target folder has been selected, click on the **Next >** button to continue.

Basic Page

The **Basic** page contains the Basic information of the package.

Basic information on the is page are the following:

- **Name**: The name of the product.
- **Product version**: The version of the product.
- **Manufacturer**: The name of the manufacturer of the product.
- **Package type**: The type of the package. In the example the package is a Windows Installer.

Click on the **Next >** button to proceed.

Advanced Page

On the **Advanced page** more advanced settings can be defined.
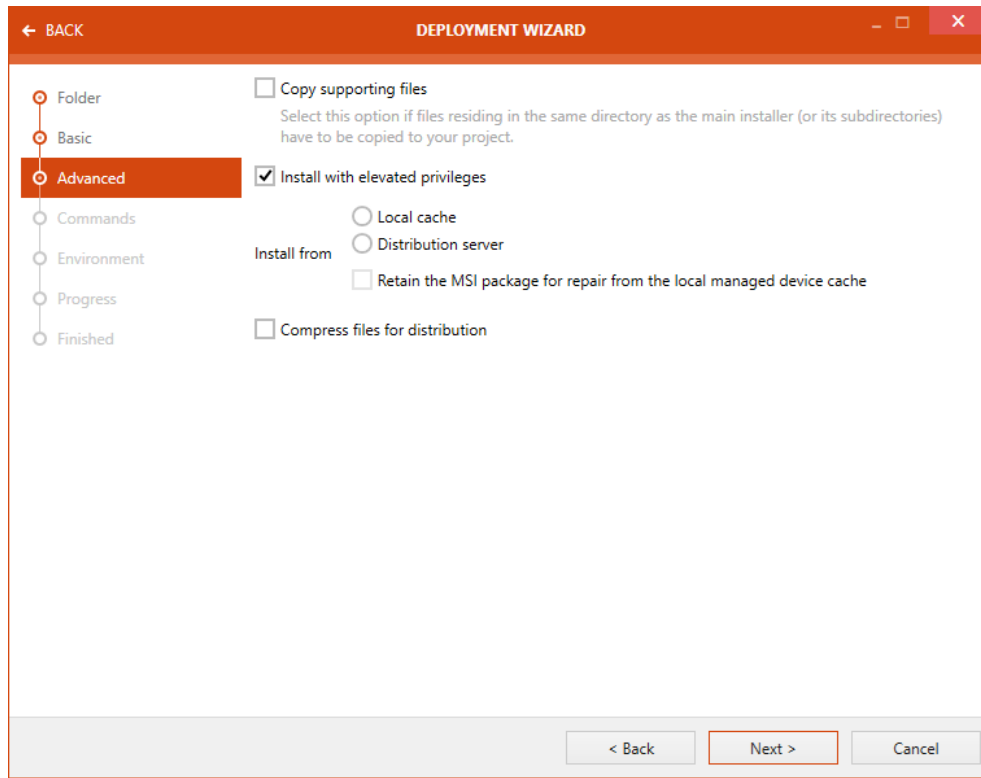
The following settings are available:

- **Install with elevated privileges**: If this checkbox is checked, the installation will be performed with elevated privileges. If not, the current privileges will be used.
- **Install from**: The source of the installation can be chosen here. The following options are available:
  - **Local cache**: The local cache will be used as source of the installation.
  - **Distribution server**: The distribution server will be used as source of the installation.
  - **Retain the MSI package for repair from the local managed device cache**: The MSI package from the local managed device cache will be used.
- **Compress files for distribution**: If this checkbox is checked, files will be compressed for the distribution. If not, the files will not be compressed.

Click on the **Next >** button to continue.

Commands Page

On the **Commands** page commands that will be executed can be defined.
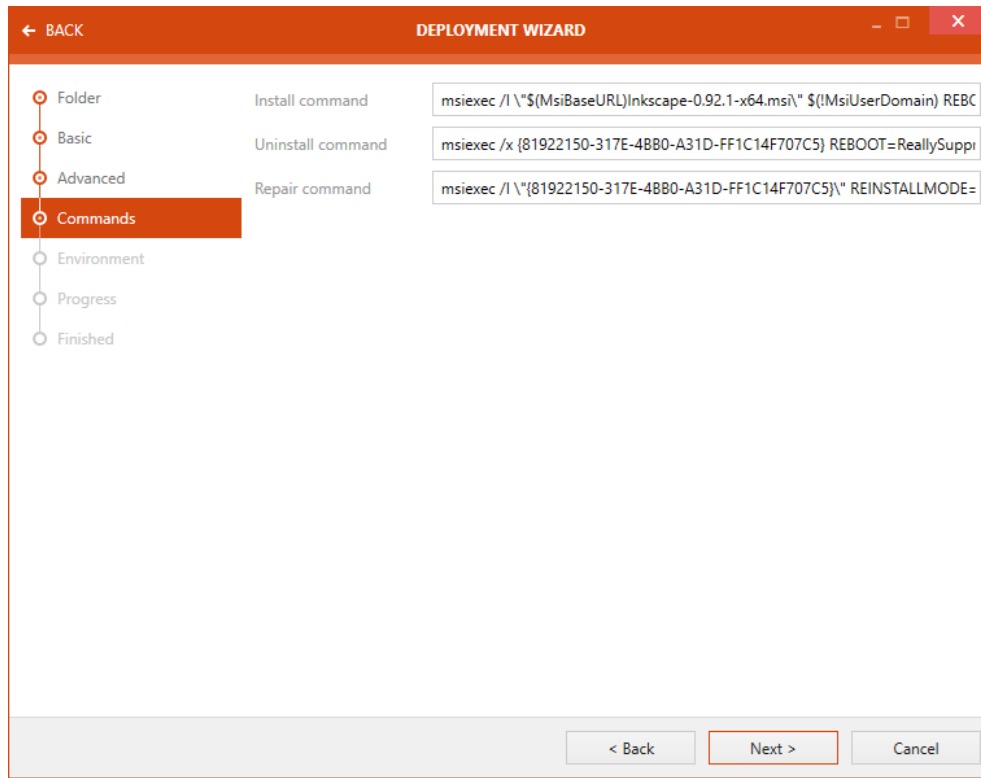
It is possible to define commands for the following options:

- **Install command**: Commands that are to be executed when installing the package are shown here.
- **Uninstall command**: Commands that are to be executed when uninstalling the package are shown here.
- **Repair command**: Commands that are to be executed when repairing an existing installation of the package are shown here.

Click on the **Next >** button to proceed to the next page.

Environment Page

On the **Environment page** the environments for the package can be selected.
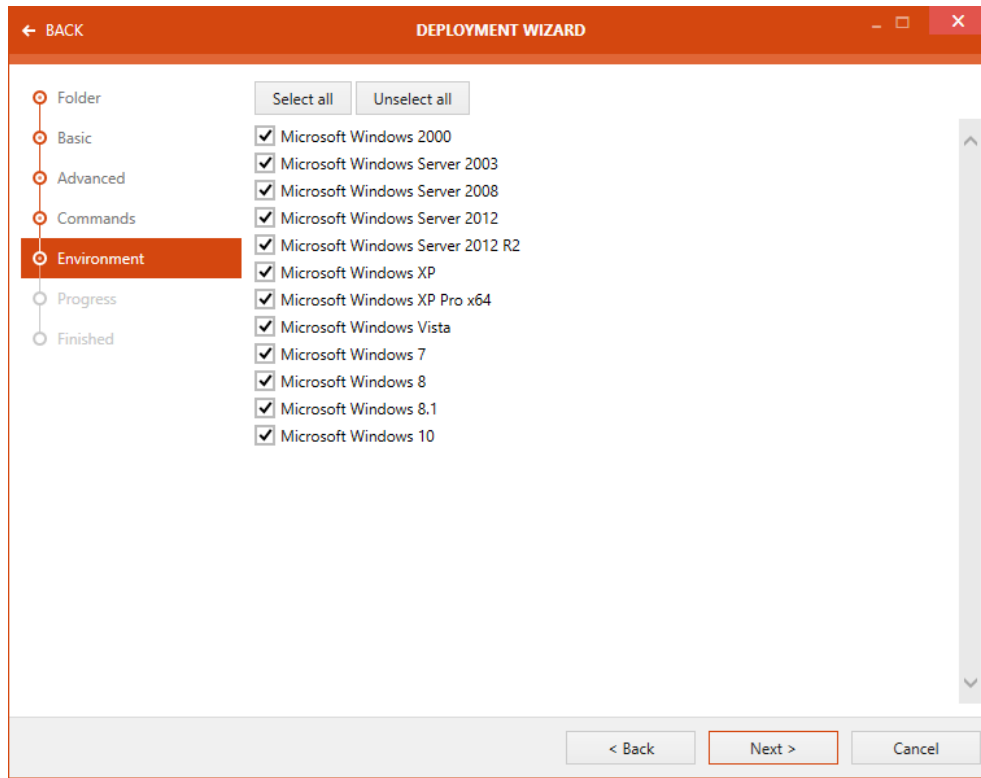
It is possible to select none, one, or more environments for a package. Furthermore, for more comfortable usage it is possible to select or deselect all environments using the **Select all** and the **Unselect all** button.

Click on the **Next >** button to proceed to the next page.

Progress Page

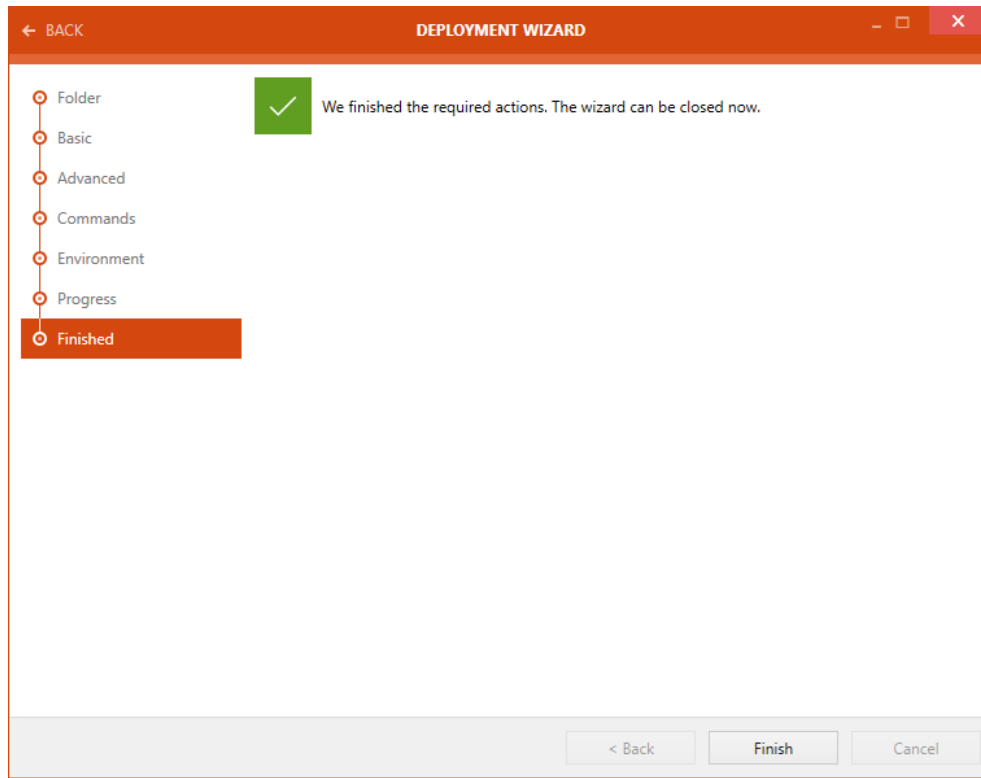On the **Progress page** the progress of the export is shown.
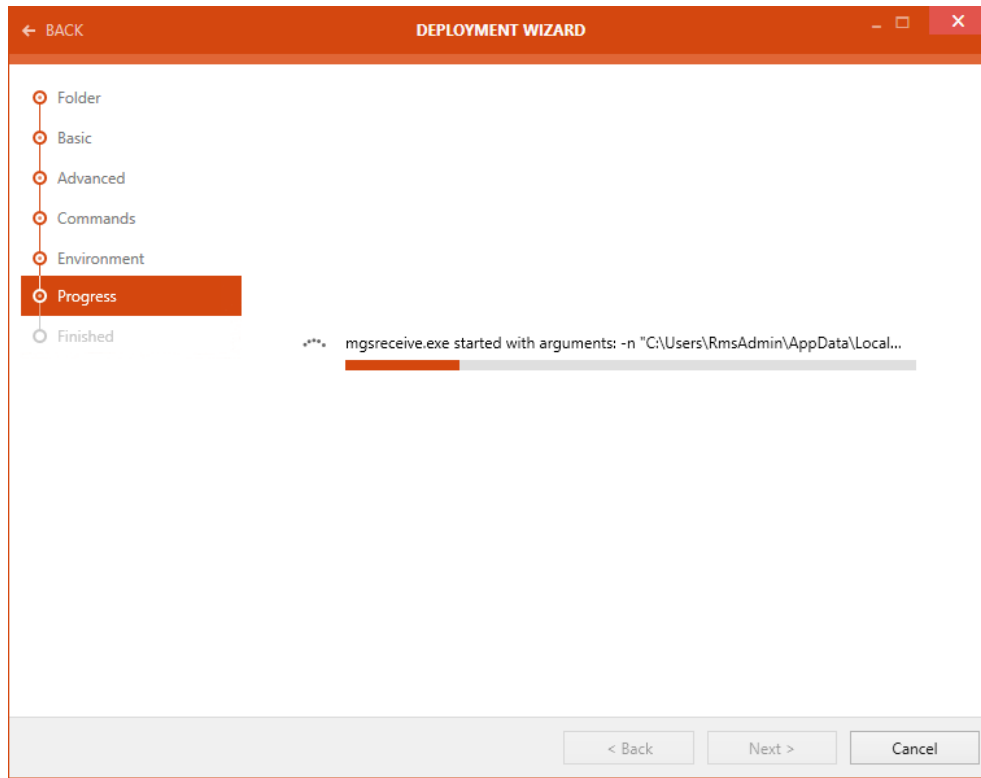
After the export has been finished the wizard will automatically continue to the next page.

Finished Page

The **Finished page** contains the information if the export has been successful.

Click on the **Finished** button to close the wizard.

Reports

Reports section of the RayQC Advanced provides an intuitive platform for users to view and export historical test results pertaining to the packages. Along with having a consistent design, this section presents information in an informative format using various symbols, color coding and pie charts.
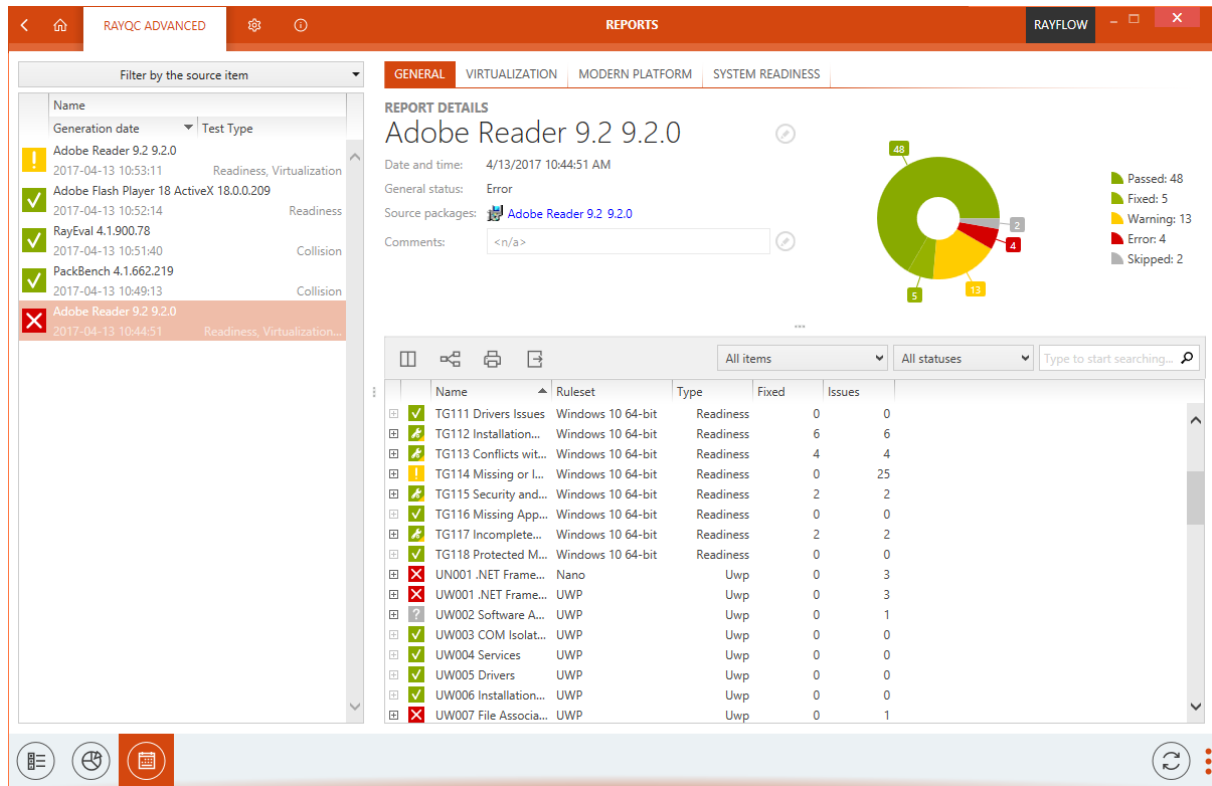
Structure of Reports viewer: The reports viewer area can be divided into three major sub-areas

1. Package List
2. Report Details
3. Swipe-bar

Package List

Package List is shown on the left side of the **Reports** viewer. It lists all the packages on which tests have been executed. The package list shows the properties of a package including package name, test date and test result under the respective column headers. These column headers can be arranged in a desired order by simply dragging and dropping it to its new position.

Symbols in Package List

Each of the packages within the package list is coupled with a status symbol. This symbol

represents the overall result of test, executed on a package.

✅	Represents that a package has passed against all the rules with the test
⚠️	Represents that a package test result contains warning for certain rules
❌	Represents that a package has failed against certain rule with the test
❓	Represents that a test has been skipped

Filtering of Packages

A user can filter the package list using the column filter icon (▼) which is available next to each of the column headers. This icon, which is initially invisible, is shown once the mouse pointer is hovered over a respective column header. Clicking on this icon will list the filtering options, which are based upon the respective package property; to which the column header is associated with. All, Blanks and Non Blanks are the default filtering options for each of the column based filtering.

- **All**: This will list all the packages.
- **Blanks**: This will list the packages for which the respective column header property is blank.
- **Non Blanks**: This will list all the packages for which the respective column header property is non-blank.
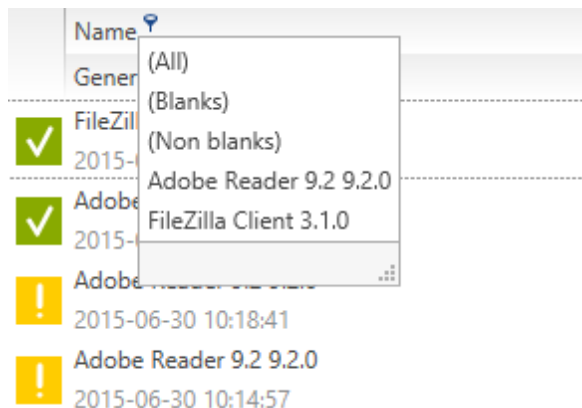
Filter Editor

When a user activates the column header filter, by default the filter editor is activated. This filter editor bar is shown at the bottom of package list. A user can edit the filter condition by directly selecting the edit icon on the filter bar. To remove filtering simply click upon the **Cancel** icon on the filter bar.

Filtering by Source Package

RayQC Advanced offers a user an ability to test a package against another package. Packages

within the package list can also be filter based on their source test package. To achieve this, select Filter by source package option. This will open a dialog with all the packages within library. Simply select a source package and click on the **Apply** button to apply this filter on the package list.

Sorting of Packages

Packages within the package list can be sorted by using the sorting icon. This icon is available in each of the column headers. When clicked upon, the package list will be sorted in an ascending or descending order for respective type of the package property (alphabetic or numeric).

Report Details

When a package is selected from the package list, details pertaining to the test of that package are shown under the Report Details section. This section is subdivided into three areas:
a. Test Type
b. Package properties
c. Result Details

Test Type

This area of Report Details consists of tabs. Each of the tabs represents a test type. When a tab is selected, all the test results pertaining to that test type is shown under the Result Details section. The General tab is available by default and when selected, test result from all the test types is shown under the Report Details section.

Package Properties

Just below the test type tabs, properties of a tested package are shown. These properties include: name and version of the package, date and time of testing, source package and comments. It is possible to edit the name and version of tested package or to add a new comment. To do so, simply click on the edit icon and make or add changes as desired. To apply the changes, simply click on the OK button and the same can be rejected by clicking on the Cancel button.

The package properties are paired up with a pie chart. The test results for the package is plotted against the number of rules, the package is tested against. Following color convention is used for plotting of this chart:

	Passed
	Fixed
	Warning
	Error
	Skipped

Result Details

In this section of Reports view, the test results pertaining to a package is shown. The test results basically include a list of rules against which the package has been tested. If a package has been tested against rules belonging to different test types, then a user can filter these rules using test

type tabs on top of the package properties section.
Each of the test rules is paired with an icon, which visually delivers the result of test.

✅	Represent that no issues have been found in the package for that particular rule
⚠️	Represents that the test result consists of a warning
🔧	Represents that the test result consist of a warning but has been fixed
❌	Represents that the test result consists of an error
🔧	Represents that the test result consists of an error but has been fixed
❓	Represents that the test has been skipped

Above the result details section, a functional bar offers following ability to users:
- **Column Chooser**
- **Advanced Sorting**
- **Print**
- **Export**
- **Filter by package**
- **Filter by status**
- **Search**
- **Column Filtering**

Column Chooser

The position of each column can be changed by dragging it to the desired place. During dragging blue arrows indicate the target position when the column is dropped at this point.

Click on the **Column Chooser** icon to display the column menu. It contains all available columns that are not displayed in the current list setting. To add a column to the view, simply drag it from the menu to the header section of the report details section. To remove a column, drag the column header to the column menu.
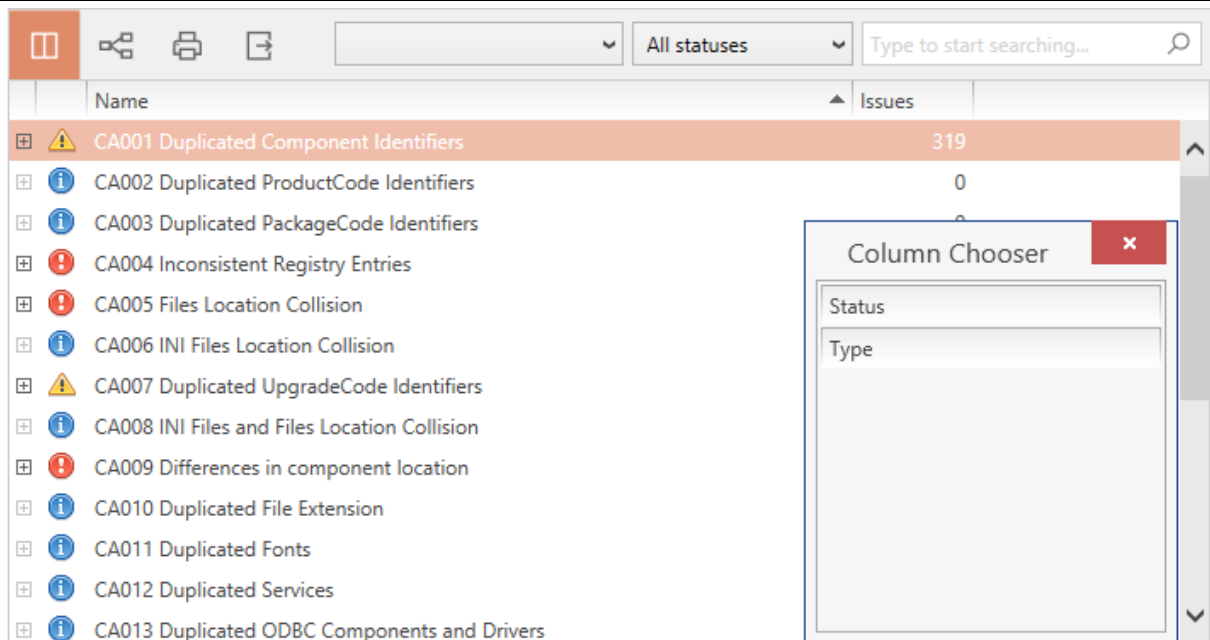
To close the **Column Chooser** menu, click on the close icon at the upper right corner of the menu, or use the **Choose Columns** icon.

Advanced Sorting

To enable the **Advanced Sorting** editor, click on the **Advanced Sorting** icon from the action bar. The advanced sorting bar is displayed. To add a criterion to the advanced sorting, drag a column header to the advanced sorting bar area and drop it there. Two blue arrows mark the exact position where the header will be dropped.


The position of the criteria within the advanced sorting bar indicates the way the list is sorted. The illustration below shows a sort algorithm that sorts by **Name**, with this it sorts by **Status** and within this it sorts by **Type**.
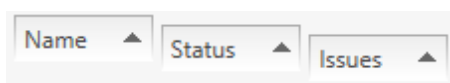
To change the sorting hierarchy drag a criteria from one position and drop it at the desired position.

After dropping the criteria into the advanced sorting bar, the sort icon in the right part of the criteria indicates the sorting order for each of the criteria. The order can be changed from ascending to descending and the other way round by clicking on the symbol. Furthermore, by clicking between the sort icon and the name of the criteria, filters can be activated. These filters can be chosen from a drop-down menu.
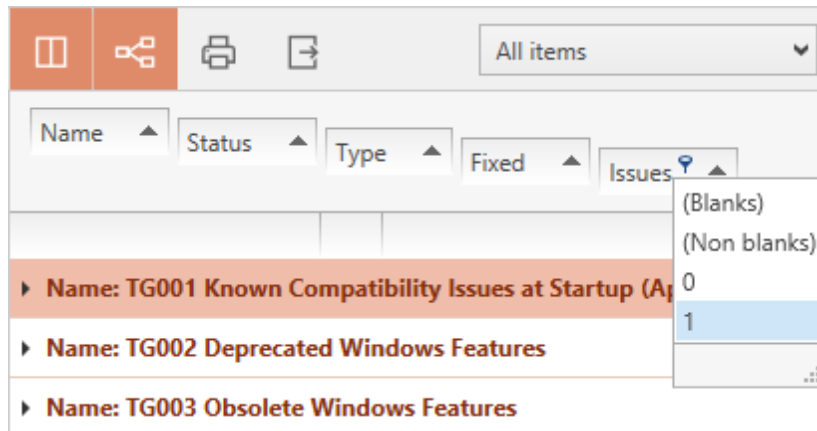
If the **Advanced Sorting** icon is displayed with a dark gray background, the advanced sorting editor is visible. Clicking the icon will close the editor. Advanced sorting will not be deactivated by this. To deactivate advanced sorting, drag all column headers back into the column header section of the list view. The **Advanced Sorting** function is inactive when the sorting editor bar is empty.

Print

To print the currently displayed content of the result details view, hit the print icon. A dialogue opens, that allows you to select the desired printer and printing options.

Export

Exporting the result details view contents can be handy for communication on certain items or structures.
The currently displayed contents of the result details view can be exported to the following formats:

- Excel
- PDF
- HTML
- CSV

To export data:

1. Click on the export icon.
A dialogue opens, in which you can select the desired format and target location for the export.
2. Click **OK** to start the export.

Filter by Package

If a test has been executed on a set of package, then the test result can be filtered per package. To achieve this, use the drop-down list in action bar to select a package for which the test results should be shown.
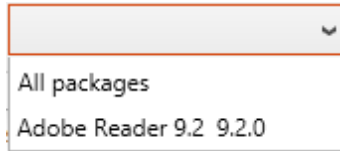
Filter by status

Test results can be filtered based upon the status (result) of test rules. To achieve this, select the desired status from the drop-down list; this will automatically filter the test result based upon the status.
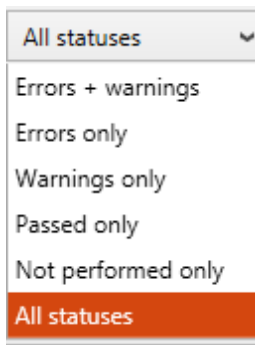
Column Filtering

It is possible to either use the column value filter to reduce the displayed test results to a certain subset or to use the keyword search field.

To filter contents by column values, move the mouse pointer over a table header. The filter icon appears. Click on the filter icon to see the set of value options available in this column. Select one of the entries to reduce the displayed test results to those projects that have the selected column value.

If the column filter is active, the filter icon is permanently displayed in the column header. Open the filter options to see the currently active filter value named above the list of available values. To remove the filter, click on the **(All)** option.
Column filters can be combined from several column headers.
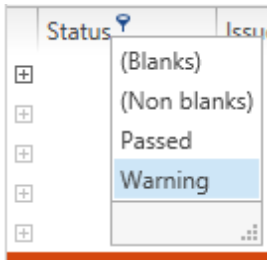
To filter the test results by a keyword, enter it into the input field at the upper right corner of the list actions area. Click on the magnifier icon or hit enter on your keyboard to search for the keyword within all displayed project properties. To deactivate this filter, remove the keyword and use either the magnifier icon or the enter key on your keyboard.

To Refresh the Reports View

The contents of the reports view are not refreshed periodically, but automatically after certain events. To refresh the list content manually, use the refresh button from the swipe-bar at the bottom of this view.

To Save the Report

Context menu option **Save as...** can be used to export the report to PDF / DOCX and other formats. Pressing the menu item opens the **Save as...** dialog.
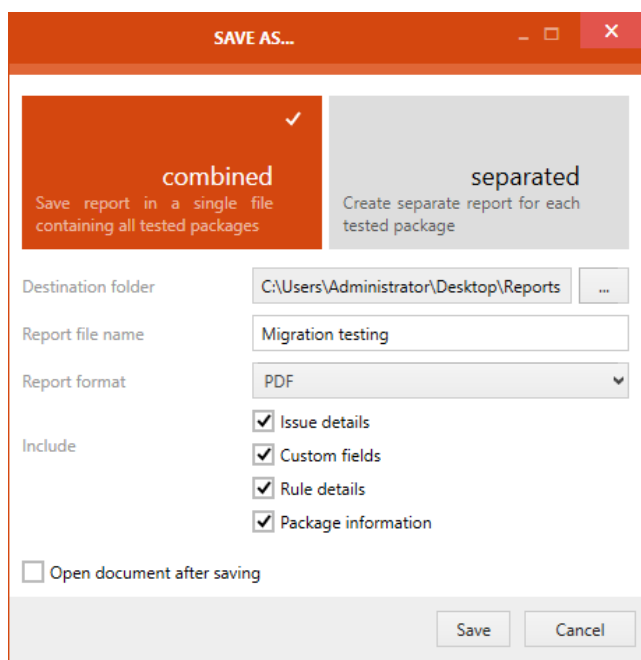
As first step in the **Save as...** dialog, users have to decide if the result of the test should be saved

either **combined** or **separated**. If the **combined** option is chosen even if multiple packages have been tested, the results for all packages will be saved in just one single report file. This is also the default option. If the **separated** option is chosen, a report file will be created for each of the packages that were part of the test.

- **Destination folder**: By clicking the Browse button [**...**] the **Select Folder** dialog will be opened. In the dialog browse to the folder in which the report should be stored and select the target folder.
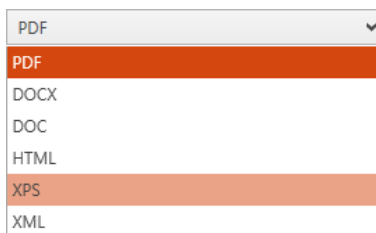- **Report file name**: This is where the name of the report is defined.
- **Report format**: The report format can be chosen by using the dropdown menu.

PDF	⌄
PDF	
DOCX	
DOC	
HTML	
XPS	
XML	

The available formats are .pdf, .docx, .doc, .html, .xps, and .xml. Choose the format in which the report should be generated

- **Include**: This option offers two checkboxes. The **Issue details** checkbox and the **Custom fields** checkbox. If the **Issue details** checkbox is checked, details on the issues will be added to the report. If the **Custom fields** checkbox is checked, the custom fields will be part of the report. Finally, if the **Package information** is checked an extra information about each tested package is printed in the header.

> **Note:**
> When exporting reports for hundreds of packages, consider disabling the **Package information** option. This way, the report will be more compact and well suited for printing.

The **Open document after saving** checkbox is only available if the **combined** option has been chosen. If the checkbox is checked, the file will be opened after it has been saved.

After everything has been defined, the report can be saved by clicking on the **Save** button.

Diagrams

Clicking on this button will open the dashboard of the report section. This **Dashboard** offers a monthly and a quarterly overview of the status of the reports that have been made.
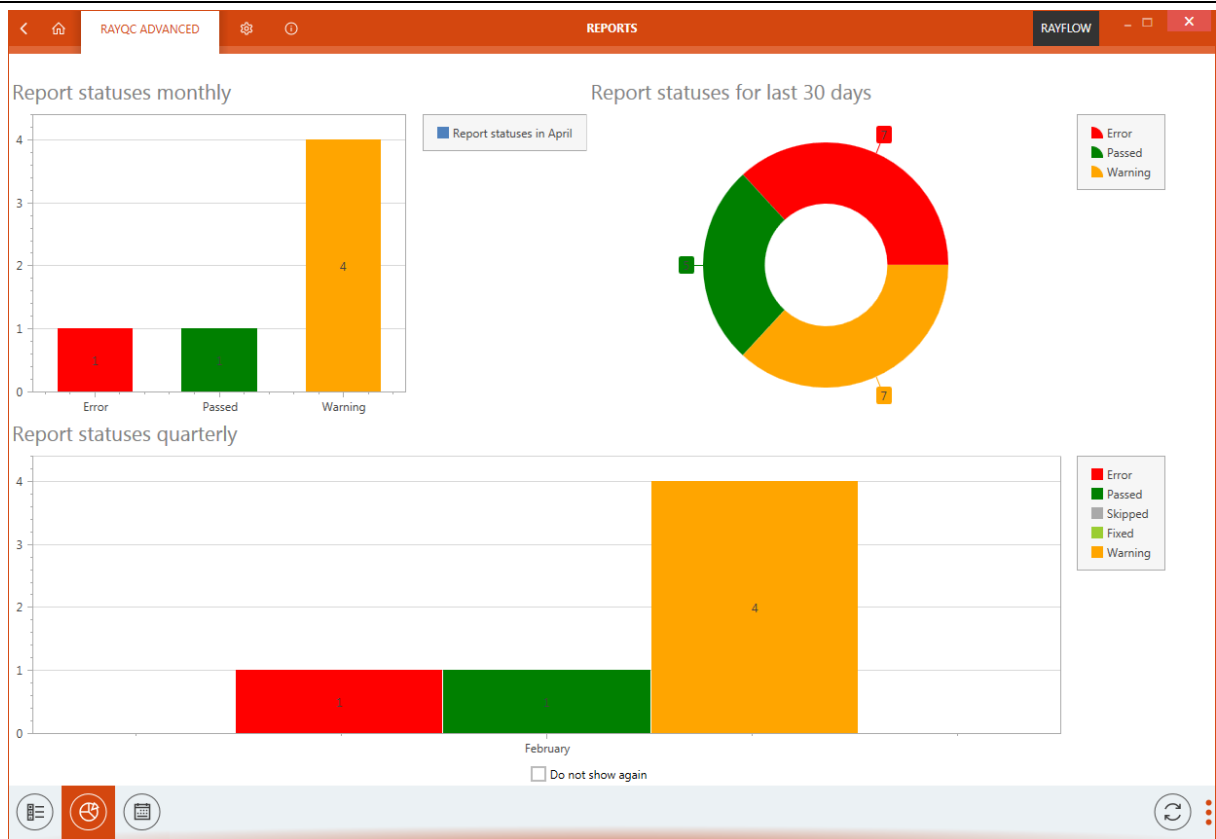
Details

Clicking on this button will open the details view of the report section. This view shows all library packages and their respective most recent test results..
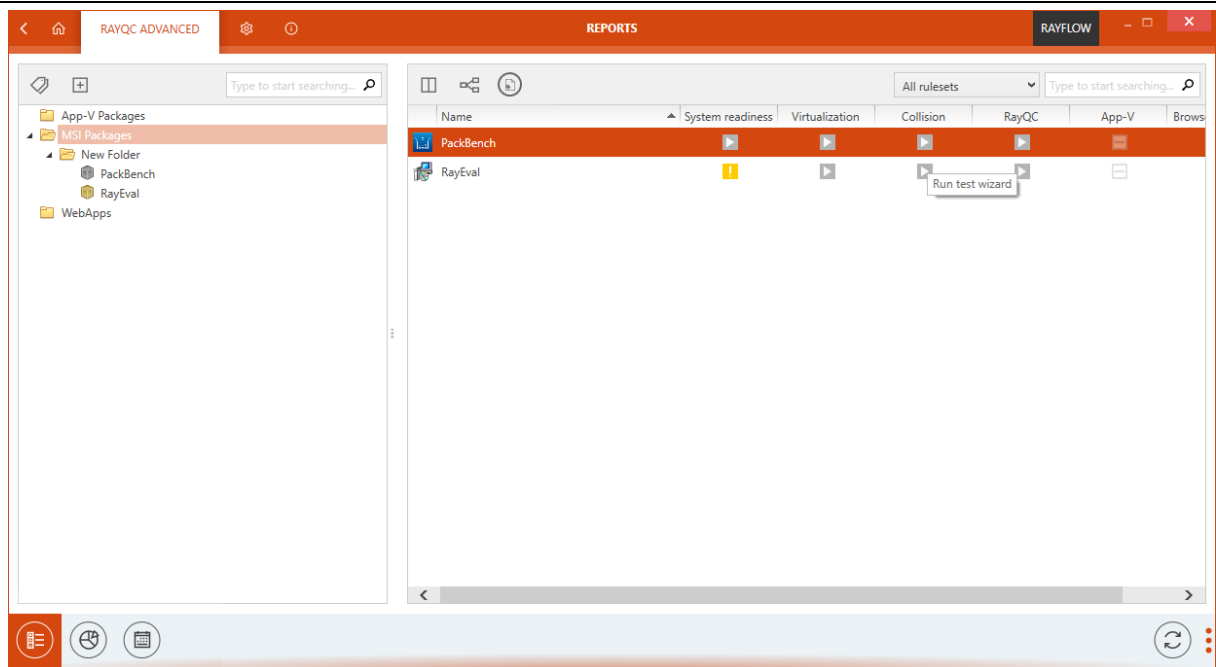
Icons represent statuses of most recent test. If a gray icon is shown, the test has not been performed on that package yet. Color statuses represent the result of the recent check.

Pressing the status button:

- for not executed tests: starts the Test Wizard.
- for already executed tests: opens the detailed report view.

Working with RayFlow

Introduction

RayFlow is a workflow process management tool with the ability to support diverse workflow processes. The possibility to be customized to fit the user's needs and requirements makes it one of the most efficient and user friendly workflow management tools. This guide shows how to configure and manage RayFlow, so that IT departments can stay ahead, save time, increase productivity, and decrease IT costs.

RayFlow is based on the client-server architecture in which all the information, data, and configuration is stored on the RayFlow server. Users work on this server remotely through the RayFlow web and Windows-based clients.

Where to find the latest information about RayFlow

For further information on RayFlow, including its features, functionality and latest updates visit www.raynet.de.

Enabling RayFlow features in RayQC Advanced

RayFlow connection are stored in profile configuration. The minimal configuration requires entering the URL address containing a valid and running instance of RayFlow server.
See RayFlow configuration for RayQC Advanced for information how to configure this feature.

Signing-in to RayFlow

Saving and opening files from RayFlow requires that the current user is signed-in to the RayFlow instance specified in the configuration screen for RayQC Advanced.

Sign-in procedure makes sure that:

- User has permissions to a specified RayFlow project
- User has permissions to see/edit required RayFlow tasks

In order to sign-in, press the RayFlow button, located in the top right corner of the screen.

If the server is not valid or not specified, the following warning will be shown:
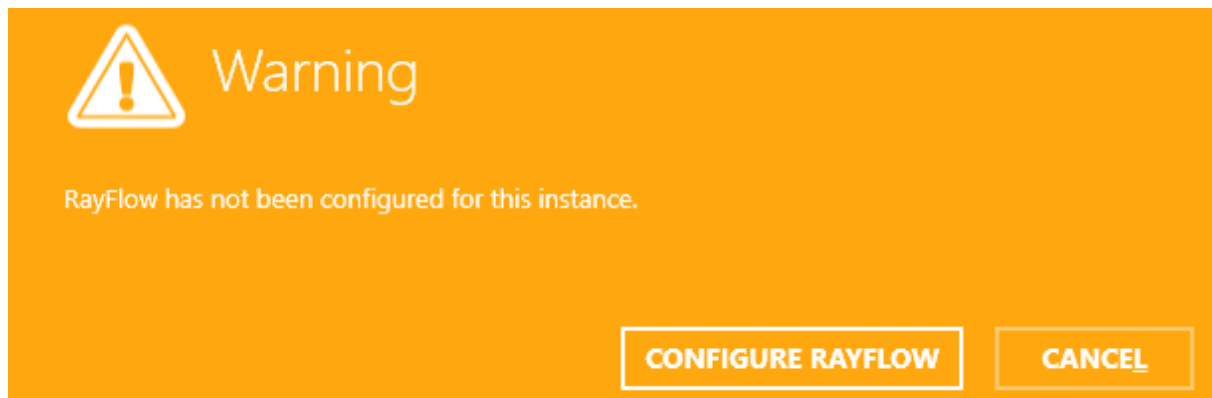
Otherwise, the sign-in overlay will be displayed over the current window:
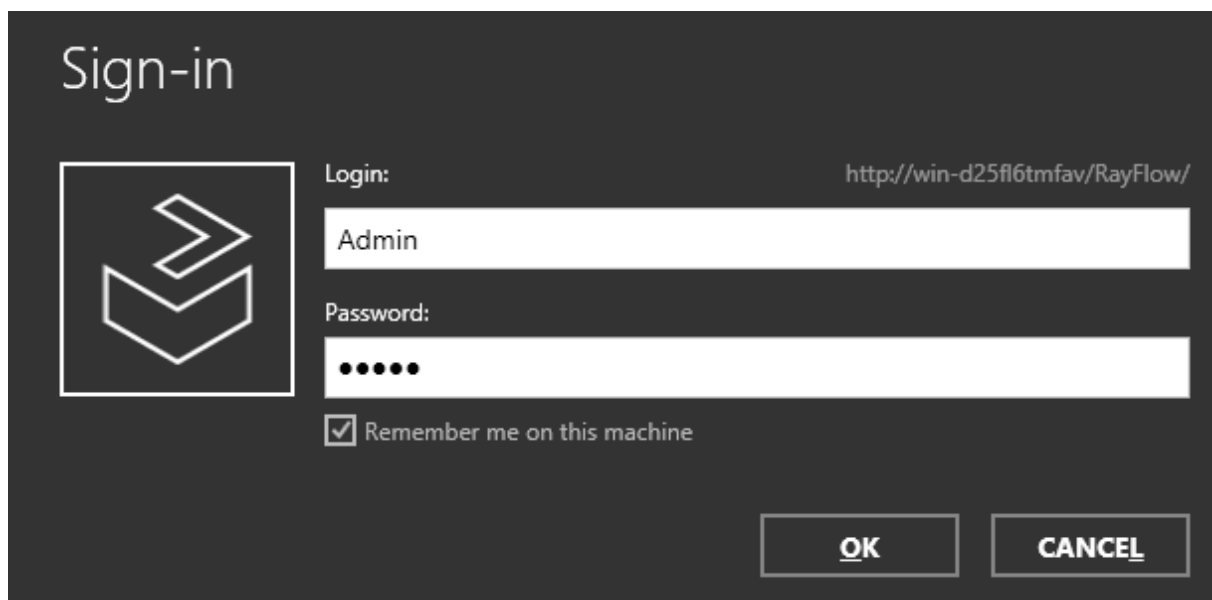
The overlay contains the following information:

- The URL address of the current RayFlow instance, as configured in the profile settings.
- The text fields for user name and user password.
- A checkbox to remember the credentials on the current machine.

> **Note:**
> RayFlow credentials have to be delivered by the local RayFlow administrator.

Login and password are required to sign-in to RayFlow. Make sure the checkbox **Remember me on this machine** is marked before pressing **OK** to save the credentials of a successful login.

Once the credentials are verified, a selection of projects available in the current RayFlow

instance will be shown.

> **Note:**
> Only projects to which the current user has view permissions are displayed.
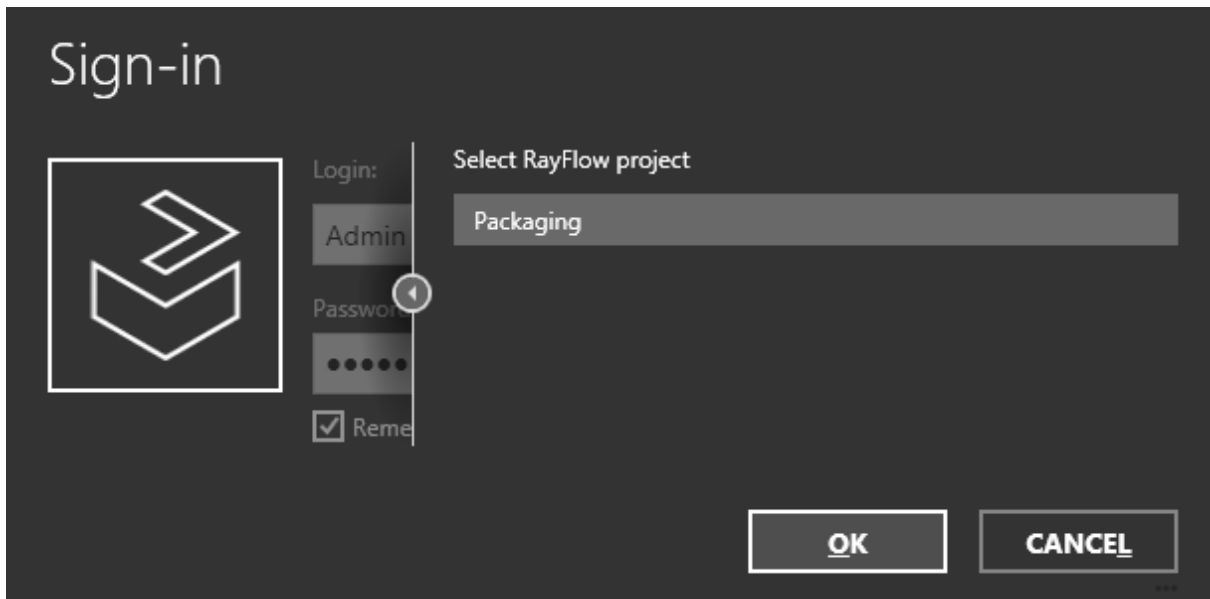
Once the project is selected the sign-in procedure is complete, and certain RayQC Advanced functions (like opening and saving files to RayFlow are available).

Once authenticated, the RayFlow button in the top right corner of the screen changes its color and displays the user name of currently authenticated user. After clicking on it additional details are shown, including:

- The logged in user.
- The current project.
- An URL address of the current instance.
- *The **Logout** button.*
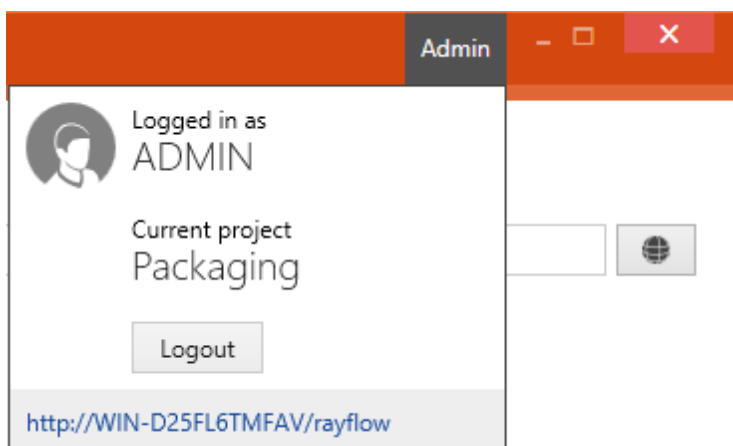
Import a RayFlow Package into the RayQC Advanced library

This section describes how to import a package from RayFlow into the RayQC Advanced library.

1. Select the item **Import package** from the swipe-bar
   The **IMPORT PACKAGE WIZARD** is initialized

2. Select RayFlow from the available options.
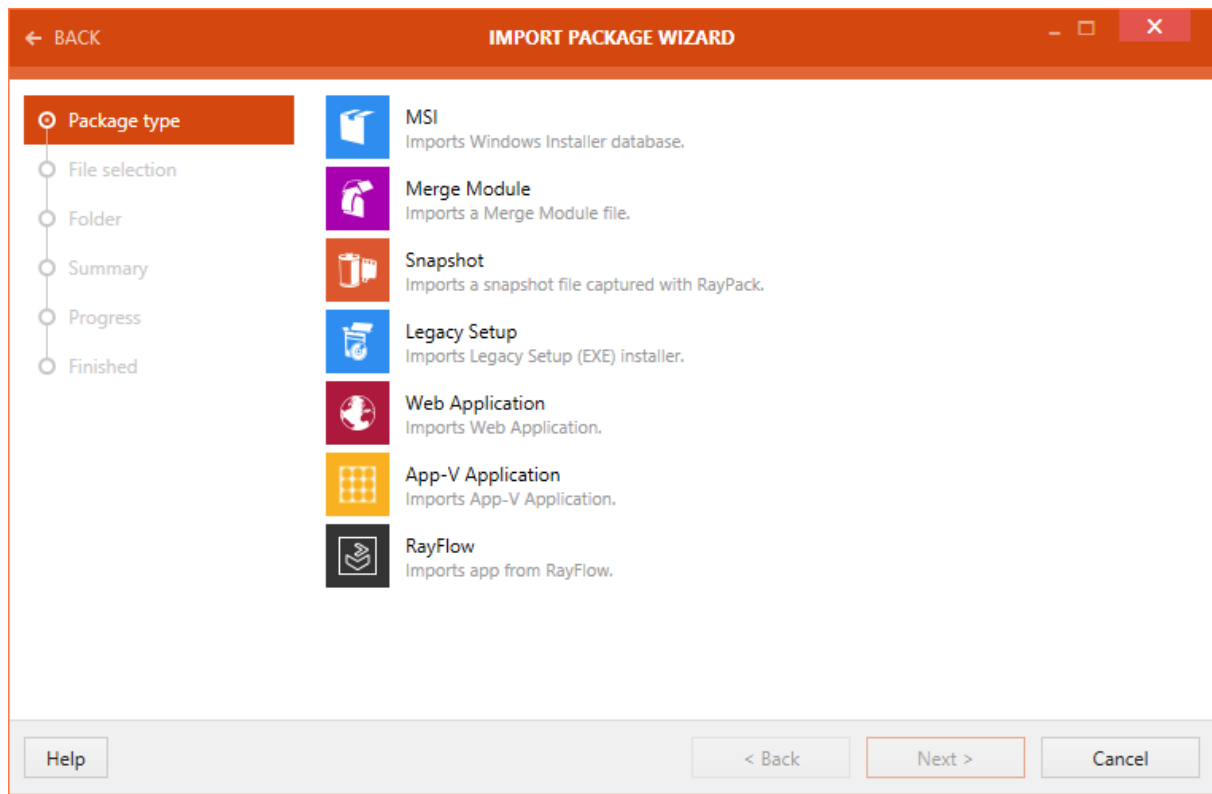
3. Click on the **Next >** button
   The **PACKAGE SELECTION** page is now available.

4. From the drop-down menu, select the phase in which the target package for import into the library can be found.
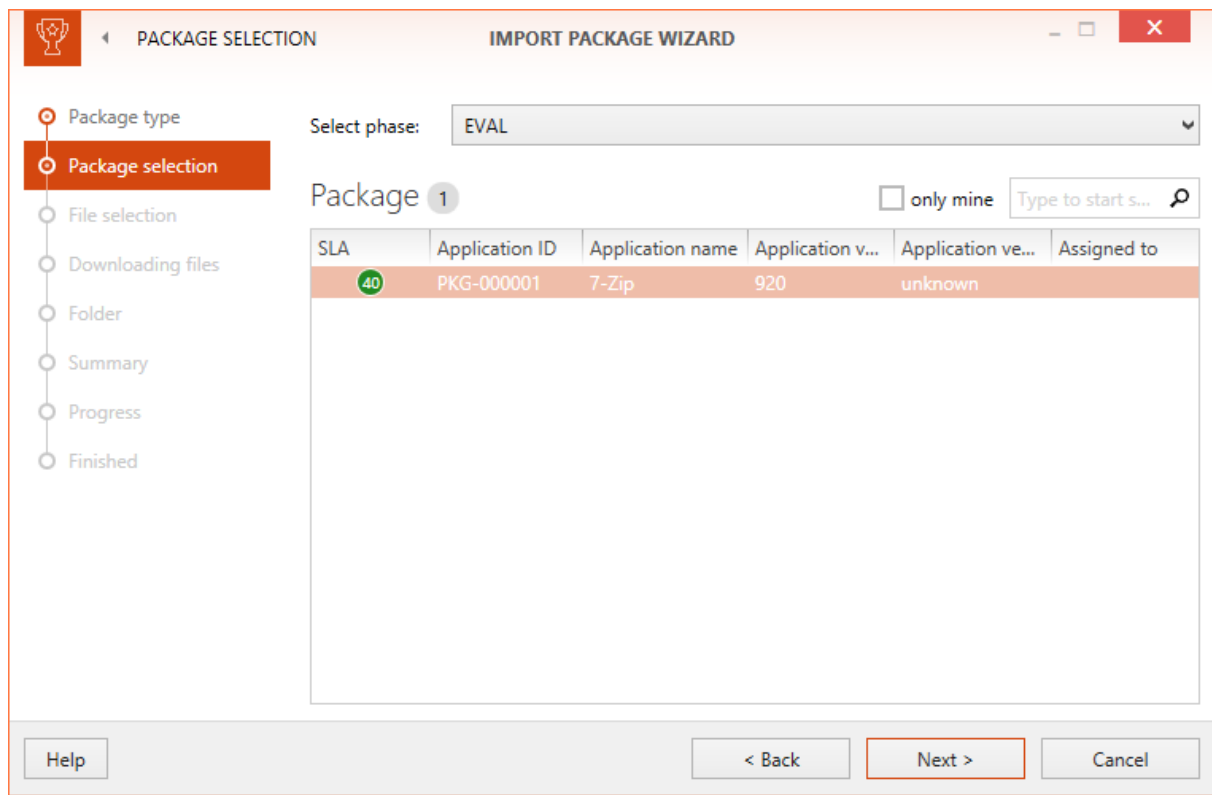
5. After selecting a phase, all packages which are currently in the selected phase will be listed. Select the target package from the list of packages. If there are a lot of package in a phase, it is possible to search the list by using the search function. Furthermore, if the **only mine** checkbox is checked, only packages assigned to the currently logged in user will be shown.

After the target package has been selected click on the **Next >** button to proceed.
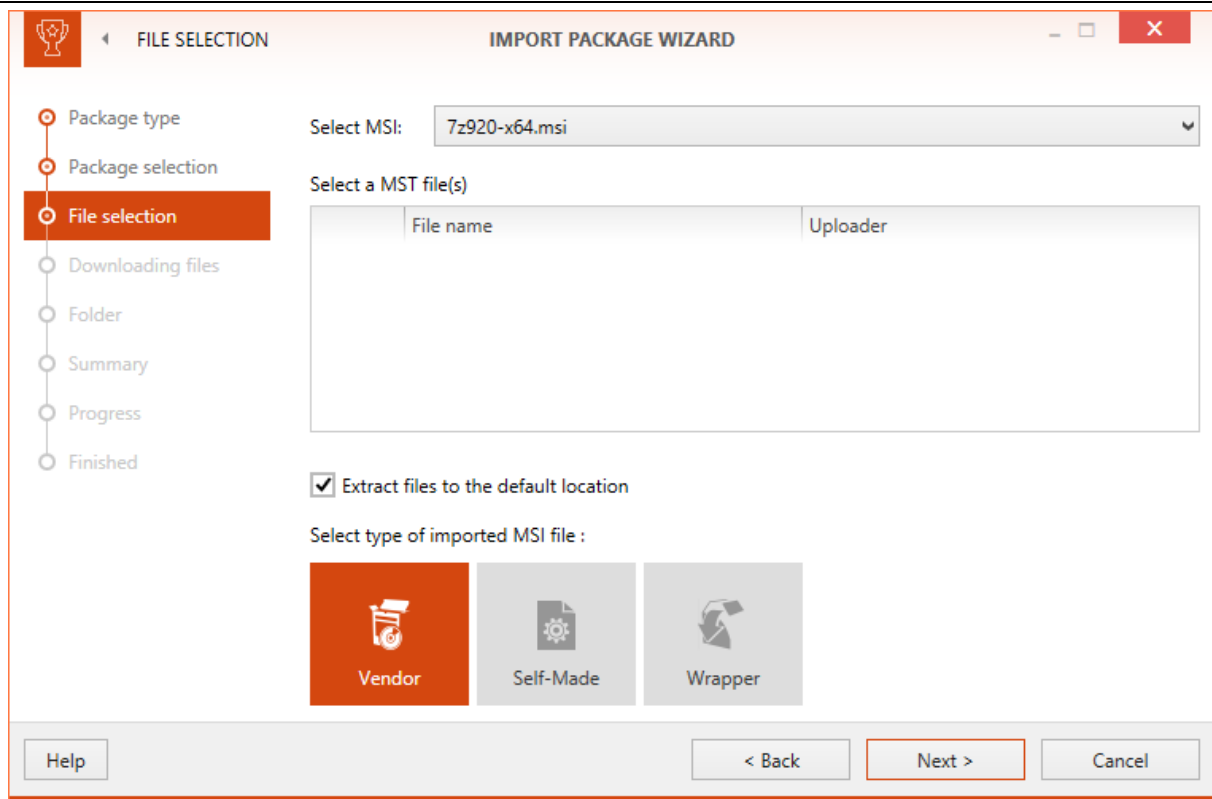
6. The **File selection** page is shown now. If a RayFlow package contains more than on file that can be imported into the RayQC Advanced **library**, the target file can be chosen by using the drop-down menu. Furthermore, if there are MST file(s) available in the package, they can also be chosen.

   A user can also choose a ZIP package which contains `.msi` and `.mst` files.

   If a ZIP package contains more than one MSI file, on the next step, the user will be asked to select one `.msi` file that will be imported into the **library**.
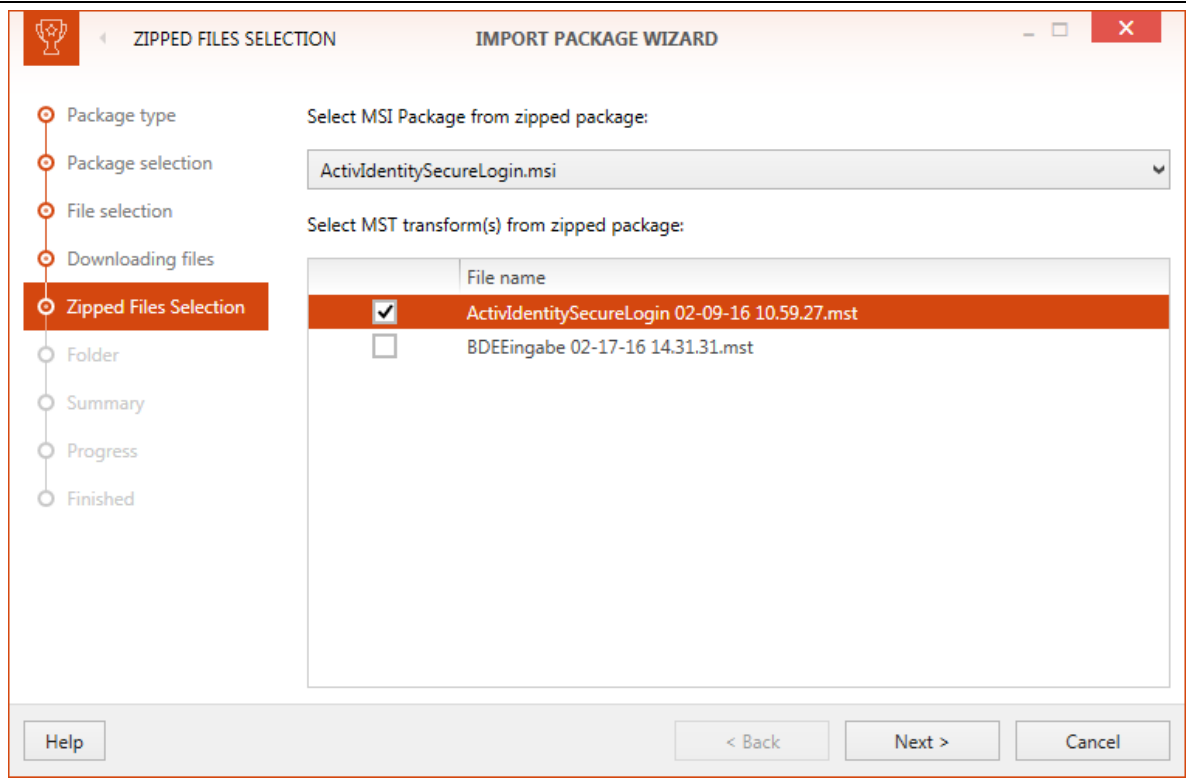
Click on the **Next >** button to proceed. The files are downloaded now. After the download has been finished, RayQC Advanced will continue to the **Folder** page.
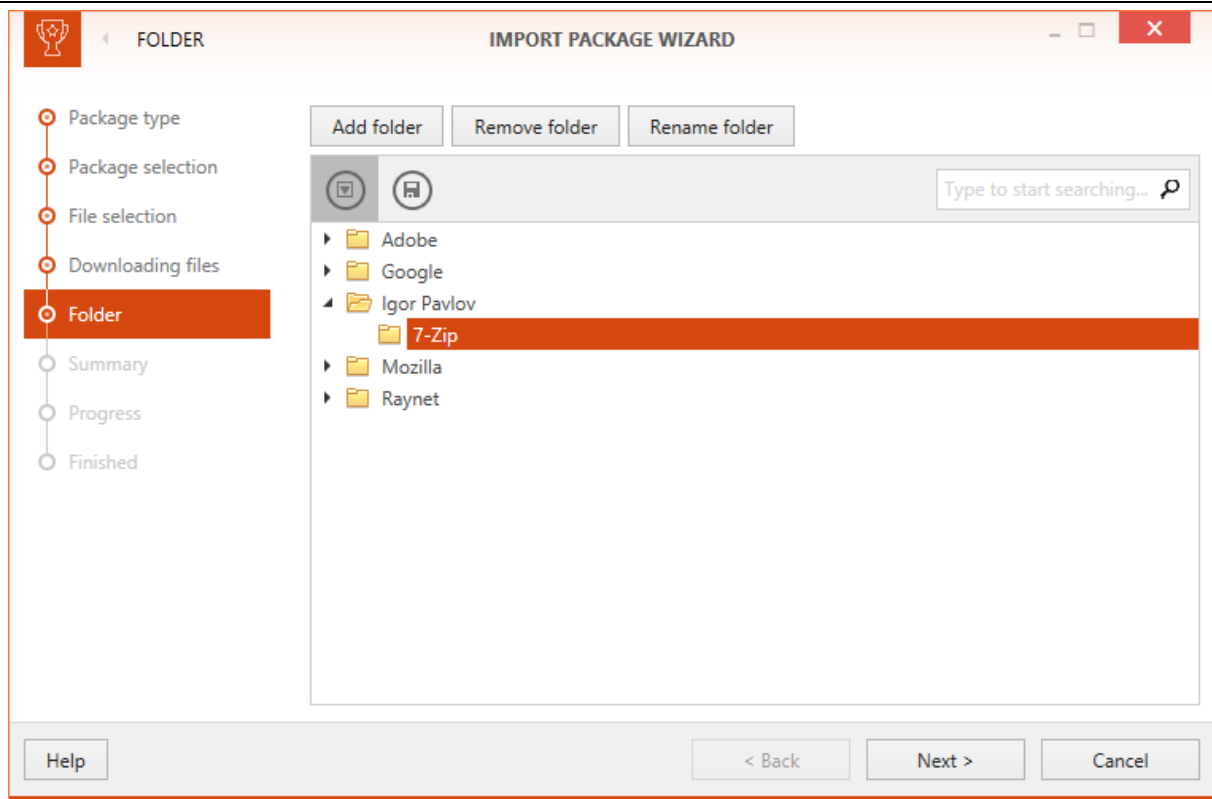
7. On the **Folder** page select an existing folder or click on the **Add folder** button to add a new folder as destination for the page. The folder shown here are the folder that are currently part of the **SOFTWARE** section of the RayQC Advanced **library**.

   After a destination folder has been chosen, click on the **Next >** button to proceed.
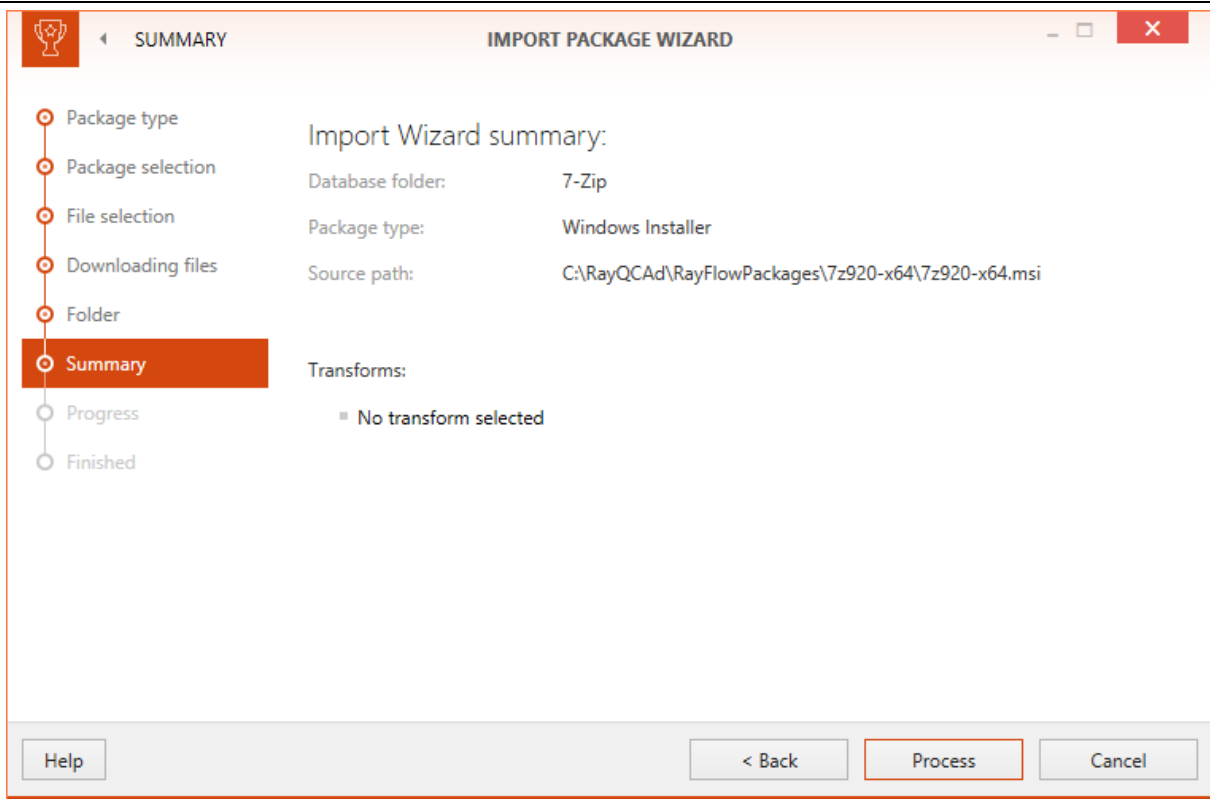
Next, the **Summary** page is shown. The user input for the package import is summarized on this page.

8. Click on the **Process** button to start importing the package.
   A progress bar is shown.

9. Confirmation on successful package import is shown on the **Finished** page.
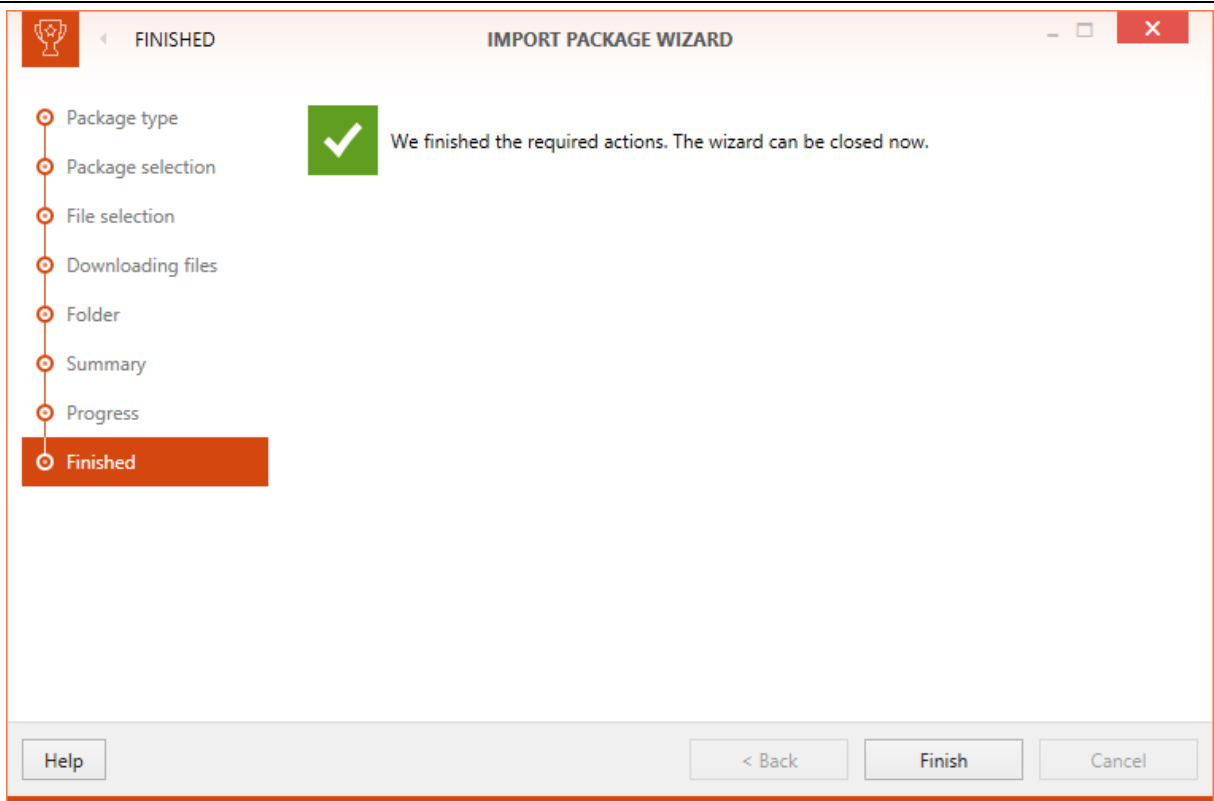
Link Existing RayFlow Package with Package from the Software Library

A user can link existing RayFlow packages with packages from the **software library**. In order to do that, go to the **library**, select the package, open the context menu, and click on **Link RayFlow package**.
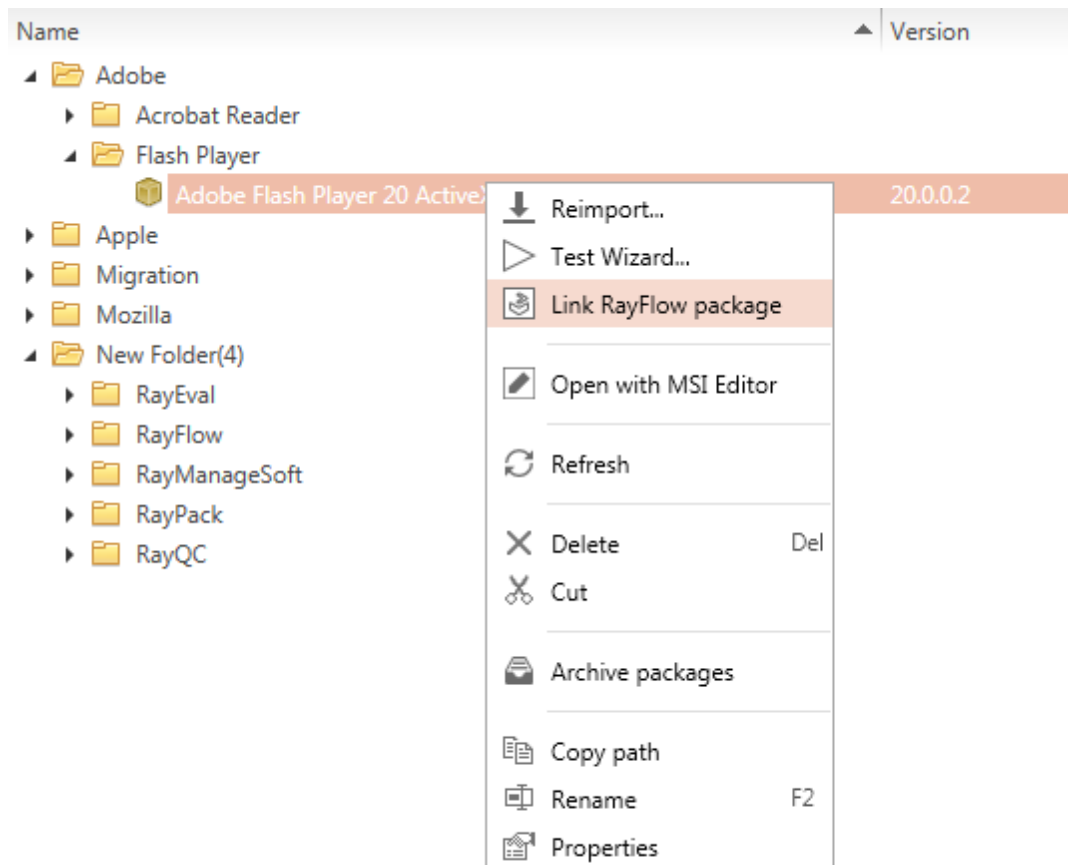
It is also possible to link a RayFlow package by choosing the **RayFlow** tab from the details section on the right hand side and then click on the **Link package to RayFlow** link.

Unlink Existing RayFlow Package with Package from the Software Library

A user can unlink a linked RayFlow packages from packages from the **software library**. In order to do that, go to the **library**, select the package, open the context menu and click on **Unlink RayFlow package**.
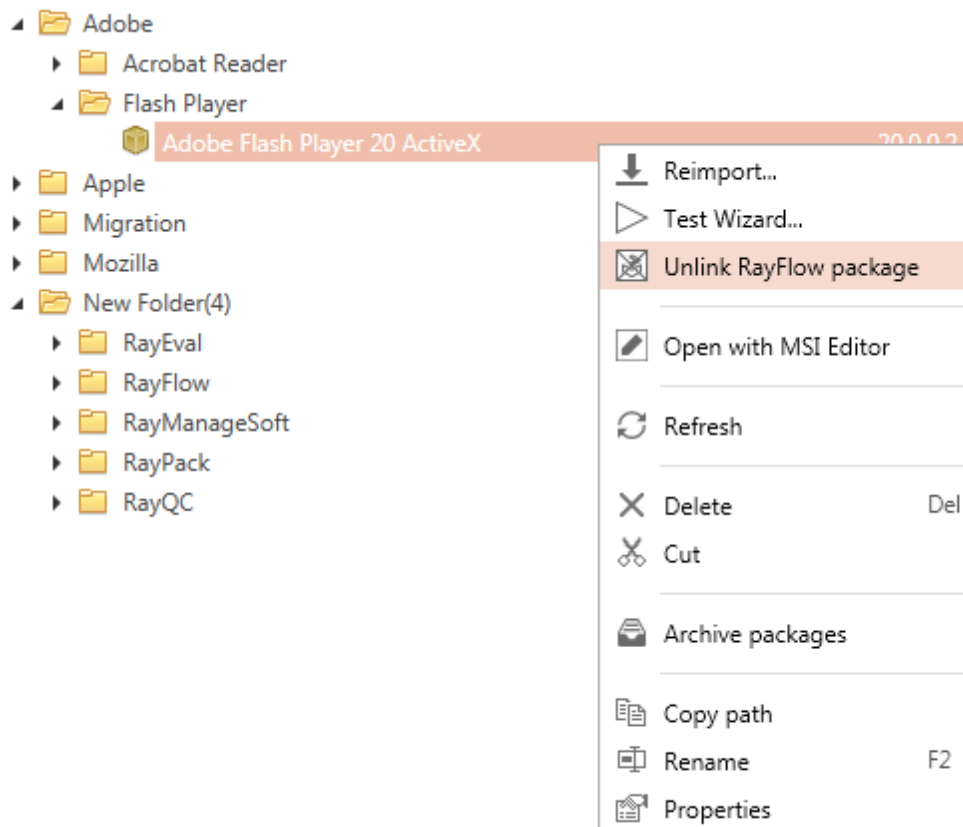
Sending a Report of a RayFlow Package Test Result to the RayFlow Server

After testing a RayFlow package, there is the possibility to automatically send the report to the RayFlow server. In order to do that, a user has to check the **After pressing FINISH save report in RayFlow server** option in the **Finish** screen of the **Test Wizard**. After that, the **Finish** button needs to be clicked.

Signing out from RayFlow

In order to sign-out from RayFlow, or sign-in as another user, press the **RayFlow** button in the right top corner:
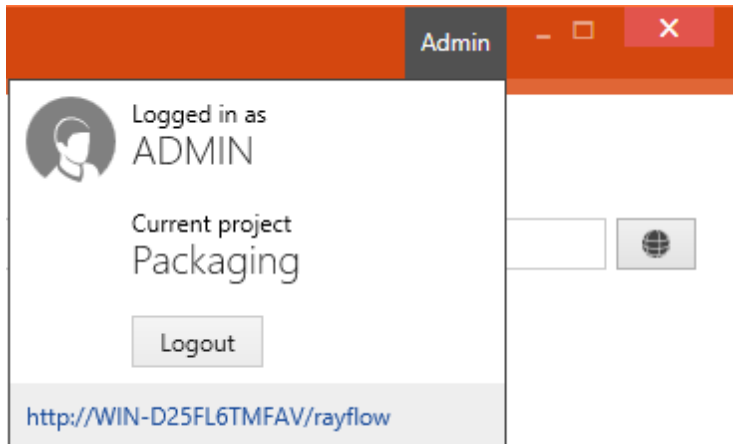
And then click the **Logout** button to sign-out from RayFlow.

Working Online or Offline

RayQC Advanced usually operates on the database that contains resources such as test results, software packages, merge modules, OS snapshots and web applications. This is called the Online mode. If the database is not available, e. g. due to connection issues, the mode automatically switches to Offline.

As long as RayQC Advanced operates in Offline mode, testing is only possible by using local software package and merge module resources. Resources that are strictly required to be obtained from the database, such as OS snapshots, are not available. Therefore, test types that depend on these resources are not available as long as the Offline mode is operational.

Since the Offline mode is an exceptional state that should be left as soon as possible, it is indicated by a message on the home screen of RayQC Advanced.

If there are issues with database availability, it is recommended to use the interface of the Settings view to check the current connection settings.

Automation

Enter topic text here.

Command-line interface

RayQC Advanced offers a standardized command line interface for automation and scripting requirements. To access the silent interface, users have to call the `RayQCAdCmd.exe`. This executable is available from the default product installation folder (e. g. `C:\Program Files (x86)\RayQCAdvanced\RayQCAdCmd.exe`).
The following actions may be performed via command line:

- Importing resources into the library
- Recaching the plug-in rule sets
- Testing package compatibility

> **Tip:**
> In order to review the available options directly from the executable interface, it is possible to simply call the help content via command prompt:
> `rqcadcmd.exe -help`

Importing Resources into the Library

Importing software packages into the library is triggered by the `-import` switch. This can also be used to import web applications into the library.

Sample command structure

```
RayQCAdCmd.exe
-import
-source = <sourceFile>
[-msiType = <v|s|w>]
[-folder = <folderPath>]
[-extract = <Yes|No>]
[-MaxCrawlcount = <number>]
[-MaxDepth = <number>]
```

Example for the import of a web application:

```
RayQCAdCmd.exe -import -source "http://www.raynet.de" -MaxCrawlCount 10 -
MaxDepth 3
```

Imports a webpage `raynet.de` using maximum depth of 3 and not more than 10 crawled files

Parameters

Parameter	Mandatory	Description
-source	Y	Specifies the path to the `.msi` file that has to be imported. Adding transforms may be performed by adding the path to one or more `.mst` files with separation by semicolon (;): `C:\file.msi;C:\transform1.mst;C:\transform2.mst`
-msiType	N	Specifies the MSI type according to the import wizard requirements. **Options:** `v` - Vendor `s` - Self-Made `w` - Wrapper
-folder	N	Specifies the folder path of the catalog in which the entry for the imported package will be created.
-extract	N	Controls whether or not the `.msi` will be extracted during import. **Options:** `Yes` `No` **Default:** `Yes`
-MaxCrawlCount	N	Specifies the maximum depth which a search engine indexes pages within a website. First level means the starting page. Next level is all pages linked from pages in previous level (0=not limited).
-MaxDepth	N	Specifies the maximum number of pages to crawl (0 = not limited).

Recaching the Plug-In Rule Sets

This option allows to recache the plug-ins from the `Libs` subdirectory of the product installation folder (e. g. `C:\Program Files (x86)\RayQCAdvanced\Libs\`) to make sure the database representation of the rules is up to date.

Sample command structure

```
RayQCAdCmd.exe
-recache
```

Parameters

None

Testing Package Compatibility

Importing software packages into the library is triggered by the `-import` switch. This can also be used to test web applications.

Sample command structure

```
RayQCAdCmd.exe
-test = <c|r|v|w|a|q>
-source = <sourceFile>
[-target = <targetFile>]
-report = <path_to_report>
[-reportFormat = <XML|PDF|DOCX|DOC|HTML|XPS>]
[-ruleSet = <ruleSet>]
[-rule = <rule>]
[-rayflow = <rayflow_configuration>]
[-saveindb = <Yes|No>]
[-reportname = <reportname>]
[-fix = <default|power|light>]
[-showMstDir = <Yes|No>]
[-overwrite = <Yes|No>]
[-MaxDepth = <number>]
[-MaxCrawlcount = <number>]
```

Example for the test of a web application:
```
RayQCAdCmd.exe -test w -source "http://www.raynet.de" -MaxCrawlCount 10 -MaxDepth 3
-report c:\Test\Test.pdf
```
This will test a web application `raynet.de` using the specified settings and will output a report as `.pdf` to `c:\Test\Test.pdf`

Parameters

Parameter	Mandatory	Description
`-test`	Y	Specifies the test areas which will be performed **Options:** `c` - Collision `r` - Readiness `v` - Virtualization `w` - Web Application `a` - App-V `q` - Checklist
`-source`	Y	Specifies the path to the `.msi` file that has to be tested. Testing more than one package may be performed by adding the path to `further` files with separation by semicolon (;): `C:\file1.msi;C:\file2.msi;C:\file3.msi`

Parameter	Mandatory	Description
-target	N (Y for test type `c`)	Specifies the path to the files that will be used to perform collision tests against. Testing against more than one package may be performed by adding the path to `further` files with separation by semicolon (;): `C:\file1.msi;C:\file2.msi;C:\file3.msi`
-report	Y	Specifies the path to the result report file or folder where reports will be generated.
-reportFormat	Y	Controls the format of the report output file. **Options:** • `XML` • `PDF` • `DOCX` • `DOC` • `HTML` • `XPS`
-ruleSet	Y/N (either `-ruleSet` or `-rule` has to be used)	The names of the rule sets that will be applied during testing. Applying more than one rule set is possible by separating rule set names by semicolon (;).
-rule	Y/N (either `-ruleSet` or `-rule` has to be used)	The names of the rules that will be applied during testing. Applying more than one rule is possible by separating rule names by semicolon (;).

-rayflow	N	Specifies required parameters to connect to a RayFlow server for test result uploading.
		The parameters have to be separated by semicolon (;) and specified in the following order:
		`<RayFlowServiceUrl>;`
		`<RayFlowServiceUser>;`
		`<RayFlowServicePassword>;`
		`<UserName>;`
		`<ProjectID>;`
		`<PackageID>`

-SaveinDb	N	Specifies whether the report will be saved in the database.
-reportname	N	Specifies the report name. If the value is omitted, the name of the report will be generated automatically.

Parameter	Mandatory	Description
`-fix`	N	Specifies fix type which will be performed.
`-showMstDir`	N	Specifies whether paths to folders with generated `.mst` files will be shown.
`-overwrite`	N	Allows overwrite if the file exists.
`-maxdepth`	N	Specifies the maximum depth which a search engine indexes pages within a website. First level means the starting page. Next level is all pages linked from pages in previous level (0=not limited).
`-maxcrawlcount`	N	Specifies the maximum number of pages to crawl (0 = not limited).

Command Line for UI Application

The command line ability for the user interface application can be used in the same way as the command line utility. If using the command line ability for the user interface the case arguments must be passed to the RayQC Advanced executable (`RayQCAd.exe`).

Sample Command Structure

```
<path>\RayQCAd.exe
-help
-open [-type = < import | test | package | report >] | [-id <value | path>]
```

-help

This command is used to open the command line help in a UI window.

Sample Command Structure

```
<Path>\RayQCAd.exe -help
Cc
```
The command line help will be opened using a window like shown in the image below.
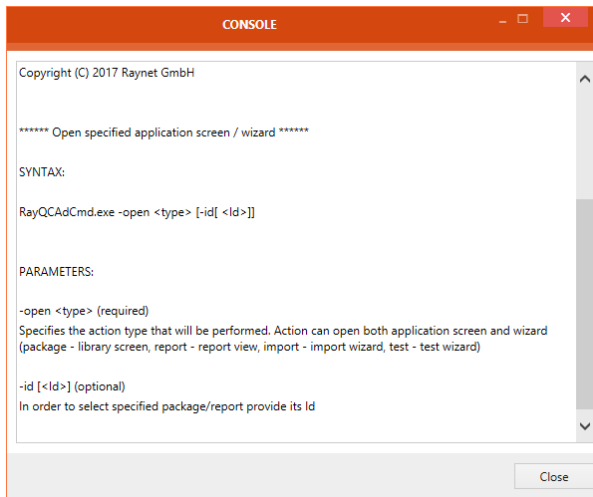
-open

The open switch can be used to open the import or test wizard and to open the **library** with or without a selected target package or the report screen with or without a report selected.

Sample Command Structure

```
<Path>\RayQCAd.exe
-open
-import
-test
-package [-id = <value|path>]
-report [-id = <value>]
```

Example for opening the **library** with a selected package:

```
C:\>C:\Program Files\RayQCAdvanced\RayQCAd.exe -open package "db:\\\MSI
Packages\pkg01\Xsd2Code"
```

This opens the **library** with the package called `Xsd2Code` selected.

Parameters

Parameter	Mandatory	Description
import	N	This command will start the import wizard.
test	N	This command will open the test wizard.
package <id>	N	This command will open the library. If the optional parameter `<id>` is not defined, the library screen will open without a selected package. If the optional parameter `<id>` is defined, the library screen will open with the specified package selected.

Parameter	Mandatory	Description
`report <id>`	N	This command will open the report screen or a specified report. If the optional parameter `<id>` is not defined, the report screen will open. If the optional parameter `<id>` is defined, the specified report will open.

`-id <value| path>`	N	If used with the `package` parameter `id` can have either the ID of a package or the path to the package can be used as value for the parameter. In combination with the `report` parameter, only the ID of the report can be used as value of `id`.
		
		Examples:
		
		`C:\>C:\Program Files\RayQCAdvanced\RayQCAd.exe -open package "db:\\\MSI Packages\pkg01\Xsd2Code"`
		`C:\>C:\Program Files\RayQCAdvanced\RayQCAd.exe -open package 12`
		`C:\>C:\Program Files\RayQCAdvanced\RayQCAd.exe -open report 12`

PowerShell Module

Certain actions on database and packages are exposed via the RayQC Advanced PowerShell module.

In order to get started, make sure that the module is imported. Invoke the following command in PowerShell terminal of your choice:

`Import-Module "<RayQCAdvancedInstallDir>\Libs\Raynet.RayQCAd.Common.Automation.dll"`

You can show the available commands by invoking the following PowerShell code:

`(Get-module  Raynet.RayQCAd.Common.Automation).ExportedCommands`

Import-Package

Imports the specified package into the Software library.

Name	Type	Mandatory	Description
`File`	`FileInfo`	Yes	The file to import (for example an MSI file)
`Transforms`	`FileInfo[]`	No	An optional list of transforms to apply upon import.

Folder	String	No	The Software Library path where the package is to be imported to
ExtractFiles	Boolean	No	A boolean value indicating whether the files should be extracted upon import (recommended).
Package	PSPackage	Yes	The instance of PSPackage object (for reimporting)

Returns `PSPackage` object with the newly imported package.

Get-Package

Gets a collection of `PSPackage` objects from a specified file path or from the library.

Name	Type	Mandatory	Description
Path	FileInfo	No	The path to a local file.
Transforms	FileInfo[]	No	An optional list of transforms (local files). This only applies to importing of MSI packages.
LibraryPath	String	No	The path in the Software library
Id	Integer	No	The internal package identifier.
All	Switch	No	If set, all packages from the library are returned.

Returns a collection of `PSPackage` objects.

Get-Rule

Gets a collection of `PSRule` rules from the database.

Name	Type	Mandatory	Description
RuleId	String	No	The name of the rule, using RayQC Advanced naming convention, for example `TG*` or `TA-`

Name	Type	Mandatory	Description
			`001-TA018`.
`RuleSetName`	`String`	No	The full name of the ruleset.
`All`	`Switch`	No	If set, all rules from the library are returned.

Returns a collection of `PSRule` objects.

Start-Test

Performs a series of tests given the specified set of packages and rules.

Name	Type	Mandatory	Description
`Rules`	`PsRule[]`	Yes	The rules to be executed. You can get them using the `Get-Rule` command.
`Source`	`PSPackage[]`	Yes	The collection of source packages to be tested.
`Target`	`PsPackage[]`	No	The collection of target packages. This applies only to conflict checks.
`Name`	`String`	No	The name of the report
`Comment`	`String`	No	The comment to be added to the report.
`DoNotAddToDatabase`	`Switch`	No	If set, the checks are executed in a passive mode, where the results are not saved in the database. You should persist the results on your own.

Returns the results of a specified test encapsulated in a `PSTestResult` object.

Execute-AutoRemediation

Performs auto-remediation (when applicable) on a given test results.

Name	Type	Mandatory	Description

TestResult	PSTestResult	Yes	The instance representing the test results. You can get them using the `Start-Test` command.
RulesToFix	PSRule[]	No	The collection of rules to be auto-remediated. You can get them using the `Get-Rule` command.
FixMode	Enum	No	When applicable, sets the preferred type of remediation. Choose between the following values: Light Power Ignore

Returns the results of a specified test encapsulated in a `PSTestResult` object.

Export-Report

Exports a report from the collection of results (contained in an object of type `PSTestResult`) and saves them

Name	Type	Mandatory	Description
TestResult	PSTestResult[]	Yes	The collection of test results. You can get them by invoking the `Start-Test` command.
Format	Enum	No	The report format.
Path	String	No	The path where the report is to be saved.
IncludeIssueDetails	Bool	No	A boolean value determining whether the issue details should be included in the output file.
IncludeRuleDetails	Bool	No	A boolean value

			determining whether the rule details should be included in the output file.
`IncludeCustomFields`	`Bool`	No	A boolean value determining whether the custom fields should be included in the output file.
`IncludePackageInformation`	`Bool`	No	A boolean value determining whether the package information should be included in the output file.

Returns an instance of `FileInfo` object representing the exported file.

Remove-Package

Removes a package from the library.

Name	Type	Mandatory	Description
`Package`	`PSPackage`	Yes	The package to be removed.

Remove-Report

Removes a report from the library.

Name	Type	Mandatory	Description
`TestResult`	`PSTestResult`	False	The instance of the `PSTestResult` object.
`ReportId`	`Integer`	False	The internal identifier of a report.

Appendix A: Toubleshooting Problems with Virtual Machines

Troubleshooting Problems with Hyper-V Connectivity

The following checklist helps to find and fix any possible issues when working with Hyper-V machines:

1. Is PowerShell 3.0 installed (both on Guest and Host Machine)?
   a. Check `$PSVersionTable.PSVersion` in PowerShell
2. Is the machine properly configured in the **Settings** > **Virtual Machines** screen (pay attention to hardcoded IP addresses which may be dynamically assigned by DHCP)
3. Is RayPack Studio Tools for Hyper-V installed on the Guest machine? Is the process `vm-proxy.exe` from RayPack Studio Tools for Hyper-V running?
4. Is WINRM configured?
   a. Check `winrm qc`
5. Does WINRM have proper `TrustedHosts` entries on both VM and server?
   a. `winrm s winrm/config/client '@{TrustedHosts="RemoteComputer"}'`
   b. `winrm g winrm/config/client` - shows the current `TrustedHosts` lists
   c. More information: https://technet.microsoft.com/en-us/library/ff700227.aspx
6. Does WINRM have a connection to the VM and vice-versa?
   `a.- Test-WSMan -ComputerName IP`
7. Are all necessary ports unblocked on the physical machine?
   a. The default port range is `48654-48999`.

Changing TCP / IP Configuration

In some cases it may be required to use custom port ranges, timeouts, etc. for PackBot related functionality. The following table summarizes the available options:

Setting name	Default value	Description
`TcpIpDefaultPort`	48654-48999	Port range used for TCP/IP communication. Use minus (-) and comma (,) to indicate which ports are valid for incoming communication. Make sure that these ports are not blocked by your firewall. PackBot tries to find first valid free port and listen on it from lower to higher numbers.
`TcpIpMaxRetry`	3	Maximum number of retries before asserting the

Setting name	Default value	Description
		machine is not available..
`TcpIpDefaultReceiveTi`	240000	Reverts to default value if Windows does not define its own timeouts.
`TcpIpDefaultSendTime out`	240000	Reverts to default value if Windows does not define its own timeouts.

Additional Information

Visit www.RayQC.de for further information regarding the product and current community incentives. It's also recommended taking a look at additional resources available at the Knowledge Base for Raynet products: https://Raynet.de/Support/.

Raynet is looking forward to receiving your feedback from your RayQC Advanced experience. Please contact your Raynet service partner or use our Support Panel to add your ideas or requirements to the RayQC Advanced development roadmap!

Help & Support

Request RayQC Advanced support

Our Raynet support team gladly assists you on any questions or issues you encounter regarding RayQC Advanced. Feel free to sign in and open incidents via our Support Panel.

Join the RaySuite community

The RaySuite community resides within our Knowledge Base: https://raynet.de/Support/. Once you have signed up for access to the Raynet support panel, you automatically have access to the Knowledge Base, too.

You will surely come to a point where you would love to suggest a new feature for the future development of RayQC Advanced. Maybe you need to find some tips & tricks to hit your target right. The RaySuite community is your place for discussing such topics, for sharing and expanding your own experience.

Step in contact with Raynet's testers, evaluators, and consultants in order to learn how to polish your quality assurance activities to a level of highest quality standards. Since Raynet has years and years of experience, we know what to do, and how to do it. Don't row your boat alone when you have the chance to join our RaySuite community for free.

Contact your Raynet sales representative

Our sales team is the right contact for any license or edition question you might encounter. You would like to benefit from a professional RayQC Advanced training? Ask for dates and locations to find the fitting training occasion. You are highly welcome to step in contact via sales@raynet.de.