

RES ONE®

Workspace

Release Notes

Version 10.1.0.0

Copyright © RES Software Development B.V. All rights reserved. Commercial Computer Software documentation/data - Restricted Rights. RES ® and RES ONE ® are registered trademarks and service marks of RES Software B.V. internationally. The software licensed by RES Software B.V. or RES Software, Inc. is covered by patents, any patents pending, granted to and/or owned by RES Software Development B.V. and as identified on www.res.com/legal-statements.

Disclaimer

While care has been taken by RES to ensure that the information contained in this document is correct and complete, it is possible that this is not the case. RES provides the information "as is", without any warranty of any kind. To the maximum extent permitted by applicable law, RES is not liable for any damage which has occurred or may occur as a result of or in any respect related to the use of this information. RES may change or remove this document at any time without notice and shall not be responsible for any consequence(s) arising therefrom. RES is not responsible for any contributions by third parties to this information.

Contents

1.	What's new in RES ONE Workspace version 10.1	1
1.1	About this Release	1
1.2	Highlighted Features	2
	Management Portal: Preview of upcoming and new feature "File Certificates security"	2
	Enhanced Application Security based on file hashes	2
	User Registry: HKEY_LOCAL_MACHINE (HKLM) support for registry settings and policies	3
	Locations and Devices: Support for Linux and Mac OS X zone rules	3
	Linux/Apple Mac OS X Agents: Support for Managed Applications security "Learning mode"	3
	Advanced Settings: Bypass Composer option now available for non-administrator accounts	4
	Licensing: Enhancements Named Users tab	4
	Licensing: License fallback options now also available for evaluation licenses	4
1.3	Important Changes	5
	Installation: RES ONE Workspace Version 10.1 requires .NET 4.5.2	5
	RES ONE Workspace Core: Relay Servers no longer available in this module	5
1.4	Enhancements and Improvements	6
	Console: Stored passwords for integrations now displayed as 14 asterisks (*)	6
	Drivers: New drivers implemented for RES ONE Workspace v10.1	6
	Enhanced Add/Remove Citrix XenApp Server Wizard	6
	Enhanced Process Interception	6
	Enhanced reliability of Usage Tracking when using Process Interception	7
	Licensing: Enhanced claiming of reserved licenses after logging on in offline state	7
	Licensing: RES ONE Workspace Core wizard enhanced	7
	Managed Application Security: Enhanced security	7
	Management Portal: Authentication type "Windows" now supported for Microsoft SQL Servers	8
	Management Portal: Security section including preview of new feature available	9
	Microsoft App-V 5.x: New parameter to use '/appvve' only if package is deployed	9
	Reporting Services: Enhanced performance	10
	Unattended Installation: New parameters to pre-load cache during offline installations	10
	Website Security: Enhanced stability	10
	Workspace Analysis: Enhanced display of Access Control for Applications	10
	Workspace Composer: Enhanced robustness of Managed Application Security based on file hashes.	11
1.5	Resolved Issues	12
	Applications: Editing applications could give error 'Invalid Key'	12
	Applications: Importing shortcut on 64-bit Windows might result in incorrect command line	12
	Building Blocks: Creating or importing Building Block for an application could give error 'Out of stack space'	13
	Building Blocks: Importing Building Block for a Workspace Container failed if Building Block was created using command-line option	13
	Citrix XenApp Publishing: ICA file might not be created when published from a Citrix Delivery Controller	14
	Console: Security log of application with no command line displayed incorrect data	14

Datastore: Database Integrity error after migrating Datastore without transferring licenses	14
File Hash Monitor: No new file hashes calculated for files changed by Windows Update.....	14
Managed Application Security: 'Authorize file hashes' generated new authorized file erroneously	15
Managed Application Security: File hash data might not be logged for hash-related security event	15
Managed Application Security: 'sidekick32.exe' blocked when using 64-bit RES ONE Automation Agent	15
Management Portal: Error message "Request too long" if multiple RES ONE Portals were installed on same machine using RES Identity Broker authentication	15
Management Portal: Gray area above the Reporting dashboard	15
Microsoft App-V 5.x: Application actions not executed after changing %TEMP% variable.....	16
Microsoft App-V 5.x: 'Application can't be started...' error when Package root folder contained a variable	16
Microsoft App-V 5.x: Logon, refresh or starting application could give error 'Subscript out of range'	17
RES ONE Automation Integration: Testing connection to RES ONE Automation environment could give error 'Subscript out of range'	17
Usage Tracking: End date/time of applications might display incorrect data	17
User Registry: Unable to import or edit registry value that contained €, ¥, ™, © etc.....	18
User Settings: Capture Wizard not working correctly if Working directory was other than default.....	18
Workspace Composer: Autodiscover not working correctly for Microsoft Outlook 2016.....	18
Workspace Composer: Desktop icons might disappear after a non-graceful logoff .	19
Workspace Composer: 'Disable file system redirector on 64-bit systems' applied incorrectly	19
Workspace Composer: Display of mini splash screen incorrect at logoff	20
Workspace Composer: 'Do not ping print server before connecting printers' not working correctly	20
Workspace Composer: Execute Command at application end could lead to endless interception loop	20
Workspace Composer: 'File not found: crc.dll' error could occur during logoff	20
Workspace Composer: Homedrives contained multiple pwruser_<MACHINENAME>.his files.....	21
Workspace Composer: Multiple shortcuts with identical command line not displayed in Start Menu	21
Workspace Composer: New ... document option missing from context menu on Windows 8.1 and higher	21
Workspace Composer: No desktop background might be displayed if limited to pre-configured pictures	22
Workspace Composer: Not all RES ONE Automation tasks executed if user clicked 'Dismiss and notify me when done'	22
Workspace Composer: Process interception might not work for executables located on a network drive	22
Workspace Composer: Process priority not applied on intercepted processes	23
Workspace Composer: Screensaver not working on Microsoft Windows Server 2016 after installing RES ONE Workspace v10	23
Workspace Composer: Shortcuts might be generated with an incorrect 'Working directory' when using registry value 'InterceptManagedApps'	23
Workspace Composer: Special user folders displayed with generic folder icons	23
Workspace Composer: Startup folder created in Start Menu at every Workspace refresh.....	23
Workspace Composer: User Settings with Zero Profile mode 'Capture, then Track' not restoring registry settings with Unicode characters.....	24

Workspace Composer: Users might be prompted to select default program for configured File Types when using User Settings on Windows 10.....	24
Workspace Composer: White icons on taskbar when using Folder Redirection for roaming profiles	24
Workspace Composer: Zone based on Computer OU membership not applied when logged on with local account	25
Workspace Start Menu: \$recycle.bin shortcut displayed when Start Menu was redirected	25
Workspace Start Menu: Folder structure might be incorrect when using identical folder names in separate branches.....	26
Workspace Start Menu: Windows 8.1 Start Menu might not appear	26

1. What's new in RES ONE Workspace version 10.1

1.1 About this Release

New installation

Before performing a new installation of RES ONE Workspace 10.1.0.0, please read the following release note carefully:

Installation: Updated ActiveReports components

As of RES ONE Workspace version 10, the third-party components for ActiveReports have been updated to address a security vulnerability (CVSS v2 Base Score: 8.8).

The ActiveReports components (libraries and object code) included in this release, is proprietary to Data Dynamics, Ltd. (acquired by: GrapeCity, Inc.). End-User by downloading and installing this release assumes and accepts sole responsibility of the use of the ActiveReports component and will not act contrary to license terms applicable and available via http://arhelp.grapecity.com/webhelp/Legacy/AR2std/HX_License_Agreement_and_Limited_Warranty_M.html.

Datastore

This table shows which Datastore revision level applies to RES ONE Workspace 10.1.0.0 and in which version it was introduced:

Datastore revision level:	Introduced in:
13	RES Workspace Manager 2014 SR3

When installing this revision, if the Datastore is of a lower revision level, it will automatically be updated.

Drivers

This table shows what drivers will be updated by installing this release.

Driver	Driver update
FileGuard	New
ImgGuard	Yes
NetGuard	Yes
RegGuard	Yes
RESNFLT	Yes
AppGuard	Obsolete

1.2 Highlighted Features

Management Portal: Preview of upcoming and new feature "File Certificates security"

With the RES ONE Workspace Management Portal Version 10.1, the preview of the upcoming new feature **File Certificates** security is introduced. This feature is subject to change, and will be updated and extended over time.

File Certificates security allows you to whitelist applications from a specific vendor or product, as identified in the (valid) file certificates of digitally signed executables. For example, you can whitelist executables that are identified in their certificate as the product Microsoft Word, or Adobe Acrobat Reader.

File Certificates security offers a level of security that is comparable to **File Hashes** security, but with more flexibility and ease of maintenance. For example, if you use **File Hashes** security to whitelist an executable for Adobe Acrobat Reader, then an upgrade of Adobe Acrobat Reader will result in an executable with a different file hash - and thus require an additional rule. On the other hand, the certificate of the new executable will still identify the product as Adobe Acrobat Reader, so no new rule will be needed.

You can find **File Certificates** security in the Management Portal at **Security > Applications > File Certificates**. This upcoming new feature can, for now, only be enabled for **Exceptions** that are based on specific workspace containers.

Please note that all RES ONE Workspace components must be running on v10.1 for File Certificates security to work. The Portable Relay Server and Agents for Linux and Mac OS X do not support File Certificates security.

You are invited to share your feedback with RES Support.

Enhanced Application Security based on file hashes

Application Security based on file hashes has been enhanced with the following changes:

File hashes now checked for all executable files

Application Security based on file hashes has been enhanced to include all executable files.

Now, when (for example) an SCR, COM or DLL file is started, its file hash can be checked against the list of allowed and blocked hashes.

File hashes now taken into account when determining if running application is still authorized

The option **Default behavior if running application is no longer authorized** (at **Security > Applications > Managed Applications**, on the **Settings** tab) now also evaluates the application's file hash.

Depending on configuration, if the file hash for a running application is no longer authorized after a Workspace refresh, the application will now be terminated.

Enhanced logging of file hash data

All Application Security log entries (at **Security > Applications > Managed Applications**, on the **Log** tab) now contain the **File hash**, **Algorithm** and **File version** data for the file in question.

User Registry: HKEY_LOCAL_MACHINE (HKLM) support for registry settings and policies

RES ONE Workspace now supports HKEY_LOCAL_MACHINE (HKLM) for registry settings and policies. With HKLM support, it is possible to control computer configuration in your RES ONE Workspace environment from one central point.

Previously it was only possible to configure registry settings and policies for HKEY_CURRENT_USER (HKCU). Registry settings and policies can be configured on global level at **Composition > Actions By Type > User Registry** or on application level at **Composition > Applications**, on the **Configuration > Actions** tab of an application.

Locations and Devices: Support for Linux and Mac OS X zone rules

Access Control based on **Locations and Devices** can now be set for the Agents for Linux and Apple Mac OS X. The following zone rules are supported:

- **Computer > Hardware > Processor architecture**
- **Computer > Operating system > Version:**
 - **Linux Operating Systems > CentOS**, for the versions:
 - 7.2.1511, 7.1.1503, 7.0.1406, 5.11
 - **Linux Operating Systems > RHEL**, for the versions:
 - 7.2-7.0, 6.8-6.6, 5.11
 - **Apple Mac OS X Operating Systems**, for the versions:
 - 10.12-10.8
- **Computer > Operating system > Bit version > 64-bit Version**
- **Computer > Hardware > Number of processors >**
 - Only 1 CPU
 - 2 CPU's (and up)
 - 4 CPU's (and up)
 - 8 CPU's (and up)
- **Configuration > Operating system > Version:**
 - **Linux Operating Systems > CentOS**, for the versions:
 - 7.2.1511, 7.1.1503, 7.0.1406, 5.11
 - **Linux Operating Systems > RHEL**, for the versions:
 - 7.2-7.0, 6.8-6.6, 5.11
 - **Apple Mac OS X Operating Systems**, for the versions:
 - 10.12-10.8
- **Configuration > Operating system > Bit version > 64-bit Version**
- **Network > Computer name > Computer (FQDN)**
- **Network > IP address > IP address**
- **Network > IP address > IP address range**

Linux/Apple Mac OS X Agents: Support for Managed Applications security "Learning mode"


The Agents for Linux and Apple Mac OS X can now be configured to run in the security mode **Learning** from the RES ONE Workspace Console at **Security > Applications > Managed Applications**. In **Learning** mode attempts to start unauthorized executables are not blocked, but can be logged. This helps you identify any executables that are started by authorized applications.

Advanced Settings: Bypass Composer option now available for non-administrator accounts

At **Setup > Advanced Settings** the option **Bypass composer for accounts and groups** can now be configured for domain users and domain user security groups. Previously, the option was only supported for local administrators and domain administrators.

With this option you can specify mask(s) of (local) administrator, user, and group accounts that should bypass the Workspace Composer on Agents that start RES ONE Workspace sessions automatically.

Licensing: Enhancements Named Users tab

The **Named Users** tab at **Setup > Licensing** has been enhanced. You can now use Ctrl+A to select all displayed users and release their licenses at once. Also, to reserve licenses for named users, you can now click  to directly go to the **Search Directory Services** window and select users/groups from Active Directory. If you select an Active Directory group, the group is expanded to display all users that belong to that group, as license reservations can only be applied to individual users.

Licensing: License fallback options now also available for evaluation licenses

In environments that use evaluation licenses, the following fallback options if no licenses are available at logon, can now be configured:

- Continue with limited functionality
- Do not continue, log off

Fallback options (If no license available at logon) can be configured at **Setup > Licensing**, on the **Licenses** tab.

1.3 Important Changes

Installation: RES ONE Workspace Version 10.1 requires .NET 4.5.2

Installing RES ONE Workspace Version 10.1 requires .NET Framework 4.5.2 or higher to be installed on your machine.

This prerequisite changed because Microsoft ended the support for .NET Framework 4, 4.5, and 4.5.1, which means that security updates, technical support and hotfixes are not available for these versions.

RES ONE Workspace Core: Relay Servers no longer available in this module

The Relay Server is no longer available in **RES ONE Workspace Core** and has been moved to the RES ONE Workspace modules **Composition**, **Governance**, and **Security**.

RES ONE Workspace Core is the free starter package offering basic RES ONE Workspace functionality.

1.4 Enhancements and Improvements

Console: Stored passwords for integrations now displayed as 14 asterisks (*)

At **Setup > Integration**, if an integration is configured for **LANDesk**, **Microsoft System Center**, **RES ONE Automation** or **RES ONE Identity Director**, the stored password is now displayed as 14 asterisks (*).

Drivers: New drivers implemented for RES ONE Workspace v10.1

For RES ONE Workspace 10.1, all existing drivers were optimized. Also, a new driver was introduced. With a new driver architecture, the v10.1 drivers offer a higher security and optimized performance. For communication with the RES ONE Workspace components, new DLLs were introduced as well.

After you upgraded to RES ONE Workspace v10.1, a system reboot is required. Without a system reboot, it is not possible to run RES ONE Workspace sessions in your environment.

The new FileGuard driver and renewed ImgGuard driver replace the AppGuard driver. Also, the NetGuard driver was upgraded to the Windows Filtering Platform.

The AppGuard driver is no longer needed in RES ONE Workspace v10.1 environments.

RES ONE Workspace v10.1 is shipped with the following drivers:

- FileGuard (new)
- ImgGuard (optimized)
- NetGuard (optimized)
- RegGuard (optimized)
- RESNFLT (updated)

Enhanced Add/Remove Citrix XenApp Server Wizard

The **Add/Remove Citrix XenApp Server Wizard** has been enhanced to better support migrating applications to a Citrix XenApp 7.x environment.

The wizard can be found at **Setup > Integration > Application Virtualization > Citrix XenApp Publishing**, on the **Settings** tab.

Enhanced Process Interception

Matching intercepted processes to managed applications has been enhanced to better handle command-line parameters that are wrapped in quotes, for example "`http://res.com`".

For more information about **Process Interception**, please refer to the RES ONE Workspace Help.

Enhanced reliability of Usage Tracking when using Process Interception

Usage Tracking has been enhanced to more reliably track usage of applications that use **Process Interception**.

For more information about **Usage Tracking** and **Process Interception**, please refer to the RES ONE Workspace Help.

Licensing: Enhanced claiming of reserved licenses after logging on in offline state

The process of claiming a reserved license on laptops, that logged on while the Datastore could not be reached, has been enhanced. When the Datastore becomes available, the session will now correctly claim the license that was reserved for the user.

Previously, when the Datastore became available, the **Named Users** tab (at **Setup > Licensing**) temporarily contained a **Denied** and a **Reserved** license.

Licensing: RES ONE Workspace Core wizard enhanced

The wizard to request a RES ONE Workspace Core License has been enhanced to match the RES ONE Workspace Core request via the RES website (<http://res.com>).


Managed Application Security: Enhanced security

Managed Application Security has been enhanced to better prevent starting of unauthorized applications.

Management Portal: Authentication type "Windows" now supported for Microsoft SQL Servers

The **Authentication type "Windows"** is now supported for the Management Portal's Datastore connections to Microsoft SQL Servers.

To enable Windows Authentication for Microsoft SQL Servers and their databases, please follow these steps:

- The Internet Information Services (IIS) Application Pool in which the RES ONE Workspace Management Portal runs needs to use an Identity (user account) that is a valid Windows authentication login to the Microsoft SQL Server.
 - To change the Identity property of the IIS application pool in which the Management Portal runs:
 - Open IIS Manager
 - In the **Connections** pane, expand the server node and click **Application Pools**.
 - On the **Application Pools** page, select the application pool in which the RES ONE Workspace Management Portal runs.
 - Open the **Advanced Settings** of the selected application pool (choose it from the application pool's context menu or click **Advanced Settings** in the **Actions** pane (under **Edit Application Pool**)).
 - In the **Advanced Settings** window, under the **Process Model** section, locate **Identity** and click .
 - In the **Application Pool Identity** window, choose **Custom account** and click **Set....**
 - In the **Set Credentials** window, provide the credentials of the account under which the application pool should run and click **OK**.
- Once the Identity of the application pool has been reconfigured, the Security Permissions for the RES ONE Workspace Management Portal's installation folder need to be adjusted as well (via the **Windows File Explorer**, on the **Security** tab).
 - The new account that was configured in IIS Manager for the application pool in which the RES ONE Workspace Management Portal runs, needs to have the following permissions on the installation folder (by default, this is `C:\Program Files (x86)\RES\Workspace\Management Portal`), its subfolders and files:
 - **Read & execute**
 - **List folder contents**
 - **Read**
 - It also needs to have **Full control** permissions on the installation folder's subfolders **Config** and **App_Data** (and their subfolders and files) (`...\Management Portal\Config` and `...\Management Portal\App_Data`).

Management Portal: Security section including preview of new feature available

The RES ONE Workspace Management Portal has been enhanced with access to the Security section and the addition of File Certificates security.

In the Management Portal, the feature **Managed Applications** security has been renamed to **Executables** security and the Executables rules list includes the **Authorized Files** rules as well. **File Hash** rules are displayed separately, but are still linked to an **Executable**. For new file hash rules, the file path is always "*" unless you specify a different file (path). **File Hashes** security follows the feature settings from **Executables** security.

File Certificates security allows you to whitelist applications from a specific vendor or product, as identified in the (valid) file certificates of digitally signed executables. For example, you can whitelist executables that are identified in their certificate as the product Microsoft Word, or Adobe Acrobat Reader.

At this moment not all Security features are fully available and configurable from the Management Portal. This is planned for a next release. Below the overview of the Security features that are available in the Management Portal and at which level:

- **Applications**
 - Executables (Rules, Log, Settings, Exceptions)
 - File Hashes (Rules, Log, Settings)
 - File Certificates (preview of the upcoming new feature)
 - User Installed Applications (Log)
- **File System**
 - Files & Folders (Log)
 - Read-Only Blanketing (Log)
- Removable Disks (Log)
- Websites (Rules, Log)
- Network Connections (Log)
- User Sessions (Log)

Microsoft App-V 5.x: New parameter to use '/appvve' only if package is deployed

RES ONE Workspace now offers the possibility to configure an application that will run inside a Microsoft App-V 5.x virtual application bubble only if the virtual application package is deployed. To enable this new feature, the parameter `/ROW:NoPkgDelivery` was introduced.

When configuring the application, add this parameter to the **Parameters** field that also contains `/appvve:<PACKAGEID>_<VERSIONID>` (on the **Properties > General** tab of the application).

Example:

```
/ROW:NoPkgDelivery /appvve:668b7873-3ecd-4a81-aa74-0136bad81e7e_31912d51-2d3c-4622-baed-b7ad136fb032
```

With this parameter, if the configured application is started in a session where:

- the App-V application package *is not* deployed, then the application will start but the `/appvve` parameter will be ignored.
- the App-V application package *is* deployed, then the configured application will run inside the bubble of the App-V application.

This is an improved version of an enhancement that was released in RES ONE Workspace 9.12.0.5.

Reporting Services: Enhanced performance

Performance of RES ONE Workspace Reporting Services has been enhanced.



Note

For this enhancement to work correctly, RES ONE Workspace Reporting Services version 10.0.200.0 or higher must be installed.

Unattended Installation: New parameters to pre-load cache during offline installations

The unattended installation has been enhanced with the possibility to pre-load a ZIP file that contains the cache. With the pre-loaded cache it is possible to install Agents in your RES ONE Workspace environment and start them in an offline state. This means that the Agents do not (yet) have a connection to a Relay Server or directly to the Datastore. The ZIP file is extracted to the Agents cache folder and is updated once the Agent connects to a Relay Server or directly to the Datastore.

Use `pwr-cache.exe /CREATEFILEFROMCACHE=<filepath>` to create the ZIP file from the cache (.zip) and in the command line for the unattended installation, use the parameter `LOADCACHEFROMFILE=<filepath>` to load the cache to the Agent. Make sure the ZIP file is stored in a secure location and can only be accessed by authorized RES ONE Workspace administrators.

Example

```
<ROW Installation folder>\pwr-cache.exe  
/CREATEFILEFROMCACHE=C:\temp\cache.zip
```

```
Msiexec /i "C:\RES ONE Workspace 10.1.0.0.msi"  
LOADCACHEFROMFILE=C:\temp\cache.zip /qn
```

Note: Elevated privileges are necessary to run this command line.

Website Security: Enhanced stability

The ResNflt driver, used for Website Security, has been enhanced to improve stability.

Workspace Analysis: Enhanced display of Access Control for Applications

In **Workspace Analysis**, display of Access Control for applications that is defined as **NOT User/Group**, has been enhanced.

These values are now marked as `NOT <UserName>` or `NOT\<GroupName>`. Previously, these values were marked `[<UserName>]` or `[<GroupName>]`.

In the **Workspace Analysis** for a user, Access Control for applications can be found at **Composition > Applications**, in the **Access granted by** column.

Workspace Composer: Enhanced robustness of Managed Application Security based on file hashes.

Managed Application Security based on file hashes has been enhanced to increase robustness.

1.5 Resolved Issues

Applications: Editing applications could give error 'Invalid Key'

If **Citrix XenApp Publishing** was configured with a **Server farm** name or **Citrix Site** name that contained only numbers, opening an application (at **Composition > Applications**) could give the following error:

Process	pwrtech.exe
Procedure	usrSelectLvw.FillXenAppFarms
Error #	35603
Error description	Invalid Key

This has been resolved.

Citrix XenApp Publishing can be configured at **Setup > Integration > Application Virtualization > Citrix XenApp Publishing**.

Applications: Importing shortcut on 64-bit Windows might result in incorrect command line

Consider the following scenario:

- A user opened the RES ONE Workspace Console on a machine that was running a 64-bit version of Microsoft Windows.
 - At **Composition > Applications**, the user imported a shortcut file (.lnk) for a 32-bit application that was not installed on the current machine.
 - In the **Import Wizard**, the user selected the option **Automatically replace folder names with their associated environment string**.

In this scenario, the **Command line** of the resulting application contained the variable `%ProgramW6432%`. This has been resolved.

Now, in this scenario, the **Command line** contains the variable `%ProgramFiles(x86)%`.

Building Blocks: Creating or importing Building Block for an application could give error 'Out of stack space'

Consider the following scenario:

- At **Composition > Applications**, two applications were configured: Application A and Application B.
 - Application A had, for example, the following configuration:
 - On the **Configuration > Actions** tab of the application, an action was configured
 - On the **User Settings > Properties** tab of the application, for **Use the User Settings from the following application**, Application B was selected.
 - Application B had, for example, the following configuration:
 - On the **Configuration > Actions** tab of the application, a **Linked Action** was configured to **Perform Actions from application A**.
 - On the **User Settings > Properties** tab of the application, User Settings were configured.
- With this configuration, both applications reference (part of) the configuration of the other application.

In this scenario, if a Building Block was created for either of the applications, the following error occurred:

```
Run-time error (28): Out of stack space
```

As a result, no Building Block was generated, or the resulting Building Block file could not be opened.

The error also occurred, when a Building Block was imported that contained a configuration as described above.

This has been resolved. Now, in this scenario, a Building Block is created or imported correctly, without displaying the error.

Building Blocks: Importing Building Block for a Workspace Container failed if Building Block was created using command-line option

If a Building Block for a Workspace Container was created using the command-line option `pwrtech.exe /export`, importing the Building Block failed. This has been resolved.

Please note, that installing RES ONE Workspace version 10.0.300.0 or higher does not resolve the failing import of existing Building Blocks for Workspace Containers, that were created using the command-line option.

These Building Blocks must be exported again from a machine with RES ONE Workspace version 10.0.300.0 or higher installed.

For more information about command-line options, please refer to the RES ONE Workspace Administration Guide.

Citrix XenApp Publishing: ICA file might not be created when published from a Citrix Delivery Controller

When **Citrix XenApp Application Publishing** was enabled for an application, with the option **Enable Instant Passthrough for computers not publishing this application** selected, no ICA file might be created if the application was published from a RES ONE Workspace Console running on a Citrix Delivery Controller without Citrix Studio installed. This has been resolved.

Citrix XenApp Application Publishing can be configured at **Composition > Applications**, on the **Properties > Publishing > Citrix XenApp Published Application** tab of an application.

Console: Security log of application with no command line displayed incorrect data

Consider the following scenario:

- At **Composition > Applications**, an application was configured with no **Command line** and no **Working directory**.
- At **Security > Applications > Managed Applications**, on the **Settings** tab, **Managed Application Security** was set to **Learning** or **Enabled**.

In this scenario, on the **Security > Log** tab of the application, all security log entries that were not related to a managed application were displayed. This has been resolved.

Datastore: Database Integrity error after migrating Datastore without transferring licenses

At **Setup > Datastore**, if a Datastore was migrated and the option **Transfer license(s) to the new Datastore** was not selected (in the **Finalize Datastore Migration** step of the **Datastore Migration Wizard**), a database integrity error occurred:

```
Licensing (Found: 0, Expected: <NUMBER > 0>)
```

The **Maintenance** action **Verify database integrity** was needed to correct the error.

This has been resolved.

Now, in this scenario, the error no longer occurs.

File Hash Monitor: No new file hashes calculated for files changed by Windows Update

When the RES ONE Workspace File Hash monitor was active and Microsoft Windows Update applied changes, the changed files were not picked up by the File Hash Monitor to calculate a new file hash. This has been resolved.



Note

For this issue to be resolved, RES ONE Workspace File Hash Monitor 10.0.300.0 must be installed.

Managed Application Security: 'Authorize file hashes' generated new authorized file erroneously

Consider the following scenario:

- At **Security > Authorized Files**, an authorized file was configured with a wildcard in the path.
Example `*\notepad.exe`.
- At **Security > Applications > Managed Applications**, on the **Log** tab, a log entry was available for the same file, containing the full path.
Example: `C:\Windows\System32\notepad.exe`
 - A Console user authorized the hash for the file, using **Authorize file hashes** from the context menu.

In this scenario, instead of adding the hash to the existing authorized file (`*.\notepad.exe`), a new authorized file was created using the file's full path. This has been resolved.

Managed Application Security: File hash data might not be logged for hash-related security event

At **Security > Applications > Managed Applications**, on the **Log** tab, if a hash-related event (for example `HASH DENIED`) was logged, the event did not contain **File hash**, **Algorithm** and **File version** data if the user did not have NTFS Read permissions for the file. This has been resolved.

Managed Application Security: 'sidekick32.exe' blocked when using 64-bit RES ONE Automation Agent

Consider the following scenario:

- At **Composition > Actions By Type > Automation Tasks**, an Automation task was configured.
- A user logged on to a RES ONE Workspace session on a machine with the 64-bit RES ONE Automation Agent installed.
 - The Automation task was started

In this scenario, in the user session, the `sidekick32.exe` process was blocked, and a **BLOCK** entry was logged in the **Managed Application Security** log (at **Security > Applications > Managed Applications**). This has been resolved.

Management Portal: Error message "Request too long" if multiple RES ONE Portals were installed on same machine using RES Identity Broker authentication

If two or more RES ONE Management Portals and/or the RES ONE Identity Director Web Portal were installed on the same machine, all using RES Identity Broker for authentication, users who signed in to a Management Portal or the RES ONE Identity Director Web Portal, could receive a browser error "Request too long". This error occurred because the cookies for the Management Portals were set on the website's root path (<https://host.domain.com/>) instead of on the application's root path (for example: <https://host.domain.com/Workspace/>). This has been resolved.

Management Portal: Gray area above the Reporting dashboard

At **Reporting**, a gray area was displayed above the Reporting dashboard. The gray area was visible because the header section was positioned too low on the page. This has been resolved.

Microsoft App-V 5.x: Application actions not executed after changing %TEMP% variable

Consider the following scenario:

- At **Composition > Applications**, a Microsoft App-V 5.x application (application 'A') was configured with the following settings:
 - On the **Configuration > Actions > At application start** tab of the application, **Environment Variables** were configured for %TEMP% and %TMP%, that did not resolve to %LOCALAPPDATA%\Temp.
- At **Composition > Applications**, another Microsoft App-V 5.x application (application 'B') was configured with one or more actions (on the **Configuration > Actions** tab of the application).
- A user logged on to a RES ONE Workspace session and first started application 'A', and then application 'B'.

In this scenario, in the user session, the actions for application 'B' were not executed. This has been resolved.

Microsoft App-V 5.x: 'Application can't be started...' error when Package root folder contained a variable

Consider the following scenario:

- At **Composition > Applications**, a Microsoft App-v 5.x application was configured with the following settings:
 - On the **Properties > General** tab of the application:
 - **Package delivery mode** was set to a value other than **None**.
 - **Always use latest version of package** was selected
 - The path at **Package root folder** contained an environment variable
- A user logged on to a RES ONE Workspace session and started the application.

In this scenario, in the user session, the following error message was displayed:

```
Application can't be started
```

This has been resolved.

Microsoft App-V 5.x: Logon, refresh or starting application could give error 'Subscript out of range'

Consider the following scenario:

- At **Composition > Applications**, a Microsoft App-V 5.x application was configured with the following configuration:
 - On the **Properties > General** tab of the application, the **Parameters** field contained one of the following:
 - `/appvve:<PACKAGEID>` (note the lack of a version ID parameter)
 - `/appvve:<PACKAGEID>-<VERSIONID>` (note that the character in between `<PACKAGEID>` and `<VERSIONID>` is **NOT** an underscore (`_`))
- At **Composition > User Settings**, on the **Settings** tab, **Application User Settings** was set to **Prefetch in background**, check on application start.

In this scenario, when a user logged on to a RES ONE Workspace session, when a Workspace refresh occurred, or when the user started the application, the following error occurred:

Process	pfwsmgr.exe
Procedure	sharedUserPreferences.fysnLoadUserSettingsInAppVContext
Error #	9
Error description	Subscript out of range

This has been resolved.

Now, when a Console user configures an App-V 5.x application with an `/appvve` parameter that does not contain an underscore (`_`), a warning is displayed.

When a user launches the application, an `Application can't be started message` is displayed, identifying an `Invalid Application Parameter error`.

RES ONE Automation Integration: Testing connection to RES ONE Automation environment could give error 'Subscript out of range'

In a RES ONE Workspace environment that used FIPS-compliant security algorithms, when configuring **RES ONE Automation Integration**, if the **Test now** button was used to verify the connection to the RES ONE Automation environment, the following error could occur:

Process	wmedit.exe
Procedure	sharedEncryption.SetupCryptoTransformEx
Error #	9
Error description	Subscript out of range

This has been resolved.

RES ONE Automation Integration can be configured at **Setup > Integration > RES Products > RES Automation**.

Usage Tracking: End date/time of applications might display incorrect data

In the **Usage Tracking Viewer**, on the **Details** tab, the column **End date/time** might display incorrect data. This has been resolved.

User Registry: Unable to import or edit registry value that contained €, ¥, ™, © etc.

At **Composition > Actions By Type > User Registry**, registry values that contained characters like €, ¥, ™, © etc. could be added to a registry setting manually, but could not be imported or edited. This has been resolved.

User Settings: Capture Wizard not working correctly if Working directory was other than default

Consider the following scenario:

- At **Composition > Applications**, an application was configured with the following settings:
 - On the **Properties > General** tab of the application:
 - for **Command line**, `C:\Windows\System32\notepad.exe` was entered (as an example).
 - for **Working directory**, a path that was different than the path in the **Command line** was entered. For example `C:\Temp`.
 - On the **User Settings > Properties** tab of the application, **Zero Profile mode** was set to **Capture targeted items....**
- On the **User Settings > Capturing** tab of the application, a Console user started the **User Settings Capture Wizard** (by clicking **Add > Discover User Settings**), and clicked **Next** to start User Settings discovery.

In this scenario, instead of the configured working directory (`C:\Temp`), the default working directory (`C:\Windows\System32`) was used. Also, if the user selected the **Working directory** field in the **User Settings Capture Wizard**, the data changed from `C:\Temp` to

`C:\Windows\System32`.

Both issues have been resolved.

Workspace Composer: Autodiscover not working correctly for Microsoft Outlook 2016

Consider the following scenario:

- At **Composition > Applications > E-mail Settings**, an E-mail Setting for **Microsoft Exchange Online (Office 365)** or for **Microsoft Exchange Server 5.5** or higher was configured to **Use Autodiscover**.
- At **Composition > Applications**, an application was configured for **Microsoft Outlook 2016**.
 - On the **Configuration > E-mail Settings** tab of the application, the E-mail Setting was selected.
- A user logged on to a RES ONE Workspace session and started **Microsoft Outlook 2016** locally, or as a **Microsoft App-V 5.x** application.

In this scenario, in the user session, the application might not start. If this occurred, one of the following error messages was displayed to the user:

`Cannot start Microsoft Outlook. Cannot open the Outlook window(...)`

Or

`Outlook cannot log on. Verify you are connected to the network(...)`

This has been resolved.

Workspace Composer: Desktop icons might disappear after a non-graceful logoff

Consider the following scenario:

- At **Composition > Actions By Type > Files and Folders > Folder Redirection**, a folder redirection was configured for the **Windows folder: Desktop**.
- The previous RES ONE Workspace session of a user ended in a non-graceful way, for example because of loss of power on the computer.

In this scenario, when the user logged on to a new RES ONE Workspace session, his desktop icons had disappeared. This has been resolved.

Workspace Composer: 'Disable file system redirector on 64-bit systems' applied incorrectly

Consider the following scenario:

- At **Composition > Applications**, on the **Settings** tab, **Windows Shell shortcut creation** was set to **Merge with unmanaged shortcuts**.
- At **Composition > Applications**, an application was configured with the following settings:
 - On the **Properties > General** tab of the application, the **Command line** pointed to a location that Microsoft Windows uses for 64-bit applications, for example `C:\Windows\System32\notepad.exe`.
 - On the **Properties > Settings** tab of the application, **Disable file system redirector on 64-bit systems** was not selected.
Based on this setting, on 64-bit versions of Windows, the command line for the application should point to a location that Windows uses for 32-bit applications.

In user sessions running on a 64-bit version of Windows, in this scenario:

- If **Managed Application Security** was enabled (at **Security > Applications > Managed Applications**, on the **Settings** tab), users could start the 64-bit version of Notepad, but not the 32-bit version.
- If the option **If managed shortcut was not used** was set to **Intercept new process and apply configuration** (on the **Properties > Shortcuts** tab of the application), only the 64-bit version of Notepad was intercepted by RES ONE Workspace.
 - If, additionally, the RES ONE Workspace registry value `InterceptManagedApps` was used, shortcuts that were generated by RES ONE Workspace pointed to the 64-bit version of Notepad.

This has been resolved.

Now, in this scenario, the correct bit-versions of the application are blocked, allowed, intercepted and/or generated.

Please note that after installing RES ONE Workspace version 10.1, the behavior of applications that match the situation above, will change. To correct this, please select the option **Disable file system redirector on 64-bit systems** for these applications.

Workspace Composer: Display of mini splash screen incorrect at logoff

In user sessions, during logoff, the mini splash screen could exhibit the following incorrect behavior:

- At **Administration > Performance > Instant LogOff**, if **Disconnect user session when logoff is initiated** was set to **Before RES ONE Workspace splash screen appears**:
 - the mini splash screen could still be visible during logoff.
 - an empty box could be displayed in the location of the mini splash screen.
- The progress bar displayed percentages that were not logical, for example progress at 125%.

These issues have been resolved.

Workspace Composer: 'Do not ping print server before connecting printers' not working correctly

If the option **Do not ping print server before connecting printers** was enabled (at **Setup > Advanced Settings**), Agents that were configured with the RES ONE Workspace registry value `ForcePrinterConnections` set to `Yes` still generated ping requests to the print server. This has been resolved.

Workspace Composer: Execute Command at application end could lead to endless interception loop

Consider the following scenario:

- At **Composition > Applications**, `Application A` and `Application B` were configured with the following settings:
 - On the **Properties > Shortcuts** tab of both applications, **If managed shortcut was not used** was set to **Intercept new process and apply configuration**.
 - On the **Configuration > Actions > At application end** tab of `Application A`, an **Execute Command** was configured, that started the executable of `Application B`.
 - On the **Configuration > Actions > At application end** tab of `Application B`, an **Execute Command** was configured, that started the executable of `Application A`.
- A user logged on to a RES ONE Workspace session, started `Application A`, and closed the application again.

In this scenario, in the user session, `Application B` was started and intercepted. If the user then closed `Application B`, `Application A` was started and intercepted again, etc., creating an endless interception loop. This has been resolved.

Workspace Composer: 'File not found: crc.dll' error could occur during logoff

Under rare circumstances, when users logged of from a RES ONE Workspace session, the following error could occur:

Process	pfwsmgr.exe
Procedure	clsCRC.AddBytes2
Error #	48
Error description	File not found: crc.dll

This has been resolved.

Workspace Composer: Homedrives contained multiple pwruser_<MACHINENAME>.his files

In environments where users logon to different machines frequently, the users' homedrives may contain multiple `pwruser_<MACHINENAME>.his` files. This has been resolved. Now, the Workspace Composer creates and maintains only one `pwruser.his` file.

When all Agents in your environment have been updated to RES ONE Workspace version 10.0.200.0 or higher, the `pwruser_<MACHINENAME>.his` files can be removed.

Workspace Composer: Multiple shortcuts with identical command line not displayed in Start Menu

Consider the following scenario:

- At **Composition > Applications**, multiple applications were configured with the following settings:
 - At **Properties > General**, the **Command line** for the applications was identical.
 - At **Properties > Shortcuts**:
 - for **Automatic shortcuts**, **Pin to Start Menu** was set to **Mandatory**.
 - for **Tile**, **Pin to Start** was set to **Take no action**.
- At **Administration > Custom Resources**, a corresponding `customAppUserModelIds.xml` file was configured as a Custom Resource.
- A user logged on to a RES ONE Workspace session on a machine running Microsoft Windows 8.1 / Server 2012 R2 or earlier.

In this scenario, in the user session, the shortcut for only one of the applications was present in the Start Menu. This has been resolved.

The Custom Resource `customAppUserModelIds.xml` is now also applied if only Start Menu shortcuts are configured, not only in combination with tiles.

Workspace Composer: New ... document option missing from context menu on Windows 8.1 and higher

If a file type association was configured for (for example) TXT files, the Windows option 'New > Text Document' was not available in the context menu in RES ONE Workspace sessions on machines running Microsoft Windows 8.1 or higher. This has been resolved.

This issue could affect all 'New ...' document options in the context menu. For example: BMP affected 'New > Bitmap image', DOC affected 'New > Microsoft Word Document' etc.

File type associations can be configured at **Composition > Applications**, on the **Properties > File Types** tab of an application.

Workspace Composer: No desktop background might be displayed if limited to pre-configured pictures

Consider the following scenario:

- At **Composition > Desktop > Background**, a **Desktop background picture** was configured.
- At **Composition > Desktop > Lockdown and Behavior**, in the **Personalization by end user** section, the option **Limit "Change Desktop Background" in Workspace Preferences to pre-configured pictures** was enabled.

In this scenario, when a new user logged on to a RES ONE Workspace session, no desktop background was displayed. This has been resolved.

The issue also occurred for any user that did not yet have a desktop background defined in his `pwruser.ini` file.

Workspace Composer: Not all RES ONE Automation tasks executed if user clicked 'Dismiss and notify me when done'

Consider the following scenario:

- At **Composition > Applications**, an application was configured with two or more Automation Tasks configured (on the **Configuration > Actions > At application start** tab of the application).
 - The Automation Tasks were configured with the following settings:
 - **Wait for task to finish before continuing** was enabled.
 - **Run before other actions** was enabled.
- A user logged on to a RES ONE Workspace session and started the application. The first Automation Task started and a splash screen was displayed, giving the user the option **Dismiss and notify me when done**.

In this scenario, in the user session, if the user clicked the **Dismiss and notify me when done** button, the other Automation Tasks for the application were not executed. This has been resolved.

Workspace Composer: Process interception might not work for executables located on a network drive

Consider the following scenario:

- At **Composition > Applications**, an application was configured with the following settings:
 - On the **Properties > General** tab of the application, the **Command line** contained the path to a network drive, for example `R:\Applications\notepad.exe`.
 - On the **Properties > Shortcuts** tab of the application, **If managed shortcut was not used** was set to **Intercept new process and apply configuration**.
- **Composition > Actions By Type > Files and Folders > Drive and Port Mappings**, a mapping was configured for drive `R:.`
- A user logged on to a RES ONE Workspace session and, without using a managed shortcut, started `R:\Applications\notepad.exe`.

In this scenario, in the user session, `notepad.exe` was not intercepted. This has been resolved.

The issue only occurred until a workspace refresh was performed in the session. If the application was started after a workspace refresh, the process was intercepted correctly.

Workspace Composer: Process priority not applied on intercepted processes

In RES ONE Workspace sessions, if the process of an application was intercepted, the **Process priority of the application** that was configured for that process was not applied. This has been resolved.

Now, if the configured process priority is other than **Normal**, it is applied to the intercepted application process.

Process priority of an application can be configured at **Composition > Applications**, on the **Properties > Settings** tab of the application.

Workspace Composer: Screensaver not working on Microsoft Windows Server 2016 after installing RES ONE Workspace v10

After installation of RES ONE Workspace v10, the RES ONE Workspace **Screensaver** might not work if the **Windows Shell shortcut creation** was set to **Replace all unmanaged shortcuts** on machines running Microsoft Windows Server 2016. This has been resolved.

The **Screensaver** can be configured at **Composition > Desktop > Screensaver**.

The setting **Windows Shell shortcut creation** can be configured at **Composition > Applications**, on the **Settings** tab.

Workspace Composer: Shortcuts might be generated with an incorrect 'Working directory' when using registry value 'InterceptManagedApps'

Consider the following scenario:

- At **Composition > Applications**, an application was configured with the following settings:
 - On the **Properties > General** tab of the application:
 - for **Command line**, `C:\Windows\System32\notepad.exe` was entered (as an example).
 - for **Working directory**, a path that was different than the path in the **Command line** was entered. For example `C:\Temp`.
 - On the **Properties > Shortcuts** tab of the application, **If managed shortcut was not used** was set to **Intercept new process and apply configuration**.
- A user logged on to a RES ONE Workspace session on a machine with the RES ONE Workspace registry value `InterceptManagedApps` set to `Yes`.

In this scenario, in the user session, shortcuts for the application were generated with an incorrect **Working directory** (the 'Start in' field in the properties of the shortcut). This has been resolved.

Workspace Composer: Special user folders displayed with generic folder icons

In RES ONE Workspace sessions, special user folders (for example `Desktop`, `Documents` and `Music`) were displayed with generic folder icons when they were viewed in their physical location in `%userprofile%` or on a remote, redirected location. This has been resolved. Now, these folders are displayed with their special, content-specific icons.

Workspace Composer: Startup folder created in Start Menu at every Workspace refresh

When a Workspace refresh was performed in RES ONE Workspace sessions, if no Startup folder was present in the Start Menu, it was created. This has been resolved.

Workspace Composer: User Settings with Zero Profile mode 'Capture, then Track' not restoring registry settings with Unicode characters

User Settings with Zero Profile mode **Capture** targeted items once, then track further changes did not restore captured registry settings that contained Unicode characters. This has been resolved.

Workspace Composer: Users might be prompted to select default program for configured File Types when using User Settings on Windows 10

Consider the following scenario:

- At **Composition > Applications**, an application was configured, for example Microsoft Word.
 - On the **Properties > File Types** tab of the application, for example DOCX was configured as a file type for the Command `Open`.
- At **Composition > User Settings**, on the **User Settings** tab, a User Setting was configured based on the Windows 10 / 2016 template for **Desktop Icons** or **All Control Panel Settings** (at **New > Templates > Windows > 10 / 2016 > Control Panel**)
- A user logged on to a RES ONE Workspace session on a machine running Microsoft Windows 10, and opened a DOCX file.

In this scenario, in the user session, the following Microsoft Windows message might be displayed to the user:

```
How do you want to open this file?  
Keep using this app
```

This has been resolved.

This issue has been resolved by updating the Windows 10 / 2016 **Desktop Icons** and **All Control Panel Settings** User Settings templates. Existing User Settings that were based on the previous templates will not be updated automatically.

To resolve the issue for an existing User Setting, open the targeted **Registry tree** `HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Associations` and add an exclusion for the **Registry value** `FileAssociationsUpdateVersion`.

Workspace Composer: White icons on taskbar when using Folder Redirection for roaming profiles

Consider the following scenario:

- At **Composition > Actions By Type > Files and Folder > Folder Redirection**, on the **Redirections** tab, the Microsoft Windows folder `AppData` was redirected.
- A user with a roaming profile logged on to two RES ONE Workspace sessions on machines that were configured with the RES ONE Workspace registry value `KeepQL` set to `Yes`.
 - The user logged off from one of the sessions.

In this scenario, in the remaining user session, the taskbar icons changed to white icons and no longer worked. This has been resolved.

Workspace Composer: Zone based on Computer OU membership not applied when logged on with local account

Consider the following scenario:

- At **User Context > Directory Services**, a **Microsoft Active Directory** was configured as a Directory Service.
- At **User Context > Locations and Devices**, a Zone was configured with a rule based on Computer OU membership for OU 'ABC'.
- A user logged on to a RES ONE Workspace session using a local computer account, on a computer that was a member of OU 'ABC'.

In this scenario, in the user session, membership of OU 'ABC' could not be determined using the local computer account and access to the Zone was denied. This has been resolved.

Now, in this scenario, the Active Directory query to determine OU membership is performed by the RES service.



Note

The issue also occurred if, instead of a local computer account, a user logged on using an account from a domain other than used for the Zone.

Workspace Start Menu: \$recycle.bin shortcut displayed when Start Menu was redirected

Consider the following scenario:

- At **Composition > Actions By Type > Files and Folder > Folder Redirection**, on the **Redirections** tab, the Microsoft Windows folder `Start Menu` was redirected to a network share.
- At **Composition > Desktop > Lockdown and Behavior**, in the **Microsoft Windows Shell** section, the option **Enable Windows 8.1 Start Menu (Windows 8.1 / 2012 R2)** was enabled.
- A user logged on to a RES ONE Workspace session on a machine running Microsoft Windows 8.1 or Windows Server 2012 R2.
 - In Windows Explorer, in the Folder Options window, on the **View** tab, the option **Show hidden files, folders, and drives** was selected and the option **Hide protected operating system files** was cleared.

In this scenario, in the user session, if the user opened the **Workspace Start Menu**, the `$recycle.bin` shortcut was displayed as a Start Menu item. This has been resolved.

Workspace Start Menu: Folder structure might be incorrect when using identical folder names in separate branches

Consider the following scenario:

- At **Composition > Applications**:
 - an application was configured that was several levels deep in the folder structure.
Example: `Start\Folder 1\Level 2\Level 3\Notepad`
 - another application was configured, where the bottom two folders had identical names and were in the same 'folder depth' as the first application.
Example: `Start\Folder 2\Level 2\Level 3\Calculator`
- At **Composition > Desktop > Lockdown and Behavior**, the option **Enable Windows 8.1 Start Menu (Windows 8.1 / 2012 R2)** was selected.
- A user logged on to a RES ONE Workspace session on a machine running Microsoft Windows 8.1 or Server 2012 R2.

In this scenario, in the user's Workspace Start Menu, the shortcut for `Calculator` was placed in the same Start Menu folder as `Notepad`. This has been resolved.

Workspace Start Menu: Windows 8.1 Start Menu might not appear

Under rare circumstances, if the option **Enable Windows 8.1 Start Menu (Windows 8.1 / 2012 R2)** was enabled, the Start Menu did not appear in user sessions. This has been resolved.

The option **Enable Windows 8.1 Start Menu (Windows 8.1 / 2012 R2)** can be found at **Composition > Desktop > Lockdown and Behavior**, in the **Microsoft Windows Shell** section.