## Contents

### Chapter 1: Introduction to the Workspace Control Administration Guide

1.1 Ivanti Training .......................................................................................................... 2  
1.2 Ivanti Support .......................................................................................................... 3

### Chapter 2: About Workspace Control

2.1 Architecture .............................................................................................................. 5  
2.1.1 Components ......................................................................................................... 5  
2.1.2 Communication Model ....................................................................................... 10  
2.1.3 The Workspace Control Agent Service and its subprocesses ......................... 11  
2.1.4 The Workspace Control Agent Cache ............................................................... 12  
2.1.5 Scalability and performance .............................................................................. 13

### Chapter 3: Installation

3.1 Prerequisites ............................................................................................................ 17  
3.2 Installation ............................................................................................................... 19  
3.3 Install Workspace Control Agent Service under different account ...................... 21  
3.4 Unattended Installation ......................................................................................... 22  
3.4.1 Installation public properties ........................................................................... 23  
3.4.2 Create a new Datastore ..................................................................................... 26  
3.4.3 Connect to an existing environment .................................................................. 28  
3.4.4 Configure Agent connection after installation ................................................. 33  
3.5 Configure the Workspace Composer ..................................................................... 34  
3.5.1 Configure Agents .............................................................................................. 34  
3.5.2 Manual Configuration ....................................................................................... 34  
3.5.3 Server-based Computing ................................................................................... 34  
3.6 Set up the Datastore ............................................................................................... 36  
3.6.1 Configure the Datastore ................................................................................... 36  
3.7 Configuration Wizard ............................................................................................ 37  
3.8 Dynamic Datastore configuration for Agents ....................................................... 38  
3.8.1 Configure the Datastore dynamically ............................................................... 38  
3.8.2 Example ........................................................................................................... 39  
3.9 Relay Servers ......................................................................................................... 40  
3.9.1 Configure Relay Servers .................................................................................. 40  
3.9.2 Dynamic Relay Server configuration ................................................................ 42  
3.10 Agents ................................................................................................................... 43  
3.10.1 Agents Settings ............................................................................................... 43  
3.11 Keep Workspace Control up to date .................................................................... 48  
3.12 Workspace Control Modules .............................................................................. 50  
3.13 Desktop Transformation ....................................................................................... 53  
3.13.1 Desktop Sampler ............................................................................................. 53  
3.13.2 Workspace Designer ....................................................................................... 55  
3.13.3 Workspace Model ........................................................................................... 56

### Chapter 4: General Functionality

4.1 Filtering .................................................................................................................... 57  
4.1.1 Where to find Filtering ..................................................................................... 57  
4.1.2 Filter Criteria and Filter Types ......................................................................... 58  
4.1.3 Nodes excluded from filtering ......................................................................... 59

Copyright © 2019, Ivanti. All rights reserved. [Privacy and Legal](#)
# Chapter 7: Composition

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.1</td>
<td>Applications</td>
</tr>
<tr>
<td>7.1.1</td>
<td>Start Menu tab</td>
</tr>
<tr>
<td>7.1.2</td>
<td>Application List tab</td>
</tr>
<tr>
<td>7.1.3</td>
<td>Settings tab</td>
</tr>
<tr>
<td>7.1.4</td>
<td>Defaults for new applications</td>
</tr>
<tr>
<td>7.1.5</td>
<td>Create and edit Applications</td>
</tr>
<tr>
<td>7.1.6</td>
<td>Workspace Control Applications for end users</td>
</tr>
<tr>
<td>7.1.7</td>
<td>Make Control Panel Applets (CPL files) available as applications</td>
</tr>
<tr>
<td>7.1.8</td>
<td>File Types</td>
</tr>
<tr>
<td>7.1.9</td>
<td>E-mail Settings</td>
</tr>
<tr>
<td>7.1.10</td>
<td>Data Sources</td>
</tr>
<tr>
<td>7.2</td>
<td>Actions</td>
</tr>
<tr>
<td>7.2.1</td>
<td>Automation Tasks</td>
</tr>
<tr>
<td>7.2.2</td>
<td>Environment Variables</td>
</tr>
<tr>
<td>7.2.3</td>
<td>Execute Command</td>
</tr>
<tr>
<td>7.2.4</td>
<td>Files and Folders</td>
</tr>
<tr>
<td>7.2.5</td>
<td>LANDesk</td>
</tr>
<tr>
<td>7.2.6</td>
<td>Microsoft System Center Configuration Manager Software Distributions</td>
</tr>
<tr>
<td>7.2.7</td>
<td>Printers</td>
</tr>
<tr>
<td>7.2.8</td>
<td>User Registry</td>
</tr>
<tr>
<td>7.2.9</td>
<td>Linked Actions</td>
</tr>
<tr>
<td>7.3</td>
<td>Desktop</td>
</tr>
<tr>
<td>7.3.1</td>
<td>Shell</td>
</tr>
<tr>
<td>7.3.2</td>
<td>Background</td>
</tr>
<tr>
<td>7.3.3</td>
<td>Lockdown and Behavior</td>
</tr>
<tr>
<td>7.3.4</td>
<td>Screensaver</td>
</tr>
<tr>
<td>7.4</td>
<td>User Settings</td>
</tr>
<tr>
<td>7.4.1</td>
<td>Where to find User Settings in the Workspace Control Console</td>
</tr>
<tr>
<td>7.4.2</td>
<td>Zero Profile Modes</td>
</tr>
<tr>
<td>7.4.3</td>
<td>Migration settings when switching to another Zero Profile mode</td>
</tr>
<tr>
<td>7.4.4</td>
<td>Flex Profile Kit INI files</td>
</tr>
<tr>
<td>7.4.5</td>
<td>What is saved as part of a Targeted Item</td>
</tr>
<tr>
<td>7.4.6</td>
<td>Storage of users' User Setting data</td>
</tr>
<tr>
<td>7.4.7</td>
<td>Additional User Setting options</td>
</tr>
<tr>
<td>7.4.8</td>
<td>Microsoft App-V applications</td>
</tr>
</tbody>
</table>

# Chapter 8: Security

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1</td>
<td>Applications</td>
</tr>
<tr>
<td>8.1.1</td>
<td>Managed Applications</td>
</tr>
<tr>
<td>8.1.2</td>
<td>User Installed Applications</td>
</tr>
<tr>
<td>8.1.3</td>
<td>Websites</td>
</tr>
<tr>
<td>8.2</td>
<td>Data</td>
</tr>
<tr>
<td>8.2.1</td>
<td>Removable Disks security</td>
</tr>
<tr>
<td>8.2.2</td>
<td>Files and Folders security</td>
</tr>
<tr>
<td>8.2.3</td>
<td>Read-Only Blanketing</td>
</tr>
<tr>
<td>Chapter 9:</td>
<td>Diagnostics</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>9.1</td>
<td>Workspace Analysis .......................................................... 304</td>
</tr>
<tr>
<td>9.1.1</td>
<td>General information about users .......................................... 304</td>
</tr>
<tr>
<td>9.1.2</td>
<td>Detailed information about users ......................................... 305</td>
</tr>
<tr>
<td>9.1.3</td>
<td>Workspace Simulation Wizard ................................................. 308</td>
</tr>
<tr>
<td>9.2</td>
<td>User Sessions ................................................................. 310</td>
</tr>
<tr>
<td>9.2.1</td>
<td>Where to find User Sessions ................................................ 310</td>
</tr>
<tr>
<td>9.2.2</td>
<td>Context menu options .......................................................... 311</td>
</tr>
<tr>
<td>9.3</td>
<td>Workspace Model Overview .................................................... 312</td>
</tr>
<tr>
<td>9.3.1</td>
<td>Where to find the Workspace Model Overview ............................ 312</td>
</tr>
<tr>
<td>9.4</td>
<td>Audit Trail ..................................................................... 313</td>
</tr>
<tr>
<td>9.4.1</td>
<td>Audit Trail options ........................................................... 313</td>
</tr>
<tr>
<td>9.5</td>
<td>Agents Overview ................................................................. 314</td>
</tr>
<tr>
<td>9.6</td>
<td>Usage Tracking Overview ....................................................... 315</td>
</tr>
<tr>
<td>9.7</td>
<td>Errors ................................................................................. 316</td>
</tr>
<tr>
<td>9.7.1</td>
<td>Where to find Errors ............................................................. 316</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 10:</th>
<th>Administration</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1</td>
<td>Administrative Roles ......................................................... 317</td>
</tr>
<tr>
<td>10.1.1</td>
<td>Where to find Administrative Roles ....................................... 318</td>
</tr>
<tr>
<td>10.1.2</td>
<td>Permissions ........................................................................ 318</td>
</tr>
<tr>
<td>10.1.3</td>
<td>Technical Manager .................................................................. 319</td>
</tr>
<tr>
<td>10.1.4</td>
<td>Scope Control ....................................................................... 319</td>
</tr>
<tr>
<td>10.1.5</td>
<td>Filters .................................................................................. 319</td>
</tr>
<tr>
<td>10.1.6</td>
<td>Solve a Console lockout .......................................................... 319</td>
</tr>
<tr>
<td>10.2</td>
<td>Agents ................................................................................. 320</td>
</tr>
<tr>
<td>10.3</td>
<td>Relay Servers ....................................................................... 321</td>
</tr>
<tr>
<td>10.3.1</td>
<td>Troubleshoot Relay Servers .................................................... 321</td>
</tr>
<tr>
<td>10.4</td>
<td>Custom Resources .................................................................. 324</td>
</tr>
<tr>
<td>10.5</td>
<td>Maintenance ......................................................................... 325</td>
</tr>
<tr>
<td>10.6</td>
<td>Performance ......................................................................... 327</td>
</tr>
<tr>
<td>10.6.1</td>
<td>Access Balancing .................................................................... 327</td>
</tr>
<tr>
<td>10.6.2</td>
<td>CPU Optimization .................................................................. 329</td>
</tr>
<tr>
<td>10.6.3</td>
<td>Instant LogOff ....................................................................... 331</td>
</tr>
<tr>
<td>10.6.4</td>
<td>Memory Optimization ................................................................ 333</td>
</tr>
<tr>
<td>10.7</td>
<td>Workspace Model .................................................................... 337</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 11:</th>
<th>Registry settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1</td>
<td>ActiveSetupTimeout .............................................................. 338</td>
</tr>
<tr>
<td>11.2</td>
<td>BlockPicaSvCFix .................................................................... 339</td>
</tr>
<tr>
<td>11.3</td>
<td>ChangePasswordTimeout .......................................................... 339</td>
</tr>
<tr>
<td>11.4</td>
<td>CheckDisabledFolders ............................................................ 339</td>
</tr>
<tr>
<td>11.5</td>
<td>CheckShutDown ....................................................................... 340</td>
</tr>
<tr>
<td>11.6</td>
<td>CheckUpdateOsdFile ............................................................... 340</td>
</tr>
<tr>
<td>11.7</td>
<td>ConsoleNoAppIcons</td>
</tr>
<tr>
<td>11.8</td>
<td>CorrectTaskbar</td>
</tr>
<tr>
<td>11.9</td>
<td>CorrectWorkArea</td>
</tr>
<tr>
<td>11.10</td>
<td>CTX_PFDesktopUsesPwrStart</td>
</tr>
<tr>
<td>11.11</td>
<td>CTX_PNLaunchUsesFarmName</td>
</tr>
<tr>
<td>11.12</td>
<td>CTX_PublishAppCmdLineFlag</td>
</tr>
<tr>
<td>11.13</td>
<td>DirectoryServiceRetryLimit</td>
</tr>
<tr>
<td>11.14</td>
<td>DisableDHCP</td>
</tr>
<tr>
<td>11.15</td>
<td>DisableExternalGroupCheck</td>
</tr>
<tr>
<td>11.16</td>
<td>DisableFolderSyncLocalCheck</td>
</tr>
<tr>
<td>11.17</td>
<td>DisableIconRefresh</td>
</tr>
<tr>
<td>11.18</td>
<td>DisableTileManagement</td>
</tr>
<tr>
<td>11.19</td>
<td>DoNotAllowOverlappedDesktopItems</td>
</tr>
<tr>
<td>11.20</td>
<td>DoNotAnalyzeDB</td>
</tr>
<tr>
<td>11.21</td>
<td>EnableMultipleIE</td>
</tr>
<tr>
<td>11.22</td>
<td>ExcludeProcesses</td>
</tr>
<tr>
<td>11.23</td>
<td>ExcludeSubscribedTasks</td>
</tr>
<tr>
<td>11.24</td>
<td>ForceComputername</td>
</tr>
<tr>
<td>11.25</td>
<td>ForceDisconnectOnIdle</td>
</tr>
<tr>
<td>11.26</td>
<td>ForceLogoff</td>
</tr>
<tr>
<td>11.27</td>
<td>ForcePrinterConnections</td>
</tr>
<tr>
<td>11.28</td>
<td>ForceShutdown</td>
</tr>
<tr>
<td>11.29</td>
<td>IncludeProcesses</td>
</tr>
<tr>
<td>11.30</td>
<td>Instrumentation</td>
</tr>
<tr>
<td>11.31</td>
<td>InterceptManagedApps</td>
</tr>
<tr>
<td>11.32</td>
<td>KeepSeamlessHostAgent</td>
</tr>
<tr>
<td>11.33</td>
<td>KeepSharesWithROB</td>
</tr>
<tr>
<td>11.34</td>
<td>KeepTmpDDEMACros</td>
</tr>
<tr>
<td>11.35</td>
<td>KeepUnicodePath</td>
</tr>
<tr>
<td>11.36</td>
<td>KeepUserDefaultMAPIProfile</td>
</tr>
<tr>
<td>11.37</td>
<td>KeepWordRunning</td>
</tr>
<tr>
<td>11.38</td>
<td>LingerDisconnectTimerInterval</td>
</tr>
<tr>
<td>11.39</td>
<td>LingerTerminateTimerInterval</td>
</tr>
<tr>
<td>11.40</td>
<td>LocalCacheOnDisk</td>
</tr>
<tr>
<td>11.41</td>
<td>LocalCachePath</td>
</tr>
<tr>
<td>11.42</td>
<td>LocatePrintersByIP</td>
</tr>
<tr>
<td>11.43</td>
<td>LogAdapterInfo</td>
</tr>
<tr>
<td>11.44</td>
<td>LogPerformance</td>
</tr>
<tr>
<td>11.45</td>
<td>MSLimitOnProcIDs</td>
</tr>
<tr>
<td>11.46</td>
<td>NoAgentScreenSaver</td>
</tr>
<tr>
<td>11.47</td>
<td>NoFullScreenKiosk</td>
</tr>
<tr>
<td>11.48</td>
<td>NoListConcurrentUsers</td>
</tr>
<tr>
<td>11.49</td>
<td>NoPrecedingSlashInPNFolder</td>
</tr>
<tr>
<td>11.50</td>
<td>OutlookNotificationCheck</td>
</tr>
<tr>
<td>11.51</td>
<td>PDoNotSetEnvVars</td>
</tr>
<tr>
<td>11.52</td>
<td>PWMAutoAllowFolders</td>
</tr>
<tr>
<td>11.53</td>
<td>PwrGateAppId</td>
</tr>
<tr>
<td>11.54</td>
<td>PwrGateFileMapping</td>
</tr>
<tr>
<td>11.55</td>
<td>PwrGateSleep</td>
</tr>
<tr>
<td>11.56</td>
<td>PwrMapiDelay</td>
</tr>
<tr>
<td>11.57</td>
<td>RefreshAllMappedDrives (Workspace Control 10.2.0.1 and earlier)</td>
</tr>
<tr>
<td>11.58</td>
<td>RefreshAllMappedDrives (Workspace Control 10.2.500.0 and higher)</td>
</tr>
<tr>
<td>11.59</td>
<td>RemoveStartmenuPinList</td>
</tr>
<tr>
<td>11.60</td>
<td>RestoreMappingsAtLogoff</td>
</tr>
<tr>
<td>11.61</td>
<td>RunCPUShid</td>
</tr>
<tr>
<td>11.62</td>
<td>RunWMFileSync</td>
</tr>
<tr>
<td>11.63</td>
<td>SCCMDelayBeforeRunningProgram</td>
</tr>
<tr>
<td>11.64</td>
<td>SelfServicePoll (Workspace Control 10.1.400.0 and higher)</td>
</tr>
<tr>
<td>11.65</td>
<td>SessionCheckInterval (RES ONE Workspace 10.0 and earlier)</td>
</tr>
<tr>
<td>11.66</td>
<td>SessionCheckInterval (Workspace Control 10.1 and higher)</td>
</tr>
</tbody>
</table>
Chapter 12: Registry settings for Relay Servers

12.1 CertificateAlgorithm ................................................................. 376
12.2 CertificateKeyLength ................................................................ 376
12.3 CustomCertificate ...................................................................... 377
12.4 DBCleanupDuration ..................................................................... 379
12.5 DoNotAcceptSelfSignedCert ......................................................... 380
12.6 RemoveObsoleteLogFiles .............................................................. 381
12.7 RSConnectTimeout ...................................................................... 381

Chapter 13: Command line Options

13.1 Pwrtech ...................................................................................... 382
13.2 Pwrgate ..................................................................................... 383
13.2.1 Building Blocks and using FIPS compliant security algorithms ........................................... 383
13.2.2 Import file hashes ................................................................... 383
13.2.3 Obtain encrypted version of Environment password ......................................................... 387
13.2.4 Process Building Blocks and Custom Resources in batches ............................................. 387
13.2.5 Republish a published application .............................................. 390
13.3 Setprint ....................................................................................... 390
13.4 Network Security Log .................................................................. 390

Chapter 14: The order of events in Workspace Control sessions

14.1 The order of events when a session starts .................................... 391
14.2 The order of events at a session refresh ....................................... 394
14.3 The order of events when a session ends ...................................... 396

Chapter 15: Compatibility Matrix Workspace Control

Chapter 16: Feature deprecation

Chapter 17: Index
Chapter 1: Introduction to the Workspace Control Administration Guide

Welcome to the Workspace Control version 10.3 Administration Guide. This document provides detailed information about the installation and configuration of Workspace Control features and components.

Note that the content of this Administration Guide is based on the latest available version of Workspace Control.

For additional documents and information, please refer to our website https://www.ivanti.com, and to our Online Support at https://forums.ivanti.com.

For feedback about the Workspace Control version 10.3 Administration Guide, please contact the Ivanti documentation team at documentation@ivanti.com.
1.1 Ivanti Training

Ivanti has developed a mix of learning materials to help our customers and channel partners get the most out of our products. Our goal is to give you a choice in how you learn; whether that is in the classroom, online tutorials and virtual workshops, or downloading our self-study kits. Please visit https://www.ivanti.com/services/training-certifications for more information on Training.

Ivanti Academy - Ivanti Academy provides an engaging way to learn about Ivanti products and technologies. It consists of short video tutorials, including practice questions, informative links and more. These tutorials cover a broad range of subjects: from planning, installing and configuring an environment to using the functionality of the Ivanti product.

Workshops - For customers and partners Ivanti organizes free interactive online workshops. These one-hour events are intended for experienced users of our software and deal with specific use cases and troubleshooting. Due to the interactive nature of these workshops, the number of seats per session is limited.

Training Classes - For partners and customers, Ivanti has developed several technical courses that deal with the installation and configuration of Workspace Control, Automation and Identity Director.

Certification - Ivanti offers a certification program designed to validate IT professionals with the technical capabilities and expertise needed to effectively use the Ivanti product portfolio, giving companies the confidence that their IT employees have the skills and experience needed to be successful.
1.2 Ivanti Support

At Ivanti, our core business is to help heighten productivity in your organization. Ivanti Support helps us to achieve this goal, and has been embedded in the core principles of our company since it was founded. Ivanti is dedicated to supporting everyone who uses or wants to use its proven products with Ivanti Support, which elevates our enterprise solutions above and beyond technology.

**Support** - If you are experiencing difficulties with any of our products, you may find the solution in our Knowledge Base or you can contact Ivanti Support directly.

**Product Upgrades and Service Releases** - To upgrade your product to the latest standard, you can install Product Upgrade Packs and Service Releases from the Ivanti Community.

**Solution Assurance** - To protect your investment, it is mandatory that you purchase one initial year of Solution Assurance with each license purchase. Solution Assurance unlocks access to Technical Support, Product Updates and Upgrades and the Knowledge Base. Solution Assurance is extended automatically, unless you specify otherwise. For more information: [http://www.ivanti.com/support/ivanti-support](http://www.ivanti.com/support/ivanti-support).

**Early Adopter Program** - Participants of the Early Adopter Program are actively involved in taking Ivanti solutions to the next level. The Early Adopter Program unlocks access to interim releases of our products. These releases are production-ready and allow you to test drive and explore new functionality.

**Community** - Ivanti invites you to become part of our community to share best practices and tips with fellow IT professionals, find solutions and more.

Please visit the Ivanti Online Support ([https://forums.ivanti.com](https://forums.ivanti.com)) for more information.
Chapter 2: About Workspace Control

On any regular Microsoft Windows desktop there are important items that enable productivity, such as the application to read e-mail, access to documents shared with other people, and the ability to print documents. There are also useful items on the desktop that make it more comfortable, such as personalized settings for using the e-mail application, a favorite background picture, or other preferences. These useful items do not directly affect productivity, but they make life easier.

Desktop items include:
1. Applications
2. Documents and other data
3. Printing capabilities
4. Personal settings

The availability of desktop items depends on the computer and the user account. Switching to a different computer or using a different user account does not guarantee you the same list of desktop items.

Workspace Control User Workspace Management transforms desktops into User Workspaces.

A User Workspace is composed each time a user logs on to a Windows desktop. After composition, the desktop contains configured Applications, Data, Printer settings and Personal Settings.

Composition of these items is dynamic and based on context: who you are (Identity), where you are (Location), what computer you are using (Device), and when (Date and Time). Composing and Securing a User Workspace takes a short time and is independent from any underlying technologies. User Workspace Management allows you to manage this process easily for many user workspaces at once.

Once the unique User Workspace has been composed, it is secured simply and effectively by only allowing the use of the available Applications, Data, Devices and Network connections.

The User Workspace exists until the user logs off from the Windows desktop.

The navigation map contains links to the various nodes of the Console, which makes it easier to set up and manage the user workspace.
2.1 Architecture

2.1.1 Components

Workspace Control consists of a central database (Datastore) and several software-based components. Each component relies on the Datastore for timely information regarding the user's environment.

The Workspace Control Console

The Workspace Control Console is the central point of administration of the User Workspace. It is usually run from an administrator's workstation. The Management Console stores all the provided information in a database.

In the Management Console, the administrator can centrally manage context-aware workspaces that contain all the right applications, data, printing and personal settings essential for the user’s productive working. It offers the Workspace Designer and several Wizards, helping the administrator to create workspace items according to business rules and compliance. With the Workspace Model, the administrator can control which parts should be composed and secured in the User Workspace.

Throughout the Console the size of the columns as they appear on screen can be adjusted. Customized column width or order of columns is saved automatically on the user's home drive or, if not available, in the user's registry. The option Reset all column properties to defaults in the Options menu, will reset any changes that you made to the order or widths of columns in the Console.

In every list view in the Console, one column is by default configured to auto size to fill out any remaining screen width. If you adjust the width of an auto-sizing column, it will no longer auto size and so you may end up with white space to the right of the columns.

The Workspace Control Console process, pwrtech.exe, has only one instance per device.

Some of the Wizards run as a single instance subprocess called wmwzrds.exe. Some configuration windows run as a single instance subprocess called wmedit.exe.

The Management Portal

The Workspace Control Management Portal is an optional, web-based application that works alongside the Console. In time, as features are added, it will replace the Console.

For more information about Management Portal functionality, installation and prerequisites, please refer to the Workspace Control Management Portal documentation that is available at https://forums.ivanti.com.

The Workspace Control Datastore

The Datastore is the central database for your Workspace Control environment. All computers in a Workspace Control environment connect to this database (optionally through a Relay Server). It runs on a central database server that you have installed prior to installing the Workspace Control Console.

See the Compatibility Matrix for a list of supported database types.
The Workspace Control Agents

An important aspect of Workspace Control is the architecture of each Workspace Control Agent (i.e. each Terminal Server, workstation, virtual desktop, or laptop that runs Workspace Control). The following illustration provides a schematic overview:

Configuration data received from the Datastore is cached locally. Each Workspace Control Agent uses its cached data instead of connecting to the SQL database directly.

The data cache also stores user information (log files and monitoring data) that is collected by each Workspace Control Agent. The Workspace Control Agent Service sends this data from the local cache to the Datastore for centralized access from the Management Console.

Read more about the Workspace Control Agent Service (res.exe) and about the communication processes to and from the Datastore in the chapter "The Workspace Control communication architecture".

Each Agent cache consists of:

- log files
- objects
- registry settings

Log files

The log files contain monitoring files, error logs and PowerTrace data from Workspace Control end-user components. These files are stored in a dedicated cache folder:

```plaintext
%programfiles%\Ivanti\Workspace Control\Data\DBCache\Transactions
```

They are forwarded to the Workspace Control Datastore by the Workspace Control Agent Service.
Objects

The objects stored in the local cache are XML files containing part of the Workspace Control configuration data, and various resources in different formats.

These files are stored in subfolders of %programfiles%\Ivanti\Workspace Control\Data\DBCache:

- \Objects contains XML files specifying application settings, PowerLaunch settings and other configuration settings.
- \IconCache contains icons for your programs and shortcuts.
- \Resources contains several subfolders that store your ICA files, OSD files, ADM files, files used as desktop images, and files used in your folder maintenance. The \Resources folder functions much like a distributed fileshare.

The Workspace Control Agent Service forwards these objects from the Workspace Control Datastore to the local cache.

Registry Settings

The remainder of the Workspace Control configuration data is implemented as Registry settings. The data is forwarded from the Workspace Control Datastore to the agent cache by the Workspace Control Agent Service, and is stored in the following registry key:

HKLM\Software\Policies\RES\Workspace Manager\Settings

This concerns settings that have a restricted set of possible values, such as:

- MemoryShield > "Enabled": the value of the setting can only be Yes or No.
- Maximum number of simultaneous logons: the value of the setting can only be a number.

You can define exceptions per user by customizing the registry key:

HKCU\Software\Policies\RES\Workspace Manager\Settings

These exceptions can be implemented using the Workspace Control Actions technology.
Workspace Control Relay Servers

The Relay Server component makes it possible to create a flexible architecture that consolidates and centralizes all Workspace Control configuration data into one central database, while ensuring that dispersed Agents across multiple sites obtain configuration data efficiently and in a timely manner.

Relay Servers are an optional infrastructure component. Relay Servers cache information from the Datastore and pass it on to Agents or to other Relay Servers. Agents can be configured to contact the Datastore directly, or to use Relay Servers. In a Workspace Control site, both methods can be used at the same time, with some Agents connecting to the Datastore and others using Relay Servers.

Relay Servers offer several advantages:

- Improved scalability in all kinds of distributed network topologies.
- Reduced network traffic in multiple-site environments, as fewer components connect directly to the central Datastore over relatively slow data connections.
- Reduced Datastore load, as fewer components connect directly to the central Datastore.
- Agents that connect to Relay Servers do not need to have a database driver installed for the Workspace Control Datastore.

Cascaded Relay Servers

In an environment with cascaded Relay Servers where more than 50,000 transactions exist in the queue of one of the Relay Servers or there is less than 500 MB free disk space on the Relay Server, the Relay Server will stop to accept new transactions from Agents or other Relay Servers. They are then redirected to another Relay Server. When the queue has been reduced to 40,000 queued transactions or free disk space increased by 10% to 550 MB, the Relay Server will accept new transactions again.

For further details about Relay Servers, see the document Getting Started with Workspace Control Relay Servers.
The Workspace Composer

The Workspace Composer is the Workspace Control-managed uniform workspace that the end users are presented with, regardless of the technology stack used. The Workspace Composer provides only the functionality that the end user needs. This includes all applications, menu items and settings to which the user is granted access.

The desktop can be displayed using either the Workspace Control Shell or the Microsoft Windows Shell. Both shells are managed by Workspace Control, but the Workspace Control Shell presents a classic windows-like shell with some additional Workspace Control-only technology, whereas the Microsoft Windows Shell is the exact shell as it is presented by Microsoft, including the various available themes. After installation of Workspace Control you need to configure the Workspace Composer as the default shell for your users (see Configure the Workspace Composer (on page 33)).
Chapter 2: About Workspace Control

2.1.2 Communication Model

Workspace Control stores all configuration data and resources in an Oracle or SQL-based database: the Workspace Control Datastore. You can set all your Terminal Servers, workstations, virtual desktops, and laptops to use a single database or you can use replication to set up multiple databases.

Workspace Control Console communicates directly with the Workspace Control Datastore. All Workspace Control Agents receive a local cache containing configuration data from the Workspace Control Datastore or a Relay Server. Agents use their cached data, they do not connect to the Datastore directly.

The local cache also stores user information (log files and monitoring data) that is collected by each Workspace Control Agent. The Workspace Control Agent Service, which runs on each Workspace Control Agent, sends this data from the local cache to the Datastore or a Relay Server.

Local caches are updated through selective synchronization: the Workspace Control Agent Service retrieves only changed information from the Datastore to place in the local data cache. This reduces the load on the central database significantly. This downstream communication is asynchronous: if the Datastore/Relay Server is busy or unavailable, the request is deferred until the Datastore/Relay Server can process it.

The Workspace Control Datastore also stores the user information (log files and monitoring data) that is collected by all Workspace Control Agents. The Workspace Control Agent Service pushes each Agent’s log files and monitoring information from the local cache to the Datastore/Relay Server. This upstream communication is also asynchronous: if the Datastore/Relay Server is busy or unavailable, the information remains in cache until the Datastore/Relay Server can receive it.
2.1.3 The Workspace Control Agent Service and its subprocesses

Each desktop that has the Ivanti Workspace Composer installed, has an agent service that retrieves the information from the database and stores it locally. The Workspace Composer running on the Windows desktop will use this local information and the context of the user to compose and secure (parts of) the User Workspace. As someone works in their User Workspace, information is collected by the Workspace Composer in transactions. These transactions are stored in the central database by the agent service whenever it can access the central database.

The Workspace Control Agent Service is named `Res.exe`. `Res.exe` and its sub processes have only one instance per device.

- The following information is stored at `HKLM\Software\RES\Workspace Manager` / `HKLM\Software\Wow6432Node\RES\Workspace Manager`:
  - Root Datastore Connection Properties
  - UpdateGUIDS Update GUIDs
  - Data Access Balancing

The tasks of the Workspace Control Agent Service (`Res.exe`) consist of:

- Checking Datastore connectivity
- Unlocking and locking the user Registry
- Handle License requests (session and application)
- Handle logging
- Check its own running processes

The Workspace Control Agent Service contains the following sub processes:

- `Pwrcache /download` (checks the Datastore for changes that should be downloaded to the Agent)
- `Pwrcache /upload` (checks the Agent for transactions that need to be processed by the Datastore)
- `CPUShield` (CPU Optimization)
- `islogoff`

On the Agent, also the driver service `Workspace Control PE (respesvc64.exe)` runs. This service runs under the local system account, which may not be changed.
2.1.4 The Workspace Control Agent Cache

- There is one Workspace Control Agent Cache per device.
- The Workspace Control Agent cache is located at: %programfiles%\Ivanti\Workspace Control\Data\DBCache\n- The sub folders contain the following data:
  - IconCache - contains icons for programs and shortcuts
  - Objects - contains XML files specifying Application, and other configuration settings
  - Resources - contains several subfolders that store files like OSD, ICA, BMP etc.
  - Transactions - Log files waiting for transfer

HKLM\Software\Policies\RES\Workspace Manager\Settings\.... - Integer values and Booleans
- A User Session only needs read permissions on the Agent Cache.
- The Agent Cache is protected by Workspace Control Security.

pwrcache.exe

The tasks of the pwrcache.exe subprocess are:
- Update the Agent Cache from the Workspace Control Datastore
- Agent Cache Resources, XML and registry
- Updates are based on GUID tree information

Pwrcache.exe /upload
- Upload Agent/Session stored logging to the Workspace Control Datastore from %programfiles%\Ivanti\Workspace Control\Data\DBCache\transactions
2.1.5 *Scalability and performance*

Workspace Control provides a flexible architecture that can use either direct database connections or indirect database connections through a Relay Server. Depending on the network topology, you can either use the capacity of the chosen database platform and connect the Agents directly or use Relay Servers to serve the Agents in a distributed network infrastructure. The database can also use standard high availability best practices.

Network traffic generated by Workspace Control is approximately 128KB per managed object upon installation of Workspace Control. This means that approximately 250MB local cache is required for configuration data in an environment with 2000 applications. Any changes to the configuration will be downloaded in the background.

Workspace Control Composer manages the entire workspace with the use of the local cache. There is no dependency on the Datastore or Relay Server.

This section describes sizing and performance of all Workspace Control components that take care of personalization, advanced administration and security.
Chapter 2: About Workspace Control

Architecture Overview

This architecture overview displays the key components of Workspace Control and how they relate to each other.

![Architecture Diagram]

**Workspace Control Datastore**

Workspace Control requires a database to store its configuration data, logging and usage tracking information. Workspace Control provides the capability to store logging and usage tracking in a separate database from the configuration information.

**Relay Server (optional)**

As of Workspace Manager 2012, the use of optional Relay Servers is supported. Relay Servers are data brokers between the high-availability database server and the Agents. Relay Servers can be chained together to support any enterprise network topology. The Relay Server is a lightweight component with a small footprint. It stores a cache of the Datastore. Agents relay data to and from the database via one or more Relay Servers which are automatically detected. Agents do not need a Relay Server to operate. For more information about Relay Server installation and prerequisites, please refer to the Workspace Control Relay Server documentation that is available at [http://forums.ivanti.com](http://forums.ivanti.com).

**Agent**

The Workspace Control Agent communicates with the Relay Server or Datastore and creates the local cache with the configuration data. The local cache is kept in sync by the Agent in the background and does not impact the workspace composition by the Workspace Composer. Communication intervals can be configured to optimize the network topology in place. Please refer to Workspace communication for more detail.

**Workspace Composer**

The Workspace Composer is responsible for the context detection and workspace composition. Any configuration data needed to manage the workspace is stored in the local cache by the Agent. This local cache is used by the Workspace Composer to build the desktop. There is, therefore, no direct dependency on the Relay Server or Datastore for a user to logon.

In multi-user environments, one Workspace Composer is active per session.
File Server

Workspace Control stores personalization data (personal settings) on a common file server. By default, the location for the personalization data is the user’s home directory. Most Microsoft Windows infrastructure have a home directory in place, which may prevent you from managing a separate storage for personalization data only. If necessary, this location can be changed.

Drivers

Drivers are used for security and personalization. In multi-user environments, one instance of each driver is active per system, shared with all sessions.

Console

Workspace Control is managed through the Workspace Control Console. The Console communicates directly with the Datastore and cannot work offline.

Management Portal

The Workspace Control Management Portal is an optional, web-based application that works alongside the Console. Currently, you can access Workspace Analysis, the Audit Trail, Security section from the Management Portal. For more information about the Management Portal installation and prerequisites, please refer to the Workspace Control Management Portal documentation that is available at http://forums.ivanti.com.
Distributed environment

The following illustrates an example of a distributed Workspace Control infrastructure with a central database and Relay Servers on each site:

Large sites can have multiple Relay Servers that serve Agents randomly. Placing multiple Relay Servers on a site increases availability of Relay Servers on that site.

Relay Servers can also be chained to each other.
## Chapter 3: Installation

### 3.1 Prerequisites

<table>
<thead>
<tr>
<th>Prerequisites</th>
<th>Software</th>
</tr>
</thead>
</table>
| **Software**  | The following Workspace Control installation file, available for download at the Ivanti Community:  
- Ivanti Workspace Control Installer [version].exe - This is an installation package that contains the MSI files for the Workspace Control components.  
  Individual components can be extracted from the installer and are also available for download.  
  If you want to use the Relay Server, separate installation files are required. The installation of Relay Server requires Microsoft .NET Framework 4.7 or higher. For more information, please refer to the document Getting Started with Workspace Control Relay Servers. |
| **Software installed on Agent** |  
- A supported operating system. See the Compatibility Matrix.  
- Microsoft .NET Framework 4.6 or higher for Ivanti Workspace Control versions 10.2 and earlier.  
- Microsoft .NET Framework 4.7 or higher for Ivanti Workspace Control versions 10.3 and later.  
- Microsoft .NET Framework 4.6 Client Profile or higher when using User Setting caching, for Ivanti Workspace Control versions 10.2 and earlier.  
- Microsoft .NET Framework 4.7 Client Profile or higher when using User Setting caching, for Ivanti Workspace Control versions 10.3 and later. |
# Prerequisites

## Hardware

- Each full installation of Workspace Control requires approximately 125 MB of hard disk space for the application files. This does not include the data stored in the local cache. The hard disk space required for cached data entirely depends on the configuration of your Workspace Control environment.
- Each Console-only installation of Workspace Control requires approximately 50 MB of hard disk space. These installations do not require any additional disk space for the local cache.
- Each Agent-only installation of Workspace Control requires approximately 75 MB of hard disk space.
- The memory needed for the Workspace Control Agent depends on the configuration. For example, in an environment with applications enabled and 100 authorized files configured, the Agent needs around 27 MB of memory during a normal user session (applications are running, other applications are started and stopped again).
- Each Agent requires drive space on the home drive for storing Workspace Control settings. As User Settings are stored in the same location, this amount increases if User Settings are available to the user. The required amount of space then depends on the size of the stored User Settings. All Workspace Control settings, including User Settings, are compressed when stored.

## Database

- A supported database. See the [Compatibility Matrix](#).

## Database prerequisites

<table>
<thead>
<tr>
<th>Database</th>
<th>Prerequisites</th>
</tr>
</thead>
</table>
| Microsoft SQL Server* | - Mixed Mode authentication (only when using SQL Server login for Authentication)  
- MDAC 2.6 or later on all Agents  
- A named SQL Server System Administrator login ID  
- If Force protocol encryption is enabled: Microsoft Native Client |
| Microsoft SQL Azure* | - Microsoft Windows Azure credentials  
- Microsoft SQL Server Native Client on all Agents connecting directly to the Datastore |
| Oracle | - Oracle DBA credentials  
- Oracle database drivers on all Agents connecting directly to the Datastore |
| MySQL | - MySQL DBA credentials  
- MySQL ODBC driver on the database server and on all Agents connecting directly to the Datastore |

* For Microsoft SQL Servers and Microsoft SQL Azure, if you have the option **Always On Failover Cluster Instances** enabled (High-Availability solution), in case a failover to a secondary database happens, (global) objects in the Management Console are displayed with a blue icon with an “i” inside. This means the objects have read-only access to the database at that moment.
3.2 Installation

The first step in setting up User Workspace Management is to install Workspace Control version 10.3 on the computer on which you want to manage User Workspaces. With the installation of Workspace Control version 10.3, the Management Console and an Agent will be installed.

- To install Workspace Control version 10.3 on your computer, use the Workspace Control Installer (Ivanti Workspace Control Installer [version].exe).

  The Workspace Control Installer is an installation package that contains the MSI files for the different components of Workspace Control, grouped in one executable making it easier to install all necessary Workspace Control components. When using the Workspace Control Installer, you can either Select and install components on the machine on which you are currently working or Extract all components for later use.

  Choosing the option Select and install components, allows you to select which component(s) should be installed on the machine. The installation wizard of the selected component(s) will then guide you through the actual installation. The Workspace Control Installer auto-detects whether the 64-bit or 32-bit version of the component(s) needs to be installed.

  You can install the following components:
  - **Clients**: Workspace Composer, Management Console
  - **Services**: Relay Server, Reporting Services
  - **Extra**: Desktop Sampler

- When extracting all components, individual MSI and EXE files will be saved in the specified location.

  Instead of installing Workspace Control fully, you can choose to perform:
  - an Agent-only installation, if you want to install Workspace Control without a Console (use Ivanti Workspace Control Agent [version].msi).
  - a Console-only installation, if you do not want to install a Workspace Control Agent on the computer on which you want to manage your environment (use Ivanti Workspace Control Console [version].msi).

  Please note that it is not possible to install an Agent-only and a Console-only installation side by side on the same machine. To go from a partial installation to a full installation, first uninstall the Agent-only or Console-only installation, then install the full Workspace Control.

When installing Workspace Control, the Setup Wizard will guide you through the installation process.

- After reading and accepting the End-User License Agreement and specifying the installation folder, you will be asked whether you want the Workspace Composer to launch the next time someone logs on to the computer. If you have not yet created a Datastore, select No, I will configure this later in the Management Console. This option is not available for installations on Terminal Servers and with Console-only installations.

- After the installation of Workspace Control has completed, the Connection Wizard will start. This wizard helps you to connect the installed Agent to a Workspace Control environment.
Warning

Workspace Control is an End User Workspace Management Product. Its brand purpose it to balance flexibility and control of the User workspace by means of Profile, Policy and Access Control management. The IWC Agent has been designed and tested to operate on both Single and Multi-user platforms (See Maintained Platform Matrix) to secure, manage and customize the End User experience. We do not recommend running the IWC Agent on Servers that operate Mission critical roles such as that of a Domain Controller. To deliver the earlier referenced end-user experience the Agent loads various drivers, hooks processes and intercepts system calls. Whilst these operations are all managed by means of configuration they do have the potential to disrupt mission critical operations and therefore should not be in use on backend operational servers.

Note

- Ivanti installation files are signed with certificates. Microsoft Windows tries to verify a certificate’s validity before installing software products. This process (Certificate Revocation List (CRL)) is run to check to see if a certificate was revoked because it was expired or compromised. This process is not unique to Ivanti and is something that happens for any product that contains a certificate and is run on Microsoft Windows (unless CRL is turned off which is not recommended by Microsoft). It is also possible under specific cases that a CRL check is done during process startup. An example of this is when the Workspace Control Agent Service is configured to connect to a Relay Server, it will perform a CRL validation on startup. A logon could potentially be delayed if the environment does not use a Corporate/Enterprise license and the user attempts to logon immediately after the restart of the computer or the service, before the CRL check has been done.
- On computers without Internet access, the CRL validation may cause a delay of, for example, 20-30 seconds before an installation starts. This is by design of Microsoft Windows. To avoid this delay to occur, make sure machines can connect to the Internet. If this is not possible, implement a (manual/automatic) distribution system to keep the publisher's certificate revocation lists up to date.
- For new installations of Workspace Control, the file capicom.dll will be installed if it is not yet present on the machine on which you install Workspace Control. Capicom.dll is a third-party component, supplied by Microsoft. The Capicom component version 2.1.0.2 (available at https://www.microsoft.com/en-us/download/details.aspx?id=3207) included in this Workspace Control release, is subject to the Microsoft Software License Terms, Microsoft Capicom, which solely govern End-User’s use of that component. By installing Workspace Control version 10.3 on a machine on which capicom.dll is not yet present, the End-User assumes and accepts sole responsibility of the use of the Microsoft Capicom component and compliance with the applicable license terms.

Also see

- Install Workspace Control Agent service under different account (on page 20)
- Unattended Installation (on page 21)
3.3 Install Workspace Control Agent Service under different account

1. Create a domain user account and assign **Log on as a service** and **Act as part of the operating system** through Domain Security Policy to this account.
2. Assign access privileges for this account to the database in SQL Server.
3. Use Orca MSI Editor to open the Workspace Control Windows Installer Package.
4. Select **Transform > New Transform** from the menu.
5. Select the **ServiceInstall** table from the list.
6. Change **StartName** and **Password** to the user account and password of the user account.
7. Select **Generate Transform...** from the menu and save the MST-file.
8. Invoke Windows Installer unattended and apply the transform (msiexec /i <msi> TRANSFORMS=<mst> /qn+). Tip: check with msiexec command-line parameters.
3.4 Unattended Installation

It is possible to perform an unattended installation of Workspace Control using a command line. This is useful if you need to install Workspace Control on several computers, and/or if you do not want to interrupt your users.

To install Workspace Control unattended on a computer, you can apply public properties to the Workspace Control installation package. In the next section, the available public properties are grouped per use case. Unless otherwise mentioned in their descriptions, each of these properties can be used for the full installation (Ivanti Workspace Control [version].msi), Agent only installation (Ivanti Workspace Control Agent [version].msi) and Console only installation (Ivanti Workspace Control Console [version].msi).
### 3.4.1 Installation public properties

The following public properties are available for general use during installation:

#### Installation settings

<table>
<thead>
<tr>
<th>Public property</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AI_DESKTOP_SH</td>
<td>1 (default) or 0</td>
<td>Specifies if desktop shortcuts should be created during installation of Workspace Control.</td>
</tr>
<tr>
<td>AI_STARTMENU_SH</td>
<td>1 (default) or 0</td>
<td>Specifies if Start menu shortcuts should be created during installation of Workspace Control.</td>
</tr>
</tbody>
</table>
| APPDIR            | <FOLDERPATH>           | Specifies the directory where Workspace Control will be installed. If not specified, Workspace Control will be installed in:  
|                   |                        | - C:\Program Files (x86)\Ivanti\Workspace Control (64-bit)  
|                   |                        | - C:\Program Files\Ivanti\Workspace Control (32-bit) |
| AUTORUNCOMPOSER   | YES or NO (default)    | Specifies if the Workspace Composer should start automatically when users log on to the Agent.  
|                   |                        | Does not apply to Console-only installations. |
| INHERITSETTINGS   | YES or NO (default)    | Specifies whether the Agent should revert to inherited settings after establishing its initial connection to the environment.  
|                   |                        | With NO (or INHERITSETTINGS not provided), the above-mentioned settings will be set specifically for the Agent, overruling inheritance.  
|                   |                        | With YES, the Agent will initially connect to the environment with the above-mentioned settings, but will then be set to inherit its connection settings (from a Workspace Model or from the global settings). |
| ADDTOWORKSPACE    | <CONTAINER1>|<CONTAINER2>       | Specifies the names of the Workspace Containers that this computer should be a member of after finishing installation.  
|                   |                        | Separate multiple Workspace Container names using bagpipes "|" (optional).  
|                   |                        | Does not apply to Console-only installations. |

**Example:** ADDTOWORKSPACE=Desktops|Marketing|64Bit
### Claim license

<table>
<thead>
<tr>
<th>Public property</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLAIMLAPTOPLICENSE</td>
<td>YES or NO (default)</td>
<td>Specifies if a concurrent (=laptop seat) license must be claimed and cached from a mixed license pool. By default, an Agent will not claim a license until a user starts a session on that Agent. Claiming a license requires the Agent to have connection to the Datastore or a Relay Server. If the first session on a laptop is offline, a license cannot be claimed and the license policy will apply unless a license was claimed and cached locally during the installation. Use CLAIMLAPTOPLICENSE with the value YES to claim a laptop seat license during the unattended install. (A license will be claimed for the laptop even if no user is logged on. Different users of the laptop use the same claimed laptop seat license). Other values or if left empty will result in the default behavior, which means that the laptop will attempt to claim a named license when a user starts a session.</td>
</tr>
<tr>
<td>CLAIMUSERLICENSE</td>
<td>&lt;DOMAIN&gt;&lt;USER&gt;</td>
<td>Specifies that a named user license should be claimed for a specified user and cached locally. By default, an Agent will not claim a license until a user starts a session on that Agent. Claiming a license requires the Agent to have connection to the Datastore or a Relay Server. If the first session on an Agent is offline, a license cannot be claimed and the license policy will apply unless a license was claimed and cached locally during the installation. Use CLAIMUSERLICENSE to claim and cache a named license for the specified user during the unattended install. When that user starts a session, a license is available and the session will proceed. Example: CLAIMUSERLICENSE=DEMO\ACavendish</td>
</tr>
</tbody>
</table>
Add Technical Managers

<table>
<thead>
<tr>
<th>Public property</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADDGROUPTOTECHMGR</td>
<td>&lt;GROUPNAME&gt;</td>
<td>Optionally adds the group to the Technical Manager Security Role.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Example:</strong> ADDGROUPTOTECHMGR=DEMO\DomainAdmins</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Does not apply to Agent only installations.</td>
</tr>
<tr>
<td>ADDUSERTOTECHMGR</td>
<td>&lt;DOMAIN&gt;&lt;USER&gt;</td>
<td>Optionally adds the user to the Technical Manager Security Role.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Example:</strong> ADDUSERTOTECHMGR=DEMO\Administrator</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Does not apply to Agent only installations.</td>
</tr>
</tbody>
</table>

Example:

```
Msiexec /i "C:\Ivanti Workspace Control [version].msi" APPDIR="C:\Program Files (x86)\RES Software\Workspace Manager" ADDTOWORKSPACE=TestWorkspace ADDUSERTOTECHMGR=DEMO\John ADDGROUPTOTECHMGR=DEMO\TestGroup AUTORUNCOMPOSER=yes CLAIMLAPTOPLICENSE=yes /qn
```
3.4.2 Create a new Datastore

If there is no existing database to which Workspace Control can connect, you can add the following public properties to create a new database during the unattended installation. After creating a new database, you can optionally import a license file and Building Block. Please note that it is not possible to create a new database when installing an Agent-only installation.

<table>
<thead>
<tr>
<th>Public property</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DBTYPE</td>
<td>MSSQL, DB2, ORACLE, MYSQL or MSSQLAZURE</td>
<td>Specifies the database type.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Example:</strong> DBTYPE=MSSQL</td>
</tr>
<tr>
<td>DBSERVER</td>
<td>&lt;SERVERNAME&gt;</td>
<td>Specifies the database server that Workspace Control should connect to.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Example:</strong> DBSERVER=SQLServer01</td>
</tr>
<tr>
<td>DBCREATE</td>
<td>YES or NO (default)</td>
<td>Specifies whether a new database should be created using the specified values.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Does not apply to Agent only installations.</td>
</tr>
<tr>
<td>DBCREATEUSER</td>
<td>&lt;USERNAME&gt;</td>
<td>Specifies the database user name that should be used to create the new database.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Example:</strong> DBCREATEUSER=SA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Does not apply to Agent only installations.</td>
</tr>
<tr>
<td>DBCREATEPASSWORD</td>
<td>&lt;PASSWORD&gt;</td>
<td>Specifies the database password that should be used to create the new database.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Example:</strong> DBCREATEPASSWORD=SAPassword</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Does not apply to Agent only installations.</td>
</tr>
<tr>
<td>DBPROTOCOLENCRYPTION</td>
<td>YES or NO (default)</td>
<td>Specifies whether protocol encryption should be used when connecting to Microsoft SQL Server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Please note, that the default value of this public property is different from the default setting when creating a new Datastore using the Management Console</td>
</tr>
<tr>
<td>DBCERTVALIDATION</td>
<td>YES or NO (default)</td>
<td>Specifies whether the certificate that is provided by the database server must be validated against the list of Trusted Root Certificate Authorities on the Agent.</td>
</tr>
<tr>
<td>DBFIPS</td>
<td>YES or NO (default)</td>
<td>Specifies that FIPS compliant security algorithms should be used to encrypt data in the database.</td>
</tr>
<tr>
<td>DBNAME</td>
<td>&lt;DATABASENAME&gt;</td>
<td>Specifies the name of the database that Workspace Control should create.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Example:</strong> DBNAME=Workspace</td>
</tr>
<tr>
<td>DBUSER</td>
<td>&lt;DBUSERNAME&gt;</td>
<td>Specifies the database user name that Workspace Control should create to connect to the database.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Example:</strong> DBUSER=WorkspaceUser</td>
</tr>
<tr>
<td>DBIMPORTLICENSE</td>
<td>&lt;FILEPATH&gt;</td>
<td>Specifies a license file to be imported after creating a new database (optional).</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Example:</strong> DBIMPORTLICENSE=C:\TEMP\License.xml</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Does not apply to Agent only installations.</td>
</tr>
</tbody>
</table>
Public property | Value | Description
--- | --- | ---
DBIMPORTBB | `<FILEPATH>` | Specifies a Building Block file to be imported after creating a new database (optional).

**Example:**

DBIMPORTBB=C:\TEMP\BuildingBlock.xml

Does not apply to Agent only installations.

Example:

When the server name is SQLSERVER01, the Database name is Workspace, username/password is WorkspaceUser/WorkspaceUserPassword, the license file is located at C:\license.xml, and connections to the Datastore must be secured, the command line would be:

```
Msiexec /i "C:\Ivanti Workspace Control [version].msi" DBSERVER=SQLSERVER01 DBNAME=Workspace DBUSER=WorkspaceUser DBPASSWORD=WorkspaceUserPassword DBTYPE=MSSQL DBPROTOCOLENCRYPTION=Yes DBCERTVALIDATION=Yes DBCREATE=Yes DBCREATEUSER=SA DBCREATEPASSWORD=SAPassword DBIMPORTLICENSE=c:\license.xml DBIMPORTBB=C:\buildingblock.xml /qn
```

Example using FIPS compliant security algorithms:

When the server name is SQLSERVER01, the Database name is Workspace, username/password is WorkspaceUser/WorkspaceUserPassword, the license file is located at C:\license.xml, and the Database must be FIPS compliant, the command line would be:

```
Msiexec /i "C:\Ivanti Workspace Control [version].msi" DBSERVER=SQLSERVER01 DBNAME=Workspace DBFIPS=Yes DBUSER=WorkspaceUser DBPASSWORD=WorkspaceUserPassword DBTYPE=MSSQL DBPROTOCOLENCRYPTION=No DBCREATE=Yes DBCREATEUSER=SA DBCREATEPASSWORD=SAPassword DBIMPORTLICENSE=C:\license.xml /qn
```
### 3.4.3 Connect to an existing environment

Using the following public properties, you can connect Workspace Control to an existing environment.

If you want to use dynamic Datstore configuration in your environment (Agents will obtain their Datstore connection settings from a DHCP server), it is not necessary to specify these settings in a command line when installing Workspace Control unattended. See Dynamic Datstore configuration for Agents (on page 37) for more information.

**Connect Workspace Control directly to a Datstore**

<table>
<thead>
<tr>
<th>Public property</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
</table>
| CONNECTFILE     | `<FILEPATH>` | Specifies the path and filename of a Workspace Control Datstore connection string stored in a text file. In a connection string, the database password is encrypted to prevent exposure.  
Create the connection string file from Primary Datstore properties at Setup > Datstore, in the Management Console.  
Example: `CONNECTFILE=C:\TEMP\Connectfile.txt` |
| CONNECTSTRING   | `<CONNECTIONSTRING>` | Specifies the connection string to connect to a Workspace Control Datstore. In a connection string, the database password is encrypted to prevent exposure.  
Create the connection string from Primary Datstore properties at Setup > Datstore, in the Management Console.  
Example: `CONNECTSTRING=RESPFDB=MSSQL;SRV=DB01.MyDomain.com;RESPFDBNAME;/<ENCRYPTED DATA>` |
| DBTYPE          | `MSSQL, DB2, ORACLE, MYSQL or MSSQLAZURE` | Specifies the database type.  
Example: `DBTYPE=MSSQL` |
| DBSERVER        | `<SERVERNAME>` | Specifies the database server that Workspace Control should connect to.  
Example: `DBSERVER=SQLServer01` |
| DBNAME          | `<DATABASENAME>` | Specifies the name of the database that Workspace Control should connect to.  
Example: `DBNAME=Workspace` |
| DBUSER          | `<DBUSERNAME>` | Specifies the database user name that Workspace Control should use to connect to the database.  
Example: `DBUSER=WorkspaceUser` |
| DBPASSWORD      | `<DBPASSWORD>` | Specifies the plaintext password that Workspace Control should use to connect to the database.  
Example: `DBPASSWORD=WorkspaceUserPassword` |
<table>
<thead>
<tr>
<th>Public property</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DBPROTOCOLENCRYPTION</td>
<td>YES or NO (default)</td>
<td>Specifies whether protocol encryption should be used when connecting to Microsoft SQL Server.</td>
</tr>
<tr>
<td>DBCERTVALIDATION</td>
<td>YES or NO (default)</td>
<td>Specifies whether the certificate that is provided by the database server must be validated against the list of Trusted Root Certificate Authorities on the Agent.</td>
</tr>
<tr>
<td>SERVICEACCOUNTNAME</td>
<td>&lt;DOMAIN&gt;&lt;USER&gt;</td>
<td>Specifies the account name that should be used as the Agent service account when using Windows authentication. The service account name must be a member of the Local Administrator group. When not using Windows authentication, providing SERVICEACCOUNTNAME is optional. If not provided, the Agent service will run under the LocalSystem account. Example: SERVICEACCOUNTNAME=MyDomain\AgentServiceAccount</td>
</tr>
<tr>
<td>SERVICEACCOUNTPASSWORD</td>
<td>&lt;PASSWORD&gt;</td>
<td>Specifies the plaintext password that should be used if a service account is specified for SERVICEACCOUNTNAME. Example: SERVICEACCOUNTPASSWORD=AgentServiceAccountPassword</td>
</tr>
</tbody>
</table>

Example:

Msiexec /i "C:\Ivanti Workspace Control [version].msi" DBSERVER=SQLServer01 DBNAME=Workspace DBUSER=WorkspaceUser DBPASSWORD=WorkspaceUserPassword DBTYPE=MSSQL DBPROTOCOLENCRYPTION=Yes DBCERTVALIDATION=Yes /qn

Msiexec /i "C:\Ivanti Workspace Control [version].msi" CONNECTFILE=C:\TEMP\WMDBconn.txt /qn

Example including the Agent service account:

When the server name is SQLServer01, the Database name is Workspace, Agent service account name/password is AgentServiceAccount/AgentServiceAccountPassword, the command line would be:

Msiexec /i "C:\Ivanti Workspace Control [version].msi" DBTYPE=MSSQL DBSERVER=SQLServer01 DBNAME=Workspace DBPROTOCOLENCRYPTION=No SERVICEACCOUNTNAME=MyDomain\AgentServiceAccount SERVICEACCOUNTPASSWORD=AgentServiceAccountPassword /qn
## Connect Workspace Control to a Relay Server

<table>
<thead>
<tr>
<th>Public property</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSENVGUID</td>
<td>&lt;GUID&gt;</td>
<td>Specifies the GUID that uniquely identifies the Workspace Control environment that the Agent should connect to. This GUID can be found in the Management Console, at Administration &gt; Relay Servers, on the Settings tab. <strong>Example:</strong> RSENVGUID={076FC22E-B7A1-477E-A021-94601893B568} Does not apply to Console only installations.</td>
</tr>
<tr>
<td>RSPASSWORD</td>
<td>&lt;PASSWORD&gt; or &lt;ENCRYPTED RSPASSWORD&gt;</td>
<td>Specifies the plaintext or encrypted password of the Workspace Control environment that the Agent should connect to. This password must already be set in the Administration &gt; Relay Servers node in the Management Console. When using an encrypted password, the public property RSPWENC must be specified as YES (see below) Does not apply to Console only installations.</td>
</tr>
<tr>
<td>Public property</td>
<td>Value</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| RSPWENC (version 10.2 and higher) | YES or NO (default) | Specifies whether the value that is specified at RSPASSWORD is encrypted. Technical managers can obtain the encrypted version of the Environment password by using one of the following command lines on a machine running the Management Console:  
- `pwrtech.exe /getrspassword`  
  With Ctrl+C, the encrypted password can be copied from the dialog box to the clipboard.  
- `pwrtech.exe /getrspassword /f=<full file path>`  
  The encrypted password is saved in the specified file at the given location.  
Alternatively, the encrypted password can be found in the XML configuration file that was generated on a Relay Server that connects to another Relay Server. Create the configuration file from the Relay Server Configuration Tool, by clicking Save to XML.  
Example: RSPASSWORD=<ENCRYPTED RSPASSWORD> RSPWENC=YES  
Does not apply to Console only installations. |
| ACCEPTSELFSIGNEDCERT (version 10.2 and higher) | YES or NO (default) | Specifies whether the Agent should accept a self-signed certificate from the Relay Server to secure the Agent - Relay Server connection.  
When installing Workspace Control version 10.2 or higher, use ACCEPTSELFSIGNEDCERT=YES if the Relay Server is not configured to use a certificate that was issued by a Trusted Root Certification Authority. |
| RSDISCOVER | YES or NO (default) | Specifies whether the Agent should discover Relay Server(s) using multicast.  
Does not apply to Console only installations. |
<table>
<thead>
<tr>
<th>Public property</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
</table>
| RSLIST          | <SERVERNAME1>:<PORTNUMBER>; <SERVERNAME2> | Specifies the list of Relay Servers to connect to, separated by a semicolon (;). When a Relay Server in this list uses a non-default listening port, its server name should be followed by a colon (:) and the listening port.  
**Example:**  
RSLIST=Server1;Server2:2012; Server3.MyDomain.com  
Does not apply to Console only installations. |
| RSRESOLVE       | <RELAY SERVER FQDN> | Specifies the FQDN of a Relay Server to be resolved by DNS.  
**Example:**  
RSRESOLVE=Relay.MyDomain.com  
Does not apply to Console only installations. |

**Examples:**

Msiexec /i "C:\Ivanti Workspace Control [version].msi" RSENVGUID={7C1FF8AB-5FC8-40C9-AB4C-E285A788A2C0} RSPASSWORD=password RSDISCOVER=yes/no  
RSLIST=server1;server2 RSRESOLVE=Relay.MyDomain.com /qn

Msiexec /i "C:\Ivanti Workspace Control [version].msi" RSENVGUID={7C1FF8AB-5FC8-40C9-AB4C-E285A788A2C0}  
RSPASSWORD=YuSaVRGyjk7LubF9LMzez3XMAexQF5xkADcRKM1Vd0gYQi6sPA2YRbFDg=  
RSPWENC=yes RSDISCOVER=yes/no RSLIST=server1;server2  
RSRESOLVE=Relay.MyDomain.com /qn
Pre-load Agent cache (ZIP file) during offline installations

With a pre-loaded cache, it is possible to install Agents in your Workspace Control 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.

Please note that no logging is available in the Datastore for the Agents with a pre-loaded cache until they connect to a Relay Server or directly to the Datastore.

<table>
<thead>
<tr>
<th>Public property</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CREATEFILEFROMCACHE</td>
<td>&lt;FILEPATH&gt;</td>
<td>Creates the ZIP file from the cache (.zip). Elevated privileges are necessary to run this command line. Make sure the ZIP file is stored in a secure location and can only be accessed by authorized Workspace Control administrators. Example: <code>&lt;IWC Installation folder&gt;\pwrcache.exe /CREATEFILEFROMCACHE=C:\temp\cache.zip</code></td>
</tr>
<tr>
<td>LOADCACHEFROMFILE</td>
<td>&lt;FILEPATH&gt;</td>
<td>Loads the cache to the Agent. Elevated privileges are necessary to run this command line. Example: <code>Msiexec /i &quot;C:\Ivanti Workspace Control [version].msi&quot; LOADCACHEFROMFILE=C:\temp\cache.zip /qn</code></td>
</tr>
</tbody>
</table>

3.4.4 Configure Agent connection after installation

After Workspace Control is installed, you can (re)configure the Agent connection to the Datastore or to a Relay Server using the command `res.exe /config`, followed by the relevant public properties. By default, `res.exe` is located in the SVC folder of the Workspace Control installation folder.

- Configuration to connect the Agent directly to the Datastore:
  `/config /DBSERVER= /DBNAME= /DBUSER= /DBPASSWORD= /DBTYPE= /DBPROTOCOL= /INHERITSETTINGS=`

- Configuration to connect the Agent to a Relay Server:
  `/config /RSENVGUID= /RSPASSWORD= /RSPWENC= /ACCEPTSELFSIGNEDCERT= /RSDiscover= /RSLIST= /RSRESOLVE= /INHERITSETTINGS=`

For more information about these public properties, see Installation public properties (on page 22) and Connect to an existing environment (on page 27).
3.5 Configure the Workspace Composer

You can make the Workspace available to the users, through the Workspace Composer. The Workspace Composer uses the data in the local data cache to build the User Workspace, including applications, menu items and settings to which the user is granted access. It is therefore important that the Workspace Composer starts automatically when the user logs on to a computer. In Workspace Control, you can set this up in the Management Console in the Administration section at the Agents node.

3.5.1 Configure Agents for desktop OS

If, during installation, you choose not to run the Workspace Composer automatically, you may change the shell later via the Workspace Control Console at Administration > Agents.

The Run Workspace Composer column on the Agents tab shows if an Agent is configured to start the Workspace Composer automatically when users log on. If the value in this column is Automatic (pending) or Manual (pending), the Agent cache has not been updated yet.

With the option Run Workspace Composer (in the context-menu of an Agent, or on the Settings tab of the Edit Workspace Control Agent window), you configure if the Workspace Composer should run automatically when a user logs on.

For Remote Desktop Servers, and Citrix XenApp/XenDesktop servers that do not have the Citrix Virtual Delivery Agent installed, this option is not available. See Configure Agents for server OS for information on how to start the Workspace Composer when users log on to these servers.

The Run Workspace Composer column on the Agents tab only reflects the status of the option Run Workspace Composer configured in Workspace Control. This status does not take into account, for example, Microsoft Group Policy Objects or Active Directory configuration to start the Workspace Composer automatically.

3.5.2 Manual Configuration for desktop OS

Setting the Run Workspace Composer option to Automatic sets specific registry keys. Of course, it is also possible to set these values manually. Use the registry key located in:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon.

Edit the value "Shell" (REG_SZ) and set the data field to the location of “pwrstart.exe” (by default, this is at C:\Program Files\Ivanti\Workspace Control\pwrstart.exe).

For VDI environments, this registry setting can be applied to the Golden Image, or to individual virtual desktops using, for example, Automation. Alternatively, you can apply this setting in Active Directory, using Microsoft Group Policy Preferences.

If you want a user-specific Shell, you need to set the applicable registry keys manually. Use the registry key in:

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon.

Create a new value "Shell" (REG_SZ) and set the data field to the location of pwrstart.exe (by default, this is at C:\Program Files\Ivanti\Workspace Control\pwrstart.exe).
3.5.3 **Configure Agents for server OS**

If you use server-based computing and you want all users to log on to a session with the Ivanti Workspace Composer, you can configure this in the Microsoft Group Policy Object Custom User Interface. Go to User Configuration > Administrative Templates > System > "Custom user interface" and fill in the correct path to pfwsmgr.exe.

When using one of these options, Workspace Control will start as the Shell in a user session and the Windows Desktop will not be started.

Use the following steps to configure this in a GPO.

1. **Create the GPO:**

   Go to User Configuration > Administrative Templates > System > "Custom user interface"
   Enter the correct path: `%respfdir%\pfwsmgr.exe`

2. **Enable loopback processing on this GPO:**

   Go to Computer Configuration > Administrative Templates > System > Group Policy > "Configure user Group Policy loopback processing mode"
   Enable this setting in Replace mode.

3. **Enable synchronously processing of Group Policies:**

   Go to Computer Configuration > Administrative Templates > System > Logon > "Always wait for the network at computer startup and logon"
   Enable this setting.

4. **Configure security to the GPO:**

   On the security tab of the GPO-properties add the group holding all users you want a Managed Desktop for.
   You can remove (or deny) the "apply-rights" for your administrator accounts.

   The Authenticated Users group needs Read Permissions on the Group Policy Object (GPO) if KB3159398 in Microsoft Security Bulletin MS16-072 has been applied.

5. **Link the GPO:**

   Link the GPO to The OU where your RDS Servers/Citrix Servers exist in Microsoft Active Directory.
Chapter 3: Installation

3.6  Set up the Datastore

After installing Workspace Control and optionally changing the Shell to the Workspace Composer, it is time to create a Datastore or to connect to an existing one.

3.6.1  Configure the Datastore

When you start the Console for the first time and there is no Datastore connection yet, you will be prompted to either create a new Datastore or connect to an existing one.

To create a new Datastore, click Create. This opens the Datastore wizard, which guides you through the process.

- Follow the prompts to provide:
  - the database server type and name and any relevant (existing) DBA credentials.
  - a name for the database that will become the Workspace Control Datastore.
  - database file locations.
  - a user name and password to access the Datastore from the Workspace Control Console.
    - With Authentication set to SQL Server Login, the wizard will create a new SQL Server login with the necessary permissions.
    - With Authentication set to Windows account, Database permissions will be based on membership of a specified Active Directory group. The Workspace Control Agent Service on every Agent must be configured to run under an account that is member of that Active Directory group.
    - Using Windows authentication with designated account (see page 72), you can optionally specify a designated account to use for Console-users who are not member of that Active Directory group.
  - the Workspace Control license edition you wish to evaluate.
  - You can create a Datastore that uses Federal Information Processing Standard (FIPS) compliant security algorithms by selecting the option Use FIPS compliant security algorithms on the New database properties page of the wizard.
    - This option is only available for new Workspace Control Datastores and all Management Consoles, Agents, and Relay Servers must be running on RES ONE Workspace 2015 or higher.
    - In migration scenarios, it is possible to import Building Blocks to fill your Datastore. Please refer to the Workspace Control version 10.3 Upgrade Guide for more information on these Building Block scenarios.
    - Please note that it is not recommended to make your Workspace Control environment only use FIPS compliant security algorithms, if not all components have been upgraded. In a mixed environment with RES Workspace Manager 2014 SR3 or lower and RES ONE Workspace 2015 or higher, some functionalities are not working.
  - After clicking the Finish button in the final step of the Datastore Wizard, the Datastore will be created. When the Datastore has been created, the Console will refresh, after which all nodes will be available.
3.7 Configuration Wizard

After creating the Datastore, the configuration wizard will automatically start and guide you through setting up a basic configuration in Workspace Control in a few easy steps. When setting up a new Workspace Control site you have the choice to create scenarios and features for either Evaluation or Production purposes. When you choose Evaluation, the Configuration Wizard will set the options to create example objects for selected features. For Production purposes, these options will not be set.

Configuration for a new Workspace Control site

- When starting the configuration wizard, an introductory window will be shown welcoming you to the configuration wizard. You can either choose to view the online tutorial to be informed about the concept of workspace management or click Next if you already know our product.
- You will be asked to select the type of Workspace Control site you wish to create.
- Select one or more Workspace Containers to create. Workspace Containers are logical groups of Agents (for instance, physical or virtual desktops, laptops or remote desktop servers). At least one Workspace Container must be selected. Besides the Workspace Containers you selected, a Workspace Container "Unmanaged desktops" will be created, with all features disabled. The settings for the other Workspace Containers will be determined in the next steps of the wizard. If you want to know more about Workspace Containers click View tutorial or click Next.
- Select the features you want to start using. Depending on the module(s) you selected when creating the Datastore, more or less features may be available. Use Ctrl + A to (de)select all features. These features will be configured per Workspace Container. Click Next.
- Specify the settings for each feature you selected in step 4. Most features can be enabled or disabled by selecting the relevant check box under the Workspace Container heading. If you want to create example objects for the feature you enabled, select the check box Create example objects. Example objects are disabled by default when they are created. If you want more information about a specific feature (for example, Workspace performance or Application Management), click View tutorial. After you have specified the settings per feature, click Next.
- Additionally, the following example objects (besides the example objects you selected with the feature selection) can be selected:
  - Managed Applications
  - Settings executed at the start of a user session
  - An Administrative Role "Helpdesk"
  - Location-based printing
- Click Next.
- Your site configuration settings are shown in a summary. If you want to change any of the settings click Back; if you agree with the settings, click Next.
- The configuration process will start, showing status and result information.
- In the final step, you will see that the configuration has been completed and an Action list is shown, stating the items you still have to configure manually. The Action list must be saved or copied on the clipboard. You can use the Action List afterwards as a reminder of the items you still have to configure. Click Finish.

After closing the configuration wizard, you will return to the top node in the Console: the Navigation map.

Note

If you click Cancel during any of the steps of the configuration wizard, the wizard will exit without changing anything in the configuration of the site. The next time the Console is started, the configuration wizard will start up automatically, as long as no configuration items have been saved.

Running the Configuration Wizard in an existing site can be used to create example objects. See Configuration Wizard for existing Workspace Control site (on page 70).
3.8 Dynamic Datastore configuration for Agents

Each Agent is configured to connect to a specific Datastore when it runs a Workspace Control session. Normally, each Agent always connects to the same Datastore: the Datastore specified in the Console at Datastore in the Setup menu. In environments with multiple, replicated Datastores, this setup can cause problems for users on laptops or other mobile devices. In such cases, you can set up dynamic Datastore configuration.

Dynamic Datastore configuration uses the DHCP servers in your network. A DHCP server not only allocates IP addresses to Agents, but can also be used to provide other information. To set up dynamic Datastore configuration, you store Datastore connection information in Server options or Scope options on the DHCP servers in your environment. When a computer connects to the network, the operating system ensures that the Datastore connection information on the local DHCP server is transferred to the computer's registry. When the Workspace Control Agent starts up, it will use the information in its registry to connect to a Datastore.

3.8.1 Configure the Datastore dynamically

Note: The following procedure is based on DHCP server with Microsoft Windows Server 2016. Procedural steps may differ for other server versions.

For each DHCP server in your environment, do the following:

- Open the Console on a computer from which the Console connects to the Datastore that should be specified by the DHCP server.
- At Datastore > Connections in the Setup menu, click . This opens the Primary Datastore properties window. Click Export to open the Export Database connection string window, containing an encrypted string of the Datastore connection settings.
- Click the Copy to clipboard button or click the Export to file button to export the string into a text file for later reference.
- Close the Console.
- Log on to the DHCP server and open the DHCP snap-in.
- Select the DHCP server in the list and click Action > Set Predefined Options. This opens the Predefined Options and Values window.
- At Option class, select Microsoft Windows 2000 Options.
- Click Add to add an option. This opens the Option Type window, in which you can specify a name for the option (for example, "Workspace Control").
- At Data type, select String.
- At Code, specify an option ID with a free number in the range from 0 until 255. See http://www.networksorcery.com/enp/protocol/bootp/options.htm for a list of usable options.
- At Description, specify a description for the option and click OK.
- At String, paste the database connection string that you copied from the Console and click OK. This string may not exceed 255 characters.
- Right-click either the Scope Options node or the Server Options node (depending on the option that you want to configure) and choose Configure Options. This will open either the Scope Options window or the Server Options window.
- On the Advanced tab, select Microsoft Windows 2000 Options in the Vendor class field.
- In the Available Options area, browse to the option that you created earlier and select its check box. This will also show the string value that you specified earlier.
- Click Apply and OK.
- Repeat the process for all your DHCP servers, making sure that each DHCP server refers to the correct Workspace Control Datastore.
Notes

- When specifying Scope options or Server options at your DHCP servers, you can only use option class Microsoft Windows 2000 Options.
- If the Datastore as specified by a DHCP server cannot be reached, the Agent will automatically revert to its last known Datastore connection settings.
- To set a specific Agent to ignore the DHCP information, set the registry key `HKEY_Local_Machine\Software\RES\Workspace Manager\DisableDHCP` in the registry of the Agent, with value "True", "yes" or "1".
- In the node Administration > Agents, the Connection column reflects how an Agent obtained its Datastore connection settings.
  - **Local** specifies that the Agent connects to the Datastore using its local settings.
  - **DHCP** specifies that the Agent connects to the Datastore using the settings of a DHCP server.
  - **Local (DHCP disabled)** specifies that the Agent connects to the Datastore using its local settings and that location sensing has been disabled for the Agent.
- Configuring location sensing in your environment can also be very useful when performing unattended installations of Workspace Control. When configured, an Agent will obtain its Datastore connection settings from a DHCP server: it is not necessary to specify these settings in a command line when installing Workspace Control unattended. See Getting Started with Workspace Control for more information.

3.8.2 Example

IvantiDemo has its head office in New York, and the Workspace Control Datastore is located on a server there. The IvantiDemo satellite office in Singapore uses a replicated Datastore, because Agents in Singapore cannot connect directly to the Datastore in New York.

Amanda Cavendish is based in the New York office, and her laptop uses the New York Datastore. Wu Shen is based in Singapore, and his desktop computer uses the Singapore Datastore.

In the setup with fixed Datastore configuration for Agents, Amanda cannot start a Workspace Control session on her laptop if she is in the Singapore office: the Agent on the laptop tries to connect to the New York Datastore, which cannot be reached from the Singapore office. It would make more sense for her laptop to connect to the replicated Datastore in Singapore while she is there.

With dynamic Datastore configuration, you can create a setup where Amanda's laptop automatically connects to the New York Datastore when she is in New York, and to the replicated Datastore in Singapore when she is in Singapore.
3.9 Relay Servers

Relay Servers cache information from the Datastore and pass it on to Agents upon request, so that Agents do not need to contact the Datastore directly. Alternatively, Relay Servers can pass the cached information from the Datastore on to other Relay Servers.

For further details about Relay Servers, see the document *Getting Started with Workspace Control Relay Servers*.

Relay Servers that are assigned to a Workspace Control environment can be found in the Management Console at Administration > Relay Servers.

Tip
For optimum security, we recommend that Agents connect to Relay Servers; and that Relay Servers with a Datastore connection use a service account (Windows credentials) and SQL encryption to connect to SQL Server.

3.9.1 Configure Relay Servers

Relay Servers are configured to host Workspace Control environments in the Relay Server Configuration tool. For each environment, you can select if the Relay Server connects to the Datastore directly or to other Relay Servers in that environment.

When a Relay Server is assigned to an environment, specific Workspace Control settings can be configured on the Settings tab of Administration > Relay Servers.

- With Fetch change information, you determine the interval at which Relay Servers check whether they need to download any changes that have been made in the Datastore. A longer interval reduces network traffic.
- Push change information - Select to push change notifications to the Relay Servers that are connected to another Relay Server. These Relay Servers then check for change notifications every 5 seconds.
- The time span set at Update relay server cache on change determines the timing for Relay Servers to download data and update their cache. A short interval increases the speed at which changes are reflected, but also increases network traffic. A longer interval decreases network traffic, but there is a delay before Relay Servers reflect any configuration changes.
- By default, synchronization of a Relay Server’s cache with the central Datastore is aborted if an error occurs. If this happens, the cause of the failure must be solved before Relay Servers can be synchronized successfully. If this is undesirable, change the Synchronization policy to Continue on error.
- The Environment name is a name by which this Workspace Control environment is identified in the Relay Server Configuration tool, making it easier to select the correct environments to host on a Relay Server.
To secure your Relay Servers from unauthorized access, please provide an environment password before installing the first Relay Server. All Relay Servers will require this password before accepting a connection from an Agent or child Relay Server. To set or change the password, choose **Manage environment password**.

When changing an existing password, Agents will by default automatically be updated with a new password; and the old password will be honored during a grace period of 30 days. This grace period ensures that Agents using the old password can connect and receive the updated password. To change the password immediately, without any grace period, clear the option **Update Agents and Relay Servers with the new password and keep old password valid for 30 days**. You will need to manually change the password on all Agents by running "%respfdir%\svc\res.exe /config"; and on all Relay Servers by using the Relay Server Configuration tool.

You can export Relay Server connection information from Workspace Control by clicking **Export Connection string to file**. The **Workspace Control Relay Server** window then opens and allows you to select one or more Relay Servers to pre-populate the connection string. The Relay Server connection string will be exported to a text file.

Some of these global settings can be overruled for individual Relay Servers.

**Notes**

- If your Workspace Control environment contains a Relay Server, Event Logs are updated asynchronously. This can cause ‘missing file’ errors in Event Logs. These errors will disappear automatically when the Relay Server has processed all data and the Event Log has been fully updated.
- Event Logs are available when viewing the detailed Workspace Analysis of a user at **Diagnostics > Workspace Analysis**.
- As of RES Workspace Manager 2012, the traffic between two Relay Servers is compressed by default. The traffic between Relay Servers and Workspace Control Agents is compressed as well.
- Upgrading Relay Servers can be done when necessary and one by one in no particular order.
3.9.2 Dynamic Relay Server configuration

Dynamic Relay Server configuration uses the DHCP servers in your network. To configure dynamic Relay Server configuration, you need to add Relay Server connection information as Server options or Scope options on the DHCP servers in your environment. When computers connect to the network, they will receive parameters defined at scope level from the DHCP servers. This allows Relay Server connection information defined in DHCP scope to be transferred to the computer’s registry. When the Workspace Control Agent starts up, it will use the information in its registry to connect to the proper Relay Server.

You can export Relay Server connection information from Workspace Control to easily add it to the DHCP Scope. To export this data, at Administration > Relay Servers, on the Settings tab, click the button Export Connection string to file. The Workspace Control Relay Server window then opens and allows you to select one or more Relay Servers to pre-populate the connection string. The Relay Server connection string, in the first DHCP option 'RESWMRS=...', will automatically include all known items (Relay Server name(s) (with port number if a different than the default port number 1942 was specified), Environment ID and password, FQDN name (DNS)).

In the connection string, if the Relay Server list exceeds 253 characters, Workspace Control will automatically generate new lines with 'RESWMRSLIST=...' for the remainder of the Relay Server list. It is important to add all lines to the DHCP servers in your environment.

The Relay Server connection string will be exported to a text file. The lines in the text file need to be added as Server options or Scope options on the DHCP servers in your environment.

Example - Relay Server names in the Relay Server connection string:
- relay1.example.com:2012 (Relay Server name with port number 2012)
- relay2 (Relay Server name without port number)

Example - an FQDN name in the Relay Server connection string:
- FQDNrelayserver.res.com

For more information about how to configure your DHCP server, see Configure the Datastore dynamically (on page 38).

Note

A restart of the Agent service is necessary for the change in connection to take place.
3.10 Agents

The **Agents** node (at **Administration**) allows you to view and change the settings of all Agents in your environment and the way in which they are identified. The **Agent Overview** in the **Diagnostics** section shows a read-only overview of these settings.

3.10.1 Agents Settings

At the **Agents** node, you can change the following settings:

**Fetch change information**

All configuration data in the Datastore is cached to the Agent. Because most Workspace Control components use this cached data instead of directly connecting to the Datastore, this significantly reduces the load on the central Datastore and eliminates it as a single point of failure in a Workspace Control environment.

The local cache is kept up-to-date by the Workspace Control Agent Service, which is also responsible for uploading log and Usage Tracking information to the Datastore/Relay Server. If a connection to the Datastore/Relay Server is not available, all log and Usage Tracking information will be cached locally until the connection is re-established.

The setting **Fetch change information** determines the interval at which Agents check whether they need to download any configuration changes, but also whether they need to execute any tasks. A longer polling interval means that it takes longer before Agents execute tasks, such as remote publishing to Citrix XenApp servers, forcing a session refresh, restoring User Settings from the Workspace Control Console, sending messages to users, and disconnect, log off and reset users.

- Select **Push change information** to push change notifications to the Agents that are connected through a Relay Server. These Agents then check for change notifications every 5 seconds. After the Agent has processed the change notification, configuration changes, for example adding a printer, are fetched and applied according to the interval specified for the option **Update agent cache on change**. Tasks, such as the tasks mentioned for the option **Fetch change information**, are fetched and applied immediately.

The settings **Fetch change information** and **Push change information** can be configured at global level (applies to all Agents) and for individual Agents (by editing the **Settings** of an Agent):

- **Every <period>:** checking the database will occur at the selected interval. A longer interval decreases the traffic on your network but delays the execution of tasks and lengthens the time during which Agents are not aware they need to update their cache to reflect any changes in the Datastore.

**Update agent cache on change**

The time span set at **Update agent cache on change** determines the timing for Agents to download data and update their cache. A short interval may result in many Agents starting to download data simultaneously. A long interval will spread the network load more evenly, but as a result it will take longer before all Agents reflect the necessary changes.

**Update agent cache on change** can be configured at global level (applies to all Agents) and for individual Agents (by editing the **Settings** of an Agent):

- **Immediately:** each Agent will update its local cache as soon as it the fetch change information mechanism detects a relevant change in the Datastore. If many Agents detect changes at the same time, they may all start downloading data at the same time.

With the option **Push change information** enabled, it is recommended to set the option **Update agent cache on change** to any other value than **Immediately**. Setting this option to **Immediately** will cause all Agents in your environment to immediately connect to the Relay Server and fetch the configuration changes.
- **Within <period>:** the update of the local caches will be randomized and spread out over the selected period. Although this decreases the traffic on your network, it also means that the local caches on your Agents will not immediately reflect any changes in the Datastore.

You can also update Agent caches immediately from the context menu.

**Synchronization policy**

The synchronization policy of Workspace Control determines what should happen if the synchronization of an Agent fails. The policy that you select will first be applied when you click **Save Settings** (global level) / **OK** (Agent level). The setting **Synchronization policy** can be configured at global level (applies to all Agents) and for individual Agents (by editing the **Settings** of an Agent):

- **Abort on error:** the synchronization process will be aborted if the synchronization of an Agent fails (for example, because it is not possible to update the local cache or because an error occurs). If this happens, you first have to correct the cause of the failure before the synchronization of the Agent will be successful again. This option is selected by default.
- **Continue on error:** the synchronization process will continue, even if an error occurs.

If a synchronization fails, Workspace Control will attempt a new synchronization after minimally one hour, irrespective of the synchronization policy that you specified.

**Identify Agents by**

By default, Agents are identified by Computer domain name and NetBIOS name. At **Identify Workspace Control Agents**, select a different method of identification if:

- the operating system is re-installed on Agents.
- several virtual machines use the same image.
- several computers are deployed using imaging.

**Automatic Agent Removal**

- **None:** inactive Agents will not be removed automatically.
- **After 45 / 60 / 90 / 120 days of inactivity:** the RES Service or Relay Server will remove inactive Agents after the specified number of days of inactivity (45, 60, 90, or 120)

Please note that automatically removing inactive Agents will not remove Agents on Citrix XenApp servers, as they may be used for application publishing.

**Datastore connection**

You can configure the default behavior of Agents: **Connect directly to the Datastore or Connect through Relay Server**. If they should connect to relay servers, you can select the **Connection method(s):**

- **Discover (using multicast):** Relay Servers in the environment will be discovered automatically
- **Preconfigured (using list):** Relay Servers will be selected according to the provided list. The Relay Servers can be entered manually, or previously discovered Relay Servers can be selected from the list.
- **Resolve name (using DNS):** The FQDN of a Relay Server will be resolved through DNS.

These connection options do not exclude one another and can be used in combination.

For Linux and Apple Mac OS X Agents, the connection options are limited to **Inherited** and **Connect through Relay Server**.
Run Workspace Composer automatically

You can configure Agents to run the Workspace Composer automatically from the context menu, and by editing the Settings of an Agent:

- **Automatic**: the Workspace Composer will run automatically when users log on.
- **Manual**: users need to start the Workspace Composer manually (for example, from the Start Menu).

These settings are reflected in the Run Workspace Composer column in the Agents list. If the column shows the value Automatic (pending) or Manual (pending), the Agent cache has not been updated yet.

- This option is not available for Terminal Servers that are not Citrix XenApp/XenDesktop servers.
- For Agents running on Citrix XenApp special considerations apply. See the document Migrating Existing Citrix XenApp Published Applications to Workspace Control, where various scenarios are explained, depending on whether you want to republish your existing Citrix published applications or want to manage them using the Intercept option if managed shortcut was not used. The setting Run Workspace Composer of the Agent must be configured according to the scenario you choose. The workings of the Intercept option are discussed in the section Composition, Application Properties, General of this Administration Guide.

Workspace Container membership

You can configure membership of Workspace Containers of Agents at User Context > Workspace Containers, but also by editing the Settings of an Agent.

Deleting Agents

Deleting Agents can be useful if Agents have become obsolete or if they, for some time, fail to synchronize with a Datastore in your environment. If you delete an Agent, but it manages to re-establish a connection to a Datastore in your environment, it will automatically be included again in the list of Agents.
Notes

- The **Agents Overview** node shows a read-only overview of all Agents and their settings.
- If you use identification method MAC address of the first enabled network interface and an Agent has multiple network cards, Workspace Control will use the MAC address of the first enabled network card, based on the order as defined on the agent by Microsoft Windows. You can find this order in Microsoft Windows by clicking **Start > Settings > Network Connections > Advanced > Advanced Settings**.
- When using Workspace Control in combination with Citrix XenApp/XenDesktop 7.x, the **XenApp version** and **Server farm** columns in the **Agents** node and **Agents Overview** node will only contain data if the Agent is a member of a Citrix Delivery Group.
- The **FQDN** column displays the Fully Qualified Domain Name, once the option **Use computer's FQDN instead of domain\computername in Logs and Usage tracking** has been enabled at **Advanced Settings** in the **Setup** menu.
- The columns **AppGuard version**, **NetGuard version**, **RegGuard version**, **ImgGuard version**, and **WebGuard version** in the **Agents** node and **Agents Overview** node reflect the internal driver versions that Workspace Control uses. These version numbers can be used for troubleshooting purposes, should issues arise in your environment following an upgrade or downgrade or after installing a revision.
- The **Synchronization status** column in the **Agents** node and **Agents Overview** node shows when the last synchronization of an agent took place and whether this was successful.
- Licensing information is always updated immediately, irrespective of the settings that you specify.
- When using Relay Servers, we recommend creating separate Workspace Containers for each subsite with different Relay Server lists. This way, it is easy to identify to which Relay Server an Agent or group of Agents normally connects.
- An Agent can connect directly to the Datastore OR it can use Relay Servers.
- An Agent configured to connect to Relay Servers will never connect to the Datastore directly. If it cannot connect to a Relay Server, it will use information stored in its local cache. An Agent configured to connect to the Datastore directly will never connect to Relay Servers. If its connections are not available, an Agent will use information stored in its local cache.
- The **Push change information** option has been introduced in RES ONE Workspace 2015. To use this option successfully, all components must be running this version or higher.
- On the **Agents** node, the value for **Run Workspace Composer** will not change when setting the registry value **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell to pwrstart.exe or pfwsmgr.exe**.
- In VDI environments that use a non-persistent/pooled model, and where the Workspace Control Agent cache is stored on a persistent disk, most likely the latest versions of the UpdateGUIDs and Workspace Control policy settings are not in the registry of the golden image/template. Therefore, the cache will be updated with information from the Datastore or Relay Server, even though the most recent versions of the cache files are already present in the Workspace Control cache on the persistent disk. The update causes I/O load and network traffic. With the registry value **LocalCacheOnDisk** it is possible to make the cache independent of the Operating System's (OS) registry. Setting this registry value will convert the UpdateGUIDs and policy settings automatically from the OS' registry to two new XML files in the Workspace Control DBcache folder on the persistent disk: **UpdateGUIDs.xml** and **Settings.xml**. See **LocalCacheOnDisk** (on page 354) for more information.
Check the connection settings of an Agent to a Datastore or Relay Server

For troubleshooting purposes, you can check the settings that Agents use to connect to a Datastore or Relay Server. You can do this by running the command "%ProgramFiles%\Ivanti\Workspace Control\svc\res.exe" /config on every relevant machine.

After running the command, the Workspace Control Agent - Configure connection window will open. If necessary, use this window to make any changes to the connection settings to the Datastore or a Relay Server. For example, you can change the settings of the Agent from a direct Datastore connection to a connection through a Relay Server and vice versa.

- In the **Connection type** field, select either **Database** or **Relay Server**.
  - If you select **Database**, specify the settings to connect to the Workspace Control Datastore.
  - If you select **Relay Server**, specify the settings to connect to the Relay Server:
    - Select **Discover (using multicast)** to let Agents find a Relay Server (for the correct environment) automatically.
    - Select **Preconfigured (using list)** to let Agents try connecting to a Relay Server from a list in random order. Use semi-colons (;) to separate servers.
    - Select **Resolve name (using DNS)** to use DNS to resolve the FQDN of a Relay Server. This is particularly useful to identify a Relay Server that can be reached by Agents connecting from outside the network.
  - The specified connection methods are handled in order of appearance; the Agent will stop looking for additional connections as soon as a valid connection is found. Therefore, if all three methods are configured and enabled, an Agent will proceed as follows:
    - Did discovery yield a Relay Server? If so, it will use that Relay Server. If not, try the list.
    - Did the list yield a Relay Server? If so, it will use that Relay Server. If not, try the fallback Relay Server. This means that if the options Discover and Preconfigured did not yield a Relay Server, the Relay Server will be tried that is specified at Resolve (using DNS).
    - Can DNS resolve the FQDN to a Relay Server that can be reached? If so, it will use that Relay Server. If not, it will use local cache.

- In the **Once connected to the datastore**:
  - Select **Keep using specified settings** to let the Agent connect to the Datastore with the specified settings. These settings will be stored as specific settings for the Agent: the Agent will keep connecting with these settings from that point on.
  - Select **Use connection settings from datastore** to let the Agent initially connect to the Datastore with the specified settings. When connection has been established, it will then look in the Datastore to see which connection settings should be used (the Agent's global settings, Workspace exceptions).
  - Instead of typing the connection settings of the target Datastore manually, you can also copy the connection string from the clipboard (by clicking the **Copy from clipboard** button) or import these settings from a TXT file (by clicking the **Import from file** button).
  - **Copy from clipboard** and **Import from file** buttons can be used to copy connection settings of the target Datastore to the local Agent. The **Import from file** option only supports TXT files.
  - To test the specified connection settings, click **Test**.
3.11 Keep Workspace Control up to date

You can keep your version of Workspace Control up to date by installing Workspace Control Upgrade Packs, that contain new functionality, enhancements of existing functionality, and resolved issues.

Solution Assurance

Upgrade Packs require Solution Assurance. Solution Assurance is a service that you can buy from Ivanti, based on a yearly subscription. If you subscribe to Solution Assurance, you are entitled to technical support, product upgrades, and access to the Online Knowledge Base.

When you buy Workspace Control, Solution Assurance is automatically included for one year. After that first year, your Solution Assurance subscription is automatically renewed, unless you cancel it. For more information about Solution Assurance, please contact the Sales department.

If you are entitled to Solution Assurance, you can download Upgrade Packs at http://forums.ivanti.com. Here, you can also download general and technical documents about Workspace Control.

Installation

- Upgrade Packs must be installed on each machine running Workspace Control. They can be installed by double-clicking the file and completing a setup wizard.
- Before using Auto Upgrade Packs, you need to install at least one Upgrade Pack manually once. This ensures that the Datastore is correctly updated. After this first Upgrade Pack, you can install Auto Upgrade Packs on all other computers.
- Auto Upgrade Packs are installed unattended. This does not require your attention and can be scheduled for a specified time.
- The installation of Upgrade Packs / Auto Upgrade Packs may require a reboot of the system.

The new version of Workspace Control becomes available to users when they start a new session.

Downgrade

- Initial installations of RES ONE Workspace version 10.1 or higher, or Workspace Control version 10.2 or higher cannot be downgraded to a version of RES ONE Workspace before version 10.1. In such cases, Workspace (Control) must be completely uninstalled before the installation of the earlier version can be done.
Note

30 days after installing Workspace Control for the first time, or 30 days after creating a new Datastore, the Software Improvement Program wizard will automatically be displayed on screen when starting the Console. The Software Improvement Program gives you the opportunity to contribute to the design and development of Workspace Control. When you enroll in the program, Ivanti collects anonymous information about your deployment, which is used to improve product quality, reliability, and performance. At all times, you can control the information that is supplied to Ivanti.

On the start screen of the wizard, you can specify at what level you would like to participate in the Software Improvement Program:

- **Yes, I agree that feature usage information is submitted:** every 90 days usage information about your site will be sent to Ivanti
- **No, only submit version information:** the version you are currently using will be sent to Ivanti
- **Ask me again in 30 days:** you will receive a reminder after 30 days.

Clicking *More information* will display the information that will be sent to Ivanti.

If no level of participation has been selected, a reminder will automatically be displayed on screen after 30 days. Once *Yes, I agree that the feature usage information is submitted* or *No, only submit version information* has been selected, the possibility *Ask me again in 30 days* will not be available anymore. You can change your level of participation at any time at Help > Software Improvement Program.

Any information that is being sent to Ivanti is for internal use only. Your information will be kept entirely confidential and used only by authorized members of Ivanti staff. Ivanti will never disclose your information to third parties without your consent. The information will not be used to contact you.

Tip

When installing an upgrade pack of Workspace Control, Release Notes of current and previous versions are available in the Console under the menu Help.
3.12 Workspace Control Modules

The Workspace Control product family consists of different modules in which different sets of Workspace Control version 10.3 features are available:

**Workspace Control Core**

**Workspace Control Core** is the free starter package offering basic Workspace Control functionality. It supports 25 named users when unregistered and supports unlimited named users when registered. Workspace Control Core contains:

- **Basic Workspace Composition:**
  - Workspace Designer
  - Managed applications
    - Workspace Extensions
  - Data Sources
  - Session-level User Settings
  - Session-level Folder Synchronization
  - Locations and Devices (Zones)
- **Integrations:**
  - Citrix XenApp, TS RemoteApp, and Application Virtualization
  - Ivanti products: Identity Director, Automation, and Ivanti VDX
  - Microsoft System Center Integration and LANDesk Integration.
- **Management:**
  - Building Blocks and Instant Reports
  - Workspace Control
  - Workspace Analysis
Base Features

The three paid modules - Composition, Governance, and Security - all contain the following:

- Relay Servers
- Advanced Workspace Control
- Delegation of Control
- Auditing
- WiFi Zones
- Workspace Branding
- Connection State
- Time Restrictions
- Workspace and Printing Preferences for end user

Composition

The Composition module contains features for creating a personalized (dynamic) desktop. Provide users with a context-aware and centrally managed workspace that contains all the right applications, data, printing and personal settings essential for their productive working.

It contains the following:

- Advanced Workspace Composition
- Application level:
  - User Settings
  - Actions, such as Folder Synchronization
  - Data Sources
  - Zero Profile Technology
  - E-mail Settings
  - Desktop background
  - Screensaver
  - Lockdown and Behavior

Governance

The features in the Governance module provide insight into what is configured, changed, and used, and increase your ability to manage your infrastructure with change logs, current status reporting, and license usage data from all users.

It contains the following:

- Alerting
- Usage Tracking
- License Management
- Workspace Performance
- Workspace Simulation
- Filtering and Scope Control
- Advanced Access Control
Security

This module delivers a context-aware security layer that is created around the workspace, to effectively protect against internal and external threats. You will be able to deliver a personalized desktop according to company business rules and compliance. Unauthorized actions such as executing certain applications and the use of removable disks are prevented based on the user’s context.

It contains the following:

- Application Security (i.e. blacklisting and whitelisting)
- Authorized Files
- Network Connections Security
- Dynamic Privileges
- Data Security
- Website Security
- Access tokens (USB Zones)
- User Session Security
- User Installed Applications

For more details, please check the Workspace Control Module Comparison Chart on http://res.com/res-one-workspace-editions.

Notes

- Additional functionality is unlocked by adding additional Module licenses. No downtime or additional software deployment is needed.
- During the evaluation period, you can simply switch between modules (at Licensing in the Setup menu). You can also switch if you have extended your evaluation period by importing evaluation licenses, or if you have NFR licenses (Ivanti partners only).
3.13 Desktop Transformation

Desktop Transformation is a concept that transforms an existing desktop infrastructure into managed user workspaces using live data and a step-by-step approach that minimizes the risk and impact on the desktop user.

The transformation process consists of the following steps:

- Gather live data from existing desktops.
- Analyze the data for context.
- Create workspace items and review impact.
- Transform existing desktops in small steps with focus on today's challenges first.

Desktop transformation makes use of the following components:

- The Desktop Sampler (see page 53) - collects data from unmanaged environments.
- The Workspace Designer (see page 55) - designs managed workspace objects based on the collected data.
- The Workspace Model (see page 55) - defines which features of Workspace Control are used.

3.13.1 Desktop Sampler

The Desktop Sampler allows the IT administrator to collect information from a desktop. The standalone software can be installed and launched on a desktop. It runs unobtrusively and it collects the following information:

**User Context**

- User name, logon domain, logon server
- Domain group membership
- Organizational Unit of user
- Computer name, computer domain
- Organizational Unit of computer
- Operating System
- Device Capabilities (CPU/Memory)
- Network IP address

**Composition**

- Applications exposed in Start Menu
- Drive and Port Mappings
- Network Printers
- Drive Substitutes
- Data Sources

The collected information is stored as a file on a designated file share on the network. One file is created per unique user/computer combination. The IT administrator can configure the Desktop Sampler to uninstall itself after a number of days.
Install the Desktop Sampler

You need to install the Desktop Sampler on each computer that is to be sampled. This can be a desktop, but also a Terminal Server. The Desktop Sampler installation file can be downloaded from [http://forums.ivanti.com](http://forums.ivanti.com).

**Installation**

- When you install the Desktop Sampler, it will be installed in the following directory:
  - `%ProgramFiles%\Ivanti Workspace Control Desktop Sampler` (32-bit)
  - `%ProgramFiles(x86)%\Ivanti Workspace Control Desktop Sampler` (64-bit)
- Additionally, a DTSampler key will be added to the following registry key:
  - `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run` (32-bit)
  - `HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run` (64-bit)
- No shortcuts will be added to the user's Start menu.

**Command line**

You can install the Desktop Sampler by double-clicking the MSI file or by using a command line. If you use a command line, you can apply the following parameters to the MSI file:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAMPLEPATH=</td>
<td>Specifies the location of the sampled data. This location can also be set in the registry at <code>HKLM\SOFTWARE\RES\Desktop Sampler</code>. If you do not supply a location, the sampled data will be stored in the installation folder of the Desktop Sampler.</td>
</tr>
<tr>
<td>EXPIREDAYS=</td>
<td>Specifies the number of days the Desktop Sampler needs to remain installed. After the specified number of days, the Desktop Sampler will uninstall itself. If this parameter is not used, the Desktop Sampler will continue to run until it is manually uninstalled.</td>
</tr>
<tr>
<td>DELAY=</td>
<td>Specifies the number in seconds the desktop sampler should wait after a user logs on before it starts sampling data. This is useful when logon procedures take a long time. Specify a number in seconds. By default, the desktop sampler waits for 30 seconds.</td>
</tr>
<tr>
<td>NOICONS</td>
<td>Specifies that no icons will be saved to the desktop sampler files.</td>
</tr>
<tr>
<td>ALLICONS</td>
<td>Specifies that 256-color and 16-color icons will be saved to the desktop sampler files.</td>
</tr>
<tr>
<td>256ICONS</td>
<td>Specifies that only 256-color icons will be saved to the desktop sampler files.</td>
</tr>
</tbody>
</table>

**Example:**

```msiexec.exe /i "C:\INSTALL\Ivanti Workspace Control Desktop Sampler [version].msi" SAMPLEPATH=\fileserver\SampleData EXPIREDAYS=30 DELAY=120 /q```

Command line parameters are case insensitive.

After installation, the Desktop Sampler will sample which applications, printers and data are used by which users at which locations, irrespective of the way in which these settings are managed (manually, scripting, Workspace Control, etc.). It stores this information as a Workspace Control sample file (.dts). The Workspace Designer uses these files to analyze the sampled information.
All command line parameters can also be used directly when invoking `dtsampler.exe`. For example, after the Desktop Sampler is installed it is also possible to start `dtsampler.exe` with the `/SAMPLEPATH` parameter specifying the path of the generated sample files. This allows the Desktop Sampler also to be distributed as a Custom Resource. This `/SAMPLEPATH` parameter overrules a possible `SAMPLEPATH` parameter used when installing the MSI.

**Example:**

```
C:\Program Files\Ivanti Workspace Control Desktop Sampler\dtsampler.exe /SAMPLEPATH="C:\Temp"
```

### 3.13.2 Workspace Designer

You can start the **Workspace Designer** by clicking **Workspace Designer** in the Console. This starts a wizard with which you can analyze the sample files generated by the Desktop Sampler and create and adjust rules based on the sampled data. The Workspace Designer covers the following steps:

- Selection of the type of data to be analyzed (applications, Data Source, Directory Services, Drive & Port Mappings, Drive Substitutes, Locations and Devices, Printers)
- The location of the sample files
- Selection of the objects to be created
- Review of the proposed context rules and their impact, based on:
  - **Coverage**: the percentage of users who currently have the setting, and who will keep it with the suggested rules. (Ideally 100%)
  - **Missed**: the percentage of users who currently have the setting, but who will lose it with the suggested rules. (Ideally 0%)
  - **Slack**: the percentage of users who currently do not have the setting, but who will receive it with the suggested rules. (Ideally 0%)

- Selection and automatic creation of the Workspace Control objects.
- Review of the workspace object, including its **Type** and **Access Control**.
3.13.3  **Workspace Model**

The **Workspace Model** shows you the mode in which each feature is running and allows you to change this if necessary. You can also make this change from the relevant node itself.

It is possible to enable specific parts of Workspace Control, and to disable other parts. This makes it possible to implement Workspace Control gradually, which is very practical if Workspace Control is going to be introduced into an existing environment. Each section of the Workspace Control Management Console has an option to enable or disable it. The settings and configurations of a disabled section are not implemented or executed.

For example, a small number of applications can now be configured in Workspace Control and merged into the existing Start Menu presented to users. If this goes well, a couple more can be added. In this way, the number of applications managed by Workspace Control can be increased gradually over time, in a controlled manner.

You can change a feature's mode directly from the **Workspace Model**. However, you may prefer to do so from the relevant node itself. There, you can see and amend any related settings, find information about any prerequisites, and access the specific Help about that node (by pressing F1).

You can change a feature's mode directly from the **Workspace Model**. However, you may prefer to do so from the relevant node itself. There, you can see and amend any related settings, find information about any prerequisites, and access the specific Help about that node (by pressing F1).

Diagnostics > **Workspace Model Overview** shows you at a glance which features are active/enabled, which are disabled, and which are set in learning mode.

If the global settings of features are overridden by exceptions for specific Workspace Containers, the Workspace Model node shows per Workspace Container which settings apply; either the global settings of a feature or the settings of the exception.

**Managed Applications**

Managed Applications can be implemented fully, partially or not at all. In a new environment, Managed Applications is disabled: Windows Shell shortcut creation is set to **Do nothing**, so that users get the same Start Menu, Desktop and Quick Launch area in their Workspace Control session as they had outside of the Workspace Control session. With this setup, Workspace Control does not manage any of the user's applications. At this point, you can configure applications in the Workspace Control Management Console, but these are not made available to any users.

If you do not want to manage applications at all, select the option **Disable process interception for unmanaged shortcuts**. This operates on a global level and means that even managed applications that have been configured with interception, will not be intercepted. For a description of the process of intercepting applications, see General at the Properties section of Managed Applications, If managed shortcut was not used.

When you are ready to start managing users' applications through Workspace Control, you can enable Managed Applications partially or fully:

- To give users Workspace Control-managed applications in addition to their existing, non-Workspace Control-managed applications, choose Windows Shell shortcut creation: **Merge with unmanaged application shortcuts**. You can combine this option with setting the Unmanaged shortcuts that point to same executable option to **Replace with managed shortcut** (at Properties > Settings of a Managed Application). With this option you prevent that the user's environment contains both managed and unmanaged shortcuts to the same application.

- To give users only Workspace Control-managed applications, choose Windows Shell shortcut creation: **Replace all unmanaged shortcuts**. This replaces the Start Menu of your users with the Start Menu and application shortcuts as configured in Workspace Control. Unmanaged applications are no longer available.
Chapter 4: General Functionality

4.1 Filtering

A filter restricts the current view of the Workspace Control Console. This allows you to focus on a specific aspect or part of your environment. For example, you can set a filter so that the Management Console only shows objects for which Access Control has been set based on a specific Organizational Unit, or for which Access Control has been set according to Zones. Filtering is especially useful in large Workspace Control environments that contain a very large number of settings and applications.

4.1.1 Where to find Filtering

<table>
<thead>
<tr>
<th>What</th>
<th>Where</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indicator of unfiltered view:</td>
<td>☐ in the lower right-hand corner on the Workspace Control Console and on the Command Bar</td>
</tr>
<tr>
<td>Indicator of filtered view:</td>
<td>☑ in the lower right-hand corner on the Workspace Control Console and in the toolbar and on the Command Bar</td>
</tr>
<tr>
<td>Configure and apply a filter</td>
<td>Action menu &gt; Configure filter</td>
</tr>
<tr>
<td></td>
<td>or</td>
</tr>
<tr>
<td></td>
<td>right-click ☐ &gt; Configure filter</td>
</tr>
<tr>
<td>Remove filtering and return to a full view</td>
<td>Action menu &gt; Apply filter, click to remove the check mark</td>
</tr>
<tr>
<td></td>
<td>or</td>
</tr>
<tr>
<td></td>
<td>right-click ☑ &gt; Apply filter, click to remove the check mark</td>
</tr>
<tr>
<td>Apply the same filter that was used last time</td>
<td>Action menu &gt; Apply filter</td>
</tr>
<tr>
<td></td>
<td>or</td>
</tr>
<tr>
<td></td>
<td>right-click ☐ &gt; Apply filter</td>
</tr>
</tbody>
</table>
4.1.2  Filter Criteria and Filter Types

Filter criteria

There are three types of filter criteria:

- Base a filter on **Access Control** criteria to see only objects to which specific users, groups, Organizational Units and/or Zones have access. For example, see all the objects that apply to users in the Organizational Unit “Netherlands”.
- Base a filter on **Access Type** criteria to see only objects for which access depends on a specific access method. For example, see all the objects for which access is set according to administrative role (regardless of which administrative role), or see all the objects for which access is set depending on Language (regardless of which Language) (for example E-mail Settings).
- Base a filter on **Workspace Control** to see only objects for which access depends on specific Workspace Containers. For example, see all the objects that are available to computers in the Workspace Container “Terminal Servers”.

Filter types

There are two types of filter:

- A **default filter** shows all the objects for which at least one of the specified criteria applies either directly or indirectly.
- An **exclusive filter** shows all the objects to which at least one of the criteria applies directly.

Notes

- If the option **Exclusive filter** is not selected for a filter, items that would be affected if the option was checked are marked with an “i” (informational) in their icons.
- When filtering on Organizational Unit (OU), nested groups or users across bound-aries are not taken into account.

Example

Suppose you want to configure a filter based on the Access Control criterion Organizational Unit (OU) London. The Management Console contains four applications:

- **Calculator**, with Access Control set to membership of OU London (which is part of OU Great Britain).
- **Notepad**, with Access Control set to membership of OU Great Britain (with inheritance).
- **WordPad**, with Access Control set to membership of Group Trafalgar Square (part of OU London).
- **Paint**, with Access Control set to “All users”.

This results in:

<table>
<thead>
<tr>
<th>Object</th>
<th>Filtering</th>
<th>Exclusive Filtering</th>
</tr>
</thead>
</table>
### Object Filtering

<table>
<thead>
<tr>
<th>Object</th>
<th>Filtering</th>
<th>Exclusive Filtering</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paint (Access Control = All users)</td>
<td>Result: Paint is shown in filtered Management Console. Reason: Indirect relationship, because &quot;All users&quot; also includes users who are members of OU London (lower in hierarchy).</td>
<td>Result: Paint is hidden in filtered Management Console. Reason: No direct relationship.</td>
</tr>
</tbody>
</table>

**Warning**

Avoid combining filters that combine Access Control, Access Type and/or Workspace Control criteria, as the results are difficult to predict.

### 4.1.3 Nodes excluded from filtering

The following nodes are never restricted in a filtered view:

- Composition > Desktop > Shell
- Security > Applications > User Installed Applications

All objects in these two nodes remain visible, regardless of the filter that is applied.

Other Management Console nodes will appear empty if they do not contain objects that match the criteria of the filter that is applied.
4.2 Instant Reports

**Instant Reports** allow you to document the entire Workspace Control site, or specific parts of it.

This allows you to create complete configuration, license metering and usage reports of your Workspace Control environment, to gain a complete overview of used resources and their costs.

Instant Reports include information about the properties and values of the documented item(s) and can include additional information about the Workspace Control version.

Please note that some Workspace Control nodes in the **Diagnostics** section are not included by default when creating an Instant Report. This is because these nodes may contain large amounts of data.

### 4.2.1 Where to find Instant Reports

<table>
<thead>
<tr>
<th>What</th>
<th>Where</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create an Instant Report of a node</td>
<td>click the button in any Workspace Control Console node or select the node and right-click &gt; Create Instant Report</td>
</tr>
<tr>
<td>Create an Instant Report of the entire site</td>
<td>Action menu &gt; Create Instant Report</td>
</tr>
<tr>
<td>Create an Instant Report of specific parts of the site</td>
<td>Action menu &gt; Select items for Instant Report, then Action menu &gt; Create Instant Report of selected items</td>
</tr>
<tr>
<td>Create an Instant Report of a specific setting or application</td>
<td>right-click the item &gt; Create Instant Report</td>
</tr>
</tbody>
</table>

### 4.2.2 Instant Report format

Instant Reports can be stored as a PDF file including a Table of Contents.

Alternatively, they can be printed directly from the window **View Instant Report**.

### 4.2.3 Customize the contents and presentation

The following customization choices are available for Instant Reports:

- Whether or not to include a cover page.
- Whether or not to include a title on the cover page. The title is editable.
- Whether or not to include a Table of Contents.
- Whether or not to include a page About Workspace Control. This page shows details about the version of Workspace Control and its subprocesses running in your environment, plus the start level and the installation directory.
- Whether or not to include empty pages.

To set these options, go to the **Action** menu and choose **Select Items for Instant Report**. At the top of the tree the section **Instant Report Settings** will appear.
4.2.4 Information excluded from Instant Reports

The following nodes cannot be included in an Instant Report:

- Diagnostics > Usage Tracking Overview
- Administration > Maintenance
4.3 Building Blocks

A Building Block stores information about the configuration settings of a Workspace Control site. A Building Block can be imported back into its original site to recreate these settings. A Building Block can also be imported into a different environment to copy the settings. This makes Building Blocks useful for change management, and data exchange. Please note that Building Blocks contain all configuration information (except Licensing), but not all operational information (e.g. Logging, Audit Trail, Delegated Users). Therefore, Building Blocks can be used as configuration backup of your environment, but not as a full backup.

A Building Block is an XML file that can be edited manually. This makes it possible to use a Building Block as a template: before importing a Building Block into another site, you can replace site-specific information such as server names with the information applicable to the target environment.

4.3.1 Where to find Building Blocks in the Workspace Control Console

<table>
<thead>
<tr>
<th>What</th>
<th>Where</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create or import a Building Block (node-specific)</td>
<td>click the button in any Workspace Control Console node &gt; Create Building Block or &gt; Import Building Block or select the node and right-click &gt; Create Building Block or &gt; Import Building Block</td>
</tr>
<tr>
<td>Import a Building Block of all or selected items</td>
<td>Action menu &gt; Import Building Blocks</td>
</tr>
<tr>
<td>Create a Building Block of a specific setting or application</td>
<td>right-click the item &gt; Create Building Block</td>
</tr>
<tr>
<td>Create a Building Block of selected items</td>
<td>Action menu &gt; Select items for Building Blocks, then Action menu &gt; Create Building Block of selected items</td>
</tr>
<tr>
<td>Import Building Block of all or selected items</td>
<td>Action menu &gt; Import Building Blocks</td>
</tr>
<tr>
<td>Update or delete all managed applications using a Building Block</td>
<td>at Composition &gt; Applications, click the button &gt; Add/Update Applications or Delete Applications</td>
</tr>
<tr>
<td>Update or delete a selected managed application using a Building Block</td>
<td>at Composition &gt; Applications, right-click the application &gt; Building Blocks &gt; Add/Update Applications or Delete Applications.</td>
</tr>
</tbody>
</table>
4.3.2 Create Building Blocks

By default, a Building Block created from the **Action** menu contains all the settings of the Workspace Control site, but individual nodes, settings and applications can be excluded manually before the Building Block is created.

A Building Block created using the **button or by right-clicking a specific node contains all the settings or applications within that node.**

A Building Block created right-clicking a specific settings or applications contains only that setting or application.

**Note**

If multiple applications with the same Title exist in one menu, when creating Building Blocks for these applications from the Application List tab (at Composition > Application), the XML of the second/third/… Building Block will include the application ID in its file name.

**Tip**

It is possible to create a Building Block of a Workspace Container with access control set to an OU in domain "A" and import the building block in a Workspace Control environment in domain "B" where the OU is available under the same path. Access control on the Workspace Container in domain "B" will then be set to the same OU, but in domain "B".

4.3.3 Import Building Blocks

Importing a Building Block from the **Action** menu imports all the settings and applications contained in that Building Block into the Workspace Control site. Individual nodes, settings and applications can be excluded manually before the Building Block is imported.

Importing a Building Block using the **button or by right-clicking a specific node, imports only the settings or applications relevant to that node. Other information in the Building Block is not imported.**

Importing a Building Block by right-clicking a specific setting or application only imports that setting or application. Other information in the Building Block is not imported.

When importing a Building Block, if the Building Block contains data for a feature that is not available in the Management Console, this data will be ignored. This could occur, for example, with deprecated features (see “Feature deprecation” on page 399).

**Merge vs. overwrite**

In certain parts of the Workspace Control Console, settings imported from a Building Block can either overwrite the existing contents of these nodes in the target site or can be added to them as a merge. This applies to the following nodes:

- User Context > Directory Services
- Composition > User Settings
- Security
**Chapter 4: General Functionality**

The **Merge** option:
- replaces existing settings in that node by settings in the Building Block that have the same GUID.
- adds settings from the Building Block to the target node if the target node contains no existing settings with the same GUID.

The **Overwrite** option removes the entire contents of the target node and replaces it with the contents of that node as defined in the Building Block.

**Example**

If your target node contains 10 settings, and you import a Building Block that contains 1 setting (with a GUID that is not matched in the target site):
- the import option **Merge** results in 11 settings in the target node, namely the 10 original settings plus the imported one.
- the import option **Overwrite** results in 1 setting in the target node, namely the imported one.

**Note**

When importing a Building Block manually, the account SIDs can be added. Beware however that, when importing a Building Block "unattended", account names will be used.

**Add/Update Applications and Delete Applications**

Using a Building Block that contains only application settings, you can delete or add and update existing applications in the target site.

The options **Add/Update Applications** and **Delete Applications** compare the GUIDs of the existing applications in the Workspace Control Console with the GUIDs of the applications in the Building Block.

With the option **Add/Update Applications**, the Building Block is a list of applications to be created or updated:
- applications are added from the Building Block to the target site if the target site does not contain an application with the same GUID. If no GUID is available for the application in the Building Block, a new GUID is generated during the import.
- applications in the target site are replaced with the applications in the Building Block that have the same GUID.

With the option **Delete Applications**, the Building Block is a list of applications to be deleted: any application in the target site that has the same GUID as an application in the Building Block is deleted from the target site.

**Notes**
- When importing Building Blocks with custom application icons, the icon information must refer to the full path to the icon. For example, to specify a different application icon, replace the element `<icon32x256>XXX</icon32x256>` (where “XXX” represents encoded data) with `<icon32x256 filename=\srv-abc\Applications\Notepad\32x256.ico></icon32x256>`.
- Only default environment variables are supported in the full path to the application icon.
- When importing a Building Block that includes application IDs, this ID will be placed in the sequence of already existing application IDs in the Datastore. If the ID is already used by an existing application, the next available ID will be assigned to the imported application.
- When importing a Building Block, the option **Convert Citrix published apps to local apps** can be selected to convert all Citrix published applications that exist in the Building Block to Workspace Control local applications. You are then responsible yourself for publishing them if this is desired.
Import Building Blocks into a specific workspace

When importing a Building Block, the option **Import objects into specific workspace** sets the selected Workspace Container as Workspace Control on the imported settings and applications. This overwrites any Workspace Control information originally contained in the Building Block for these objects. If the imported objects already existed and already had Workspace Control, their Workspace Control is also overwritten.

Importing a Building Block into a specific workspace makes it possible to isolate imported settings and applications from the rest of the Workspace Control site, for example for testing purposes.

If the option **Import Objects into a specific workspace** is selected, only settings that can be restricted with Workspace Control are imported from the Building Block into the target environment. Settings that cannot be restricted with Workspace Control, such as Shell settings and Desktop lockdown settings, are not imported.

**Administrative roles**

If your Administrative Role grants limited access to the Workspace Control Console, this impacts your ability to import Building Blocks:

- If you only have **Read** access to the Management Console, it is not possible to import Building Blocks.
- If you have **Modify** access to only certain nodes of the Management Console, the **Import Building Block** window will show which Building Block settings you can import.

**Associated items**

- A Building Block stores information about any Zones, Data Sources, E-mail Settings and linked User Settings associated with an object. At import, these links are also established in the target site. The associated objects are created in the target site if they do not exist there.
- If you create a Building Block that includes an object containing resources (such as desktop pictures), an additional (XBB) file is automatically created that contains these resources. When you import this Building Block into a target site, the items in the XBB file are also added to the target site.
### 4.3.4 Command line parameters

The executable program of the Workspace Control Console is `pwrtech.exe`. The following command line parameters are available for Building Block actions:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>/add &lt;path + name XML-file&gt;</code></td>
<td>Imports a single Building Block into the Console. For example:</td>
</tr>
<tr>
<td></td>
<td>• C:\Progra<del>2\RESSof</del>1\Worksp~1\pwrtech.exe /add</td>
</tr>
<tr>
<td></td>
<td>H:\xml\security_network.xml</td>
</tr>
<tr>
<td></td>
<td>• C:\Progra<del>1\RESSof</del>1\Worksp~1\pwrtech.exe /add</td>
</tr>
<tr>
<td></td>
<td>H:\xml\security_network.xml</td>
</tr>
<tr>
<td><code>/add &lt;path + wildcards&gt;</code></td>
<td>Imports multiple Building Blocks into the Management Console. For example:</td>
</tr>
<tr>
<td></td>
<td>{%respfdir%\pwrtech.exe} /add H:\example.xml</td>
</tr>
<tr>
<td></td>
<td>If the Building Block contains settings from the Composition node,</td>
</tr>
<tr>
<td></td>
<td>Authorized Files or Blocked Resources, add the option <code>/overwrite</code> to</td>
</tr>
<tr>
<td></td>
<td>specify that these settings should replace any existing settings (for the</td>
</tr>
<tr>
<td></td>
<td>Composition node, only settings for the same type (&quot;Mapping&quot;) and level</td>
</tr>
<tr>
<td></td>
<td>(&quot;Global&quot;) will be replaced). If you do not add this option,</td>
</tr>
<tr>
<td></td>
<td>all settings in the specified Building Block files will be merged with</td>
</tr>
<tr>
<td></td>
<td>the current settings in the Console.</td>
</tr>
<tr>
<td><code>/del &lt;path + XML-file&gt;</code></td>
<td>Deletes an application from the Console. For example:</td>
</tr>
<tr>
<td></td>
<td>C:\Progra<del>1\RESSof</del>1\Worksp~1\pwrtech.exe /del</td>
</tr>
<tr>
<td></td>
<td>H:\xml\startmenu_accessories_calculator.xml</td>
</tr>
</tbody>
</table>

### 4.3.5 Information excluded from Building Blocks

The following nodes cannot be included in a Building Block:

- **File Types**
- **Diagnostics**
- **Workspace Model**
- **Licensing**
- **Datastore** in the Setup menu
- **Administration > Maintenance**
4.3.6 The structure of Building Blocks

Because of its XML format, the contents of a Building Block can be edited manually using any text editor or XML-authoring solution.

For example, if you have installed a new print server to replace an existing one, then all network printer settings in your environment need to point to the new server. Instead of editing each setting individually, create a Building Block of these settings. Open the XML file and replace all references to the old printer server with references to the new one. Finally, import the edited Building Block back into the Workspace Control site.

Warning
Modifying a Building Block may lead to unexpected results. Before you modify a Building Block, make sure you have created a backup.

GUIDs

Each setting in a Workspace Control environment contains a GUID, with which it is uniquely identified in the Datastore. When you create a Building Block of a setting, its XML structure contains an overview of this setting, followed by its GUID.

If you adjust the GUID of a setting in a Building Block (by replacing a number or character with another number or character), you can prevent overwriting the original setting by creating a clone of it. This method can be useful if it is not possible to create a clone of a setting using the Management Console or if you want to test a modified setting first without overwriting the original setting.

Edit references to external files

For the following settings, encoded information in the Building Block refers to files:

- Application settings (application icons)
- E-mail Settings (Outlook signatures)
- Registry and Policy settings
- Desktop and screensaver background images

These references can be edited manually in a Building Block to refer to different external files. The file(s) specified must be located in the same folder as the Building Block.

Specify a different application icon, Outlook signature or Registry setting

Follow this procedure:

- Find the relevant element in the XML (see table below).
- Remove the encoded data in the element contents.
- Add the replacement file name as attribute for the empty element.

For example, to specify a different application icon, replace the element `<icon32x256>XXX</icon32x256>` (where “XXX” represents encoded data) with `<icon32x256 filename="32x256.ico"></icon32x256>`. 
Chapter 4: General Functionality

<table>
<thead>
<tr>
<th>Setting</th>
<th>XML element(s)</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application icon</td>
<td><code>&lt;icon32x256&gt;XXX&lt;/icon32x256&gt;</code> <code>&lt;icon32x16&gt;XXX&lt;/icon32x16&gt;</code> <code>&lt;icon16x256&gt;XXX&lt;/icon16x256&gt;</code> <code>&lt;icon16x16&gt;XXX&lt;/icon16x16&gt;</code></td>
<td><code>&lt;icon32x256 filename=&quot;32x256.ico&quot;&gt;&lt;/icon32x256&gt;</code></td>
</tr>
<tr>
<td>Outlook signature</td>
<td><code>&lt;htmlfile&gt;XXX&lt;/htmlfile&gt;</code> <code>&lt;plainfile&gt;XXX&lt;/plainfile&gt;</code> <code>&lt;rtffile&gt;XXX&lt;/rtffile&gt;</code></td>
<td><code>&lt;htmlfile filename=&quot;companysign.htm&quot;&gt;&lt;/htmlfile&gt;</code> <code> </code>&lt;plainfile filename=&quot;companysign.txt&quot;&gt;&lt;/plainfile&gt;<code> </code>&lt;rtffile filename=&quot;companysign.rtf&quot;&gt;&lt;/rtffile&gt;`</td>
</tr>
<tr>
<td>Registry file</td>
<td><code>&lt;registryfile&gt;XXX&lt;/registryfile&gt;</code></td>
<td><code>&lt;registryfile filename=&quot;setting.reg&quot;&gt;&lt;/registryfile&gt;</code></td>
</tr>
</tbody>
</table>

Specify a different Policy settings file

Follow this procedure:

<table>
<thead>
<tr>
<th>Element</th>
<th>Edit actions</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. <code>&lt;policysettings&gt;XXX&lt;/policysettings&gt;</code></td>
<td>Delete the encoded contents and add the replacement file name as attribute to the empty element.</td>
<td><code>&lt;policysettings filename=&quot;policy.set&quot;&gt;&lt;/policysettings&gt;</code></td>
</tr>
<tr>
<td>2. <code>&lt;registryfile&gt;XXX&lt;/registryfile&gt;</code></td>
<td>Delete the encoded contents and add the replacement registry file name as attribute to the empty element.</td>
<td><code>&lt;registryfile filename=&quot;setting.reg&quot;&gt;&lt;/registryfile&gt;</code></td>
</tr>
<tr>
<td>3. <code>&lt;filename&gt;xxx.adm&lt;/filename&gt;</code></td>
<td>Replace the name of the ADM file in the element contents with the replacement ADM file.</td>
<td><code>&lt;filename&gt;wmplayer.adm&lt;/filename&gt;</code></td>
</tr>
<tr>
<td>4. <code>&lt;embeddedbinary&gt;XXX&lt;/embeddedbinary&gt;</code></td>
<td>Delete the encoded contents and leave the element empty.</td>
<td><code>&lt;embeddedbinary&gt;</code></td>
</tr>
</tbody>
</table>

Specify a different desktop background image

- Replace the name of the desktop image file in the element `<desktoppicture>` with the replacement desktop image, for example `<desktoppicture>companylogo.bmp</desktoppicture>`.
- Delete the encoded contents of the element `<desktopbinary>` and leave the element empty.

Specify a different screensaver image

- Replace the name of the screensaver image in the element `<screensaverpicture>` with the replacement screensaver image, for example `<screensaverpicture>companyoffices.bmp</screensaverpicture>`.
- Delete the encoded contents of the element `<screensaverbinary>` and leave the element empty.
4.4 Change language of Management Console

Use the Change Language option in the Menu bar of the Management Console to change the language used in the Management Console.

Changing the language of the Management Console is not user-specific: If you change the language, all users with access to the Management Console will experience this change.

**Configuration**

- You can change the language of the Management Console by clicking Options > Change Language.
- You can only select languages that have been mapped in the node User Context > Languages (on page 146).

4.5 Disabled Features

If a feature is Disabled at global level and you add an object related to this feature for the first time, a message will be shown that the configuration will not take effect until the feature is enabled. This message will not be shown if the feature is in Learning mode.

The following examples show situations in which a notification is shown:

- At Security > Applications, Managed Applications Security is disabled. The first time you configure an Authorized File when editing a Managed Application, a message will be shown that Managed Applications Security must be enabled first before the rule will take effect. If you have sufficient rights, the rule will be added anyway.
- At Composition, User Settings is disabled. The first time you configure User Settings when editing a Managed Application, a message will be shown that User Settings must be enabled first before the user setting will take effect. If you have sufficient rights, the rule will be added anyway.

**Exception**

Global nodes for which Actions exist on application level (e.g. Drive and Port Mappings, Drive Substitutes, Folder Synchronization, etc.) form an exception. In this case, an additional message will be shown, stating that the Actions will be performed regardless of the global disabled status.
5.1 Configuration Wizard for existing Workspace Control site

When starting the **Configuration Wizard**, an introductory window will be shown welcoming you to the configuration wizard. You can either choose to view the online tutorial to be informed about the concept of workspace management or click **Next** if you already know our product.

- The initial steps will be skipped, and you can configure additional example configurations. Example objects are disabled by default when they are created:
  - Managed Applications
  - Settings executed at the start of a user session
  - An Administrative Role "Helpdesk"
  - Location-based printing

Click **Next**.

- Your site configuration settings are shown in a summary. If you want to change any of the settings click **Back**; if you agree with the settings, click **Next**.

- The configuration process will start, showing status and result information.

- In the final step, you will see that the configuration has been completed and an **Action list** is shown, stating the items you still have to configure manually. The **Action list** can be saved or copied on the clipboard. You can use the **Action List** afterwards as a reminder of the items you still have to configure. Click **Finish**.

After closing the **Configuration Wizard**, you will return to the top node in the Console: the Navigation map.

---

**Tip**

In the **Summary** (review site configuration settings) step of the configuration wizard, you can click the **Instant Report** button to show or save the **Configuration Wizard** summary. You can use this summary as an overview or checklist which items and settings have been configured.

---

**Notes**

- To start the configuration wizard in a production site already containing configured items, click **Help > Configuration Wizard**. The steps are the same as in **Creating a Production site**, except for step 2 in which the type of site you wish to create is asked, which is skipped.

- If you want to clear the example data created by the **Configuration Wizard**, click on **Clear example data** at **Usage Tracking** in the **Setup** menu. Only **Usage Tracking** example data created by the **Configuration Wizard** will be deleted, real **Usage Tracking** data will not be cleared.

- The Console user needs the administrative role of "Technical Manager" with full rights to all nodes in Workspace Control to be able to execute the **Configuration Wizard**.
5.2 Datastore Management

At Setup > Datastore you can manage the configuration of the Primary Datastore and optionally configure a Secondary Datastore.

5.2.1 Connections

Datastore in the Setup menu shows to which primary Datastore the current Workspace Control site connects. From here, you can also connect to other existing Workspace Control sites, create new ones, migrate your Datastore, split or join primary and secondary Datastores and generate a string of the database connection settings.

Primary Datastore

- To connect to a different Datastore, click and then click Connect. This opens the Datastore Connection Wizard, which will guide you through the process. Instead of typing the connection settings of the target Datastore manually, you can also copy the Datastore connection settings of a different Datastore from the clipboard (by clicking the Copy from clipboard button) or import these settings from a TXT file (by clicking the Import from file button). You can also use this functionality to revert accidental changes to the connection settings of the current Datastore, or to set up Datastore location sensing for Agents.

- When connecting to a Datastore that was previously migrated, you can choose between the following options:
  - Select Ignore this and connect anyway to connect to the “old” Datastore. Optionally also select Remove referral to new database to remove the Datastore already migrated notification. Note that other Agents will not automatically also connect to this Datastore. See Datastore Migration Wizard (on page 73) for more information.
  - Select Connect to the new database to connect to the migrated Datastore.

- To create a new Datastore, click and then click Create. This opens the Datastore Wizard, which will guide you through the process. When creating a new Datastore, you can choose which module to use. See Select Workspace Control Modules. For more information about the features available in the modules, see Workspace Control Modules (on page 49).

- To migrate to a new Datastore, click and then click Migrate. This opens the Datastore Migration Wizard (on page 73), which will guide you through the process.

- To export a string of the current, primary database connection settings, click and then click Export ( ). This opens the Export database connection string window, from which you can copy the Datastore connection settings to the clipboard (by clicking the Copy to clipboard button) or export these settings to a TXT file (by clicking the Export to file button). This functionality makes it easier to transfer all connection settings to another Console or to set up Datastore location sensing for Agents.

Secondary Datastore

- It is possible to split the Datastore into two separate databases. One database is used for State and Configuration data (with or without Logging) and one database is used for Usage Tracking data (with or without Logging).

- To change the credentials, click at Secondary Datastore.

- To split or join Datastores, click at Secondary Datastore and then click Split/Join. The Split/Join Datastore Wizard will guide you through the process.
Database prerequisites

<table>
<thead>
<tr>
<th>Database type</th>
<th>Prerequisites</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft SQL Server</td>
<td>• Mixed Mode authentication (only when using SQL Server login for Authentication)</td>
</tr>
<tr>
<td></td>
<td>• A named SQL Server System Administrator login ID</td>
</tr>
<tr>
<td></td>
<td>• If Force protocol encryption is enabled: Microsoft Native Client</td>
</tr>
<tr>
<td>Microsoft SQL Azure</td>
<td>• Microsoft Windows Azure credentials</td>
</tr>
<tr>
<td></td>
<td>• Microsoft SQL Native Client</td>
</tr>
<tr>
<td>Oracle</td>
<td>• Oracle DBA credentials</td>
</tr>
<tr>
<td></td>
<td>• Oracle database drivers on all Agents connecting directly to the Datastore</td>
</tr>
<tr>
<td>MySQL</td>
<td>• MySQL DBA credentials</td>
</tr>
<tr>
<td></td>
<td>• MySQL ODBC driver on the database server and on all Agents connecting directly to the Datastore</td>
</tr>
<tr>
<td></td>
<td>• For MySQL ODBC Driver versions 5.2.2 - 5.2.4, Workspace Control only supports the ANSI version of the driver.</td>
</tr>
</tbody>
</table>

For an overview of supported versions, see Supported Database systems in the Compatibility Matrix.

Notes

- If allowed by the SQL server, you can specify a Login without a Password.
- When using Windows Authentication, Agents and users must be part of a trusted Domain.
- It is not possible to connect to a Datastore created by a previous version of Workspace Control.
- It is not possible to migrate a secondary Datastore. To move the secondary Datastore to another location: Join the primary and secondary Datastores and create a new secondary Datastore at another location.
- Verify that all Workspace Control Agents can connect to your Migrated / Split Datastores.

Tip

- You can also connect to another existing Workspace Control site by going to File > Connect remote database in the Management Console menu, providing the relevant information there. It is possible to import a Database connection string here.
Windows authentication with designated account

When using a Microsoft SQL Datastore and connecting to it with Windows authentication, you can specify a Designated Windows account for Workspace Control Datastore access. This makes it possible for the Workspace Control Console to connect to the Datastore using a designated account if the Console-user does not have Datastore access with his own Windows account.

For new Datastores, the designated account can be specified in the Datastore Wizard. At Setup > Datastore, the designated account can be specified for existing and migrated Datastores. After having migrated a Datastore, make sure the designated account is also member of the new Active Directory group.

To check if the specified designated account still works for your migrated or split Datastore, on the Datastore node in the Console, click . A message will be displayed if the designated account does not work for the migrated Datastore.

When a user is connected to the Console and a designated Windows account is used for access to the Datastore, switching to another Datastore and back again to the initial Datastore will cause failed connection to the Datastore with the designated account.

Please note that in the Datastore Connection Wizard the credentials of the Datastore connection are displayed. For SQL authentication, the credentials can also be changed, for Windows authentication, the credentials are grayed out.

When using Windows authentication with a designated account, in the Audit trail (at Diagnostics > Audit Trail) the changes in your environment are logged with the current user information. On your Microsoft SQL Server, the changes in the Datastore are logged with the designated account information.

Datastore Migration Wizard

The Migrate button on the Primary Datastore properties screen makes it possible to migrate your existing Workspace Control Datastore to a new type and/or location. This allows you to easily relocate your exiting Workspace Control Datastore, or, for instance, to migrate from a Microsoft SQL 2005 Datastore to a Microsoft SQL Azure Datastore. Migrations between all supported Database types are possible. Workspace Control Agents and Relay Servers running Workspace Control will connect to this new Datastore as soon as they update their cache.

Configuration

- To migrate to a new Datastore, click Migrate to start the Datastore Migration Wizard, which will guide you through the process.
- Optionally choose to migrate your Usage Tracking data to the new database.
- After clicking Finish the Datastore will be migrated to the new location.
- The last step of the wizard offers the option to transfer your Workspace Control licenses to the new database. If you select this option, the old database license activation will expire in 30 days. If you do not choose to transfer your licenses the new database gets no licenses but does get a new site ID.

⚠️ Warning

Do not take the migrated database offline before all directly connected agents and Relay Servers have switched to the new database. This may take minutes to weeks, depending on cache intervals and off-line Agents (laptops).
Notes

• If you use a designated Windows account, after migrating your Datastore, make sure the designated account is also member of the new Active Directory group. To check if the specified designated account still works for your migrated Datastore, go to the Datastore node in the Console, and click . A message will be displayed if the designated account does not work for the migrated Datastore.
• When migrating a Microsoft SQL Datastore with Windows authentication and a designated account to a non-Microsoft SQL Datastore or a Microsoft SQL Datastore with SQL authentication, the designated account will be migrated. If both the primary and the secondary Datastore are non-Microsoft SQL or Microsoft SQL with SQL authentication, this designated account can be removed.

5.2.2 Datastore Split/Join Wizard

The Split/Join... button on the Primary Datastore properties screen makes it possible to split your existing Workspace Control Datastore to a primary and secondary location. One database is used for State and Configuration data in- or excluding Logging and one database is used for Usage Tracking data in- or excluding Logging. Since Logging and Usage Tracking data may cause very large database sizes, storing that data in a separate database can for instance allow the design of the database infrastructure to be more flexible. For the secondary database, all Database types are possible. All Workspace Control Agents running Workspace Control version 10 will automatically connect to this new Datastore.

Configuration

• To migrate to a new Datastore, click Split/Join... to start the Split/Join Datastore Wizard, which will guide you through the process.
• Choose what data needs to be stored in your secondary database.
• Choose to create a new secondary Datastore or use an existing one:
  • If you are creating a new Datastore, select the server and supply credentials.
  • If you use an existing Datastore, specify the connection settings for the existing secondary location.
• If a secondary Datastore already exists, the Split/Join Datastore Wizard will display the records that are already available in that location.
• An overview of all actions to be taken is displayed, before actually splitting or joining the Datastore.
• In the last step of the wizard you must make the changes permanent or click Cancel to revert to the original situation. A confirmation of all choices made in the wizard will be displayed.
5.3 Licensing

Workspace Control offers two license types: Named User and Concurrent. (See Licensing Model (on page 76))

- **Named User** licenses are based on the Microsoft Windows logon name of single users.
- **Concurrent User** licenses used in earlier versions of Workspace Control can still be used after upgrading to this version of Workspace Control and can be used alongside Named User Licenses. Concurrent User licenses are based on the number of simultaneous User Workspace sessions.
- Upon request, Concurrent User licenses can still be purchased for Workspace Control.

When Workspace Control is installed, an evaluation license for 25 Named Users is made available automatically, as well as an evaluation license for Ivanti VDX for 25 VDX clients. During the evaluation period, you can easily switch between the different Workspace Control Modules (on page 49) by clicking the **Module(s)** link. This allows you to try out the different sets of functionalities that Workspace Control modules offer. See Select Workspace Control Modules (on page 78).

Evaluation licenses are valid for 45 days, after which Workspace Control automatically blocks user sessions. To use VDX and other modules of Workspace Control after the evaluation period, you need to buy licenses from your reseller or activate **Workspace Control Core**.

After licenses have been imported, it is no longer possible to switch between modules. You can add new modules by buying additional Module licenses.

**Configuration**

- **At Setup > Licensing**, click **Get Licenses** to obtain (additional) licenses. This opens a web page with contact details of resellers.
- To activate **Workspace Control Core**, first deselect the paid modules (Composition, Governance, Security), then open the **License Wizard** or click the **Get Licenses** button.
- Click **View** to view the details of a license (not applicable for built-in evaluation licenses and site licenses).
- Click **Delete** to delete a license (not applicable for built-in evaluation licenses and site licenses).
- Click **License Wizard** to import, register and activate Workspace Control licenses. You can also use this wizard for VDX licenses (not available when using **Workspace Control Core**).
- Use **License alerting threshold** in combination with the **Alerting** event License threshold reached (at Setup > Integration > Alerting, on the **Events** tab) to set up an alert before all licenses have been claimed. This enables you to take action before users are not able to log on because no licenses are available in the Datastore.
  To actually show the alert, you must configure the **License threshold reached** event (at Alerting (on page 88)). Setting the **License alerting threshold** to 0 or leaving it blank, disables the alert.
• **Use If no license is available at logon** to set up a licensing policy that specifies what should happen if no license is available when a user starts a workspace session.
  
  • **Continue with limited functionality:** If no (evaluation) licenses are available when a user logs on, a message will be shown to the user: "There is no license available. Workspace Control will start a restricted session that offers only limited functionality. Please contact your administrator." The user can still log on, but only **Workspace Control Core** functionality will be available. The event of no available licenses will also be logged in the Event log with an exclamation mark.
  
  • **Continue with reminder for 45 days:** If no licenses are available when a user logs on, the user can still use Workspace Control with full functionality for 45 days, but a reminder is shown to the user: "No Workspace Control license is available. An unlicensed session will start after a short delay. In [x] days, you will not be able to start any session. Please ask your administrator to buy additional licenses.” The event of no available licenses is logged in the User Event log and in the Error log (once every 24 hours). Then, a countdown is started and if, after 45 days, there is still no license available, the user will not be able to start any session until additional licenses have been added.
  
  • **Do not continue, log off:** If no (evaluation) licenses are available when a user logs on, a message is shown to the user ("No Workspace Control license available for session"). The user will be logged off automatically and an entry will be logged in the User Event Log ("Workspace Control cannot continue because no licenses are available").

---

**Notes**

• The setting **Continue with reminder for 45 days** for the option **If no license is available at logon**, is not available during evaluation.

• If you move a **Workspace Control Core** SQL database, and the database creation date changes, then the Workspace Control environment will revert to **Evaluation** mode with a default 25 user limit. In that case, you need to re-activate the licenses again by clicking **Get Free Licenses**. This will activate your licenses immediately for an unlimited number of users and without expiration date.
5.3.1 Licensing Model

Workspace Control offers two license types: Named User licenses and Concurrent User licenses. Which license type, or combination of licenses you need, very much depends on the number of users, Workspaces and devices in your environment. Concurrent licensing is mainly used in Virtual Desktop environments and named licensing for mobile workers (laptops). For example, when a user works on a laptop and connects to a Virtual Desktop, a named user license suffices to work with Workspace Control on both, as the license is associated to the user name.

Licensing information is stored in the Datastore and cached locally on Agents. If, according to the local cache, licenses are available for the session, the session is allowed. If, according to the local cache, no licenses are available, the Workspace Control licensing policy is applied.

Licenses are pooled per environment and are claimed by Workspace Control Agents according to the rules outlined below.

Named User licenses

When using named user licenses only, the following applies:

• Workspace Control claims a named user license for each user upon first session connect. Once the license is claimed, the user can use any type of client (Terminal Server, desktop or laptop) with the assigned user account.
• A license is claimed for 45 days. The license claim is renewed at every new session connect.
• On a laptop, the claimed named license is cached. When the laptop goes offline, it is not possible for other users to start a Workspace Control session until the laptop goes online again.

Concurrent licenses

When using Concurrent licenses only, the following applies:

• Workspace Control claims a concurrent license for each active workspace (regardless of user name, client name or computer name).
• Each laptop claims a seat, regardless of user sessions or Datastore connection state. A license claimed by a laptop will remain claimed whether anyone uses the laptop or not.

Combining Named User licenses and Concurrent licenses

Concurrent user licenses and named user licenses can be used together.

When using Concurrent licenses and Named Licenses together, the following applies:

• Workspace Control will use a named user license if it has already been claimed or reserved for the user who is logging on.
• If no license is claimed/reserved, Workspace Control checks whether the current device is a laptop.
  • For laptops, Workspace Control claims a named user license by default. If none are available, the Workspace Control licensing policy is applied.
    • To claim concurrent licenses for laptops from a mixed license pool, during installation, set the public property CLAIMLAPTOPLICENSE to "yes". See (Parameters for) Unattended installation (on page 21) for more information.
    • For other types of devices, Workspace Control claims a concurrent license. If none are available, it will claim a named user license. If no license can be claimed, the Workspace Control licensing policy is applied.
## Special scenarios

- If you use more than one Workspace Control module (**Composition, Governance, Security**), you can still mix concurrent and named user licenses. However, for each license type you need the same number of licenses per module. For more information see **Select Workspace Control Modules** (on page 78).

- If you use several published applications, you only need a license for the first session originating from the same client - even if the sessions run on different servers and the client has no composer running. Prerequisite is that all sessions run using the same database.

- If the originating client uses a local composer, it already has a license in use - any subsequent remote session will not require a license, even if different databases are used.

### Named or Concurrent?

The following examples illustrate several environments with their most advantageous license types:

#### Laptops

<table>
<thead>
<tr>
<th>Case</th>
<th>Why?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000 users: 800 laptops, 200 desktops</td>
<td>Users are bound to a device, so Named is cheaper.</td>
</tr>
<tr>
<td>1000 Named licenses</td>
<td></td>
</tr>
</tbody>
</table>

#### Desktops

<table>
<thead>
<tr>
<th>Case</th>
<th>Why?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000 users: 600 desktops</td>
<td>Less Workspaces than users, so Concurrent is cheaper.</td>
</tr>
<tr>
<td>600 Concurrent licenses</td>
<td></td>
</tr>
</tbody>
</table>

#### Terminal Services

<table>
<thead>
<tr>
<th>Case</th>
<th>Why?</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000 users: 1200 Workspaces at a time</td>
<td>Less Workspaces than users, so Concurrent is cheaper.</td>
</tr>
<tr>
<td>1200 Concurrent licenses</td>
<td></td>
</tr>
</tbody>
</table>

#### Terminal Services and Laptops (1)

<table>
<thead>
<tr>
<th>Case</th>
<th>Why?</th>
</tr>
</thead>
<tbody>
<tr>
<td>800 users: 800 laptops offline, that use Terminal services in the office</td>
<td>Users are bound to a device, so Named is cheaper.</td>
</tr>
<tr>
<td>800 Named licenses</td>
<td></td>
</tr>
</tbody>
</table>

#### Terminal Services and Laptops (2)

<table>
<thead>
<tr>
<th>Case</th>
<th>Why?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1200 users: 400 laptops, 800 Workspaces</td>
<td>Different kinds of usage. Mobile workers that use Terminal Services in the office are better off with Named, but the other 400 active sessions are better off with Concurrent.</td>
</tr>
<tr>
<td>400 Named licenses + 400 Concurrent licenses</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Reserve Named User licenses for laptop users!</td>
</tr>
</tbody>
</table>
5.3.2 Select Workspace Control Modules

When creating a new Workspace Control Datastore at **Datastore > Connections** in the **Setup** menu, you can choose which Workspace Control module(s) you wish to evaluate or use, depending on the required features:

- Workspace Control Core
- Composition
- Governance
- Security

During the 45-day evaluation period, go to **Licensing** in the **Setup** menu and click the **Module(s)** hyperlink to switch modules.

**Combine modules**

When modules are combined, please consider the following:

- The modules require an equal license count to unlock the combined feature sets.
- If you have an unequal number of licenses for two or three different modules, the number of the first module for which licenses were imported becomes the default number of licenses.
  
  In any situation, adding licenses for a second or third module will not decrease the total number of licenses, nor the feature set that is available, unless you choose to do this. In this situation, you can choose an alternative combination of the unequal number of licenses for two or more modules via the module(s) hyperlink on the **Licenses** tab at **Setup > Licensing**.

**Examples**

**Scenario 1** - equal number of licenses for two modules:

- 200 Composition named licenses (initial module licenses)
- 200 Governance named licenses are added to your Workspace Control environment

Result: 200 named licenses for **Composition + Governance**

**Scenario 2** - lower license count for second module:

- 200 Composition named licenses (initial module licenses)
- 100 Governance named licenses are added to your Workspace Control environment

Result: 200 named licenses for **Composition**

Alternative: 100 Composition + Governance named licenses - this decreases the number of available licenses from 200 to 100 in your Workspace Control environment.

**Scenario 3** - higher license count for second module:

- 100 Governance named licenses (initial module licenses)
- 200 Security named licenses are added to your Workspace Control environment

Result: 100 named licenses for **Governance + Security**. Note that this means that you have 100 unused **Security** licenses.

Alternative: 200 Security named licenses - this increases the number of available licenses from 100 to 200 in your Workspace Control environment, but you lose the features that belong to the Governance module.
Scenario 4 - Named and concurrent license combinations:

- 200 Security named licenses (initial module licenses)
- 100 Security concurrent licenses (initial module licenses)

Result: 300 Security licenses (200 named + 100 concurrent).

If you add:

- 200 Composition named licenses

Result: 300 Security licenses (200 named + 100 concurrent)

Alternative: 200 Composition + Security named licenses. Note that this means that you have 100 unused Security concurrent licenses.

If you then add:

- 100 Composition concurrent licenses

Result: 300 Composition + Security licenses (200 named + 100 concurrent)

Choose alternative license combinations

If one or more alternative choices are available, the Module(s) label (on the Licenses tab at Setup > Licensing) becomes a hyperlink to open a window where you can set the active license combination.
5.3.3 Licensing Process

In Workspace Control, licenses need to be imported, registered and activated, using the License Wizard.

![Diagram showing the process of importing, registering, and activating licenses]

**Step 1: Import licenses**

1. Save the license file that you received by e-mail to an accessible location.
2. Open the License Wizard and select Add license.
3. Follow the prompts to import a license into the Datastore.
4. At the end of the process, you will be prompted to activate your license(s). If you have more licenses to import, first import these.
5. When you have completed the import process, your licenses and all relevant information will be shown in the Licensing node.

**Step 2: Register and activate the licenses**

Imported licenses need to be activated within 30 days.

Start the License Wizard. Workspace Control will scan for any license that has not been activated and activate all of them at the same time. The Site ID will be activated automatically when you activate your licenses: it does not need to be registered separately.

1. In the License Wizard select Register and automatically activate license(s).
2. Follow the prompts to register and activate your licenses.
   - The name of your site links your licenses to your business and must therefore be a unique name.

   In certain situations, automatic activation of licenses is not possible. In these situations, follow the prompts to activate your license(s) manually. The information is stored in a text file that you can send to Ivanti:
   - **Web**: e-mail the activation request from the Ivanti website.
   - **E-mail**: e-mail the activation request to Ivanti directly from an e-mail client on the computer running the Console (requires a configured MAPI-compliant e-mail client).
   - **Save to file**: save the activation request as a text file that you send to activations_emea@ivanti.com.

   Within 24 hours during workdays, Ivanti will send an activation file to the mail recipient that you specified. Save the activation file to an accessible location, open the License Wizard and select Import activation file for license(s).

When you have activated your licenses, the Licensing node will display an overview of your licenses, including license type, site and license status and the number of licenses that are available and claimed. The active Workspace Control Modules are also displayed on this node.

⚠️ **Warning**

License files and activation files contain crucial information. **Do not edit these files, because it will render them useless.**
5.3.4 **VDX Licensing**

If you use Workspace Control in combination with VDX, you can choose to manage VDX licensing through Workspace Control. In that case, VDX licenses are stored in the Workspace Control Datastore.

At **Licensing > VDX Clients** in the **Setup** menu, you can view a list of all VDX Client licenses that are in use in your Workspace Control environment. Workspace Control offers the following functionality for VDX Licenses:

- When a user workspace session is started, the VDX Engine will retrieve its license through Workspace Control.
- If no licenses are found or if the number of available licenses is insufficient, the VDX Engine will start looking for a VDX licensing server outside the Workspace Control environment.
- Click **Reserve** to reserve a license for a specific client. Once a license is reserved, this license will remain reserved until released or used.
- To release a reserved VDX Client license, select it and click **Release**.

**Note**

For more information about Ivanti VDX, see the **VDX Guide**, available at [http://forums.ivanti.com](http://forums.ivanti.com).
5.4 Management Portal

At **Setup > Management Portal**, you can integrate the Workspace Control Management Portal in your environment.

**Management Portal Integration**

If you use Management Portal Integration, you are redirected to the Workspace Control Management Portal for the **Workspace Analysis** and **Audit Trail** features.

**Configuration**

Enter the **Management Portal URL** and **Port** for the Management Portal you installed separately.

For more information about the Management Portal installation and prerequisites, please refer to the Workspace Control Management Portal documentation that is available at [http://forums.ivanti.com](http://forums.ivanti.com).
5.4.1 Windows Authentication for 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 Workspace Control 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 Workspace Control 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 Workspace Control 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 Workspace Control Management Portal runs, needs to have the following permissions on the installation folder (by default, this is C:\Program Files (x86)\Ivanti\Workspace Control\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).
5.5 Usage Tracking

Usage Tracking (at Setup > Usage Tracking) allows you to monitor the actual use of applications per user, per application, or per server. It also lets you monitor active sessions and the actual CPU load of an application. You can use this information to find users or applications that use a more than average amount of system resources, to re-distribute licenses, or simply for troubleshooting.

The Usage Tracking Viewer is available from Setup > Usage Tracking and from Diagnostics > Usage Tracking Overview. In the user session, the Usage Tracking Viewer is available from the Start menu > Workspace Control settings > Workspace Preferences > Other tab. The Usage Tracking Overview is available from Diagnostics > Usage Tracking Overview.

5.5.1 Set up Usage Tracking

The following options are available when setting up Usage Tracking:

- **Log current activity**: logs all activity in real-time, making it possible to see instantly which users are using which applications.
- **Log history**: if selected, all application usage is logged.
  - **Detailed history** logs specific dates and times of usage. For example: a user started Microsoft Word on Monday between 11:00 and 13:00, and on Tuesday between 15:00 and 16:00.
    This information is shown on the Details tab of the Usage Tracking Viewer, and includes the following data:
    - when the application was used
    - by whom
    - for how long
    - on which system
    - what the processor usage was for that application during the time it was used.
  - **Cumulative history** does not include specific dates and times, but cumulates the application usage data for the specified period. For example: a user had Microsoft Word open for a total of 3 hours in Week 2017-12.
    It includes the following data:
    - when the application was used
    - by whom
    - for how long
    - on which system
    - what the processor usage was for that application during the time it was used.
- **Log Session Information**: logs all information concerning sessions. The storage duration of the session information depends on the number of days you enter in the Keep session history field.
- **Anonymous logging**: filters user names from the information provided. This can be used to protect users’ privacy.
- **Enable Usage Tracking access for end-users and application managers**: provides end users and Application Managers with access to Usage Tracking from within their Workspace Control session. A user can only see personal information about his own sessions and applications. An Application Manager can only see information related to the applications he manages.
- **Enable Website Usage Tracking and log web sites visited by Internet Explorer**: logs all websites visited by the end user. If selected, you also need to enable third-party browser extensions in Microsoft Internet Explorer (via Tools > Internet Options > Advanced > Browsing > Enable third-party browser extensions or via Microsoft Windows system policies that are set up for your company. Microsoft Internet Explorer Enhanced Security Configuration disables this option by default.
• **Log path and executable in addition to application name:** logs the application path, executable and name. This can be used to distinguish between different applications with the same name, which can be useful when comparing application usage for reporting purposes.

<table>
<thead>
<tr>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>• In some countries or companies, Usage Tracking can conflict with privacy policies. If so, it is advisable not to use Usage Tracking.</td>
</tr>
<tr>
<td>• The Usage Tracking database only stores OU information on the lowest OU level. This means that if the OU structure changes, the information displayed by Usage Tracking will change accordingly.</td>
</tr>
<tr>
<td>• The Usage Tracking settings <strong>Log current activity</strong>, <strong>Log history</strong> and <strong>Anonymous logging</strong> also apply to WebTrace.</td>
</tr>
<tr>
<td>• If you enable Usage Tracking access for end users, they can view their website usage in the Usage Tracking viewer.</td>
</tr>
<tr>
<td>• Microsoft Internet Explorer instances running as a Workspace Extension (RES Subscriber for VDX and VDX) are not tracked by WebTrace.</td>
</tr>
</tbody>
</table>

### 5.5.2 The Usage Tracking Viewer

The **Usage Tracking Viewer** shows all information gathered by Usage Tracking, either in detail or as a graphical representation. For reporting purposes, the information can be copied to the clipboard, to be pasted into a spreadsheet or word processor file.

Please note the following:

• The Usage Tracking Overview only shows information from the Datastore that is defined at **Setup > Datastore**.

• The Usage Tracking Viewer does not show any information about Organizational Units if Organizational Unit support has not been configured in the Management Console.

• The Usage Tracking database only stores Organizational Unit information on the lowest Organizational Unit level. This means that if the Organizational Unit structure changes, the information shown by Usage Tracking changes accordingly.

• If **Website Security** is enabled (at **Security > Applications > Websites**), the secured browsers that are visited by the user in a user session are shown in the Usage Tracking Overview.

• In all overviews of the Usage Tracking Viewer, you can click ![button](image) to create an Instant Report (first click **Refresh** to update your data) and ![button](image) to export data to a file (CSV for lists and JPG for graphs).

• On the tabs **Details**, **Sessions** and **Current Activity** in the Usage Tracking Viewer, you can type a search string to search for an object (e.g. user, application, computer or client). Previous search items are retained and using wildcards (*) in your search is allowed.

• Computer names of extended applications are preceded with an asterisk (*) in the Usage Tracking Overview.

• With **Microsoft Remote Assistance** integration (at **Setup > Integration**) and **Usage Tracking** enabled, when starting a Remote Assistance session via the Management Console (at **Diagnostics > User Sessions**), an entry is logged in the **Usage Tracking Overview** of the session that was remotely helped.
5.5.3 **Reporting Services for Workspace Control**

Reporting Services is an (open) Web service that allows the retrieval of Usage Tracking data from the Datastore. The Usage Tracking feature is available in the Delegation and Compliance module of Workspace Control.

This data can be used to create reports tailored to your organization's needs, without clients needing to have direct access to the Datastore. Clients can be anything from users, other Web applications to other Web services.

The information to be examined can focus on the following areas:

- Usage Tracking details
- User metrics
- OU metrics
- Application metrics
- Web Site metrics
- Computer metrics
- Sessions metrics
- Current Activity metrics

To help specify search criteria, several search methods can be used:

- Search User
- Search OU
- Search Application
- Search Web Site
- Search Computer

Workspace Control Reporting Services needs to be installed separately by someone with sufficient Administrative rights.

Workspace Control Reporting Services needs to be installed on a machine running Workspace Control that is connected directly to the Datastore.

For further details about Reporting Services, see the document **Workspace Control Reporting Services** which is available at [http://forums.ivanti.com](http://forums.ivanti.com).

---

**Note**

Existing users of the Workspace Control Reporting Services will need to review and amend their configuration file to reflect changes in the listening address.
5.6 Integration

The Integration features of Workspace Control allow you to integrate other products in Workspace Control.

- Citrix XenApp Publishing (on page 90)
- Microsoft App-V (on page 101)
- Microsoft TS RemoteApp (on page 106)
- VMware ThinApp (on page 110)
- LANDesk (on page 111)
- Microsoft Remote Assistance (on page 112)
- Microsoft System Center (on page 113)
## 5.6.1 Alerting

With Alerting, you can set up actions that are performed automatically if a certain event occurs in Workspace Control that affects the security or functioning of your infrastructure. These can be e-mail notifications, SNMP notifications, external tasks and Automation Tasks.

### Where to find Alerting

<table>
<thead>
<tr>
<th>What</th>
<th>Where</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alerting</td>
<td>Go to Alerting in the Setup menu</td>
</tr>
</tbody>
</table>

### Set up Alerting

When setting up Alerting, the Events tab gives an overview of all Workspace Control events that may trigger an automatic action. These notification types can be set up on the Notification Types tab.

- When you set up e-mail notifications, you can only send e-mails anonymously if your mail server supports this. If it does not, you need to enter a valid user name and password. The mail relay must be configured to allow access to every Workspace Control Agent and not, for example, block them based on their IP address.
- SNMP notifications ("traps") can only be received correctly in an SNMP framework (such as HP OpenView or CA Unicenter) when you import or load the "resworkspacemanager.mib" file (in the Workspace Control program folder) into this application. You also need to configure the correct destination for the SNMP traps: use "255.255.255.255" to broadcast the trap on the local network or use one or more specific IP addresses to send the traps to one or more specific computers. Workspace Control uses its own mechanism when sending SNMP traps and therefore does not require the installation of SNMP agent software on Workspace Control Agents.
- External tasks are useful to execute a specific command when an event occurs (for example, lock a user's ID after three warnings).
- You can only select Automation Tasks if you have enabled Automation Integration (at Setup > Integration > Ivanti Products > Automation).
  - If the selected Automation Project or Module contains parameters, these will be shown in the Parameters area.
  - The Schedule timeout field specifies how long Workspace Control should wait for the task to be scheduled by Automation before it will proceed with the next task or process.
  - All Automation alerting tasks will be logged in the Automation log. See Automation.
- You can configure multiple notifications per notification type (for example, a notification that sends an e-mail and executes a command).

### Alerts for Workspace Control licenses

- Use the License threshold reached event in combination with the Licensing option License alerting threshold (at Setup > Licensing, on the Licenses tab). See Licensing for more information.
- Use License alerting threshold in combination with the Alerting event License threshold reached, to set up an alert before all licenses have been claimed.
### 5.6.2 Application Virtualization

#### Citrix XenApp Publishing

With Citrix XenApp Publishing integration, you can integrate Citrix XenApp published applications and published content into the user workspace and manage it from the Management Console. A Citrix XenApp published application is an application that runs on a Citrix XenApp server, but which behaves as if it were running on the user's local computer. Citrix XenApp published content allows you to publish files (document files, media files, Web URLs, etc.) from any network location in your environment.

<table>
<thead>
<tr>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Workspace Control (full installation) must be installed on at least one of the Citrix servers in the farm to be integrated with Workspace Control. Citrix Studio must also be configured on this Citrix server. It is advised to install Workspace Control on more machines for redundancy purposes. This is necessary to be able to handle publishing activities and to retrieve updates concerning delivery groups.</td>
</tr>
<tr>
<td>• Follow the instructions described in the article &quot;How to Configure Citrix Receiver Pass-Through Authentication for StoreFront or Web Interface&quot; (available at <a href="http://support.citrix.com/article/CTX133982">http://support.citrix.com/article/CTX133982</a>) to configure your Citrix Receiver to work in combination with Workspace Control.</td>
</tr>
<tr>
<td>• The Workspace Control Agent must be installed on each Citrix Virtual Desktop Agent that needs to be managed by Workspace Control.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Tips</th>
</tr>
</thead>
<tbody>
<tr>
<td>• When integrating Citrix XenApp 7.x with Workspace Control, it is recommended to use Citrix StoreFront 2.x and Citrix Receiver 4.x.</td>
</tr>
<tr>
<td>• In case Citrix Receiver 4.x is used together with Citrix StoreFront, it is highly recommended to enable SSON to prevent authentication requests within the user session. See for more information the following Citrix article: &quot;How to Configure Citrix Receiver Pass-Through Authentication for StoreFront or Web Interface&quot; (available at <a href="http://support.citrix.com/article/CTX133982">http://support.citrix.com/article/CTX133982</a>).</td>
</tr>
</tbody>
</table>

#### Where to find Citrix XenApp Publishing

<table>
<thead>
<tr>
<th>What</th>
<th>Where</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting up integration with Citrix XenApp publishing</td>
<td>In the Setup menu, go to Application Virtualization &gt; Citrix XenApp Publishing</td>
</tr>
<tr>
<td>Setting up Citrix XenApp published applications</td>
<td>Open or create a managed application at Composition &gt; Applications and go to the Publishing tab in its Properties section.</td>
</tr>
</tbody>
</table>
Integrate Citrix XenApp Publishing

When setting up integration with Citrix XenApp Publishing, you first need to set the correct settings and defaults before you can publish applications.

Requirements

- Workspace Control must be installed on at least one of the Citrix servers in the farm to be integrated with Workspace Control. If Relay Servers are used in your Workspace Control environment, make sure the version of the Relay Servers is identical to the highest version of the Agents in the environment.

Workspace Control has two different mechanisms for Citrix XenApp publishing:

- The **local publishing** mechanism is used when the Workspace Control Console is running on a Citrix XenApp server and you publish to the farm to which this Citrix XenApp server also belongs. Local publishing is executed by the Workspace Control Console.

- The **remote publishing** mechanism is used when the Workspace Control Console is not running on a Citrix XenApp server, or when the Workspace Control Console is running on a Citrix XenApp server in a different farm than the target farm. Remote publishing is executed by the Workspace Control Agent Service running on the target Citrix XenApp server.

Publishing a single application or content to multiple farms may trigger both mechanisms.

On each Citrix XenApp server to which Workspace Control will publish, the account running the RES Agent Service must be either local system or a domain account with Full Administration Privileges in the Citrix farm.

For local publishing, the account running the Workspace Control Console must be a user account with Full Administration Privileges in the Citrix farm. For remote publishing, the account running the Workspace Control Console is irrelevant.

If you have Citrix XenApp 6.5 Session Host Only servers (Worker) configured in your environment, consider the following requirements:

- Workspace Control must be installed on one or more Citrix XenApp Controllers (Zone Data Controllers). For redundancy purposes, it is preferred to have Workspace Control installed on two or more Citrix XenApp Controllers. This is required for the following:
  - To retrieve available Citrix XenApp Worker Groups and make them available in the Workspace Control environment.
  - Execute Citrix application publishing in case applications are published from a Workspace Control Console that is running on a Citrix XenApp Session Host Only server.
  - For Agents running on a Citrix XenApp Controller, the option **Poll for changes** must be set to **Every 5 seconds** (at **Administration > Agents**, on the **Settings** tab).
Chapter 5: Setup

Notes

- Workspace Control Console users can only change the Citrix folder to which a specific application is to be published if they are running the Console on a Citrix server AND the account running the RES Agent Service has Full Administration Privileges in the Citrix farm.
- To successfully publish applications from a machine on which the Microsoft Windows option User Account Control (UAC) is enabled, the Management Console needs to be started as Run as Administrator on that machine.
- A standard 30-second timeout applies to remote publishing tasks. For Citrix XenApp servers to which managed applications will be published remotely, the Agent setting Poll for changes should therefore be set at 5 seconds (at Administration > Agents). A longer interval may cause publishing to fail. The Agent setting Update agent cache on change does not affect Citrix XenApp publishing.
- Linger Citrix XenApp applications started by Workspace Control will not show the status 'lingering' on the Citrix server. This is caused by the way Workspace Control starts Citrix published applications.
- To enable Session Linger for Citrix XenApp 7.5 and 7.6, the following registry values can be set:
  - LingerDisconnectTimerInterval (on page 353)
  - LingerTerminateTimerInterval (on page 354)
- For Citrix Session Prelaunch to work, the following prerequisites need to be met:
  - the Citrix server needs to be configured to launch the Workspace Composer automatically (Administration > Agents, on the Agents tab, select Automatic for Run Workspace Composer)
  - a Citrix Receiver needs to be started on the client.

Configuration

On the Settings tab, configure general settings for the Citrix XenApp integration in your Workspace Control site:

- Clicking the Test Publishing Ability button will, for the machine it is used on, test to which available Citrix XenApp 7.x sites within the Workspace Control environment it can publish. The machine must be a delivery controller or Citrix Studio must be installed on it.
  - For previous editions of Citrix XenApp, the Test Publishing Ability button can only be used on a Citrix XenApp server, and the publishing ability of only the farm that the server belongs to, is looked at.

Note

To successfully use the Test Publishing Ability button on a machine on which the Microsoft Windows option User Account Control (UAC) is enabled, the Management Console needs to be started as Run as Administrator on that machine. Starting the Management Console normally, would cause a message to be displayed about the user not having sufficient access rights (even if this is not the case).

- The field ID used by Workspace Control contains the name of the CMC folder used by Workspace Control when creating Published Applications. You can change this ID if you use two or more Workspace Control Datastores in one Citrix farm. The different IDs for each Workspace Control Datastore will then keep the Published Applications unique in the farm.
- It is possible to assign an application to one or more Organizational Units. When publishing this application in a Citrix environment, all users in the selected Organizational Units are listed and added to the list of users for the published application. However, the users present in the selected Organizational Units may change over time, and these changes need to be reflected in the list of users for the Published Application. Workspace Control will do this automatically at the time specified in the field Rebuild userlist for OU based Published Applications every day at: At the time specified, one of the Citrix servers using this Datastore will go through the list of applications which are configured to use OU-based access control, and which are published in Citrix. For these applications, the selected OUs are read and the resulting list of users is matched to the application's current list of configured users and changed accordingly.
• If an ICA Seamless Host Agent message should be shown when a user logs on, select **Do not suppress message from ICA Seamless Host Agent during logon.** This message is shown if the user connects seamless to a published XenApp desktop via the ICA client and the Terminal Session uses the Microsoft Windows shell. The message is suppressed if the Workspace Control shell is used.

• Select **Use RESPFDIR environment variable in command line of published application** to use the system environment variable `RESPFDIR` in the command line of a published XenApp application when that command line refers to the Workspace Control installation folder. (This system environment variable is created by the Workspace Control Agent Service.) Use of this environment variable makes it possible to publish an application across multiple computers with different Workspace Control installation locations. This option should only be used when the system environment variable `RESPFDIR` is available on all computers that the application is published to. To ensure this, either make sure RES PowerFuse 2008 or higher is installed on all computers, or manually create the system environment variable on all computers running a version of Workspace Control older than RES PowerFuse 2008.

• To make Workspace Control components available as published applications, select the relevant check boxes at **Publish the following Workspace Control components for authorized users.** The access control settings of these published applications will match those of a Workspace Control desktop session (e.g. only application managers will be added to the user list for the Access Wizard, etc.).

• To create a published server desktop, use the Citrix XenApp Console and a GPO to launch the Workspace Control desktop. See **Configure the Ivanti Workspace Composer as a Citrix XenApp Published Application** (“Configure the Workspace Composer as a Citrix XenApp Published Application” on page 94).

• The button **Add or remove Citrix XenApp servers to or from existing applications** opens a wizard that will guide you through the process of adding or removing Citrix servers to or from the list of configured Citrix servers for selected application(s). For example, you can add a new Citrix server “CTX10” to all applications that already have Citrix server “CTX01” in their list of configured Citrix servers.

**Defaults tab**

On the **Defaults** tab, you can configure the default settings for all Citrix XenApp published applications and published content. Any managed application for which you enable Citrix XenApp publishing will be preconfigured with the defined default settings.

All these default settings can then be changed for each individual managed application, with the exception of the **Instant Passthrough** (on page 95) setting **Use template ICA file.** Selecting this option defines a global custom ICA file that will be used for ALL instant passthrough connections and will overrule any ICA files configured at application level. To create a custom ICA file per published application, ensure that the global option **Use template ICA file** is NOT selected. Then, for each Citrix published application for which the default ICA file generated by Workspace Control does not suffice, go to the application’s **Publishing** tab, select **Use a custom ICA file for this application** and click [Edit].

To update the available servers / groups list, click the **Refresh** button. This button is only available when using the Workspace Control Console on a machine with Citrix Studio installed on it or when using the Workspace Control Console on the Citrix Delivery Controller. Every 12 hours, Workspace Control updates the list with available Delivery Groups for all configured Citrix Sites if both Workspace Control and a Citrix Delivery Controller (per Citrix Site) are installed on the machine or if Workspace Control and Citrix Studio (per Citrix Site) are installed on the machine.
Server Groups tab

Server Groups are a Workspace Control mechanism to combine multiple Citrix XenApp servers (only for Citrix XenApp 6.5) into a single unit. They are typically used to represent silos. After defining a Server Group, you can select this Server Group instead of selecting each individual Citrix XenApp server (only for Citrix XenApp 6.5) when publishing an application.

Whenever you change the members of a Server Group, any application that references this group will automatically be republished.

Citrix XenApp 7.x tab

On the Citrix XenApp 7.x tab, you can configure Citrix XenApp 7.x delivery controller(s) to publish applications. Multiple delivery controllers per site can be specified, to create redundancy for Citrix XenApp 7.x application publishing. Use a semicolon (;) to separate multiple Delivery Controllers. A DNS entry is allowed as a delivery controller. These delivery controllers will be used to publish applications for which delivery groups for the same site are selected (at Composition > Applications, on the Properties > Publishing > Citrix XenApp Published Application tab of an application).

Per Citrix Delivery Controller, specify the credentials for Workspace Control to use. If no credentials are specified, the credentials of the Console user (local publishing) and the Workspace Control service (remote publishing) will be used. In all cases, the credentials must be of a user with at least Citrix 'Delivery Group Administrator' role permissions.

Note

Citrix Delivery Groups cannot be created or managed from within Workspace Control. This needs to be done in Citrix Studio.

Tips

• When creating Citrix Delivery Groups in Citrix Studio, it is recommended to allow “Domain Users”. Restricting users per Delivery Group is possible, but this will affect, for example, applications that are published to All Users from the Workspace Control Console.

• At http://support.citrix.com/article/CTX200337 you can find possibilities to shorten the time Citrix Receiver needs to generate its XML cache file.

Specify credentials for Use the following credentials to communicate with Citrix XenApp servers. If no credentials are given, the credentials of the Console user and the Workspace Control service will be used. In all cases, the credentials must be of a user with at least Citrix 'Delivery Group Administrator' role permissions.
Configure the Workspace Composer as a Citrix XenApp Published Application

Configuration

To let the Workspace Control Desktop start on a Terminal Server:

- In the Citrix Console, publish a Citrix server desktop.
  - Depending on your Citrix XenApp edition, it may differ how a Citrix server desktop is published. For more information, refer to your Citrix documentation.
- In Microsoft Active Directory, configure a GPO:
  - Go to User Configuration > Administrative Templates > System > "Custom User Interface".
  - Enter the correct path to pfwsmgr.exe. This starts Workspace Control when a user launches a Citrix Desktop.
  - Create the GPO:
    - Go to User Configuration > Administrative Templates > System > "Custom user interface".
    - Enter the correct path %RESPFDIR%\pfwsmgr.exe.
  - Enable loopback processing on this GPO:
    - Go to Computer Configuration > Administrative Templates > System > Group Policy > "User Group Policy loopback processing mode".
    - Enable this setting in Replace mode.
  - Configure security for the GPO:
    - On the Security tab of the GPO properties (Delegation > Advanced), add the group containing all users for whom you want a Managed Desktop.
    - You can remove (or deny) the "apply-rights" for your administrative accounts.
  - Link the GPO:
    - Link the GPO to the OU where your Citrix Servers exist in the Microsoft Active Directory.

Notes

- For Citrix XenApp 6.5 you should use the Citrix AppCenter.
- For Citrix XenApp/XenDesktop 7.x you should use Citrix Studio.

This best practice applies to:

**Set up Instant Passthrough for Citrix XenApp published applications**

**Where to find the Instant Passthrough settings window**

<table>
<thead>
<tr>
<th>What</th>
<th>Where</th>
</tr>
</thead>
</table>
| Global default Instant Passthrough settings | In the Setup menu, go to Application Virtualization > Citrix XenApp Publishing.  
Go to the Defaults tab.  
Select Enable Instant Passthrough for computers not publishing this application  
Click the button [Settings…] |
| Instant Passthrough settings for a specific managed application | Open or create the managed application at Composition > Applications.  
Go to the Publishing tab in its Properties section  
Select Enable Citrix XenApp Application Publishing  
Select Enable Instant Passthrough for computers not publishing this application  
Click the button [Settings…] |

Use the **Instant Passthrough** mechanism to start a Citrix XenApp published application on a remote server, using either an ICA file generated by Workspace Control or a custom ICA file. The ICA file points to the application on the remote server and is stored in the Workspace Control Datastore in the \TPI\ICA subfolder.

When a user starts the application, the request will automatically be redirected to the remote server on which the application is located, after which the remote server will publish the application to the user's desktop.

**Note**

Instant Passthrough is not supported when publishing an application to multiple server farms. If the selection of Configured Servers contains servers from different farms, Instant Passthrough is automatically disabled for this application.

If an application changes from being published to multiple farms to being published to a single farm, then the Instant Passthrough option becomes available again. (The configuration of this option will have reverted to the global default configuration for Instant Passthrough.)

**Configuration**

In the **Instant Passthrough settings** window, you can configure the settings for the passthrough mechanism and the ICA file.

- If you access this window from the global Citrix XenApp Integration node, you are defining the default Instant Passthrough settings for all Citrix XenApp published applications in your environment.
- If you access this window from the Publishing tab of a managed Citrix XenApp published application, the Instant Passthrough settings apply only to that application. Please note that if global Instant Passthrough settings have been configured (at Setup > Integration > Citrix XenApp Publishing, on the Defaults tab), but the option Enable Instant Passthrough for computers not publishing this application has been unchecked, the configured settings will still be shown when enabling Instant Passthrough on application level (at Composition > Applications, on the Properties > Publishing > Citrix XenApp Published Application tab of an application).
Properties tab

- To use the TCP/IP+HTTP network protocol to locate and connect to the ICA Server, select *Use TCP/IP+HTTP browsing*.
  - To use SSL to locate and connect to the ICA Server, select *Use SSL to browse and connect* and enter the server name and port of the ICA server.
- Select how passthrough authentication should be handled:
  - If Workspace Control handles the authentication, then the parameters /username, /domain, and /password will also be passed to the ICA client with the correct values.
  - If Citrix XenApp handles the authentication, then the ICA file will be passed to the ICA Client without any additional parameters.
- By default, Workspace Control generates an ICA file for each Instant Passthrough connection.
  - To create a single custom ICA file for all Instant Passthrough connections, select *Use template ICA file* and click [Edit]. Please note that this defines a global custom ICA file that will be used for ALL instant passthrough connections and will overrule any ICA files configured at application level.
  - To create a custom ICA file per published application, ensure that the global option *Use template ICA file* is NOT selected. Then, for each Citrix published application for which the default ICA file generated by Workspace Control does not suffice, go to the application's Publishing tab, select Use a custom ICA file for this application and click [Edit].
- In the Passthrough method area, configure how the passthrough should be made available. Launching the passthru connection using the Citrix Program Neighborhood Client or Agent can be useful, for example, when smartcards are used for authentication:
  - Use the Citrix Program Neighborhood Agent: if you select this option, the passthrough connection is established by launching pnagent.exe with the correct parameters. When using Legacy Citrix Receiver 3.x (with PNA) with Citrix StoreFront, configure Citrix Receiver 3.x to connect to the Citrix XenApp Services URL (in the Citrix Storefront console at Stores -> Configure Legacy Support). In this situation, the name to fill in for XenApp Services Site Farm Name is the "Citrix Store Service Delivery Controller name".
  - Use the Citrix Program Neighborhood client: If you select this option, the passthrough connection is established by launching pn.exe with the correct parameters. Because one of these parameters is the name of the application set, you also need to provide this name.
  - Use an ICA file:
    - Standard Workspace Control ICA file or Use template ICA file: If you select either of these options, Workspace Control will launch wfcrun32.exe using the Standard Workspace Control or template ICA file.

Behavior tab

With the option Do not passthrough if application is available on local computer selected, the published application will only be launched if there is no local version of the application available.

- If the user logs on to a computer on which an application has been published (which is determined by the list of servers on the Servers tab of the Publishing > Citrix XenApp Published Application tab of the application), the application will be started directly (the original command line will be used to start the application).
- If the user logs on to a computer on which an application has not been published (again, determined by the list of servers on the Servers tab), the application will not be started directly. Instead, the Citrix ICA Client will be started with the ICA file passed as a parameter.

You can optionally choose to ignore the configured behavior inside or outside specific Zones via the Locations and Devices field.

- If you configure to passthrough anyway in specific Zones, at least one of the added Zones must apply.
- If you configure to passthrough anyway outside specific Zones, all the added Zones must apply.
**Publish Citrix XenApp Applications**

**Configure a Citrix XenApp published application**

Use the Citrix XenApp tab to configure the application as a Citrix XenApp published application or to publish content. Access to a published XenApp application or published content depends on the settings that you configured on the Access Control tab.

**Citrix XenApp published application**

A Citrix XenApp published application is an application that runs on a Citrix XenApp server, but which behaves as if it were running on the user's local computer. When you configure a Citrix XenApp published application in the Management Console, this will create the published application in the Citrix XenApp environment, including all options and access control types that have been configured in the Management Console. The command line of the Citrix XenApp published application will point to Workspace Control with the application ID as a parameter, so that the application will be managed by Workspace Control. Citrix Storefront KEYWORDS can be entered in the Description field of the application. The parent menu structure of the application will be used as the Program Neighborhood Folder property of the application. This property changes automatically when you change the name of one of the parent menus or when you move the application to another menu.

**Configuration**

- Open the relevant managed application at Composition > Applications.
- In the Properties section, go to the Publishing tab.
- On the Citrix XenApp Published Application tab, select Enable Citrix XenApp Application Publishing.
- On the Settings tab, configure the settings for the application.
  - When selecting a value in the Colors field, please note that not all settings listed are supported in all Citrix versions. If a color depth is selected that is not supported by the used Citrix version, the nearest supported color depth will be used.
  - If you use Citrix XenApp Secure Gateway, the default encryption level Basic should be sufficient.
  - Instant Passthrough is a mechanism that provides a shortcut to an application located on a remote server. When a user accesses the shortcut, the request is automatically being redirected to a remote server on which the application is located. See Set up Instant Passthrough for Citrix XenApp published applications (on page 95) for more information.
  - To specify the folder in the Citrix Access Management Console to which the application needs to be published, click the button in the Citrix folder section and select the applicable folder.
    If multiple Citrix Server farms are integrated into your Workspace Control site, the browse window for selecting a folder will show a merged list of all the relevant folders on the relevant farms. If a selected folder does not exist on each farm, the folder will be created there. Please note that Citrix Administrator rights are required to create a new folder on the Citrix server. Otherwise publishing will fail to farms on which the folder needed to be created.
    - To publish configured file types as content redirection for published applications, select Enable content redirection (using configured file types).
    - To revert to the default settings as configured on the Defaults tab at the global node Setup > Integration > Application Virtualization > Citrix XenApp Publishing, click the button [Restore defaults...].
  - On the Client Settings tab, configure in which folders and with which shortcuts the published application should be exposed to the end user. Also specify the Category that should be used to group the applications in the Citrix Receiver.
  - On the Servers tab, configure to which servers, Server Groups and/or Citrix Worker Groups the application should be published.
The list of Available servers / groups is populated automatically by Workspace Control. It shows all the site's Server Groups and Agents that are Citrix servers, and all the Citrix Worker Groups from the farms in your Workspace Control site.

Changes to the Citrix Worker Groups are automatically processed every 12 hours. To refresh this information immediately in the lists of Available servers / groups and Configured servers / groups, use the Refresh icon button.

To define a Server Group, go to the Server Groups tab at Setup > Integration > Application Virtualization > Citrix XenApp Publishing (Citrix XenApp 6.5).

Optionally, click the Load Evaluators tab to assign a specific Citrix Load Evaluator to a Citrix XenApp published application (Citrix XenApp 6.5). To participate in load management, each server or published application must have a load evaluator assigned to it. The rules and their settings determine how the load of a particular server or published application is managed.

For XenApp 6.5, only one load evaluator can be selected. For earlier versions of XenApp, it is possible to assign a different load evaluator per configured server.

Note that if a server is added to a server group that is assigned a specific load evaluator, the application will be republished to all servers using the configured load evaluator.

When you click OK to close the application, it is (re)published on the specified servers with the specified settings.

**Notes**

- The value 'CTX' in the Published column on at Composition > Applications > Application List indicates that the managed application is a Citrix XenApp published application.
- The value 'CTX (failed)' in the Published column indicates that the application is configured as a Citrix XenApp published application, but that it has never been published to Citrix successfully from the current Workspace Control environment. This situation can occur if Citrix XenApp applications are imported from a Building Block.
- Refreshing Citrix Worker Groups from the Workspace Control Console is not available for Citrix XenApp 6.5 Host Only servers.
- If access to a published application is based on, for instance, OU membership or Identity Director service (configured on the Access Control > Identity tab of an application), a command line to republish a published application can be used. The command line is `%respfdir%\pwrtech.exe /republishusers {AppID | AppGUID}. See the Workspace Control Administration Guide for more information.
Configure a managed application as Citrix XenApp published content

Citrix XenApp published content is a file (such as a PDF document, a media file, or a URL) in any network location in your environment. When the content is published, a shortcut to the document is placed in the end user’s Start Menu.

**Configuration**

- Open the relevant managed application at **Composition > Applications**.
- In the **Properties** section, go to the **Publishing tab**.
- On the **Citrix XenApp Published Application** tab, select **Enable Citrix XenApp Application Publishing**.
- Select **Publish as Content**.
- On the **Client Settings** tab, configure in which folders and with which shortcuts the published content should be exposed to the end user.
  - Because Content Publishing only requires a command line and Access Control, all other application configuration options will be disabled.
- Return to the application's **General tab** in the **Properties** section and ensure that the **Command line** field specifies the path to the location of the content that you want to publish.

This check is necessary because if you enter a path to a file in the **Command line** field when creating a managed application, Workspace Control checks if there is a file type defined for that file extension. If so, the command line is automatically changed to the application executable, and the file is added as a parameter. For example, `C:\temp\test.xls` in the command line will be changed to `...\...\excel.exe` if Excel is associated with the file type XLS. This is not desirable if you are publishing the file as content.

Publish Citrix XenApp applications manually

**Configuration**

- In the Workspace Control Management Console, go to the node **Composition > Applications**.
- Click **New Application (using Wizard)** to create an application in Workspace Control. This opens a wizard. Follow the steps of the wizard to configure the basic settings of the application. When you have finished the wizard, the **Edit application** window opens. Click **OK** to close the window.
  - Remember the application GUID or ID for later use.
- Open the Citrix XenApp Management Console and create a published application.
  - When specifying the application executable, enter `pwrgate.exe` with the parameter `[application GUID or ID] "%"` to specify which application should be started.

Each managed application that is created in the Management Console has its own unique ID number and GUID.

You can find the ID of a managed application in the **Application List at Composition > Applications**.

The ID and the GUID are shown when you open the application for viewing or editing (on the **General tab in the Properties section**).

Add and remove Citrix XenApp Servers using the command line

You can use command-line parameters to add or remove Citrix XenApp servers to server groups without using the Management Console. This is typically used in an automated scenario where Automation is used to re-install a Citrix XenApp Server with new software. Tasks can be configured in Automation to remove a server from a Server Group, then to remove the old software from the server, to install the new software, and finally to (re-)add this server to the relevant Server Group.
Command lines

<table>
<thead>
<tr>
<th>Action</th>
<th>Command line</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add a Citrix XenApp server to a server group</td>
<td><code>pwrtech.exe /serveradd=&lt;server name&gt; /group=&lt;server group&gt;</code></td>
<td>C:\progra<del>1\respow</del>1\pwrtech.exe /serveradd=CTX10 /group=CTXServerGroup</td>
</tr>
<tr>
<td>Remove a Citrix XenApp server from a server group</td>
<td><code>pwrtech.exe /serverremove=&lt;server name&gt; /group=&lt;server group&gt;</code></td>
<td>C:\progra<del>1\respow</del>1\pwrtech.exe /serverremove=CTX10 /group=CTXServerGroup</td>
</tr>
<tr>
<td>Remove a Citrix XenApp server from all server groups</td>
<td><code>pwrtech.exe /serverremove=&lt;server name&gt; /group=*</code></td>
<td>C:\progra<del>1\respow</del>1\pwrtech.exe /serverremove=CTX10 /group=*</td>
</tr>
</tbody>
</table>

Citrix Provisioning Services

You can also use this technique for Citrix Provisioning Services scenarios. Suppose you have two Citrix XenApp Server silos (a Microsoft Office Silo and an SAP Silo):

<table>
<thead>
<tr>
<th>Server</th>
<th>Silo</th>
</tr>
</thead>
<tbody>
<tr>
<td>CTXSRV001</td>
<td>Office Silo</td>
</tr>
<tr>
<td>CTXSRV002</td>
<td>Office Silo</td>
</tr>
<tr>
<td>CTXSRV003</td>
<td>Office Silo</td>
</tr>
<tr>
<td>CTXSRV004</td>
<td>Office Silo</td>
</tr>
<tr>
<td>CTXSRV005</td>
<td>Office Silo</td>
</tr>
<tr>
<td>CTXSRV006</td>
<td>SAP Silo</td>
</tr>
<tr>
<td>CTXSRV007</td>
<td>SAP Silo</td>
</tr>
<tr>
<td>CTXSRV008</td>
<td>SAP Silo</td>
</tr>
<tr>
<td>CTXSRV009</td>
<td>SAP Silo</td>
</tr>
</tbody>
</table>

Because the SAP silo is overloaded, Citrix Provisioning Services is used to quickly transform servers CTXSRV004 and CTXSRV005 into SAP servers.

<table>
<thead>
<tr>
<th>Server</th>
<th>Silo</th>
</tr>
</thead>
<tbody>
<tr>
<td>CTXSRV001</td>
<td>Office Silo</td>
</tr>
<tr>
<td>CTXSRV002</td>
<td>Office Silo</td>
</tr>
<tr>
<td>CTXSRV003</td>
<td>Office Silo</td>
</tr>
<tr>
<td>CTXSRV004</td>
<td>SAP Silo</td>
</tr>
<tr>
<td>CTXSRV005</td>
<td>SAP Silo</td>
</tr>
<tr>
<td>CTXSRV006</td>
<td>SAP Silo</td>
</tr>
<tr>
<td>CTXSRV007</td>
<td>SAP Silo</td>
</tr>
<tr>
<td>CTXSRV008</td>
<td>SAP Silo</td>
</tr>
<tr>
<td>CTXSRV009</td>
<td>SAP Silo</td>
</tr>
</tbody>
</table>

However, the Citrix XenApp Server farm still thinks that CTXSRV004 and CTXSRV005 are servers on which Microsoft Office has been installed, and the farm will be load balancing Office users to CTXSRV004 and CTXSRV005. As a result, Microsoft Office users will experience that the application is unavailable (because it has not been installed) and SAP users will not be load balanced to these new servers. Therefore, the servers on which these applications are published need to be adjusted, by using the above described method. The Automation Agent can be embedded in the Citrix Provisioning Services image together with a Workspace Control installation. When the image gets online, Automation and Workspace Control will automatically perform the necessary steps.

Do not passthrough if available locally

Instant Passthrough for Citrix XenApp publishing has the option to Do not passthrough if application is available on local computer. This option gives the ability to define when a published or local version of the application is launched. You can optionally choose to ignore the configured behavior inside or outside specific Zones via the Locations and Devices field.
Microsoft App-V

With Microsoft Application Virtualization integration, you can integrate Microsoft App-V applications into the user workspace. Workspace Control supports Microsoft App-V versions 4.x and 5.x.

Version 4.x

To create the integration with App-V 4.x, Workspace Control actively changes the way in which Microsoft App-V applications are invoked. This is done by launching a Workspace Control helper process from within the virtual application environment. This helper process makes configuration changes in the virtual environment (such as registry settings).

Version 5.x

With App-V 5.x virtual applications work like installed applications, allowing Workspace Control to apply actions and settings to the virtual applications directly. This eliminates the need of a helper process within the virtual application environment and enables User Settings tracking, prefetching User Settings and Process interception in Workspace Control sessions.

Where to find Microsoft App-V

<table>
<thead>
<tr>
<th>What</th>
<th>Where</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting up integration with Microsoft App-V</td>
<td>Go to Application Virtualization &gt; Microsoft App-V in the Setup menu</td>
</tr>
<tr>
<td>Setting up Microsoft App-V applications</td>
<td>Composition &gt; Applications</td>
</tr>
</tbody>
</table>
Integrate Microsoft App-V

Settings

Version 4.x

- When selecting the Microsoft App-V 4.x Client that should be used:
  - **As specified in command line of application**, Workspace Control uses the Application Virtualization helper process that is specified in the command line on the Properties tab of the App-V application at Composition > Applications.
  - `sftrun.exe` is the client launcher executable and overrides the default Microsoft App-V client as resolved by the system.
  - `sftray.exe` works similar as `sftrun.exe` but provides feedback to the user by showing a progress bar in the system tray.
  - **Store patched OSD in Workspace Control database** ensures that the OSD files of all Microsoft App-V applications that are added or changed after selecting this option are stored in the Workspace Control Datastore. This allows you to edit this file if necessary, using any editing tool (e.g. Notepad).
  - **Hide Command Window when launching application** starts the App-V application without showing a Windows command prompt.

Version 5.x

- When using Microsoft App-V 5.x Workspace Control only checks if Microsoft App-V integration is enabled. The other settings for Microsoft App-V integration (App-V Client to use, Store patched OSD and Hide Command Window) are ignored.

Notes

- Microsoft App-V was previously called SoftGrid. Workspace Control Microsoft App-V Integration also supports SoftGrid.
- Changes in the Microsoft App-V Integration will be applied to new sessions only.
- See [http://www.microsoft.com/systemcenter/appv](http://www.microsoft.com/systemcenter/appv) for more information about Microsoft App-V.
**Set up Microsoft App-V applications**

**Version 4.x**

To set up a Microsoft App-V application, add an application in the Console and let the command line of the application point to an OSD file.

- The application title, description, Microsoft App-V client version and application icon are automatically retrieved from the OSD file.
  
  If the application is correctly identified as an App-V 4.x application, the following line will appear on the Properties > General tab of the application:

  ```
  Microsoft App-V 4.x Integration will be used for this application
  ```

- When you save the application, the OSD file is copied and modified to provide integration between Workspace Control and Microsoft App-V.

- All Workspace Control technologies will automatically be configured to recognize the application listed in the OSD file.

Please note that the Microsoft App-V 4.x client needs to be installed to be able to retrieve the correct settings from the OSD file.

---

**Notes**

- If you create a Building Block of a Microsoft App-V 4.x application and its OSD file is stored in the Workspace Control Datastore, the Building Block will contain all information about the contents of the OSD file. The OSD file will be recreated when the Building Block is used to add or update the application in a different Datastore.

- The default virtual Microsoft App-V drive points to "Q:". You can change this for all computers or override this setting for a specific computer or user by setting environment variable `%SGDRIVE%`.

- Microsoft App-V 4.x applications can be set up to run with the SFTRUN or the SFTTRAY command. However, Microsoft App-V 4.x clients do no longer have the SFTRUN command. Workspace Control will now detect this situation and replace the SFTRUN on the fly with the command SFTTRAY /HIDE. This will help to resolve problems with application definitions when migrating from older Microsoft App-V versions to Microsoft App-V version 4.x.

- If the OSD file of a Microsoft App-V 4.x application is stored in the Workspace Control Datastore, you can edit this file if necessary, using any editing tool (e.g. Notepad).
To set up a Microsoft App-V 5.x application, add a new application to the Management Console.

- The command line can be specified in one of these ways:
  - On computers running Microsoft Windows Vista or higher, you can point the command line of
    the application to an App-V 5.x package (*.appv) in, for example, the shared content share.
    This file share will have been set up during the installation of your Microsoft App-V 5.x
    server, when you chose the App-V distribution method. The command line includes the App-
    V application package GUID and a variable for the version GUID. This ensures that
    the application can be started even if a new version of the App-V package is deployed.
  - If the Microsoft App-V 5 client is installed on the computer where the App-V 5 application
    is configured, you can let the command line point to the executable of a virtual application
    in the package installation root. By default, this is located at \%ALLUSERSPROFILE\%App-
    V\<PACKAGEID>\<VERSIONID>. The App-V application package GUID and version GUID are
    included in the command line. Newer versions of the App-V package will not be used.
  - The application title, description and icon are automatically retrieved from the App-V package.
    If the command line is correctly identified as an App-V 5.x application, the following line will
    appear on the Properties > General tab of the application:

    Microsoft App-V 5 Integration will be used for this application
Chapter 5: Setup

- **Use Package delivery mode** to configure if and how Workspace Control should handle App-V package delivery.
  - Selecting **Minimal (global) or Minimal (per user)** will create symbolic links for the App-V package. The App-V client will not mount the package locally, but instead will use the links to load the package from the configured (network) storage location. When using Minimal, the registry value `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\AppV\Client\Streaming\AutoLoad` must be set to 0. This will prevent the App-V client from fully downloading an App-V application when a user starts that application for the first time (default behavior).
  - Selecting **Full (global) or Full (per user)** will mount the App-V package in the background, after the application is launched. This will load the full package to the package installation root, even if `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\AppV\Client\Streaming\SharedContentStoreMode` is set to 1.
  - When selecting **Always use latest version of package**, Workspace Control will look for newer versions of the App-V package in the configured **Package root folder**, up to two levels deep.
  - To configure File Types for the application, click the **Import** button on the **File Types** tab.

With Microsoft App-V 5.x integration the Workspace Control features that can be configured are extended with User Settings Tracking, User Settings Prefetching, and Process interception.

<table>
<thead>
<tr>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Microsoft App-V 5.x</strong></td>
</tr>
<tr>
<td>- After upgrading to RES Workspace Manager 2014 SR2 or higher, configuring the <strong>Package delivery mode</strong> for existing Microsoft App-V 5 packages (packages that were configured in an earlier version than RES Workspace Manager 2014 SR2) will require you to (re)specify the central location of the Microsoft App-V 5 packages.</td>
</tr>
<tr>
<td>- When configuring the Workspace Control option <strong>Package delivery mode</strong> for Microsoft App-V 5 packages with <strong>Minimal (per user) or Full (per user)</strong>, the feature <strong>Folder Redirection</strong> for the Windows folder <strong>AppData</strong>, is not supported.</td>
</tr>
<tr>
<td>- On the <strong>User Settings &gt; Properties</strong> tab, when selecting <strong>Track any setting changed by application immediately</strong> for <strong>Zero Profile mode</strong>, the <strong>Registry to track</strong> (on the <strong>User Settings &gt; Tracking</strong> tab of the application) must be <strong>HKEY_CURRENT_USER</strong>. If this registry is changed, no User Settings can be tracked for this Microsoft App-V 5 application.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>General Microsoft App-V</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Changes in the Microsoft App-V Integration will be applied to new sessions only.</td>
</tr>
<tr>
<td>- See <a href="http://www.microsoft.com/systemcenter/appv">http://www.microsoft.com/systemcenter/appv</a> for more information about Microsoft App-V.</td>
</tr>
</tbody>
</table>
Microsoft TS RemoteApp

With Microsoft TS RemoteApp integration, you can integrate Workspace Control with the Terminal Services RemoteApp feature of Microsoft Windows Server 2008 and higher. This allows you to manage Microsoft TS RemoteApp applications from the Management Console. A Microsoft TS RemoteApp application is an application that runs on a Terminal Server, but because it integrates seamlessly with the user desktop, it behaves as if it were running on the user's local computer. If more than one Microsoft TS RemoteApp application runs in a user session, they will share the same Terminal Services session.

Notes

To use Microsoft TS RemoteApp applications, the following requirements apply:

• Servers that host Microsoft TS RemoteApp applications must be running Microsoft Windows Server 2008 or higher and have installed Terminal Services with the role Terminal Server.
• Client computers that need to access Microsoft TS RemoteApp applications must be running RDC 6.0 or higher.
• Because of a dependency between the RDC client and the Windows Explorer, it is not possible to start TS RemoteApp applications from sessions running the Workspace Control shell.

Where to find Microsoft TS RemoteApp

<table>
<thead>
<tr>
<th>What</th>
<th>Where</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting up integration with Microsoft TS RemoteApp</td>
<td>Go to Application Virtualization &gt; Microsoft TS RemoteApp in the Setup menu</td>
</tr>
<tr>
<td>Setting up Microsoft TS RemoteApp applications</td>
<td>Composition &gt; Applications, on the Properties &gt; Publishing tab of the application</td>
</tr>
</tbody>
</table>

Integrate Microsoft TS RemoteApp

Settings

• Enable Instant Passthrough for computers not publishing this application creates Instant Passthrough shortcuts to Microsoft TS RemoteApp applications located on a remote server. When the shortcut is accessed, the user will automatically be redirected to this remote server. However, if the application should start locally if possible, also select Do not passthrough if application is available on local computer.
• The Available Servers area shows which servers or server groups can be used for Microsoft RemoteApp applications. The list of available servers contains all Microsoft Windows Server 2008 servers on which Workspace Control has been installed and that point to the current Workspace Control Datastore.
• Enable "Microsoft TS RemoteApp Publishing" by default automatically deploys an application as a Microsoft TS RemoteApp deployment when you add it as a new Managed Application.
• Domain Admin credentials are required for communicating with the TS Connection Broker. With the option Use the following credentials to communicate with the broker, the Ivanti Workspace Control Agent service on the Microsoft RD Connection Broker can run under Local System or a Windows Account without having to add Domain Admin rights to that account.

Server groups

Server groups are typically used to represent silos. If your workspace contains existing server groups (e.g. server farms), these will be listed automatically. Server groups can then be used to deploy a Microsoft TS RemoteApp application. The list of available servers will be automatically populated with computers that are running Windows Server 2008 with Terminal Services enabled. You can link a Microsoft Windows Server 2008 Terminal Server to a Session Broker and have it included in a farm to facilitate load balancing between several identical Terminal Servers. When a Microsoft Windows
Server 2008 server is configured to communicate with a Session Broker and is joined to a farm, a server group is automatically created for the farm.
**Set up Microsoft TS RemoteApp applications**

To set up a Microsoft TS RemoteApp application, add an application to the Management Console and select the option *Enable Microsoft TS RemoteApp publishing* at Properties > Publishing.

- On the **Settings** tab of Microsoft TS RemoteApp, you can enable *Instant Passthrough* for the application. This will automatically detect whether the application is available directly in a session (if the session is running on a Terminal Server that deploys the application) or whether a terminal session needs to be started to one of the configured Microsoft Windows 2008 Terminal Servers to start the application as a Microsoft TS RemoteApp application. If a terminal session needs to be started, the RDC client is started with a Workspace Control generated RDP file with the correct information. See Setting up Instant Passthrough for TS RemoteApp applications.

- On the **Servers** tab, specify one or more server groups that should deploy the application. This will deploy the Microsoft TS RemoteApp application on all Terminal Servers in the server group that run Microsoft Windows 2008.

- The Management Console does not communicate directly with these servers to create or update the Microsoft TS RemoteApp application. Instead, the Workspace Control Agent process running on the Microsoft Windows Server 2008 computer will create the Microsoft TS RemoteApp application. Because of this, it is not necessary to configure Microsoft TS RemoteApp from a server running Microsoft Windows Server 2012; this can also be done from a workstation or a server running Microsoft Windows Server 2008.

- When a Terminal Server is configured for a server farm, Workspace Control will automatically create or update a server group with the same name. Therefore, when you add a new Terminal Server running Microsoft Windows 2008 to an existing server farm, it will automatically be added to the server group with the same name as the server farm. Because this new Terminal Server has become part of the server group that has been specified to
deploy the Microsoft TS RemoteApp application, it will also start to deploy the Microsoft TS RemoteApp application.

**Set up Instant Passthrough for TS RemoteApp applications**

The **Instant Passthrough** settings for Microsoft TS RemoteApp applications allow you to set up a passthrough mechanism to Microsoft TS RemoteApp applications located on a Terminal Server. This will create an RDP file for each Microsoft TS RemoteApp application. The RDP file points to the application on the Terminal Server and is stored in the DBcache of all specified Terminal Servers in the specified Terminal Server farm. When a user accesses the RDP file, the request will automatically be redirected to the Terminal Server on which the application is located, after which the Terminal Server will deploy the application to the user’s desktop.

- If set up Instant Passthrough when configuring Microsoft TS RemoteApp Integration, the Instant Passthrough settings that you configure will serve as the default values for all Microsoft RemoteApp applications in your environment.
- If set up Instant Passthrough when configuring a Microsoft TS RemoteApp application, the Instant Passthrough settings that you configure only apply to the Microsoft TS RemoteApp application.

**Properties tab**

- When specifying the server name and port, you can use the name of a Terminal Server, but also the name of a Terminal Server farm. If you want to use single sign-on, you should use the fully qualified domain name.
- Bitmap caching can speed up your connection by storing frequently used images on your local hard disk.

**Behavior tab**

- **Do not passthrough if application is available on local computer** allows you to define when a published or local version of the application should be launched. You can optionally choose to ignore the configured behavior inside or outside specific Zones via the **Locations and Devices** field.
  - If you configure to passthrough anyway in specific Zones, **at least one** of the added Zones must apply.
  - If you configure to passthrough anyway **outside** specific Zones, **all** the added Zones must apply.

**Notes**

- When an Instant Passthrough session is started from a client running Workspace Control to a Terminal Server, no extra licenses are claimed.
- If a user has logged on to a Terminal Server on which a Microsoft TS RemoteApp application has been deployed and tries to start this application, it will start directly (the original command line of the application will be used to start the application).
- If the user has logged on to a computer or server on which a Microsoft TS RemoteApp application has not been deployed and tries to start this application, an RDP session will be started, based on the values of the Instant Passthrough mechanism.
VMware ThinApp

Workspace Control can also integrate with other virtualization solutions, but the integration needs to be set up manually outside of Workspace Control.

VMware ThinApp integration:

VMware ThinApp simplifies application delivery by isolating applications from the underlying operating system and plugging directly into existing virtual and physical desktop management tools and infrastructure. ThinApp encapsulates applications inside a Virtual OS that transparently merges a virtual system environment with the real system environment.

To integrate VMware ThinApp streamed applications in the user workspace, make the following changes to capture folder of the ThinApp application:

- Add `respf.vbs` in the root of the capture (where `package.ini` is located). The `respf.vbs` must contain this text:
  ```vbs
  Function OnFirstParentStart
  WaitForProcess ExecuteVirtualProcess(GetEnvironmentVariable("pwrgrids")),0
  End Function
  ```
- Add the following folder to the root of the capture (where `package.ini` is located):
  `%Local AppData%\RES\Workspace Manager`
- In the Workspace Control folder, add `##Attributes.ini`, containing this text:
  ```ini
  [Isolation]
  DirectoryIsolationMode=Merged
  ```
- Rebuild the package by using `build.bat`.
- Make the executables located in the `\bin` folder available, either by placing them on a network share or by distributing them to all computers that run Workspace Control.
- Add the ThinApp application to Workspace Control using the Console.
- Click the Properties > Settings in the Edit application window of the ThinApp application.
- Select Use "generic isolation" integration for the ThinApp application.
5.6.3 LANDesk

LANDesk Integration

With LANDesk Integration enabled in Workspace Control, it is possible to deploy software on Workspace Control Agents on which a LANDesk client is running. It allows you to deliver, install, and configure software at the start of a Workspace Control session or when the user clicks on the application shortcut.

At LANDesk in the Setup menu, you can integrate the installation feature of LANDesk in your environment.

Global software distributions can be configured at Composition > Actions By Type > LANDesk. Configure the software distributions for Applications on the Actions tab of the Configuration section of an application.

Communication

Workspace Control uses MBSDK Web Service to communicate with LANDesk server.

When configuring LANDesk Integration, Workspace Control queries the configured MBSDK Web Service for available software distribution packages. This is to verify the correct MBSDK Web Service has been specified.

When configuring software distributions (LANDesk), Workspace Control queries the configured MBSDK Web Service for available software distribution packages. After selecting a distribution package, a reference is stored in the Workspace Control Datastore.

For global software distributions, the Workspace Control Agent creates a scheduled task for the selected distribution package on the LANDesk server at the start of a session. For software distributions configured for an application, the scheduled task for the selected distribution package on the LANDesk server is created when the user starts the application.

If the Wait for action to finish before continuing is enabled for a software distribution action for an application, a Dismiss and notify me when done notification is displayed in the user session when a user starts the application and the distribution package is deployed. This allows the user to continue working with already available applications while the package is being installed. The user receives a message once the installation is completed.

After deployment of the program, the scheduled task will remain on the LANDesk server.

Notes

- Software distributions require a LANDesk client to be installed on the Workspace Control Agent.
- Workspace Control supports LANDesk 9.5 and 9.5 SP1.
5.6.4 **Microsoft Remote Assistance**

Microsoft Remote Assistance allows a helpdesk to quickly remote control a user’s desktop and diagnose and repair problems remotely. This decreases resolution time for helpdesks, which in turn decreases their workload.

**Where to find Microsoft Remote Assistance**

<table>
<thead>
<tr>
<th>What</th>
<th>Where</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting up Remote Assistance</td>
<td>Go to Microsoft Remote Assistance in the Setup menu</td>
</tr>
<tr>
<td>Starting a Remote Assistance session</td>
<td>Right-click a user session at Diagnostics &gt; User Sessions</td>
</tr>
</tbody>
</table>

**Set up Remote Assistance**

**Settings**

- **Mode:** When setting up Remote Assistance, you can choose between three different modes:
  - **Allow helpers to only view the computer:** users belonging to a specified helper group can only view the computer of other users; they cannot make any changes.
  - **Allow helpers to remotely control the computer:** users belonging to a specified helper group can make changes to the computer of other users.
  - **Do not allow helpers to remote control or view the computer:** disables Remote Assistance.
- **Helper groups:** Users belonging to a specified helper group must have access to the Management Console and they must at least have Read permissions to the nodes Setup > Integration > Remote Assistance and Diagnostics > User Sessions.
- **Automatically configure Windows Firewall:** If your infrastructures use a firewall, its settings need to be adjusted to allow Remote Assistance functionality. Select this option to let Automation do this for you.

**Notes**

- Microsoft Remote Assistance must be enabled on the computer of the helper and on the remote computer.
- To use Remote Assistance from a Windows 2008 server to a Workstation, the Remote Assistance feature must be installed which it is not by default. To install Remote Assistance in Windows 2008, open Server Manager - Go to Features - click Add feature - and select Remote Assistance.

**Start a Remote Assistance session**

Users who belong to a specified helper group can start a Remote Assistance session by right-clicking a user session at Diagnostics > User Sessions in the Management Console.

Please note that the administrator needs at least read rights on the Setup > Integration > Microsoft Remote Assistance node to be able to start a Remote Assistance session. Remote Assistance is possible on workstations, laptops, and Terminal Servers.
5.6.5 Microsoft System Center

Microsoft System Center Configuration Manager Integration

With **Microsoft System Center ConfigMgr Integration** enabled in Workspace Control, it is possible to deploy software distribution Programs on Workspace Control Agents on which a Microsoft System Center Configuration Manager client is running. It allows you to deliver, install, and configure software at the start of a Workspace Control session or when the user clicks on the application shortcut.

At **Microsoft System Center** in the **Setup** menu, you can integrate the installation feature of Microsoft System Center Configuration Manager (SCCM) in your environment. To set up the integration, provide credentials of an administrator with at least the "Application Administrator role" within SCCM.

Global software distributions can be configured at **Composition > Actions By Type > Microsoft ConfigMgr**. Configure the software distributions for Applications on the **Actions** tab of the **Configuration** section of an application.

**Communication**

Workspace Control uses Windows Management Instrumentation (WMI) to communicate with both Microsoft Configuration Manager server and client.

When configuring Microsoft System Center Configuration Manager Integration Workspace Control queries the configured Management Server for available software distribution Packages. This is to verify the correct Management Server has been specified.

When configuring Software distributions (Microsoft ConfigMgr), Workspace Control queries the configured Management Server for available software distribution Packages and Programs. After selecting a Program, a reference is stored in the Workspace Control Datastore.

For global software distributions, the Workspace Control Agent creates an advertisement for the selected Program on the Microsoft System Center Management Server at the start of a session. For software distributions configured for an application, the advertisement for the selected Program on the Microsoft System Center Management Server is created when the user starts the application.

The advertisement that was created is based on a temporary Collection that contains only the Configuration Manager client from the computer on which the Workspace Control Agent is running.

The Workspace Control Agent, then notifies the Configuration Manager client about this new advertisement.

If the option **Create subfolder for the temporary Device Collection** is selected, you can specify the **Subfolder name used by Workspace Control**. The subfolder that will be used for the temporary Device Collection, will be created in the SCCM Console in the **Devices** folder (at **Overview > Devices**).

- Microsoft System Center does not support the following characters in the subfolder names for the temporary Device Collection: `\ / : " ? " < > |`. If unsupported characters are used in the subfolder name, when saving, a message is displayed informing you about replacing these characters with an underscore ("_"). You can then also decide to change the name and save again.

If the **Wait for action to finish before continuing** is enabled for a software distribution action for an application, a **Dismiss and notify me when done** notification is displayed in the user session when a user starts the application and the package is deployed. This allows the user to continue working with already available applications while the package is being installed. The user receives a message once the installation is completed.
After deployment of the program, the Workspace Control Agent removes the advertisement from the Management Server.

**Warning**

Support for Microsoft Configuration Manager 2012 application deployments was introduced in RES Workspace Manager 2014 RC. If you access a RES Workspace Manager 2014 RC (or later) Datastore using an older Management Console, be aware that Microsoft ConfigMgr actions that deploy applications (rather than packages/programs) will be hidden from view.

Important: when accessing a RES Workspace Manager 2014 RC (or later) Datastore using an older Management Console, do not delete any managed application that is configured with a (hidden) Microsoft ConfigMgr 2012 task to deploy an application. Doing so will cause newer Management Consoles to report a Datastore integrity error.

**Notes**

- Software distributions require a Microsoft System Center Configuration Manager client to be installed on the Workspace Control Agent.
- See the Workspace Control [Compatibility Matrix](#) for supported versions of Configuration Manager.
- For more information, refer to Microsoft documentation.
5.6.6  Ivanti Products

At Setup > Integration > Ivanti Products you can integrate other Ivanti products in Workspace Control.

Automation

At Setup > Integration > Ivanti Products > Automation, you can integrate Automation. This allows you to run Automation Tasks in the user workspace.

Automation Tasks can be integrated when:

- a session starts.
  - Configure this at Composition > Actions By Type > Automation Tasks.
- an application starts.
  - Configure this at Composition > Applications.
- a security event occurs.
  - Configure this at Setup > Integration > Alerting.

Integrate Automation Tasks

When you integrate Automation Tasks in Workspace Control, you can run specific Automation Tasks in the user workspace, for example to install software or to create user profiles. Automation Tasks can run when a user session starts or when an application starts, but also when a security event occurs.

Settings

- On the Settings tab, select the Dispatcher detection settings that Workspace Control should use to detect the Automation Dispatchers:
  - Autodetect (Ivanti Automation 2018.x and lower) allows Workspace Control to search for available Automation Dispatchers by sending a multicast signal.
  - Use Dispatcher address list allows Workspace Control to search for specific Automation Dispatchers. If you select this option, you need to specify the IP address of at least one Dispatcher.
- Integrate with Automation by selecting an Automation Environment.
- Specify a dedicated Automation login for Automation Authentication. This dedicated login must at least have read permissions on the Modules and Projects nodes in Automation.
- When you have set up the above settings, you can use the Test now button to test whether you can connect to the selected Automation environment.
- The Log tab shows a log of all Automation actions, including alerting actions.

Notes

- Automation Integration requires RES Automation Manager Series 4 SR2 or higher. If the Automation environment to which you are connected is not up-to-date, it will not be possible to use Tasks from this environment.
- See the Automation Help for more information about Automation.
- In Ivanti Automation 2019.0, all autodetect functionality is no longer supported. For more information see Dispatcher Detection settings in the Automation Administration Guide.

Tip

With the Unified Console, you can easily access the Workspace Control and Automation Consoles from a single view.
Identity Director

Integrate Identity Director at Setup > Integration > Ivanti Products > Identity Director. Identity Director Integration allows you to base access to an application or object on the availability of Identity Director Services (already available or created from Workspace Control).

For applications, access control based on a delivered Identity Director Service, can be configured on the application's Access Control > Identity tab at Composition > Applications. For objects, this is configured on the object's Access Control tab.

**Integrate Identity Director services**

When you integrate Identity Director services in Workspace Control, you can base access to an application or object on the availability of Identity Director Services (already available or created from Workspace Control with the Identity Director Service Wizard). For example, you can base Access Control to the managed application Microsoft Visio on the Identity Director Service "Microsoft Visio". This enables you to use the Identity Director workflow to approve and install the application, while Workspace Control automatically makes the managed application available as soon as the service has been delivered in the end user's workspace.

The **Identity Director Service Wizard** is used to create new Identity Director services directly from the Workspace Control Console. All communication of this wizard to the Catalog Services of Identity Director is SSL-encrypted.

**Settings**

- **The Catalog host** is the machine on which the Catalog Services run. The Catalog Services are used by Workspace Control to query which Identity Director services have been delivered to a user.
- Each user's list of delivered Identity Director Services is cached to ensure availability of this information in case the Catalog Service cannot be reached. The name of the **Catalog host** can be found in the Identity Director Management Portal, at Setup > Components.
- **The port** of the Catalog host.
- **The Publication name** and **Publication password** are used by Workspace Control to connect to an Identity Director Catalog host. This Catalog host contains a selection of available Identity Director Services that can be used as Access Principle in Access Control. The **Publication name** can be found in the Identity Director Management Portal, at Setup > Service publications.
- **When you have setup the above settings**, you can use the Test now button to test whether you can connect to the specified Catalog host. If connection is possible, an overview of all available Identity Director Services will be shown.

---

**Note**

If Access Control is based on a **Not Identity Director Service** rule and Identity Director Integration is disabled, all users will comply with this rule.

---

**Tip**

With the Unified Console, you can easily access the Workspace Control and Identity Director Consoles from a single view.
Chapter 5: Setup

VDX

Virtual Desktop Extender

At Setup > Integration > Ivanti Products > VDX, you can enable integration for Virtual Desktop Extender. The Virtual Desktop Extender merges local applications and a remote desktop into a single workspace. This technology eliminates the need to switch between a local and remote desktop providing an optimized user experience. This is useful if you run applications that do not function properly in a server-based computing environment, or if you have other reasons to keep some applications running locally.

With the Virtual Desktop Extender, a virtual channel is created between the session and the locally installed desktop extender as soon as a session is initialized. If the user has been granted access to an application that is installed locally, that application will be presented in the end user’s session.

To configure an application to run from the local desktop using VDX, select Run as Workspace Extension at its Properties > General tab.

Configuration

Enable Virtual Desktop Extender (VDX) integration - Enable or Disable the integration of VDX with Workspace Control. If disabled, the VDX functionality remains intact but is no longer managed by Workspace Control.

• Enable VDX Engine - Enable or Disable the VDX Engine. This disables VDX altogether, not just the integration with Workspace Control.

• Let VDX override Workspace Extender - If both VDX and the RES Workspace Extender are installed, this option will force Workspace Control to use VDX.

• Hide client taskbar at session start
  Autodetect - Uses the settings as they are used in the scenarios as described in the VDX documentation.
  Yes - Hides the local taskbar when starting a remote session.
  No - Shows the local taskbar when starting a remote session.

• Show already running client applications
  Autodetect - Displays running client applications that would be obscured when starting a remote session.
  Yes - Allows applications windows from applications that were running before the VDX session started to be managed by VDX.
  No - Only new applications windows from applications that were not running before the VDX session started will be managed by VDX.
  Exception: In case applications share the same process (e.g. explorer.exe and iexplorer.exe), newly started application windows will not be managed by VDX if the process was already running at the start of the VDX session.

When choosing Yes or Autodetect, running client applications can be freely moved in and out of the session by users.

• End running client applications at log off - Ends any applications that are running on the client when logging off.

• Windows keys passthrough - Allows the use of the following keyboard shortcuts for Microsoft Windows in VDX sessions:
  • Windows key Open / Close Start Menu
  • Windows key+E Open Windows Explorer
  • Windows key+R Open Run dialog box
  • Windows key+M Minimize all windows
  • Windows key+D Show desktop
• **Windows key+<nr>**
  
  *Start the program pinned to the taskbar in the position indicated by the number (from left to right). If the program is already running, switch to that program.*

• **Ctrl+Esc**
  
  *Open / Close Start Menu*

• **Ctrl+Shift+Esc**
  
  *Open Task Manager*

*Note: When Windows keys passthrough is enabled for user sessions running on Microsoft Windows 8/8.1 and 2012/2012 R2, the Alt+Tab key combination to switch between application windows, does not work.*

• **Let users access client start menu through VDX** - Enable this option to show the start menu of the client in an alternative start menu, accessible from the VDX tray icon on the remote desktop. The client start menu offers a **Search** option. This enables VDX users to search for applications easier by typing in (part) of the application name.

• **Let users access client desktop through VDX** - Enable this option to show the desktop shortcuts of the client in an alternative start menu, accessible from the VDX tray icon on the remote desktop.

• **Let users access client notification area through VDX** - Enable this option to show the notification area of the client in an alternative start menu, accessible from the VDX tray icon on the remote desktop.

• **Mode**
  
  • **a (recommended):** Enables VDX to run in the reverse seamless mode and supports Microsoft Windows 8 / 8.1 and 2012 / 2012 R2.
  
  • **b:** Enables VDX to run in reverse seamless mode. This mode is not supported for Microsoft Windows 8 / 8.1 and 2012 / 2012 R2.
  
  • **Disabled:** Enables VDX to run in native “Extender mode”. Extender mode means that local applications run seamlessly within the remote desktop, but the local application windows are not managed by VDX: the local applications are not part of the Z-order, but they are present on the taskbar as if they are running in the remote desktop. Switching to Extender mode can be useful when you are dealing with applications that cannot properly be managed by VDX.

• **Disable virtual Z-order for the following processes** - Excludes specific local processes from the remote session. This forces classic behavior: Application on top of the remote session or the remote session on top of the application. Enter the process names separated by semicolons (;) (example: proc1.exe;proc2.exe;proc3.exe). This setting can only be configured for **Mode: b**.

• **Ignore the following client processes** - Ignores running client processes from VDX integration. These applications will not be available through VDX and/or the client desktop / client Start Menu folders. Enter the process names separated by semicolons (;) (example: proc1.exe;proc2.exe;proc3.exe). This setting can be configured for **Mode: b** and **Mode: disabled**.

• **Custom message for the run balloon** - Allows you to adapt the title and message of the information balloon that is displayed with the VDX icon in the notification area.

---

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note</strong></td>
</tr>
</tbody>
</table>

When a VDX session is started from a Workspace Control session, the screensaver of the client will be used by default. It is possible to force the use of the Workspace Control session screensaver by setting the registry value **NoAgentScreenSaver**.
5.6.7 Web Portal

Besides creating a physical desktop by replacing the shell, it is also possible to create a virtual web-based desktop. This allows you to integrate the interface with an existing portal environment for remote access purposes, so that users can connect to their desktop from a remote location via a web interface.

To create such a web-based desktop, you need to enable Web Portal rendering at Web Portal in the Setup menu. When Web Portal rendering is enabled, Workspace Control will render a Web Portal in the \Webtop folder located in the user's temp directory. The Web Portal can be started by launching a web browser with startup parameter %temp%\webtop\webtop.html.

You can change the Web Portal's appearance by selecting a Web Portal style. There are three default Web Portal styles to choose from. If you have a basic knowledge of HTML, you can edit the Web Portal style to fit your needs.

To make the Web Portal available to the user, Microsoft Internet Explorer 6 or higher needs to be made available as a managed application. For this purpose, the installation folder of Workspace Control contains the Building Block file web-portal-integration.xml with a preconfigured version of Microsoft Internet Explorer. By importing the Building Block file into the Management Console, the application Web Portal Integration will be added at Composition > Applications > Applications.

It is also possible to offer the Workspace Composer through the application Web Portal Integration only:

- At Composition > Applications, open the application Web Portal Integration.
- At Properties > General, copy the number in the ID field (for example 63) and close the application.
- At Composition > Applications > Settings, select When online, start a specific application () instead of Workspace Control taskbar.
- Enter the copied number of the application and click OK. This application ID is now shown in parentheses in the text. When the user starts a new session, only the application Web Portal Integration will be started; the desktop will not be shown.

Notes

- You can also make a Web Portal available manually, by adding Microsoft Internet Explorer as a managed application to the Management Console and adding the parameter %temp%\webtop\webtop.html to its properties.
- If the user session uses the Workspace Control shell, you can hide the Start button on the Web Portal by selecting Hide "Start"-button on Workspace Control Shell taskbar at Composition > Desktop > Lockdown and Behavior.
Configure Web Portal styles

Use the Web Portal Style Editor window to configure the appearance of the Web Portal.

Configuration

You can change the basic settings of the Web Portal style at Settings:

- The **Title** field specifies the caption of the Web Portal.
- The image file that you select for the Web Portal in the **Logo** field (e.g. your company logo) will be saved as a resource in the Datastore.
- If necessary, you can specify in the **Root URL** a URL that is different from the default root of the Web Portal.
- The **Menu split** field specifies the number of menu items that is shown on the Web Portal before a split of the menu occurs.
- The **Application split** field specifies the number of applications that is shown on the Web Portal before a split of the menu occurs.
## 5.7 Advanced Settings

At **Setup > Advanced Settings**, you can configure general settings for your Workspace Control environment. Below an overview of the different settings.

<table>
<thead>
<tr>
<th>Item</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td># minutes until AutoRefresh check</td>
<td>Specifies the time frame in which active users’ sessions should automatically refresh after clicking the button <strong>Refresh active</strong>. For instance, if you have 10 active user sessions in your environment and the interval is set to 10 minutes, approximately every minute a user session is forced to refresh.</td>
</tr>
<tr>
<td># days to keep log files</td>
<td>Specifies how long log files should be kept. This applies to the following logs:</td>
</tr>
<tr>
<td></td>
<td>• Security &gt; Applications &gt; Managed Applications</td>
</tr>
<tr>
<td></td>
<td>• Security &gt; Applications &gt; User Installed Applications</td>
</tr>
<tr>
<td></td>
<td>• Security &gt; Applications &gt; Websites</td>
</tr>
<tr>
<td></td>
<td>• Security &gt; Data &gt; Removable Disks</td>
</tr>
<tr>
<td></td>
<td>• Security &gt; Data &gt; Files and Folders</td>
</tr>
<tr>
<td></td>
<td>• Security &gt; Data &gt; Read-Only Blanketing</td>
</tr>
<tr>
<td></td>
<td>• Security &gt; Network Connections</td>
</tr>
<tr>
<td></td>
<td>• Security &gt; User Sessions</td>
</tr>
<tr>
<td></td>
<td>• Diagnostics &gt; Workspace Analysis/User Sessions &gt; Event Logs</td>
</tr>
<tr>
<td></td>
<td>• Diagnostics &gt; Errors</td>
</tr>
<tr>
<td></td>
<td>• Administration &gt; Performance &gt; Access Balancing</td>
</tr>
<tr>
<td></td>
<td>• Administration &gt; Performance &gt; CPU Optimization</td>
</tr>
<tr>
<td></td>
<td>• Administration &gt; Performance &gt; Instant LogOff</td>
</tr>
<tr>
<td></td>
<td>• Administration &gt; Performance &gt; Memory Optimization</td>
</tr>
<tr>
<td></td>
<td>• Setup &gt; Integration &gt; LANDesk</td>
</tr>
<tr>
<td></td>
<td>• Setup &gt; Integration &gt; Microsoft System Center</td>
</tr>
<tr>
<td></td>
<td>• Setup &gt; Integration &gt; Ivanti Products &gt; Automation</td>
</tr>
</tbody>
</table>

| Remove obsolete log files every day at    | Specifies the time when log files should be cleaned up, for example after office hours. A cleanup can only run once a day. When a user starts a session, Workspace Control will check whether it has already performed a cleanup that day. If it has not, Workspace Control will check whether the time the session was started is less than one hour after the specified time when the log files should be cleaned up. If it is, Workspace Control will perform a cleanup of the log files. If not, the cleanup will be performed the next day. For Relay Servers that are connected directly to the Datastore, the duration of the daily cleanup can be specified with the registry value `DBCleanupDuration`. See the *Workspace Control Administration Guide* for more information. |

| # seconds until timeout "Application Not Responding" | Specifies when the user will be notified about an unresponsive application. This setting only applies if you selected Notify user about not responding applications at Composition > Desktop > Lockdown and Behavior. |
### # seconds to wait before refreshing after network change or resume

Allows you to configure a delay before the Workspace Composer will perform a Workspace refresh after a network connectivity change or system resume occurred. Such a delay may be helpful in situations where a laptop changes network connectivity several times within a short period of time, for example when switching from a LAN connection to a WiFi connection. This might result in two changes in network connectivity:

- LAN connection > No connection (triggers a Workspace refresh)
- No connection > WiFi connection (triggers a Workspace refresh)

In this situation, configuring a delay can limit the number of Workspace refreshes.

<table>
<thead>
<tr>
<th>Item</th>
<th>Function</th>
</tr>
</thead>
</table>
| # seconds to wait before refreshing after network change or resume | Allows you to configure a delay before the Workspace Composer will perform a Workspace refresh after a network connectivity change or system resume occurred. Such a delay may be helpful in situations where a laptop changes network connectivity several times within a short period of time, for example when switching from a LAN connection to a WiFi connection. This might result in two changes in network connectivity:  
  - LAN connection > No connection (triggers a Workspace refresh)  
  - No connection > WiFi connection (triggers a Workspace refresh)  
  In this situation, configuring a delay can limit the number of Workspace refreshes. |

### Backtrack passthrough sessions to originating client for Zones

Allows Workspace Control to use the IP address of the originating client to resolve Zones if a published application on a Terminal Server is launched from another Terminal Server.

### By default do not grant concurrent/seat license when database is not available

 Specifies the default setting for application licenses for new applications. If selected, access to an application will be denied if licenses and seats cannot be checked by Workspace Control because there is no database connection.

### Bypass composer for accounts and groups

You can specify local/domain administrator accounts, users, and/or groups to exempt specific users from getting Workspace sessions when they log on to an Agent, even when the Agent is configured to run the Workspace Composer automatically. This can be useful when troubleshooting. For example, enter `<DomainName>\<SecurityGroup>`, to allow members of the local administrator group to log on to a machine without starting a Workspace Control session (=bypassing the Workspace Composer).

Multiple entries can be separated by a semicolon (;).

Please note that the asterisk wildcard (*) is only supported for user or group names. Also, nested groups are only supported if they are within the same domain as the logged-on user account.

Valid formats for this field:

- `domain\username`
- `\username`
- `domain\use*`
- `domain\*`

**Example:** `demo\domain admins; demo\admin-gt; win7-1234\root; resqa\support*`
### Item | Function
--- | ---
**Do not establish communication with any Workspace Extender** | Specifies that the Workspace Extender should not be used. This option is only available if Enterprise or Standard licenses (RES PowerFuse 2010) are active within your environment.

**Do not log security events for Workspace Control program folders and subfolders** | If Security restrictions prevent a user from accessing the Workspace Control program folders, legitimate access to these folders by the Workspace Composer is also logged as a security event. Select this option to keep the log free of security events reporting access to the Workspace Control program folders by anyone. Selecting this option will also keep the log clear of the security events that are triggered by the Workspace Control installation and/or cache folders.

**Do not ping print server before connecting printers** | This is useful if the print server uses a different network protocol (e.g. Novell print server with IPX).

**Do not prevent applications in the Run key or RunOnce key from starting** | In Microsoft Windows, applications set in HKCU\...\Windows\CurrentVersion\Run or HKCU\...\Windows\CurrentVersion\RunOnce will automatically run at start up.

By default, this mechanism is disabled in sessions running the Windows Shell where Windows Shell shortcut creation is set to Replace all unmanaged shortcuts (at Composition > Applications > Settings). Select this option to allow applications to run automatically from the Run and RunOnce keys.

The Run and RunOnce mechanism are always:
- enabled in sessions running the Windows Shell with Windows Shell shortcut creation is set to Do nothing or to Merge with unmanaged shortcuts.
- disabled in sessions running the Workspace Control Shell.

⚠️ **Warning**: Applications started from the Run key or RunOnce key are always unmanaged applications.

**Do not setup workstation license virtual channel** | When starting a terminal session from a desktop, Workspace Control will set up a virtual channel (either Citrix ICA or Microsoft RDP) to communicate with the terminal session and to have it acquire a license from the Workspace Composer. This setting prevents Workspace Control from enabling this virtual channel.

**Do not verify UNC path of security rules when offline** | If selected, Workspace Control will not try to verify availability of the UNC path in a security rule if the connection state of a computer is offline. Instead, it will assume that the server can be reached. This setting is selected by default when a new Datastore is created. This setting requires an unqualified server name (e.g. `\server` instead of `\server.domain`) that can be resolved at DNS level. Alternatively, the authorization rule must be changed so that it contains a fully qualified domain name in the UNC path.
<table>
<thead>
<tr>
<th>Item</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ping file server to verify UNC path</td>
<td>If selected, Workspace Control will ping the file server in an UNC path in a security rule, to determine whether the server can be reached, before it will verify the entire UNC path. By default, this setting is not selected when a new Datastore is created. This setting requires an unqualified server name (e.g. \server instead of \server.domain) that can be resolved at DNS level. Alternatively, the authorization rule must be changed so that it contains a fully qualified domain name in the UNC path.</td>
</tr>
<tr>
<td>UNC path of security rules when online</td>
<td></td>
</tr>
<tr>
<td>Remove policy based registry keys</td>
<td>Prevents registry tattooing for policies set by Workspace Control. After logging off, all policy-based registry keys will be removed by Workspace Control. Windows will take care of recreating Group Policies and NT4-based policies, while Workspace Control will reprocess the policies as configured in the Management Console.</td>
</tr>
<tr>
<td>before logging off</td>
<td></td>
</tr>
<tr>
<td>Use all valid IP addresses when</td>
<td>Uses all valid IP addresses on all network interfaces to evaluate Zone rules. This is useful when using e.g. multi-homed computers (a computer with more than one IP address).</td>
</tr>
<tr>
<td>evaluating Zones</td>
<td></td>
</tr>
<tr>
<td>Use cached user context if latency</td>
<td>If at session start the network latency to the domain controller is above the specified threshold, the Ivanti Workspace Composer will use the cached user context. The user may experience a session refresh due to changes in context. This is useful when high latency connections to Active Directory cause long delays in the retrieval of user context at session logon or refresh.</td>
</tr>
<tr>
<td>to AD is above: x ms</td>
<td></td>
</tr>
<tr>
<td>Use computer's FQDN instead of domain</td>
<td>Enables you to identify computers by their Fully Qualified Domain Name (FQDN), rather than having identical names in Log and Usage Tracking reports. At Administration &gt; Agents and Diagnostics &gt; Agents, an extra column is displayed with the FQDN name.</td>
</tr>
<tr>
<td>computername in Logs and Usage Tracking</td>
<td></td>
</tr>
<tr>
<td>Lift policy restrictions for current</td>
<td>Removes all policy-related registry keys and values for the current user of the Management Console.</td>
</tr>
<tr>
<td>user</td>
<td></td>
</tr>
</tbody>
</table>

5.8  Workspace Branding

In the Setup menu, you can find **Workspace Branding**, that allows you to customize the splash screen that is displayed when starting, refreshing and ending a Workspace Control session and when starting the Workspace Control Console. The custom image that is selected is automatically resized to fit the splash screen. This image (same size as used in the splash screen) also replaces the Workspace Control logo in the background of the Management Console.

Display scaling (using the Microsoft Windows option 'Make text and other items larger or smaller') may not exceed 200% for **Workspace Branding** to display correctly.
Chapter 6: User Context

The Context of a user defines who the user is. Based on that context a workspace will be built that is tailored for that specific user.

6.1 Access Control based on context

Access Control determines users' access to Workspace Control settings and applications. Access Control consists of:

- **Identity**: which users get the setting or application. By default, all users are allowed access.
- **Locations and Devices**: in which Zones or on which clients the setting or application is available. By default, access is allowed from all zones and clients.
- **Date and Time**: in which time span (start and end date) the application or object is or becomes available. For applications, time restriction is possible for certain times and days of the week. By default, access is allowed at all times and on all days.

If none of these areas is configured for an object, the object is available to all users throughout the Workspace Control environment.

If one or more of these areas is configured for an object, users get access if they meet the criteria specified in each configured area.

6.1.1 Where to find Access Control

<table>
<thead>
<tr>
<th>What</th>
<th>Where</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control on Managed Applications</td>
<td>The application's <strong>Access Control</strong> section contains a tab for each Access Control area.</td>
</tr>
<tr>
<td></td>
<td>• Identity</td>
</tr>
<tr>
<td></td>
<td>• Locations and Devices</td>
</tr>
<tr>
<td></td>
<td>• Date and Time</td>
</tr>
<tr>
<td></td>
<td>• Workspace Containers</td>
</tr>
<tr>
<td></td>
<td><strong>Access Control</strong> is also available from the <strong>Quick Edit</strong> menu, which enables you to set the items above for one or multiple applications at the same time.</td>
</tr>
<tr>
<td>Access Control on settings and on User Installed Applications</td>
<td><strong>Access Control</strong> tab:</td>
</tr>
<tr>
<td></td>
<td>• Locations and Devices</td>
</tr>
<tr>
<td></td>
<td>• Identity</td>
</tr>
<tr>
<td></td>
<td>• Date and Time</td>
</tr>
<tr>
<td></td>
<td><strong>Workspace Control</strong> tab:</td>
</tr>
<tr>
<td></td>
<td>• Workspace Containers</td>
</tr>
</tbody>
</table>

Copyright © 2019, Ivanti. All rights reserved. Privacy and Legal.
### 6.1.2 Identity

The following Identity options are available for Access Control:

- All Users
- User/Group
- NOT User/Group
- Organizational Unit
- Organizational Unit including child OUs
- Controlled by Application Manager(s)
- Administrative Role
- NOT in Administrative Role
- Language (See Language Identity (on page 241))
- Identity Director Service
- Not Identity Director Service

Some of these options do not apply to all settings. For example, Access Control for User Settings allows only Organizational Units, groups, users and Administrative roles; and Controlled by Application Manager(s) is only available for applications.

#### Application Managers

In the configuration of Access Control on an application, the task of granting users access to the application can be delegated to one or more designated users. This is achieved by setting the Identity area of the application's Access Control to the option Controlled by application manager(s).

Application Managers do not need access to the Workspace Control Console. Instead, users who are listed as Application Manager for a specific application automatically get the Access Wizard in their Workspace (in the Settings section of the Start menu). The Access Wizard allows them to distribute the application(s) for which they are responsible to other users. The Access Wizard can also be opened directly from the Console by clicking the Access Wizard button.

When assigning Application Managers to an application, you can limit the range of users to whom the Application Managers can give the application. The available range limits are:

- all users.
- only users in the same OU as the Application Manager.
- only users in the same domain as the Application Manager.

On the Comments tab you can create a message that will be displayed in the Access Wizard when an Application Manager grants or revokes application access.
6.1.3 Locations and Devices: Zones

Access to a Workspace Control object can depend on the location where and the device on which a user session is started.

These locations are defined as Zones, based on various criteria such as IP-addresses, computer names, hardware requirements, environment variable values, operating system versions, USB storage device serial numbers, etc. Zones can also be configured for location-based printing to allow users to select a default printer per location based on Zones.

Zones are selected as Access Control criterion in the Locations and Devices area.

Where to find Zones

<table>
<thead>
<tr>
<th>What</th>
<th>Where</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defining the Zones applicable in the Workspace Control site</td>
<td>User Context &gt; Locations and Devices</td>
</tr>
<tr>
<td>Setting Zones as Access Control criterion on a Managed Application</td>
<td>Composition &gt; Applications &gt; the Locations and Devices tab in the application's Access Control section</td>
</tr>
<tr>
<td>Setting Zones as Access Control criterion on User Installed Applications</td>
<td>Security &gt; User Installed Applications &gt; Access Control</td>
</tr>
<tr>
<td>Setting Zones as Access Control criterion on a setting</td>
<td>on the Access Control tab of the setting</td>
</tr>
</tbody>
</table>

Zone rules

- Rules based on Active Directory Site allow you to create zones based on the Active Directory site from which users can start a Workspace Control session. This can be useful for sites with multiple Active Directory sites, divided by different domain controllers.

- Rules based on Active Directory Group membership allow you to set access on items, based on computer group membership.

- Rules based on Active Directory OU membership allow you to set access on items, based on computer OU membership.

- Rules based on Active Directory Computer property allow you to set access on items, based on computer property. For example, you can assign access to an application based on the Computer's name as stored in Active Directory. For this Zone rule, wildcards can be used in the Value field.

- Rules based on Active Directory User property are useful to create Zones for applications and/or settings that should only be available in sessions that match the value of the specified user property. For example, when an application should only be available to users in a specific company department, you can create a Zone rule based on the user property "department" and a value that specifies this company department.
• Rules based on **Computer Hardware** are useful for applications that need specific minimum system requirements (for example, AutoCAD).
  • Rules based on **Number of processors** and **Processor architecture** (under **Computer > Hardware**) are also supported for Linux and Apple Mac OS X Agents.
  • Rules based on **Processor architecture** are useful for applications that need specific processor type (x86/x64).
• Rules based on **IP address**, **IP address range** or **Computer Name** (under **Computer**, **Network** and **Remote Desktop**) are useful to link the Zone to a range of IP addresses or to a specific server, for example when configuring a printer server. When adding a Rule based on the **Computer name** for a Zone, the **Computer (FQDN)** can be used to apply the Rule to one or several Zones.

#### Syntax examples

• **To add MACHINE002 to the zone “France > Paris > Building A > Floor 1”, use the following command line:**
  
  `pwrtech.exe /clientadd=MACHINE002 /zone={7B8BF240-3682-41C5-881E-B14595593817}`

• If the command is run without a value for the parameter `/clientadd`, the current computer on which the command is run will be added at the moment of execution:
  
  `pwrtech.exe /clientadd /zone={7B8BF240-3682-41C5-881E-B14595593817}`

• If the command is run with a question mark as the value for the parameter `/zone`, a selection window opens to allow selection of the relevant Zone:
  
  `pwrtech.exe /clientadd /zone=?`

• To remove a Zone Rule for a particular client from a particular Zone:
  
  `pwrtech.exe /clientremove=MACHINE002 /zone={7B8BF240-3682-41C5-881E-B14595593817}`

• If the command is run with an asterisk (*) for the parameter `/zone`, all existing Zones are checked and any Rule where the (partial) computer name = MACHINE002 will be removed:
  
  `pwrtech.exe /clientremove=MACHINE002 /zone=*`

• **Rules based on Operating system (Bit) version** (under **Computer and Configuration**) are useful for applications that need a specific (bit) version of a Microsoft Windows OS or one of the following Linux and Apple Mac OS X versions (64-bit only):
  
  • CentOS Linux 5.11, 7.2.1511, 7.1.1503, 7.0.1406
  • RHEL 5.11, 7.2-7.0, 6.8-6.6
  • Apple Mac OS X 10.8-10.12.

• Rules based on **Vendor ID**, **Product ID** or **Serial number of USB storage devices** (under **Computer and Configuration > Hardware token**) allow you to create advanced scenarios in which, for example, an application is only available or a laptop can only be accessed if a specific USB storage device is present. For examples of how to use this rule, see **Example: Use a USB device for authentication purposes** (on page 134).

• Rules based on **Environment variable** (under **Configuration**) allow you to set access on items, based on the value of a specific environment variable. This rule applies to existing environment variables only; not to environment variables that are set by the Workspace Composer when the user starts a session.

• Rules based on **File version** (under **Configuration > Files and folders**) are useful if the version of a specific file should be the reason why a setting or application should be available or unavailable. For example, access to a database can be made to depend on the version of the database client; or the availability of an application can be made to depend on the version of a DLL file. In this way, you can hide an application from a user if the application cannot function properly due to the absence of a required version of a specific file. This saves the user from opening the application and then being confronted with error messages and other problems.
• Rules based on **File or folder exists** (under Configuration > Files and folders) are useful if the existence of a specific file, folder or drive at the start of a session should be the reason why an action should be carried out or not. For example, you may want to perform a folder synchronization action with a network drive. This action is only useful if this drive mapping exists. The Zone rule **File or folder exists** can be used to check this.

• Rules based on **Federal Information Processing Standard (FIPS) compliancy** (under Configuration) allow you to set access to resources based on a FIPS-compliant Windows Operating System. The rule evaluates whether the Windows GPO for FIPS has been set on the Agent.

• Rules based on **Operating system** (under Configuration) are also supported for the following Linux and Apple Mac OS X versions (64-bit only):
  - CentOS Linux 5.11, 7.2.1511, 7.1.1503, 7.0.1406
  - RHEL 5.11, 7.2-7.0, 6.8-6.6
  - Apple Mac OS X 10.8-10.12.

• Rules based on **Registry setting** (under Configuration) offer a huge range of possibilities, because much information is stored in the Registry. Each piece of information in the Registry can serve to determine the user’s workspace, from printers to environment variables to applications to Data Sources. For example, the availability of Word 2013 can be made to depend on a Zone that checks for the Registry key `HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word`; and the availability of Word 2010 can depend on the absence of this key. Similarly, different language versions of an application can be made available to users depending on their Active Directory site, which is stored in the Registry. Or access to the plotter printer can be granted only to users who use an AutoCAD application, as information about this is also stored in the Registry.

• With the option **Registry redirection** selected, a 64-bit Operating System will redirect registry values specified for `HKLM\Software` to their corresponding locations under the `Wow6432Node`. Please take the following into consideration when selecting this option:
  - In the Workspace Control Console, when browsing the registry to configure a Zone rule, the `Wow6432Node` will NOT be visible.
  - In a user session, applying a Zone will be based on the redirected location under the `Wow6432Node`.

• With the option **Registry redirection** not selected, no redirection will be done, and the following should be taken into consideration:
  - In the Workspace Control Console, when browsing the registry to configure a Zone rule, the `Wow6432Node` will be visible on 64-bit Operating Systems. Please note that 32-bit and 64-bit applications store information in different locations in the Registry. Therefore, separate rules may need to be configured for `HKLM\Software` and `HKLM\Software\Wow6432Node`.
  - In a user session, applying a Zone will be based on the original location in the registry. Zone rules containing registry values in the `Wow6432Node` will not be applied on 32-bit Operating Systems that do not have a `Wow6432Node`.

• Rules based on **Computer name**, **IP address**, and **IP address range** (under Network) are also supported for Linux and Apple Mac OS X Agents.

• Rules based on **Remote host/URL** (under Network) allow you to verify whether a specific IP address or URL is reachable to define an Access Control mechanism. This may be useful, for instance if a specific URL is only available from within the company network. Setting Access Control on an application to a Zone based on Remote host/URL prevents the application to be started from another location.
• Rules based on Connected network (SSID), allow you to configure features (e.g. printers) that are available if a session is running on a device connected to a specific wireless network.

• Rules based on the Security option Must connect through a trusted access point apply if the Agent's connection to a wireless network with the specified SSID uses a trusted access point. This makes it possible to disregard connections to other wireless networks with the same SSID, because they will not be accessible through your trusted access points. Please note, an access point is trusted if an enabled Nearest access point (BSSID) zone rule exists for it in your Workspace Control Console. Please be sure to define a full set of relevant access points.

• Rules based on the Security option May connect through any access point apply if the Agent is connected to any wireless network with the specified SSID. This may or may not be your organization's wireless network, because wireless network SSIDs are not globally unique. This option may be sufficient if you have not defined a full set of trusted access points, and/or if security is less important.

• Rules based on Nearest access point (BSSID), allow you to configure features to be available if a session detects that a specific access point is the nearest, based on it having the greatest signal strength of all detected access points. Please note that each access point for which a zone rule is specified will become a trusted access point for the purpose of zone rules based on wireless networks.

• Rules based on the Signal detection option Limit to trusted access points will only evaluate trusted access points when determining which detected access point has the greatest signal strength. Please note, an access point is trusted if an enabled Nearest access point (BSSID) zone rule exists for it in your Workspace Control Console. Please be sure to define a full set of relevant access points.

• Rules based on the Signal detection option Do not limit to trusted access points will evaluate all detected access points from networks with the specified SSID when determining which detected access point is the nearest. Detected access points may include mobile access points to other networks with the same SSID, because wireless network SSIDs are not globally unique. This option may be sufficient if you have not defined a full set of trusted access points, and/or if security is less important.

• Rules based on Client type (Citrix Receiver only) (under Remote Desktop) allow you to create zones based on the client type detected through the Citrix Receiver on Citrix XenApp and Citrix XenDesktop. This leverages the support that Citrix Receiver provides for different devices to distinguish the various operating systems.

• Rules based on Session type (under Remote Desktop) allow you, for instance to easily distinguish various desktop types. By specifying a session type, protocol and/or platform, access to a Zone may be set accordingly. A zone specifically for XenDesktop machines, for instance, would comply to: Session type: Remote Desktop; Protocol: Citrix ICA; Platform: Desktop. Other supported protocols are: Microsoft RDP, VMware PCoIP, VMware Blast, and VMware Blast Extreme.

• Rules based on Terminal Server (TS) listener name (under Remote Desktop) allow you to create Zones that can differentiate between network connections from inside and outside the company network. This is useful for applications that should be highly secured, such as financial applications.

• Rules based on the presence (or absence) of a VDX/Workspace Extender (under Remote Desktop) are useful to create Zones for applications that should only be available when there is (or is no) active VDX or Workspace Extender Client. These rules also apply to the RES Subscriber for VDX Agent and RES Subscriber for VDX Client.
Notes

- It is also possible to add a rule based on a computer name to an existing Zone, using a command line. In the Workspace Control Console this would be done at User Context > Locations and Devices, New/Edit Zone and then selecting the Rules tab and adding a Computer Name. This option is also available in combination with the command line, which can be used, for example, for scripting.

- **Active Directory Group membership** is supported for:
  - Active Directory groups
  - NT Domain groups

- When adding rules based on the value of a specific **Computer property** in Active Directory, please note that the following symbols will give unexpected results when they are used both in entries in Active Directory and as wildcards in the **Value** field in Workspace Control:
  - asterisk (*)
  - square brackets ([ ])
  - semicolon (;)

- If an access point is configured to hide its SSID, Workspace Control will detect it as an empty SSID (i.e. empty string). If there are multiple access points with a hidden SSID, Workspace Control is not able to distinguish between the networks they belong to. In this case, a rule for the nearest access point, specified for an access point with a hidden SSID, will check the nearest access point of ALL access points that hide their SSID (even if they belong to different networks).

- The use of environment variables is not supported for SSID and BSSID names.

- Due to privacy constraints, detected wireless networks and access points are not logged in the Workspace Control Console. However, during a user session they are shown to the end user on the **Diagnostics** tab of the Workspace Preferences tool, so end users can provide their administrator with this information upon request.
Multiple Rules for a Zone

By default, a Zone applies if a user logs on from a computer that matches one of the specified rules.

By grouping Zone rules using the **ampersand button** ( \( \& \) ), you can divide rules into groups. The ampersand functions as a group separator, and the Zone applies when one of the groups of rules is met.

**Examples**

<table>
<thead>
<tr>
<th>Item</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zone A</td>
<td>Accessible when Rule 1 OR Rule 2 applies (or both).</td>
</tr>
<tr>
<td>Rule 1</td>
<td></td>
</tr>
<tr>
<td>Rule 2</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Zone B</th>
<th>Accessible when Rule 1 AND Rule 2 apply.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule 1</td>
<td></td>
</tr>
<tr>
<td>&amp;</td>
<td></td>
</tr>
<tr>
<td>Rule 2</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Zone C</th>
<th>Accessible when Rule 1 OR Rule 2 applies (or both), AND Rule 3 applies.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule 1</td>
<td></td>
</tr>
<tr>
<td>Rule 2</td>
<td></td>
</tr>
<tr>
<td>&amp;</td>
<td></td>
</tr>
<tr>
<td>Rule 3</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Zone D</th>
<th>Accessible when Rule 1 OR Rule 2 applies (or both), AND Rule 3 OR Rule 4 applies (or both).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule 1</td>
<td></td>
</tr>
<tr>
<td>Rule 2</td>
<td></td>
</tr>
<tr>
<td>&amp;</td>
<td></td>
</tr>
<tr>
<td>Rule 3</td>
<td></td>
</tr>
</tbody>
</table>

When adding Zones in **Access Control / Locations and devices**, it is possible to require all Zones to be valid by using the AND option. For example, if you have a Zone for a particular OS and another Zone for a particular hardware requirement, you can combine these two by using AND in one Zone Rule. This way you do not have to create a third Zone to combine the two Rules.
Zone Members: Nested Zones

A Zone can be a member of another Zone. This allows you to arrange Zones in a parent/child hierarchy.

If a Zone contains no rules but only members, the Zone applies if the user logs on at a computer for which at least one of the member Zones is accessible.

If a Zone contains rules as well as members, the Zone applies if the user logs on at a computer for which all the Zone rules are met.

If a Zone contains rules and it also has a parent Zone, then the Zone applies if the Zone rules are met.

Example

• Zone A (no rules, only member Zone)
  • Zone B (no rules, only member Zones)
    • Zone C (contains rules)
    • Zone D (contains rules)

In this example:

• Zone A can be accessed if Zone B can be accessed.
• Zone C can only be accessed if the rules of Zone C are met.
• Zone D can only be accessed if the rules of Zone D are met.

Pattern matching in Zones

Pattern matching allows you to use wild card characters, character lists and character ranges in any combination to match a certain value (for example, client names or IP addresses). The specified pattern is used to find the desired data. If necessary, you can test a certain pattern before you use it in a field.

You can use the following pattern matching characters when configuring Zones:

<table>
<thead>
<tr>
<th>Character</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>?</td>
<td>Any single character</td>
</tr>
<tr>
<td>*</td>
<td>Zero or more characters</td>
</tr>
<tr>
<td>#</td>
<td>Any single digit (0-9)</td>
</tr>
<tr>
<td>[Charlist]</td>
<td>Any single character in charlist</td>
</tr>
<tr>
<td>![Charlist]</td>
<td>Any single character not in charlist</td>
</tr>
</tbody>
</table>
Example: Use a USB device for authentication purposes

By restricting an application or setting to a Locations and Devices Zone based on the unique serial number of a USB storage device, you can turn this specific USB storage device into a key to the application or setting.

Common scenarios when using USB Storage Device Identification in Zones are:

- **Removable Disks Security**
  By using Zones that contain USB Storage Device Identification rules, you can control which USB devices can be used by specific users.

- **Application Control**
  By assigning Identity and Zones that contain USB Storage Device Identification rules to an application, you enable multi-factored authentication for this application (based on user credentials and USB Storage Device doubling as unique token).

- **Workspace Control**
  By assigning Identity and Zones that contain USB Storage Device Identification rules to a Workspace Container, you enable multi-factored authentication for specific computers (only if these computers are exclusively assigned to this Workspace Container).

- **RES Workspace Extender**
  When a user starts a remote session using the RES Workspace Extender, any Zone that contains USB Storage Device Identification rules applies, as in a “normal” session. This means that users can also use USB Storage Devices as an access token in remote sessions using the Workspace Extender. For example, when a user has started a remote session and plugs in a USB device with a specific serial number on his local computer, this information is passed on to the remote session. As a result, applications and settings whose accessibility or applicability depends on the availability of this specific USB device serial number become available in the remote session when this session is refreshed.

  If you run the Management Console in a remote session using the Workspace Extender and plug in a USB device on your local computer, this device is automatically recognized by the Management Console. This allows you to create new Zones in the remote session using the serial number of the local USB device.

**Procedure**

1. At **User Context > Locations and Devices**, create a Zone based on the rule **USB storage device > Serial number**.
2. At **Composition > Desktop > Lockdown and Behavior**, in the Workspace Composer section, select **Refresh Workspace on USB storage device change**.
3. Set the Access Control of the application or setting to require the Zone.

With this setup, the user’s session is refreshed when a USB storage device is plugged in. If the serial number of the USB storage device matches the Zone rule, the application or setting becomes available. When the USB storage device is unplugged, the session refreshes again and the application or setting is no longer available.

This setup also works if the session is a Workspace Extension using the Workspace Extender.

**6.1.4 Date and Time**

The following **Date** and **Time** options are available for Access Control:

- **Start** and **End Date** and **Time**
- **Time Restrictions** (only for applications)

Date and time configured on objects are evaluated and applied at the start and refresh of a Workspace Control session. Date and time evaluation are based on the local time of the Workspace Control Agent.
6.2 Directory Services

At the **User Context > Directory Services** node of the Console you can configure Directory Services. The directory services used in your organization are the basis for your Workspace Control environment: Workspace Control delivers applications and resources based on the user, OU and group information that it retrieves from the directory services listed.

A directory service is used to store information about resources (such as printers), services (such as e-mail) and users in a network. The directory service provides information on these objects, organizes them, and provides authentication and validation. A well-planned and well-maintained directory service reflects the hierarchical and functional structure of an organization and is a powerful tool in the delivery of applications and resources to users.

Workspace Control can retrieve information from:

- **Microsoft Windows Domains** (also called NT Domains)
- **Microsoft Active Directory Services** (also called AD or ADS)
- **Novell Directory Services** (also called NDS)
- the local computer

The Primary Domain of the Agent will be configured by default. However, you can use multiple directory services concurrently. This makes it possible to use Workspace Control for specific parts of your IT environment. This can be particularly useful in very mixed environments, in environments where different administrators manage different sections, or if you wish to introduce Workspace Control gradually rather than all at once.

6.2.1 Configure directory services

- Workspace Control will use your environment’s name resolution mechanism to resolve the selected **Fully Qualified Domain Names** to the correct paths.
- When configuring a **Security Context**:
  - the account must be in the same domain as the directory service you are configuring.
  - the account requires sufficient rights to query the domain in Active Directory or in Microsoft Windows Domain.

These credentials will only be used when viewing data in the Management Console.

- If your environment does not include trusted domains, **not allowing query from external domains** will make sessions start up faster.
- With a **Mount Point**, objects in the tree above the mount point cannot be used in the Management Console unless another directory service starts in the same tree at a higher point.
- **Group Nesting** determines whether Access Control based on a parent group also applies to members of a subgroup. For example, suppose that Access Control for an application depends on membership of the group "AppUsers", and that this group contains the subgroup "AppAdmins".
  - **Without** support for group nesting, users must be member of the group "AppUsers" to get the application. Users who are only member of the subgroup "AppAdmins" do not get the application.
  - **With** support for group nesting, users who are only member of the group "AppAdmins" also get the application.

- You can select the method of resolving users and groups:

  **Account names** is preferable if user and group names do not change often. Renamed users and groups lose their current access because Workspace Control cannot find a match for their name. This method is recommended if Building Blocks are used to transfer objects from test to production environments, since names then are the same, but SIDs are not.
Account SIDs is preferable if user and group names change frequently. If a user or group is renamed, the account name changes but its SID does not. With Access Control based on SID, renamed users and groups keep their existing access and the Console reflects their new names.

When importing a Building Block, this can be done based on either Account names or Account SIDs. Based on this option the import process will automatically either resolve SIDs based on configured account names or resolve account names based on configured SIDs. The default setting is Account names. Unattended Building Block import will always use Account names.

- Select the method for Get group membership using (for Microsoft Active Directory and Windows Domain):
  - **Domain controller** - Select this method to have the Workspace Composer query the domain controller to get group membership for the current user. With this method, in a user session, changes in group membership are detected during a workspace refresh. To get the group membership faster, choose the method **Local tokens (faster)**.
  - **Local tokens (faster)** - Select this method to have the Workspace Composer resolve the user's group membership from its logon token. This option is especially interesting for multi-domain environments, in which resolving cross domain group membership does not work properly or causes performance degradation. With this method, in a user session, a user needs to log off and logon again to detect changes in group membership. To detect changes during a workspace refresh, choose the method **Domain controller**. This option should only be used in environments that have a Global Catalog server.
  - **Local tokens, until administrative refresh** - Select this method to combine the benefits of both methods **Local tokens (faster)** and **Domain controller** to get group membership for the current user. Local tokens are used until the first administrative refresh. From then on, until the session is logged off, the domain controller is queried to get the group membership for the current user. In multi-domain environments, all domains must be configured with this method. Administrative refreshes are initiated from outside the Workspace Composer, for instance, through the Management Console, Identity Director Services, or Automation. It is advised to select the same method for all defined directory services in the Workspace Control Console.

- In some situations, the order in which Directory Services are processed may be important. When a user starts a session, Workspace Control starts at the top of the list of Directory Services configured in the Console. The first configured Directory Service that matches the user's logon domain becomes the primary directory service for the session. The following order is usually advisable:
  - all Active Directory Services
  - all Microsoft Windows Domain Directory Services
  - the Local Computer Directory Service

In complex environments, you may need to experiment with this order.

---

**Notes**

- In Active Directory, due to stricter security rules, it may occur that users are not allowed to read their group membership. In this case, Domain Users must be added to the Pre-Windows 2000 Compatible Access group. The Pre-Windows 2000 Compatible Access group grants all users read-only access to objects in the OU to which it has been assigned.
- When using Account SIDs to process Access Control, any changes in a user’s group membership are not reflected until the next time the user logs on again.
6.2.2 Citrix XenApp Integration

If Citrix XenApp Integration is enabled in your Workspace Control environment, ensure that the Security Context fields of the Directory Service are filled out. Give the full path to the user name, for example: admin1.administrators.newyork.resone

6.2.3 Novell Directory Services

This feature is scheduled to be removed from Workspace Control. See also Feature deprecation (on page 399).

The following instructions apply specifically to Novell Directory Services:

Order of Directory Services

When a user logs on to a computer using the Novell Client, the Novell Client silently also logs that user on to a Microsoft Windows domain, or creates a new local user for this purpose. The way in which this is set up in your environment influences the identification of the user for the purposes of Workspace Control:

• If the Novell Client also logs the user on to a Windows domain, and you have also listed a Workspace Control Directory Service that includes that same domain, then you must place the Novell Directory Service higher in the list than the domain Directory Service. (Otherwise Workspace Control will find the user in the other Directory Service and will not check the Novell Directory Service anymore.)

• If the Novell Client also logs the user on as a local user, and you have also listed a Local Computer Directory Service in Workspace Control that will apply to the computer on which the user is logging on, then you must place the Novell Directory Service higher in the list than the local computer Directory Service. (Otherwise Workspace Control will find the user in the other Directory Service and will not check the Novell Directory Service anymore.)

Group Names

In Novell Directory Services, group names do not need to be unique. By default, Workspace Control Directory Services based on Novell will use the full paths of these groups to distinguish between them. This can be disabled, so that Workspace Control will treat all groups with the same name as one.

For example, you have the Organizational Units "New York" and "Amsterdam", which both contain a group "Helpdesk". Users from both those groups need access to the application "Knowledge Base". The way in which Access Control is set for this application, depends on the option Use full group names in the Workspace Control Directory Service for this Novell environment:

• If the option Use full group names is selected for the Directory Service for this Novell environment, Access Control on the application "Knowledge Base" must be set on the group Amsterdam/Helpdesk AND on the group New York/Helpdesk.

• If the option Use full group names is not selected, Access Control on the Knowledge Base can be set to the group "Helpdesk", and this will automatically include all groups with that name in that Novell Directory Service.

Notes

• Per Workspace Control site, only one Novell Directory Service can be configured.

• Workspace Control support for Novell Directory Services requires NetWare 4.x or higher. In combination with Citrix, NetWare 6.5 or higher is required.

• If the Novell client has not been installed on the target computer, Workspace Control will use standard Windows NT user and group enumeration for any user who logs on.
6.2.4 *Examples multiple Directory Services*

- configure a Workspace Control Directory Service for tree A, and one for tree B, but not (yet) for tree C.
- configure a Workspace Control Directory Service for a part of an Active Directory or Novell tree (by setting a mount point).
- use several Active Directory forests in one Workspace Control environment.
- combine different parts of several Active Directory forests, plus several Microsoft Windows Domains.
6.3 Workspace Containers

Workspace Containers are teams of Workspace Control Agents, grouped according to the logic of a specific Workspace Control site.

While Agents are grouped into Locations and Devices (Zones) based on objective rules, you can use Workspace Containers to group Agents according to more complex factors that cannot be defined in Zone rules.

Access to applications and settings can be restricted to specific Workspace Containers.

Examples:
- group a diverse set of test computers into a Workspace Container "Test environment". This allows you to restrict new settings and applications to this test space before they are made generally available.
- in a shared infrastructure, create a set of Workspace Containers to group the Agents belonging to different customers.
- group Agents according to responsibility (e.g. corporate administrators and local administrators)

6.3.1 Where to find Workspace Containers

<table>
<thead>
<tr>
<th>What</th>
<th>Where</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defining the Workspace Containers applicable in the Workspace Control site</td>
<td>User Context &gt; Workspace Containers</td>
</tr>
<tr>
<td>Setting Workspace Containers as Access Control criterion on a Managed Application</td>
<td>Composition &gt; Applications &gt; the Workspace Containers tab in the application's Access Control section</td>
</tr>
<tr>
<td>Setting Workspace Containers as Access Control criterion on User Installed Applications</td>
<td>Security &gt; User Installed Applications &gt; Workspace Control</td>
</tr>
<tr>
<td>Setting Workspace Containers as Access Control criterion on a setting</td>
<td>on the Workspace Control tab of the setting</td>
</tr>
<tr>
<td>Letting a user choose the Workspace Container when an application starts</td>
<td>Composition &gt; Applications &gt; the Workspace Containers tab in the application's Access Control section &gt; Let user decide which accessible workspace container to use.</td>
</tr>
<tr>
<td>Letting a user choose the Workspace Container when the Workspace Control session starts</td>
<td>start the session using the command line: %ProgramFiles%\Ivanti\Workspace Control\pfwsmgr.exe /ew ?</td>
</tr>
<tr>
<td>Forcing a user session to start in a specific Workspace Container</td>
<td>start the session using the command line: %ProgramFiles%\Ivanti\Workspace Control\pfwsmgr.exe /ew &lt;name of Workspace Container&gt;</td>
</tr>
<tr>
<td>Hiding a Workspace Container from the list when a user can choose a Workspace Container at the start of the session or application</td>
<td>on the Properties tab of the Workspace Container at User Context &gt; Workspace Containers</td>
</tr>
</tbody>
</table>
6.3.2 Computer Control

The Computer Control tab of a Workspace Container lists the Workspace Control Agents that belong to this Workspace Container.

When defining the computers that form a Workspace Container, there are 2 options:

1. only specifically identified Agents are members.
2. all Agents in the Workspace Control site are members automatically. Agents that are added to the site later, also become member automatically.

The first option enables you to create a hand-picked set of Agents.

The second option removes the Agent-based aspect of the Workspace Container (since all Agents are always a member of this Workspace Container). This enables you to use this Workspace Container as a set of Access Control principles.

Agents can be member of multiple Workspace Containers.

6.3.3 Access Control on Workspace Containers

Workspace Containers can be used part of Access Control on applications and settings.

Optionally, Workspace Containers themselves can also be restricted with Access Control criteria. This adds an additional layer of control over the availability of the Workspace Container: users who log on to an Agent that is member of the Workspace Container will also need to meet the Access Control criteria.

The following Access Control Identity criteria are available for Workspace Containers:

- User/Group
- NOT User/Group
- Organizational Unit
- Organizational Unit including child OUs
- Language
- Identity Director Service
- Not Identity Director Service

The following Access Control Locations and Devices criteria are available for Workspace Containers:

- Zone
- NOT in Zone
- Client Name

The following Access Control Date and Time criteria are available for Workspace Containers:

- Start date and time
- End date and time
6.3.4 Use Workspace Control to create different configurations for an application or the user session

By setting different Workspace Control on different settings in Workspace Control, you can configure an application or the user session to behave differently depending on the Workspace Container that applies when the user logs on.

Consider the following setup based on the application Microsoft Outlook:

- Workspace Container "Laptops" is limited by Access Control criteria to the OU "\...\Sales".
- Workspace Container "Desktops" is limited by Access Control criteria to the OU "\...\Manufacturing".

Both OUs can access the application Microsoft Outlook, for which two E-mail Settings exist:

- Mail setup "Outlook for Sales", which is limited by Workspace Control criteria to the Workspace Container "Laptops".
- Mail setup "Outlook for Manufacturing", which is limited by Workspace Control criteria to the Workspace Container "Desktops".

This leads to the following situation:

- If a user in the OU "\...Sales" logs on to an Agent in the Workspace Container "Laptops", only the E-mail Settings that belong to the Workspace Container "Laptops" will be applied.
- If a user in the OU "\...\Manufacturing" logs on to an Agent in the Workspace Container "Desktops", only the E-mail Settings that belong to the Workspace Container "Desktops" will be applied.

This allows you to configure a single Microsoft Outlook application that behaves differently, depending on the Workspace Container that applies to the user.

Allow users to choose a configuration set based on Workspace Container

If you create different configuration sets for an application or for the user session, and give these sets different Workspace Control settings, then you can let the user choose between predefined, differently configured versions of an application or a session.

This setup can be achieved if different configuration sets are created to depend on two or more Workspace Containers, and two or more of those Workspace Containers are available in the user session.
**Example: allow a user to choose a pre-set application configuration**

An application can connect to two different databases. To change the connection, the user needs the database credentials and other related information, but this information should not be available to the user. Information about the currently configured connection is stored in the registry.

To let the user choose which database to connect to when the application starts up:

- Create two Workspace Containers, both with the same Computer Control and the same Access Control. Make sure the names of the Workspace Containers are meaningful to the user of the application, for example by including the database name.
- On the application, create a User Registry Action for each database connection. Link each Action to a different Workspace Container.
- Add both Workspace Containers to Access Control of the application, and select the option *Let user decide which accessible workspace container to use*.

As a result, when users start the application, they will be asked to choose an option (= Workspace Container), and the database connection data in the registry will be set according to the Workspace Container selected.

**Example: allow a user to choose a pre-set session configuration**

If a user works in different roles on different days of the week, this user requires different applications and settings depending on the current role.

To let the user indicate today's role at logon:

- Create two Workspace Containers, both with the same Computer Control and the same Access Control. Make sure the names of the Workspace Containers are meaningful to the user, for example by including the role names.
- Create the full set of applications for both roles, with Access Control set to the relevant Identity (always the same user) and Workspace Container (depending on the role for which the application should be available).
- Create variants of any other settings that may be required, such as E-mail Settings, User Registry Actions, etc.; each with the appropriate Access Control (Identity and Workspace Control).
- Ensure that the user starts the Workspace Control session with the command line:
  
  `%ProgramFiles%\Ivanti\Workspace Control\pfwsmgr.exe /ew ?`

As a result, when the user starts the session, he will be asked to choose a role (= Workspace Container). This choice determines the applications and settings that become available in the session.
Example: force a session to start in a particular, exclusive Workspace Container

When publishing desktops on a Terminal Server, you may want to deliver only one specific Workspace Container to a user. This can be achieved by configuring the Ivanti Workspace Composer to start up in an exclusive Workspace Container. This means that only this specified Workspace Container will be processed for the user session. All other Workspace Containers will be ignored, even if the Agent is member of additional Workspace Containers. If the specified Workspace Container is not accessible, access to the session will be disallowed.

If you have sets of applications and settings that are mutually exclusive, you must ensure that they are never both available at the same time in one session.

To determine which Workspace Container applies when a user session starts, while ignoring all other Workspace Containers that may also apply:

- Create two Workspace Containers, both with the same Computer Control and the same Access Control.
- Create the full set of applications, with Access Control set to the relevant Identity and Workspace Container (depending on the set in which the application should be available).
- Create variants of any other settings that may be required, such as E-mail Settings, User Registry Actions, etc.; each with the appropriate Access Control (Identity and Workspace Control).
- Ensure that the user starts the Workspace Control session with the command line:
  \%ProgramFiles\%\Ivanti\Workspace Control\pfwsmgr.exe /ew <name of Workspace Container>

As a result, the Ivanti Workspace Composer will use only the Workspace Container specified in the command line. All other Workspace Containers are ignored.

Hide this workspace container if user needs to select one

If your Workspace Control site uses the setup where users can choose a Workspace Container when they start a session or an application, then your site will contain Workspace Containers with different purposes:

a) Workspace Containers intended for use in the chosen scenario,
b) Workspace Containers used to organize Agents for other purposes.

Workspace Containers in category (b) should never appear in a user's list of choices.

For these Workspace Containers, select the option Hide this workspace container if user needs to select one.
6.3.5 Use Workspace Containers to configure exceptions to the global settings of a feature

For global Workspace Control features that do not have Access Control or Workspace Control, you can create alternative configurations for specific Workspace Containers. This is achieved by adding one or more Workspace Container tabs to the feature node. The standard configuration is set on the feature node itself, and then any exceptions get their own tab.

For example, you may wish to enable the Sessions feature in your environment in general but disable it for test machines. This can be achieved by enabling Sessions Security at Security > Sessions and configuring the feature as required for the environment in general. Then, click the [+] next to the Audit Trail tab to add a Workspace Container tab for the Workspace Container “Test Machines”. On this tab, you disable the Sessions feature. As a result, the feature is disabled for all sessions to which the Workspace Container “Test Machines” apply. Sessions started outside of this Workspace Container get the global settings as configured in the Sessions node.

Availability

Workspace Container tabs for exceptions are available at nodes in Composition, Security, Administration, and Setup sections.

Order of processing

If a feature has several Workspace Container tabs with exceptions, the order in which the Workspace Container tabs appear determines their priority. The first tab on the left has the highest priority. The last tab on the right has the lowest priority.

- If a user session does not fall into any of the Workspace Containers for which exceptions are configured, it gets the global settings of the feature.
- If several of the Workspace Container tabs apply in a user session, the Workspace Container tab with the highest priority applies. For example, if the Sessions feature has a Workspace Container tab for Workspace Container "A", followed by a tab for Workspace Container "B", then a user session that falls into both these Workspace Containers gets the settings configured for "A".
6.4 Connection States

Use the Connection States node of the User Context section to configure the connection state settings of computers in your Workspace Control environment. This allows you to specify which applications and/or settings that are configured for off- and online use will be available to the user.

6.4.1 Methods

Workspace Control knows two different methods of detection of the connection state:

Default detection of Connection State: if the connection state of the computer is required for a setting or for accessibility to an application, the IP address of the local network connection will be used for this task. If no IP address is available, an "offline" Connection State will be assumed.

Advanced detection of Connection State: in certain conditions, the default method to detect the Connection State will fail. For example, if a fixed IP address is assigned to the local network connection, the detected Connection State will always be "online". By using "Advanced detection", this problem can be solved.

Advanced detection can be based on reachability of a specific
- host (Ping remote host on IPv4, Ping remote host on IPv6; specify a host name or IP address)
- port (Open remote port; specify an IP address and port number)
- URL (Open URL (http), Open URL (https))
- share (Open remote share)

to define an online or offline Connection State. Computers with access to the specified Zone will only have an "online" Connection State if the specified address can be detected on the network.

A timeout for the detection can be specified, except for Open remote share.

Advanced detection of Connection State may be useful, for instance if a specific URL is only available from within the company network. Setting the advanced connection state to detect this URL allows you to use Advanced detection of Connection state to determine whether a laptop is used inside or outside the company network. This might especially be useful to, for example, prevent company-sensitive information to be available outside the company.
6.5 Languages

Use the Languages node of the User Context section to extend multilingual support in your Workspace Control environment. Multilingual support in Workspace Control is primarily based on LanguagePacks. LanguagePacks provide different languages for all Workspace Control components, which end users can select in their Workspace Preferences tool.

By mapping languages to a LanguagePack, you can present the end user with a choice of additional languages to those available in LanguagePacks. This allows you to configure environment variables or registry settings that can be used to base applications on the language selection of the end user.

To map a language to a LanguagePack select Enable mapping of language to LanguagePack. This will display a list of available languages. Select a LanguagePack in the Installed LanguagePacks area and select the language(s) that you want to map to this LanguagePack.

6.5.1 Access principle

You can also use languages as access principle when configuring Access Control criteria for a certain setting in Workspace Control. For example, if the Management Console contains an Automation Task to install a French version of Adobe Acrobat, you can use the language French as access principle in Access Control, to ensure that the task is only executed for users that selected the language French in their Workspace Preferences tool.

6.5.2 Languages Example

If you highlight LanguagePack English and select the language Norwegian (Nynorsk), the variable %LCID% will contain the Windows identifier of that language. You can then use this variable to make changes in the registry on language level. For example, if you change the registry using this variable, you can change the display language of Microsoft Office.

After you have mapped Norwegian (Nynorsk), the user can select Norwegian (Nynorsk) in his Workspace Preferences tool. After refreshing the Workspace Composer, Workspace Control will display an English interface, whereas Microsoft Office will display the Norwegian (Nynorsk) interface.
Chapter 7: Composition

7.1 Applications

At Composition > Applications, managed applications are configured. Workspace Control-managed applications can be made available to users in their Start Menu, Desktop, Quick Launch area, and on the taskbar.

7.1.1 Start Menu tab

The Start Menu tab shows the applications in the folder structure in which they will appear in the Start Menu. Applications and Start Menu folders are added, edited, disabled and imported from this tab, and existing Windows shortcuts imported. LNK and OSD files can be used to import applications. The # applications at the bottom of the overview is dynamic.

The menu structure is created in the Workspace Control Console at the Applications node. Here you can also make applications available to end users.

There are four ways of creating a menu structure with applications:

- Creating a menu structure by hand and adding applications manually. This can be done by clicking the New menu button and selecting Application from the drop-down menu. The Edit application window will open allowing you to enter all application properties manually.
- Adding applications using a Wizard. When clicking the New menu button, select Application (using Wizard) from the drop-down menu to add an application using the Wizard.
- Importing applications with their menu structure to match. With the Import Wizard you can import an existing menu and application structure. Of course, it is possible to make alterations to the menus to be imported. When importing applications, select Do not add root folder to prevent the creation of the folder Start Menu. Select Do not add Programs folder to prevent the creation of the folder Programs. The folders can be skipped to make the applications fit better in an existing menu.
- A combination of the above.

When you disable a menu item, the menu item as well as the applications in that menu, will not be available in the user's Workspace Control session. Also, the configuration on those applications is then not applied in the user session.

When you disable an application, you are prompted to provide a message for users who try to start the disabled application. You can also provide such a message on the application's Notifications tab (in the application's Properties section).
7.1.2 Application List tab

The Application List tab shows the same applications as listed on the Start Menu tab, but in a sortable list with columns showing additional information.

- Multiple applications can be deleted at once or moved at once to another menu on this tab by selecting Delete or Move from the Menu at Action > Applications or from the context menu.
- Use the Search field to search for the desired application(s).
- The # applications at the bottom of the overview is dynamic.

You can sort columns by clicking on the column headers. Columns can be moved and resized by dragging and dropping the column headers. In the Options menu, the option Reset all column properties to defaults can be used to restore the columns to their original position and size.

7.1.3 Settings tab

On the global Settings tab of Applications, you can configure:

- whether managed applications should be fully implemented, partially implemented or disabled.
- additional settings for the behavior of applications and the Start Menu.
- the defaults that should be used for each new application.

Workspace Control managed applications can be implemented fully, partially or not at all. In a new environment, Applications is disabled: Windows Shell shortcut creation is set to Do not create shortcuts, so that users get the same Start Menu, Desktop and Quick Launch area in their Workspace Control session as they had outside of the Workspace Control session. With this setup, Workspace Control does not manage any of the user’s applications. At this point, you can configure applications in the Console, but these are not made available to any users.

When you are ready to start managing users’ applications through Workspace Control, you can enable Applications partially or fully:

- To give users Workspace Control-managed applications in addition to their existing, non-Workspace Control-managed applications, choose Windows Shell shortcut creation: Merge with unmanaged shortcuts.
- To give users only Workspace Control-managed applications, choose Windows Shell shortcut creation: Replace all unmanaged shortcuts. This eliminates non-Workspace Control managed applications from the Workspace Control session.
- Replace all unmanaged tiles on the start screen is applicable to user sessions running on Microsoft Windows 8.1 / 2012 R2 / 10.

Notes

- If Windows Shell shortcut creation (see “Applications” on page 148) is set to Replace all unmanaged shortcuts, this may lead to unpredictable results for global User Settings that preserve information in %desktop%\%startmenu% or %appdata%\Microsoft\Internet Explorer\QuickLaunch. This does not affect application-level User Settings for those folders.
- For users with a new profile or logging on to a system in a VDI environment that uses a non-persistent/pooled model, Workspace Control automatically creates a tile layout on the user’s Start screen that is similar to the default Start screen created by Microsoft Windows 8.1 / 2012 R2 / 10. If you would like to place different default tiles on the user’s Start screen, you can create the file DefaultTileLayout.xml (Windows 8.1 / 2012 R2) or DefaultTileLayout_Windows10.xml (Windows 10) and add it as a Custom Resource to Workspace Control, in the root (at Administration > Custom Resources).
The following settings determine the behavior of applications and the Start Menu:

<table>
<thead>
<tr>
<th>Setting</th>
<th>With this setting, Workspace Control will:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Autolaunch new applications on refresh if new application is configured to launch automatically</td>
<td>If access to applications is based on location, and a user starts a Terminal Server session at a certain location, he will have access to the applications that have been configured for that particular location. If the user disconnects from this session and reconnects from a different location, Workspace Control will refresh the Workspace, to update this change. As a result, the user will then have access to the applications that have been configured for the new location. If these applications have been configured for AutoLaunch, selecting this option will automatically launch these applications on a refresh of the Workspace.</td>
</tr>
<tr>
<td>Check actively for disabled applications in Workspace Control shell</td>
<td>Check for disabled applications each time the user opens the Start Menu. Disabled applications are marked with a red cross.</td>
</tr>
<tr>
<td>Disable Active Setup</td>
<td>Active Setup compares registry keys at HKLM\Software\Microsoft\Active Setup\Installed Components%APPNAME% and HKCU\Software\Microsoft\Active Setup\Installed Components%APPNAME%. If the HKCU registry entries do not exist, or the version number of HKCU is less than HKLM, then the specified application is executed by Active Setup for the current user. Enabling this option skips the “First Time Shell Init” that occurs for users that do not have an existing, locally stored profile (for example when using mandatory profiles). Disabling Active Setup may have a positive effect on login times, but certain features (for example Microsoft Internet Explorer and Windows Themes) depend on the actions it performs.</td>
</tr>
<tr>
<td>Disable autolaunch for managed applications</td>
<td>This option prevents the automatic start of managed applications that have the application-level option Autolaunch at session start configured as Mandatory. Applications that have Autolaunch at session start configured as Voluntary are not affected.</td>
</tr>
<tr>
<td>Disable process interception for unmanaged shortcuts</td>
<td>Select this option to disable Process interception for unmanaged shortcuts (on page 151) globally or for exception tabs. This overrules the application-level setting If managed shortcut was not used: Intercept new process and apply configuration.</td>
</tr>
<tr>
<td>Do not show offline applications when computer is online</td>
<td>Hides applications if the configured connection state does not match the computer's current connection state. If this option is not selected, users who try to start an &quot;offline&quot; application will be confronted with a message.</td>
</tr>
<tr>
<td>Do not show online applications when computer is offline</td>
<td>Hides applications if the configured connection state does not match the computer's connection state. By default, &quot;online&quot; applications are always shown in the user's Start Menu. When a user launches an application, the connection state of the computer is only checked against the required connection state of the application. This allows the user to change the connection state of the computer (by connecting to the corporate network), to gain access to the application without having to refresh the Start Menu. If this option is not selected, users who try to start an &quot;online&quot; application will be confronted with a message.</td>
</tr>
</tbody>
</table>
### Chapter 7: Composition

<table>
<thead>
<tr>
<th>Setting</th>
<th>With this setting, Workspace Control will:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do not show Workspace Extensions when VDX / Workspace Extender not detected</td>
<td>Hides applications configured to run as a Workspace Extension on computers on which the Workspace Extender has not been installed.</td>
</tr>
</tbody>
</table>

- **Refresh start menu if new software is installed**
  - Enabling this option will refresh Workspace Control sessions that use the application shortcut mode **Merge with unmanaged shortcuts** whenever the content of the common Start menu changes due to an (un)install of a software package. As a result, the user's Start menu will reflect this change. After a software package installation has finished, it may take up to 5 seconds before the refresh is performed.

  - **This option is not available when Windows Shell shortcut creation is set to Do not create shortcuts or Replace all unmanaged shortcuts.**

- **Remove all empty menus**
  - Enabling this option will automatically hide any empty menus (both managed and unmanaged) from the user's Start Menu.

- **Remove empty managed menus only**
  - Enabling this option will automatically remove all managed empty folders in the user's Start Menu. Managed folders are folders that were created on the **Start Menu** tab at **Composition > Applications**.

- **When offline, start a specific application () instead of Workspace Control taskbar and When online, start a specific application () instead of Workspace Control taskbar**
  - Start a specific application if the connection state of a computer is "Offline", or if it is "Online".

  - These two settings allow you, for example, to configure a laptop to connect to a published Ivanti Workspace Composer when online and to a local Ivanti Workspace Composer when offline.

  - You can specify which application should start:
    - By clicking the browse button and selecting it or by entering its ID. (You can find this ID on the application's **General** tab).
    - By specifying an environment variable, in which you have specified the application ID as its value. The application ID or environment variable that you specify will be shown between the brackets.

  - It is possible to configure an application timeout and configure the session's behavior if the application is terminated before the set timeout, or when the application exceeds the set timeout.

  - **By checking Launch before other actions**, the application will be run before other actions are performed, except for Automation Tasks and Execute Commands, if these have also been configured to 'run before other actions'.

---

**Note**

In a user session, if a user starts an application using **Run as different user** / **Run as administrator**, actions configured for the application (on the **Configuration > Actions** tab of the application) will not be applied. In this situation, only the settings related to the start of the application (configured on the **Properties > Settings** tab of the application) are applied:

- Parameters
- Startup style of application
- Process priority of application

**Disable file system redirector on 64-bit systems**
Process interception for unmanaged shortcuts

Workspace Control can intercept processes that are started through unmanaged shortcuts and treat them as if they were a managed application. Process interception for unmanaged shortcuts detects the start of a process and checks whether a managed application is available to the user that also uses the same process. If such a match is found, all the settings and configurations for the managed application are applied before the process is allowed to continue.

For example, in a session where Microsoft Word is available as a managed application, a user finds and double-clicks an unmanaged shortcut to Microsoft Word. This launches \winword.exe, which Workspace Control intercepts. Workspace Control first checks that Microsoft Word is allowed to start, based on date and time restrictions, maximum number of instances, licensing etc. If so, Workspace Control applies the settings and actions configured for Microsoft Word, such as User Settings, Drive and Port Mappings and Environment Variables. As a result, Microsoft Word starts up, and it has all its familiar Workspace Control configurations for the managed application Microsoft Word.

Configuration

On the Settings tab at Composition > Applications, the option Disable process interception for unmanaged shortcuts determines whether Workspace Control will intercept any processes at all. This option can be set for the global Workspace Model and for Workspace exceptions.

To start using process interception, clear the global option Disable process interception for unmanaged shortcuts, then configure individual managed applications to intercept their processes if started unmanaged. This is determined by the option If managed shortcut was not used (on the application’s Properties > Shortcuts tab, under Automatic shortcuts):

- **Ignore**: Take no additional action. The process will start without any configuration by Workspace Control.
- **Intercept new process and apply configuration**: Intercept the process and apply the configuration defined for the managed application.

If a process is intercepted that matches several available managed applications, Workspace Control applies the settings and configurations of the first managed application it finds. This may occur if multiple configurations of the same managed application exist.

If a user starts several processes that are intercepted, they are processed one at a time.

A process started from an unmanaged shortcut will continue without any Workspace Control configurations in the following situations:

- if there is no managed application available in the user session for the same process.
- if the managed application is not configured to intercept.
- if process interception for managed shortcuts is disabled.

Process interception for Citrix published applications

To use Process interception for Citrix published applications, set the option Run Workspace Composer to Automatic for servers running XenApp (at Administration > Agents). If an unmanaged Citrix published application is started on these servers, it will always be launched by the Workspace Composer. If there is a managed application that uses the same process and that is configured with If managed shortcut was not used: Intercept new process and apply configuration, it will be intercepted.
Process interception for Microsoft TS Remote published applications

To use Process interception for Microsoft TS Remote published applications, on servers hosting the applications:

- Make sure that the Workspace Composer (pfwsmgr.exe) is started when users log on (for example using the Microsoft Group Policy 'Custom user interface').
- Set the Workspace Control registry value XenDesktop7Intercept.

If there is a managed application that uses the same process and that is configured with **If managed shortcut was not used: Intercept new process and apply configuration**, it will be intercepted. With this feature you can, for example, implement Workspace Control in an existing environment, without republishing existing TS Remote published applications.

### Notes

- If the Managed Application Security setting Only Workspace Control is allowed to launch this application is selected (on the application's Authorized Files tab), users will only be able to start the process using managed shortcuts. This will prevent process interception from taking effect.
- Process interception for unmanaged shortcuts is not supported for virtualized applications such as Microsoft App-V 4.x and VMware ThinApp.
- When using process interception for unmanaged shortcuts, application environment variables cannot be used in the Target field of the unmanaged shortcut to the application.
Workspace Control and Microsoft Windows 8.1, 2012 R2, and 10

Default behavior of Microsoft Windows 10 affecting Workspace Control

Start Menu folder structure

The Start Menu in Microsoft Windows 10 uses a folder structure that is only one level deep.

This affects Workspace Control sessions in the following scenario:

- At Composition > Applications, on the Start Menu tab, applications are sorted into a nested folder structure.
- A Workspace Control session is running on Microsoft Windows 10.

In this scenario, only the top-level folder is displayed in the Start Menu. Applications from any subfolders are listed by application name as if they were in the top folder.

Group Policy “Remove and prevent access to the Shut Down, Restart, Sleep, and Hibernate commands” results in a black box in the Start Menu

If the Microsoft Group Policy “Remove and prevent access to the Shut Down, Restart, Sleep, and Hibernate commands” is enabled, on Windows 10, a black box appears in the user’s Start Menu instead of the actual options.

This affects Workspace Control sessions when using the following Lockdown and Behavior options that make use of the same policy:

- Disable "Shutdown" for all users on all computers
- Disable "Shutdown" for end users on workstations.
Recommended Configuration when using Microsoft Windows 10

Uncheck 'Disable Active Setup (skips first-time shell init)'

Microsoft Windows 10 performs several important actions during the Active Setup. At Composition > Applications, on the Settings tab, uncheck the setting Disable Active Setup (skips first-time shell init) to allow these actions to be executed correctly (the setting is checked by default).

Recommendation when starting to use Workspace Control Managed Applications for users with pre-existing Microsoft Windows 10 profiles

If you are installing Workspace Control in an environment where users have existing Start Menu lay-outs for Microsoft Windows 10, and want to use Windows Shell shortcut creation in Merge mode, the following configuration will preserve these Start Menu lay-outs:

- At Composition > Applications, on the Settings tab, set Windows Shell shortcut creation to Merge with unmanaged shortcuts.
- Ensure that each managed application at Composition > Applications is configured as follows on the Shortcuts tab of the application:
  - Disable the options Replace existing unmanaged shortcuts and Create Start Menu shortcut.
  - Set the option If managed shortcut was not used to Intercept new process and apply configuration.

Result:
In the user’s first Workspace Control session, no tiles will be added to the Start Menu for new managed applications (those that are not yet present in the user's Windows 10 profile). As of the user’s second logon, tile management as defined in the Workspace Control Console will be applied in all sessions.

In this scenario, if you configure options in the Automatic shortcuts section differently than recommended above, users will experience changes to the lay-out of tiles pinned to their Start Menu for unmanaged applications for which a managed equivalent exists in the Workspace Control Console, but with a different name:

- The tile sizes of these applications will all be set to medium.
- The Start Menu groups to which these applications belonged will be lost. All tiles will be put in a single, nameless group.
Known limitations of Workspace Control on Microsoft Windows 8.1, 2012 R2, and 10

Universal apps with User Settings

Universal apps* (such as Microsoft Edge) interact with the Operating System in a changed way. This affects our User Settings, which may not behave as expected for Microsoft universal apps.

* Universal apps are also referred to as Metro, Windows 8-style, Modern, Windows Store and Windows apps.

Workspace Control with Windows Shell shortcut creation set to Replace mode (only Microsoft Windows 10)

Consider the following scenario:

- The Windows Shell shortcut creation is set to Replace all unmanaged shortcuts.
  - The option Replace all unmanaged tiles on start screen is selected.
- In your Workspace Control environment, no tiles are configured for managed applications.

In this scenario, in user sessions, the Windows default tile layout will be used.

Switching between ‘Windows Shell shortcut creation’ modes may cause unmanaged tiles not to be restored (only Microsoft Windows 10)

At Composition > Applications, on the Settings tab, if Windows Shell shortcut creation is changed, unmanaged application tiles from a previous session might not be restored at next logon.

RES VDX Integration (only Microsoft Windows 8/8.1, 2012/2012 R2)

When the option Windows keys passthrough is enabled (at Setup > Integration > Ivanti Products > VDX, on the Settings tab) for user sessions running on Microsoft Windows 8/8.1 and 2012/2012 R2, the Alt+Tab key combination to switch between application windows does not work.

7.1.4 Defaults for new applications

New applications are created with certain default settings, for example for Access Control type, maximum number of instances, etc. You can edit a number of these application defaults to reflect the configuration that is most commonly used in your own Workspace Control environment.

- Click Set to configure the defaults for new applications.
- Click Reset to revert to the Workspace Control defaults for new applications. Resetting the defaults for new applications does not affect existing applications. It does not affect the other options on the Settings tab of the Applications node either.
7.1.5 Create and edit Applications

In the Edit Application window, you can review and edit the settings that have been configured for the application. There are different sections:

- **Properties** (on page 157)
- **Access Control** (on page 174)
- **Configuration** (on page 174)
- **User Settings** (on page 256)
- **Security** (on page 179)
- **Diagnostics** (on page 182)

**Properties**

The Properties section includes several tabs that together define the application and its behavior in user sessions.

Tabs in Properties section:

- **General** (on page 157)
- **Shortcuts** (on page 162)
- **Settings** (on page 164)
- **File Types** (on page 167)
- **Licensing** (on page 169)
- **Notifications** (on page 173)
- **Publishing** (on page 174)

**General**

On the General tab of the Properties section you can review (and edit) the settings that have been made for the application. If you add an application without the wizard, these settings must be entered manually.

How to configure the general properties of an application

- Open the application and click **Properties > General**.
- Use the information in the **ID** and the **GUID** field e.g. when configuring published applications, in which Workspace Control takes care of the necessary registry settings, mappings, substitutes, printer connections, etc. These fields cannot be changed and are first shown when you edit an existing application.
- Enter a title for the application in the **Title** field.
- Enter a description for the application in the **Description** field. This will be shown when the user moves his mouse pointer over the application in his Start Menu. The user can disable this function in his "Personalize My Workspace" tool. You can use hyperlinks (e.g. mailto:, http://, file://).
- Click 📋 in the **Command line** field to select the executable for the application.
  - You can use environment variables.
  - Right-click the **Command line** field and select Replace folder names with their associated environment string to automatically replace the selected folder in the command line with corresponding environment variables. This option is also available for the fields Working directory and Parameters.
  - You can also use a wildcard (*). This means that instead of: `%ProgramFiles%\Microsoft Office\Office14\Winword.exe` you could also use: C:\*\Winword.exe or *\Winword.exe. The wildcard is resolved into a path when the application is started in a user session. The more specific the path, the faster the application will be found.
When using a wildcard, keep the following in mind:

- In the command line only one wildcard can be used. Only the use of "*" is allowed, not "?".
- The wildcard cannot be used to replace (part of) an application name.
- The application will only be searched in local drives.
- You should only use a wildcard if no additional instances of the application are present (as only the first instance will be found).
- **Examples of valid use:**
  
  *notepad.exe*  
  C:\\*notepad.exe  
  C:\\progra*\\notepad.exe  
  %ProgramFiles%\\*\\notepad.exe  
  
  **Examples of invalid use:**
  
  *notepad.exe*  
  C:\\note*\\exe  
  C:\\note*.exe  
  notepad.*  
  *.exe

**Notes**

- Depending on the number of files and folders on the local drives, searching for a matching file can take a considerable amount of time. Once the file has been found, its location will be cached on the local machine.
- When Disable file system redirector on 64-bit systems has been enabled at Composition > Applications on the Properties > Settings tab, the file will be searched in both the actual and redirected folders if applicable.

- If necessary, select the working directory of the application by clicking in the Working directory field. Although this field is populated automatically when you select the application's executable in the Command line field, you can select a different folder.
  - You can use environment variables.
  - You can use wildcards (*).

- If necessary, enter startup parameters for the application by clicking in the Parameters field. For example, use %password% (Password$ for applications configured to run as Workspace Extensions) to pass the cached version of the user's password to the application. You can use environment variables.
  - If the application that you are configuring is a Microsoft App-V 4.x application, the Parameters field specifies the location of the OSD file that is needed to start the application.
  - To configure an application that will run inside a Microsoft App-V 5.x virtual application bubble, the Parameters field specifies the PACKAGEID and VERSIONID of the virtual application as /appvve:<PACKAGEID>_<VERSIONID>.  
  
  Example:  
  /appvve:668b7873-3ecd-4a81-aa74-0136bad81e7e_31912d51-2d3c-4622-baed-b7ad136fb032  

To configure that the application will run inside a Microsoft App-V 5.x virtual application bubble only if the virtual application package is deployed, add the parameter /ROW:NoPkgDelivery.  

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.

- To view a preview of the application's icon, double-click the application icon in the Icon field. This will open the Icon Preview window, which shows a preview of the various sizes of the application icon.
To refresh the icon, click 📚 in the Icon field. To select a different application icon, click 📚 in the Icon field. If you select a custom icon, it is always shown in the size in which it was uploaded. If this size is not large enough for Microsoft Windows 7, Windows Server 2008 R2 or Windows Vista, this icon will not look good if users opt to see larger icons. If this is undesirable, you have two choices:
- obtain a larger version of the custom icon and set the application to use that version instead. To do so, open the application at Applications and browse to the icon file at Icon.
- disable the use of large icons in Workspace Control sessions. To do so, go to Composition > Desktop > Start Menu and Taskbar, and clear the option Use high quality icons (Windows Vista and higher) under Microsoft Windows Shell only.

To run the application as a Workspace Extension, select Run as Workspace Extension. This is useful if the application is located on a desktop and it should run as a Workspace Extension via a Terminal Server session using the Workspace Extender. See Workspace Extensions (on page 160) for more information.

When configuring a Microsoft App-V 4.x application, select the option Use SCCM to deploy App-V application if the application is deployed with Microsoft Configuration Manager. This option is only available if both the Microsoft App-V 4.x client and the Microsoft Configuration Manager client are detected on the machine on which the Console is running. It automatically selects Hide application if executable was not found on the Settings tab of the application which hides the application from the Start Menu unless Microsoft Configuration Manager has distributed the application. In the background, the Workspace Composer will check the registry for the availability of Configuration Manager distributed App-V 4.x applications on the client. As soon as the App-V application is available and the menu is refreshed, the application will become available.

For Microsoft App-V 5 packages, the option Package delivery mode is available. Choose to only load the minimal parts of the Microsoft App-V 5 package that are needed to start the application or choose to load the full Microsoft App-V 5 package in the background as well once the application has started. Loading the full Microsoft App-V 5 package might be useful if the application needs to be available when the user session is offline, for instance, on laptops.

- By default, the Microsoft App-V client will fully download a Microsoft App-V application when a user starts that application for the first time. When selecting Minimal (global) or Minimal (per user) for the Package delivery mode, the registry value HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\AppV\Client\Streaming\AutoLoad must be set to 0.

- After upgrading to RES Workspace Manager 2014 SR2, configuring the Package delivery mode for existing Microsoft App-V 5 packages (packages that were configured in an earlier version than RES Workspace Manager 2014 SR2) will require you to (re)specify the central location of the Microsoft App-V 5 packages.

- When configuring the Workspace Control option Package delivery mode for Microsoft App-V 5 packages with Minimal (per user) or Full (per user), the feature Folder Redirection for the Windows folder AppData, is not supported.

- In a user session, when starting a Microsoft App-V 5 application that has been configured to be deployed by Workspace Control and is not yet available from the Microsoft App-V cache on the system, a Splash screen in the lower-right corner of the primary monitor will be displayed to the user. The Splash screen informs the user that the Microsoft App-V application will be deployed. Once it has been deployed successfully, the application will start automatically. Starting multiple Microsoft App-V applications (almost) simultaneously, a Splash screen per application will be displayed (with a maximum of 7 Splash screens at once). With the option Hide mini splash at application start enabled (at Composition > Desktop > Lockdown and Behavior, in the Workspace Composer section), these Splash screens will be hidden in the user session.
Chapter 7: Composition

- Optionally enter an **Administrative note**. This can be any comment or remark useful for administering the application.

<table>
<thead>
<tr>
<th>Notes</th>
</tr>
</thead>
</table>
| - The Citrix Integration Toolkit can be used to convert unmanaged Citrix published applications to managed equivalents.  
- The option *Allow users to restore their own settings* at Composition > User Settings will only work if the Workspace Preferences tool used by the end user fetches its data from the same homedrive as the application itself.  
- To create the name of an application shortcut, the application's title and its Start Menu path are used. This name may not exceed 255 characters. Microsoft Windows cannot handle application shortcut names that are >255 characters, which will result in an application shortcut that does not work properly.  
- Due to Microsoft Windows limitations, multiple *explorer.exe* shortcuts with different parameters that are pinned to the taskbar, will not stack on the proper taskbar icon. |
Workspace Extensions

RES VDX enables the integration of locally installed applications into Centralized (Server Based) Computing Workspace Control environments. This makes it possible to manage and control the access to local applications as well as Terminal Server applications from one central point: the Workspace Control Console.

Where to find Workspace Extensions

<table>
<thead>
<tr>
<th>What</th>
<th>Where</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workspace Extensions</td>
<td>Composition &gt; Applications, on the Properties &gt; General tab of an application</td>
</tr>
</tbody>
</table>

Configure Workspace Extensions

Workspace Extensions are applications that are managed centrally with the Workspace Control Console. If you configure an application to run as a Workspace Extension, it will be displayed in the Workspace Control menu like any other application. The only difference is that you need to specify the local path on the client for the application.

To run an executable on a local workstation as a Workspace Extension in a Centralized Computing session (for example a CAD program), complete the following steps:

- Install the VDX Client plugin on the client.
- Create an application with the Workspace Control Console. Select the option Run as Workspace Extension.
- Test the configuration by starting the Application.
- Check Usage Tracking to see whether the application usage is logged.

You may also associate the application with a Zone:

- Open the Application's properties in the Workspace Control Console.
- Add a Zone at the Access Control > Locations and Devices tab.
- Select a previously created Zone or create one.

This restricts the Workspace Extension to a specific Zone. This can be useful, for example, if the application is not locally installed on all workstations. As an alternative, assign the application to a specific Workspace Container.

Integrate File Types with Workspace Extensions

File Types seamlessly integrate with Workspace Extensions.

If you configure a File Type and select Also register this command as Workspace Extension, the File Type will also be registered on the client using the Workspace Extender (provided that your environment uses the Workspace Extender).

- If the user runs an application configured to run as Workspace Extension and accesses a file that is associated with an application that is located on a Terminal Server, Workspace Control will automatically open this application. For example, if you have configured Microsoft Outlook to run on a Terminal Server and associate it with the "mailto" special file type, Workspace Control will automatically open Microsoft Outlook in the Terminal Server session if the user opens a mail link in Internet Explorer that runs locally.
- If you have configured a File Type for a Workspace Extension and the user double-clicks this file type in the Terminal Server session, Workspace Control will automatically start the associated Workspace Extension and open the selected file (or resource). For example, if you have associated the file type "http" with the Workspace Extension Internet Explorer and the user double-clicks an Internet URL from any application in the Terminal Server session, Workspace Control will start the Internet Explorer which was configured to run as Workspace Extension.
In both cases, the files (or resources) must be available on the Terminal Server AND the local client. For example, if the user double-clicks a PDF file on a network share that has been mapped with drive letter "T:" and you have associated this file type with an application configured to run as Workspace Extension on the client, the same drive letter "T:" must be accessible on the client.

You can view the location of both file and application in the File Types node of the Workspace Analysis window of a specific user, which can be accessed through the node Diagnostics > Workspace Analysis. In this way, it is always clear how the redirection of File Types takes place between VDX and Workspace Control.

**Shortcuts**

**Automatic shortcuts**

- Select Replace existing unmanaged shortcuts to ensure that the user's Workspace contains only managed shortcuts, no unmanaged shortcuts to the same application. This setting is only applicable if Windows Shell shortcut creation (see Applications (on page 148)) is set to Merge with unmanaged application shortcuts.
- Create Start Menu Shortcut is enabled by default. Disable this option to exclude the application from the user's Start Menu, and to prevent the user from adding such a shortcut using the Workspace Preferences tool. If the application will be pinned to the Start Menu on Microsoft Windows 10, it is strongly recommended to enable this option.
- To determine the behavior of the application If managed shortcut was not used (for example, if an application was started by double-clicking the application's EXE), select Intercept new process and apply configuration to treat the new process like a managed application applying:
  - User Settings
  - Actions
    - Drive and Port Mappings
    - Drive Substitutes
    - Folder Synchronization
    - User Home Directory
    - User Profile directory
    - Printers
    - User registry / policy
    - Execute Command
    - Automation Tasks
    - Environment Variables
  - E-mail Settings
  - Data Sources
  - Application Notification (only for enabled Applications)

Setting the option to Ignore, the process will remain unmanaged. The following limitations apply:

- This option is not supported for virtualized applications such as Microsoft App-V and VMware ThinApp.
- If multiple unmanaged applications are intercepted, they are processed sequentially, not yet asynchronously.
If any of the following items are configured for the Managed Application, they are ignored when starting unmanaged:

- Application is disabled
- Time restrictions
- Seat Licensing
- Concurrent Licensing
- Memory Optimization limits
- Maximum Instances
- Required Connection States
- Dynamic privileges

The Ivanti Workspace Composer can also intercept unmanaged Citrix published applications and apply configuration. At Administration > Agents, the option to Run Workspace Composer can be set to Automatic for servers running XenApp. If an unmanaged Citrix published application is started it will always be launched by the Workspace Composer. However, if there is a managed application that uses the same process with Intercept new process and apply configuration at If managed shortcut was not used, it will be intercepted. If such a managed application is not present, the unmanaged Citrix published application will be launched without further intervention.

In the Personalized Start Menu, Desktop and Quick Launch / Pin to taskbar fields, select the automatic placement settings of shortcuts to the application for the user's Start Menu, desktop, and Quick Launch bar/taskbar. For example, this allows you to create mandatory applications in the user's Start Menu. Via the Workspace Preferences tool, users can pin and unpin their non-mandatory application shortcuts.

- **Take no action**: No Start Menu, Desktop and/or Quick Launch/taskbar shortcuts will be created automatically.
- **Set voluntary shortcut**: This will automatically create the Start Menu, Desktop and/or Quick Launch/taskbar shortcuts, but only once. The user can remove or add the shortcuts again.
  - If you change this setting to Take no action, and the user previously removed the voluntary shortcut, the shortcut will not be placed back.
  - If you change this setting to Take no action, and the user kept the voluntary shortcut, the shortcut will remain pinned to the Start Menu, desktop and/or Quick Launch bar/taskbar.
- **Set mandatory shortcut**: This will recreate the Start Menu, Desktop and/or Quick Launch/taskbar shortcuts each time the user starts a new session.
  - If you change this setting to Take no action, the shortcut will be removed from the Start Menu, desktop and/or Quick Launch bar/taskbar.

The option Pin to Start Menu, determines whether voluntary, mandatory or no application shortcuts are pinned in the user's Start Menu. This option is only applicable to Microsoft Windows 7, 2008 and 2008 R2.

On the Pin to Start Menu tab in the Workspace Preferences tool, users can pin and unpin their non-mandatory application shortcuts.

- **Take no action**: No application shortcut will be pinned to the user's Start Menu.
- **Set voluntary shortcut**: This will automatically create the application shortcut in the user's Start Menu, but only once. Users can remove or add the application shortcuts again.
  - If you change this setting to Take no action, and the user previously removed the voluntary shortcut, the shortcut will not be placed back.
  - If you change this setting to Take no action, and the user kept the voluntary shortcut, the shortcut will remain pinned to the Start Menu.
- **Set mandatory shortcut**: This will recreate the application shortcut in the user's Start Menu each time the user starts a new session.
  - If you change this setting to Take no action, the application shortcut will be removed from the Start Menu.
Notes

• The option Run (installation) using Dynamic Privileges can be combined with the intercept option for unmanaged applications. This means that, once the process has been intercepted and is allowed to start, and the application needs elevated privileges (for the user to install the software or for a command to be executed), these will be applied on the started application.

• If an intercepted application is not allowed to start, for example due to License or Opening hours restrictions, it will be terminated.

• When allowing the “Pinned sites” feature for browsers that have the ability to pin websites to the taskbar by configuring specific settings in the Management Console (see the Workspace Control Help for details), it is advised to create a managed application for Microsoft Internet Explorer (at Composition > Applications). This is because pinned websites will always be launched with Microsoft Internet Explorer (even if another web browser is set as the default browser).

• When enabling the option Pin to Start Menu for all applications, the User Settings template Start Menu (under Windows > Vista or later > Control Panel) is not necessary. This template stores the same User Settings.

• To create the name of an application shortcut, the application’s title and its Start Menu path are used. This name may not exceed 255 characters. Microsoft Windows cannot handle application shortcut names that are >255 characters, which will result in an application shortcut that does not work properly.

• Due to Microsoft Windows limitations, multiple explorer.exe shortcuts with different parameters that are pinned to the taskbar, will not stack on the proper taskbar icon.

Tile

Workspace Control can manage tiles in user sessions running on Microsoft Windows 8.1 / 2012 R2 / 10.

• Pin to Start - select the automatic placement settings of tiles for the application on the user’s Start screen:
  • Take no action: No tile will be created automatically on the Start screen.
  • Set voluntary tile: This will automatically create the tile on the Start screen, but only once. The user can remove or add the tile again. The tile will be displayed at the end of the Start screen unless a Group name is specified.
    • If you change this setting to Take no action, and the user previously removed the voluntary tile, the tile will not be placed back.
    • If you change this setting to Take no action, and the user kept the voluntary tile, the tile will remain pinned to the Start screen.
  • Set mandatory tile: This will recreate the tile on the Start screen each time the user starts a new session. The tile will be displayed at the end of the Start screen unless a Group name is specified.
    • If you change this setting to Take no action, the tile will be removed from the Start screen.

• Tile size - select the size of the tile as it should be displayed on the Start screen:
  • Medium: the tile is displayed as a medium sized square on the Start screen.
  • Small: the tile is displayed as a small sized square on the Start screen.
  • If a user changes the size of a mandatory tile, but leaves it in its original group, then the changed size will be maintained.

• Group name - specify the group the tile should be added to on the Start screen. If the group does not exist, it will be created.
  • If no group is specified, the tile will be added to the end of the Start screen.

Note

The tile properties are part of the Managed Applications Properties that are set when a session starts.
Chapter 7: Composition

**Settings**

When you have set up the basic configuration of an application you can use the Settings tab to configure some additional options.

<table>
<thead>
<tr>
<th>Item</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application is enabled</td>
<td>Enables the application.</td>
</tr>
</tbody>
</table>

**Disabling applications via the command line**

To disable an application in Workspace Control via the command line you need to use Building Blocks.

This mechanism can be used if you want to update applications via a script and want to disable the application before you start the update and enable the application after the update.

**Steps to follow:**

- Export the Workspace Control Application as single Building Block (e.g. Internet Explorer.xml on C:\)
- Rename the Building Block to Enable_Internet Explorer.xml
- Make a copy of the Building Block (application) you need to update and rename this file to Disable_Internet Explorer.xml
- Edit the Building Block Disable_Internet Explorer.xml and change `<enabled>yes</enabled>` to `<enabled>no</enabled>`
- Before you start the update, you execute `C:\program~1\respow~1\pwrtech.exe /add C:\Disable_Internet Explorer.xml`
- Execute your update

**After the update you execute** `C:\program~1\respow~1\pwrtech.exe /add C:\Enable_Internet Explorer.xml`

**Note**

Make sure that the cache update is set to “immediately”: Administration > Agents > Update agent cache.

<table>
<thead>
<tr>
<th>Item</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum instances</td>
<td>Allows Workspace Control to preserve system capacity. E.g. if you specify that the user is allowed to start the application only once and the user tries to start a second instance, he will be prompted whether to return to the open application or to close the open application and start the application in a new window. The maximum # of instances that can be specified is 30, but setting the maximum # of instances to 0 allows an unlimited # of instances.</td>
</tr>
<tr>
<td>Startup style of application</td>
<td>Specifies the startup style of the application.</td>
</tr>
</tbody>
</table>
### Chapter 7: Composition

<table>
<thead>
<tr>
<th>Item</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Process priority of application</strong></td>
<td>Specifies the process priority of the application in the field. A high priority allows for a larger amount of processor capacity, but can result in system freezes. A low priority decreases the chance on system hiccups and freezes, but can make the application slow. When selecting this option, the option Only Workspace Control is allowed to launch this application on the tab Security &gt; Authorized files is selected automatically, to ensure that the application cannot be started unmanaged with a different priority by using e.g. a command prompt or Windows Explorer.</td>
</tr>
<tr>
<td><strong>Required connection state</strong></td>
<td>Specifies the required connection state of the computer that grants access to the application. This is useful if Workspace Control is also used on laptops and the application should only be accessible when the laptop is connected to a network. By default, the applications stay visible in the Start Menu.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Item</strong></td>
</tr>
<tr>
<td>Do not list in PowerHelp</td>
</tr>
<tr>
<td>Do not notify about running instances</td>
</tr>
<tr>
<td>Do not show in &quot;New Applications&quot;</td>
</tr>
<tr>
<td>Application availability</td>
</tr>
<tr>
<td>Do not show application in system tray</td>
</tr>
<tr>
<td><strong>Autolaunch at session start</strong></td>
</tr>
<tr>
<td>- Take no action: The application will not start automatically. The user can change this behavior on the Startup tab of the Workspace Preferences tool.</td>
</tr>
<tr>
<td>- Voluntary: Initially, this will start the application automatically, but the user can change this behavior on the Startup tab of the Workspace Preferences tool.</td>
</tr>
<tr>
<td>- Mandatory: This will always start the application automatically. The user cannot change this behavior.</td>
</tr>
<tr>
<td>When changing configuration to Voluntary, the application will not start automatically for users that previously logged on before this setting was changed. These users can still change Autolaunch behavior using the Workspace Preferences tool.</td>
</tr>
<tr>
<td>When configured as Mandatory, the Global Application Setting Disable autolaunch for managed applications can override this behavior.</td>
</tr>
<tr>
<td>Autolaunch by user not allowed</td>
</tr>
<tr>
<td>Use extra password verification</td>
</tr>
<tr>
<td>Item</td>
</tr>
<tr>
<td>------------------------------------------------</td>
</tr>
<tr>
<td>Exclude from CPU Optimization</td>
</tr>
<tr>
<td>Exclude from Memory Optimization Limits</td>
</tr>
<tr>
<td>Exclude from Memory Optimization</td>
</tr>
<tr>
<td>Run in Separate Memory (16 bit apps)</td>
</tr>
<tr>
<td>Hide application</td>
</tr>
</tbody>
</table>
| Hide application if executable was not found   | Only shows the application in the Start Menu of the user if the application’s command line is valid on the computer on which the user has logged on. The application will be hidden in the Start Menu if the application’s command line is not valid. This option also applies to Workspace Extensions.  
For Microsoft App-V 5.x application that have Package delivery mode set to a value other than None (on the Properties > General tab), this option is grayed out.  
Please note that if you want to make the application available through Instant Passthrough, it is recommendable only to use the setting Do not passthrough if application is available on local computer. The Instant Passthrough settings can be edited at Composition > Applications. Edit the application, go to the Publishing tab and then to the Citrix XenApp Published Application, Settings tab. Click the Settings button and go to the Behavior tab. |
| Hide application if file was not found          | Only shows the application in the Start Menu of the user if a specified file (for example a script file) is present at the configured location. The application will be hidden if the file is not present.  
The file’s location can be on the local computer that user logs on to, or on a network share that can be reached from the user session.  
Use of environment variables is permitted. Wildcards can only be used in the filename. |
| Use "generic isolation" integration            | Allows you to integrate with application virtualization solutions other than Microsoft App-V (e.g. Thinstall, Citrix).                                                                                     |
| Disable file system redirector on 64-bit systems| On a 64-bit system, starting an application is influenced by folder redirection. Disable this folder redirection to ensure that the application is started from its defined path. |
File Types

Use the File Types tab to associate Windows file types and commands with an application.

Configuration

- Open the application and click Properties > File Types.
- To add a File Type to the application, click Add. This will open the Add/Change File Type window.
- To import all already known file types for the application from the system, click Import. If you have edited or deleted file types, you can revert to the default file types of the application by clicking the Import button again.
- To change existing File Types, click Edit or Delete.
- If multiple applications are associated with the same file types and commands, click the arrows to assign a priority. For example, WordPad can open simple DOC files, but Microsoft Word also supports this file type. If an application is at the top of the priority list for a certain file type and command, it will be used to handle the File Type. If this application is not accessible to the user, the second application will be used, etc. You can also edit this priority in the node Composition > Applications > File Types.

The same file type and command may be entered for more than one application. For example, WordPad can open simple DOC files, but Microsoft Word also supports this file type. To determine what should happen if a user has access to both applications, assign an application priority to the file type/command. You can do this on the Properties > File Types tab of an application, or on the File Types node of Composition > Applications.

The application at the top of the priority list for a certain file type or command will handle the file type association. If this application is not accessible to the user, the second application on the list will be used, and so on. If the initial application that handles a certain file type and command is temporarily not available (that is, disabled or limited by Time Restrictions), Workspace Control will look for an alternative application. This alternative must be configured for the same file type/command and must also be available in the user's menu.

When you add or edit an association, you can configure the following options:

- **File type extension**: the extension to be associated with an application. Select a known association with the browse button or enter a new extension manually.
- **Enabled**: whether the association is to be enabled.
- **Command**: the command associated with the file type (for example "edit", "open", or "print"). Usually executed by Windows when a user double-clicks a file from the Explorer or when a file is launched from another application. The command (or its description) will show in the context menu when right-clicking a file in the Explorer. Select a known command with the browse button or enter a new command manually.
- **Description**: a short description of the command that will be shown in the context menu when right-clicking a file in the Explorer.
- **Register as default command for this extension**: the default command is the command that will be executed by Windows when a user double-clicks a file.
- **Command line parameters**: the command line parameters that should be used for the application when the user selects the command. For example, use "/p %1" when configuring the "print" command for WordPad, so that WordPad will print the selected file.
- **Also register this command as Workspace Extension**: enables support for File Types for the Workspace Extender / RES Subscriber for VDX (see Workspace Extensions (on page 160)).
• **Use DDE:** you can enable this setting and automatically load the machine default DDE settings. Using DDE (Dynamic Data Exchange) prevents Workspace Control to open an additional instance of an application when, for example, an associated file type is double-clicked from the Windows Explorer and the application is already opened. It also enables e.g. printing of documents from the context menu.
  - **DDE Message:** This field specifies the DDE command for this action.
  - **Application:** This field specifies the DDE application string that is used to start the DDE link with the application.
  - **Topic:** This field specifies the DDE topic string to start a conversation with the application. The default DDE topic string (used if this field is empty) is “System.”
  - **DDE message if application is not running:** This optional field specifies the DDE command to use if the application (specified in the Application field) is not already running. If this field is left empty, Microsoft Windows sends the same command as specified in the DDE Message field.

See also: **PwrGateKeepAlive** (on page 217)

---

**Tip**

The variables `SPF_IFA$` and `SPF_IFA_REPLACE$` have been deprecated as of Workspace Control 10.1.0.0. A possible replacement solution can be found on the Ivanti Community.
Licensing

Use the Licensing tab of the application properties screen to configure application license metering. By managing application license usage in your Workspace Control environment, you can enforce license compliance to e.g. Microsoft licensing models.

It fully depends on the type of software license whether or not preventing access is enough for license management. The method of preventing access must comply with the type of software license. Here is an overview of the license types that Workspace Control can enforce. This enforcement is done on top of the access management of the application (i.e. a user may be granted access based on a distribution group, but the license enforcement may prevent the application from being used).

Concurrent user licensing

This type of licensing is uncommon for Microsoft applications. Workspace Control keeps track of the number of unique users that simultaneously use the same application. If the threshold is reached, then no additional users can launch the application. The maximum number of concurrent users as well as the users that used the application can be tracked for later reporting.

Named user licensing

This type of licensing is uncommon for Microsoft applications. Workspace Control keeps track of the number of unique users that used the same application. If a new unique user tries to launch the application while the threshold is reached, then the application will not be accessible. A list of unique users is maintained (including the denied users). Also, the users that used the application can be tracked for later reporting.

Seat licensing

This type of licensing is very common for Microsoft applications. Workspace Control keeps track of the number of unique computers that run the same application. There is an exception: if the application is run on a remote desktop, then the client computer accessing the remote desktop is being tracked instead. If the threshold of maximum allowed seats is reached, then no additional new (client) computers can launch the application. A list of unique seats is maintained (based on domain and computer names) including the denied seats. Also, the users and computers that used the application can be tracked for later reporting.

How to configure application licensing

• Open the application and click Properties > Licensing.
• Select the application license type in the License type field and configure the selected application license type:
  • Company-wide license - Grants unlimited access to all users in the Workspace Control environment. The number of users can still be controlled through the Access Control options.
    • Enter the license cost in the License cost field.
    • Enter the number of licenses in the # of licenses field. This will automatically calculate the total cost of licenses in the Total cost field.
  • In the Max. # of users field, enter the maximum number of users that can be granted access to the application. This field is only available if access to the application is managed by application managers (on page 127).
  • Server license - Grants access to the application based on server licenses. If all server licenses are in use, additional users will not be granted access to the application. Instead, a message will be displayed that all licenses are in use.
    • Enter the license cost in the License cost field.
    • Enter the number of licenses in the # of licenses field. This will automatically calculate the total cost of licenses in the Total cost field.
In the Max. # of users field, enter the maximum number of users that can be granted access to the application. This field is only available if access to the application is managed by application managers (on page 127).

- **Per seat license** - Seat licenses limit application usage to the number of computers that have logged in and claimed a seat. By linking licenses to client names instead of users, Workspace Control can enforce seat licenses for desktops and laptops, but also for Thin Clients.

With "Per Seat" licensing, it is possible to define a maximum number of seats per Zone. This can be used for example if each physical location within a company has a certain number of seat licenses available. In this case, define a Zone for each physical location, and set the maximum number of seats for each Zone. When seat licenses have been configured per Zone, the View reserved and rejected seat licenses window will let you choose which Zone to display the seat information for. To define the maximum number of seats per Zone, click the browse button next to the # of licenses field (this button will not appear until you have selected Per seat license). As long as there are no Zone-specific seats configured, Workspace Control will work as before, with one global number of seat licenses.

- In the field If database connection not available, specify the license metering behavior if there is no connection to the Datastore and the actual number of licenses or seats cannot be determined.
  - **Always grant access**: access to the application will always be granted and the claimed license will be cached to be processed later. You can change the default setting for new applications at Composition > Applications, on the application's Properties > Licensing tab.
  - **Do not grant access**: to force compliance with the configured licensing options, access to the application will be denied if a Datastore connection is not available.

- Enter the license cost in the License cost field.
- Enter the number of licenses in the # of licenses field. This will automatically populate the Total cost field with the total cost of licenses.
  - Click to configure the number of seat licenses per Zone. This will open the Seat licenses per Zone window.

- In the Max. # of users field, enter the maximum number of users that can be granted access to the application. This field is only available if access to the application is managed by application managers (on page 127).
- Click Seats to view the number of seats currently in use and the information about the computers (users) that have claimed them. This button is only available if the application uses seat licenses.

- **Per named user license** - Grants access to the application based on specified users. This allows for back order situations, while keeping track of the actual available number of licenses. If all licenses are in use, additional users will not be granted access to the application. Instead, a message will be displayed that all licenses are in use. If application access is managed by an application manager, this message will be displayed to him.
  - Enter the license cost in the License cost field.
  - Enter the number of licenses in the # of licenses field. This will automatically populate the Total cost field with the total cost of licenses.
  - In the Max. # of users field, enter the maximum number of users that can be granted access to the application. This field is only available if access to the application is managed by application managers (on page 127).
  - Click Named users to view which users have access to the application. You can configure access to the application on the Access Control tab. If you have delegated access to the application to an Application Manager, the Information about users and applications window will open, which displays information about the application and the users with access to it.
• **Per concurrent user license** - Concurrent user licenses limit application usage to the number of concurrent users. This form of licensing is supported for desktops and server-based computing environments. When all available licenses are in use, the next user who starts the application receives the message that all licenses are in use, plus a list of the users who are using the application at that moment. This avoids the purchase of needless additional user licenses, because it allows users to arrange access to the application among themselves up to the total number of licenses. Workspace Control will automatically retry to claim a concurrent license after 30 seconds. Users can use the **Retry** button to speed up this process.

If you use this license type, you cannot configure the **Maximum instances** of the application on the application’s **Properties > Settings** tab.

• In the field **If database connection not available**, specify the license metering behavior if there is no connection to the Datastore and the actual number of licenses or seats cannot be checked.
  
  • **Always grant access**: access to the application will always be granted and the claimed license will be cached to be processed later. You can change the default setting for new applications at **Composition > Applications**, on the application’s **Properties > Licensing** tab.
  
  • **Do not grant access**: to force compliance with the configured licensing options, access to the application will be denied if a Datastore connection is not available.

• In the field **Idle timeout in minutes**, specify how long the application can remain inactive before it is forcibly closed by Workspace Control. Because an inactive application unnecessarily holds a lock on a concurrent user license, selecting this option is useful if the number of available licenses is limited. If an application is forcibly closed, this will be logged in the **Event Log** of the user.

• By default, only the application’s main process is closed when the timeout expires. To also forcibly close child processes of the application when the idle timeout expires, select **Force close of child processes**.

• Enter the license cost in the **License cost** field.

• Enter the number of licenses in the **# of licenses** field. This will automatically calculate the total cost of licenses in the **Total cost** field.

• In the **Max. # of users** field, enter the maximum number of users that can be granted access to the application. This field is only available if access to the application is managed by **application managers** (on page 127).

• Click **Concurrent usage** on the application’s **Properties > Licensing** tab to see which users are currently using the application.

---

**Note**

Tip If you select **Per seat license** or **Per concurrent license**, the setting **Only Workspace Control is allowed to launch this application** on the application’s **Security > Authorized Files** tab will be selected automatically, to ensure that the user can only start the application via his **Start Menu** or desktop. This allows Workspace Control to check how many application licenses are in use.
Difference between # of licenses and # of users

The maximum number of users that can be granted access to an application can be set in the # of users field.

This is useful if you have granted users access while awaiting the arrival of extra licenses. For example: there are 100 licenses available and all licenses are already in use. You need to grant access to an additional 10 users that entered the company today. You can do this by setting the # of users field to 110 and order an additional 10 licenses. Until the licenses arrive, you can see the difference between the number of users and the actual number of available licenses, telling you that you have a back order running of 10 licenses or that you still need to buy 10 additional licenses. When the licenses arrive, you can then set the # of licenses field to the appropriate value, in this case 110.

If an application uses Concurrent User licensing and the maximum number of users is reached on all Terminal Servers or workstations, the next user who starts up the application will receive a message that the maximum number of licenses has been reached. A list of concurrent users will also be displayed so that the user can take action without having to contact the IT department.

The Application Manager will see a similar message when he tries to grant a user access to an application for which the maximum number of available licenses has been reached.
**Notifications**

Use the **Notifications** tab in to configure user notifications for an application. These messages will be shown to a user when he starts an application that has been enabled or disabled in Managed Applications.

**How to configure user notifications for an application**

- Open the application and click **Properties > Notifications**.
- Click the upper **Edit** button to configure a notification message for disabled applications.
- Select **Show notification when user starts the enabled application** and click the lower **Edit** button to configure a notification message for enabled applications.
  - Select **Show once** to show the message only when the user launches the application for the first time.
  - Select **Clear history** if you have changed the message. This will clear the history of the message and show the new message once.

**Notes**

- The notification messages support .rtf format and can contain hyperlinks (e.g. mailto:, http://, https://, file:///).
- The size of the **Edit notification** window determines the size of the notification window as it will be shown to the user.

**Publishing**

Use the **Publishing** tab of a managed application to publish the managed application as a Citrix XenApp published application, as Citrix XenApp published content, or as a Microsoft TS RemoteApp application.

- A Citrix XenApp published application is an application that runs on a Citrix XenApp server, but which behaves as if it were running on the user's local computer. Citrix XenApp published content is a file (such as a PDF document, a media file, or a URL) in any network location in your environment. When the content is published, a shortcut to the document is placed in the end user's Start Menu. See **Publish Citrix XenApp Applications** (on page 97).
- A Microsoft TS RemoteApp application is an application that runs on a Terminal Server, but because it integrates seamlessly with the user desktop, it behaves as if it were running on the user's computer. See **Set up Microsoft TS RemoteApp applications** (on page 108).

**Access Control**

See **Access Control based on context** (on page 126) in the **User Context** section.
Configuration

The Configuration section determines the Actions (on page 175) that should be executed when the application is started or ended; the application’s E-mail Settings (on page 177) and Data Sources (see page 212, see page 179).

Actions

Use the Actions tab to configure specific actions to be invoked when a user launches or closes the application. Application actions will only be invoked whenever the application is managed by Workspace Control. This is the case if the application is started from the Start Menu, when the application is started by a configured File Type, or when the application is intercepted by Workspace Control. Applications are not managed by Workspace Control if they are started from a command prompt, directly started from the Windows Explorer or from the run command.

The user’s Event Log will be appended with the results of the applied settings. You can view the contents of this Event Log in the Workspace Analysis window of this user.

All Actions for applications are configurable at application start. The following Actions for applications can be configured both at application start and application end:

- Execute Command
  - To run an Execute Command action at application start and end, duplicate the action and change the timing.
  - For Execute Command actions configured At application end for a Microsoft App-V 5.x application, the option Run outside App-V virtual environment is grayed out. The command will always be executed outside the App-V virtual environment.

- Folder Synchronization
  - A single Folder Synchronization action can be configured to run at both application start and end.

Actions configured for a managed application are listed per timing on two subtabs At application start and At application end (on the Actions tab in the Configuration section).

- For Linked Actions a placeholder is displayed on both At application start and At application end tabs, regardless of the timing of the actions configured for the source application.
  - Please note that when changing Linked actions, this is applied to all applications for which a Linked Actions action to the same source application is configured.
  - When editing an application-level action that is configured to run At application end to At application start or to move it to global, this action will show up in the Audit Trail with a Delete entry and Add entry. This is expected behavior.
  - When running multiple instances of the same managed application, with an action configured to run at application start, the action is invoked when starting the first instance. With an action configured to run at application end, the action is invoked when ending the last instance.
Note

If Microsoft Outlook is added as a new application in Workspace Control, a registry key is automatically added on the Configuration > Actions tab. This key disables the check whether Microsoft Outlook is the default e-mail client. If Microsoft Outlook is started through a File Type a notification that Microsoft Outlook is not the default e-mail client can appear, because the associated application in the registry is pwrgate.exe [appid] instead of outlook.exe. If the user then chooses to set Microsoft Outlook as the default mail client, the associated application in the registry is changed from pwrgate.exe [appid] to outlook.exe, making the application unmanaged.

The Registry key that is added is:

[HKEY_CURRENT_USER\Software\Microsoft\Office\<officeversion>\Outlook\Options\General]

Value name and data:

Check Default Client: 0

The order in which application Actions are executed

When a managed application starts, the application's Actions are executed by category, in the following order:

1. Environment Variables
2. Drive and Port Mappings
3. Drive Substitutes
4. Printers
5. User Registry Settings
6. User Registry Policies
7. User Home Directory actions
8. User Profile Directory actions
9. Folder Synchronizations
10. Execute Commands
11. Automation tasks
12. Microsoft ConfigMgr distributions
13. LANDesk software distributions
14. Linked actions

Global Actions

Actions can also be configured on a global level.

Actions for applications are identical to global Actions ("Actions" on page 212), except:

• In Drive and Port Mappings, Hide Drive behavior is not available.
• In Printers:
  • Set as default printer is mandatory, but will not reset the user’s preference. The next time the user logs on, only the preferred default printer will be restored. The user will also be notified of this event by the "Printing Preferences" tool.
  • Fast Connect is not available.
Moving and Duplicating Actions

It is possible to Move and Duplicate settings related to Actions. This makes it possible to:

- duplicate application settings and move them from one application to another
- duplicate application settings and move them to a global level
- duplicate global settings and move them to an application
- move global actions to an application
- move application actions to global

When moving actions from an application to global, the timing changes as displayed in the table below:

<table>
<thead>
<tr>
<th>Timing of application action</th>
<th>Timing of global action</th>
</tr>
</thead>
<tbody>
<tr>
<td>At application start</td>
<td>At logon before other actions</td>
</tr>
<tr>
<td>At application end</td>
<td>At logoff</td>
</tr>
</tbody>
</table>

When moving actions from global to an application, the timing changes as displayed in the table below:

<table>
<thead>
<tr>
<th>Timing of global action</th>
<th>Timing of application action</th>
</tr>
</thead>
<tbody>
<tr>
<td>At logon before other actions</td>
<td>At application start</td>
</tr>
<tr>
<td>At logon after other actions</td>
<td>At application start</td>
</tr>
<tr>
<td>At refresh</td>
<td>At application start</td>
</tr>
<tr>
<td>At reconnect session</td>
<td>At application start</td>
</tr>
<tr>
<td>At logoff</td>
<td>At application end</td>
</tr>
</tbody>
</table>

Notes

In a user session, if a user starts an application using Run as different user / Run as administrator, actions configured for the application (on the Configuration > Actions tab of the application) will not be applied. In this situation, only the settings related to the start of the application (configured on the Properties > Settings tab of the application) are applied:

- Parameters
- Startup style of application
- Process priority of application
- Disable file system redirector on 64-bit systems
Chapter 7: Composition

**E-mail Settings**

With **E-mail Settings**, you can configure mail profiles and other mail-related settings, such as access settings to mail servers and providers, personal address books and personal information stores. See the manufacturer’s documentation for more information about the configuration of these services.

Workspace Control applies E-mail Settings before the application’s Actions are processed. This allows you to change E-mail Settings registry keys after the E-mail Settings have been configured.

**Configuration**

- Click **New** or **Edit** in the node **Composition > Applications > E-mail Settings**. This will open the **New/Edit E-mail Settings** window.
- Click the **Properties** tab to configure the basic properties of the mail setup.
  - Enter a name for the mail settings in the **E-mail Settings name** field.
  - Optionally enter a note for the mail settings in the **Administrative note** field. This helps you to differentiate your E-mail Settings.
  - Select one of the options and click **Configure**. This will open the configuration window of the selected service. You can use environment variables such as `%fullusername%` and functions such as `$adinfo(title)` and `$adinfo(email)`. You can configure the following services:
    - **HP OpenMail**
    - **IMAP (Outlook XP only)**
    - **Internet E-Mail** Supported for Microsoft Outlook XP and Microsoft Outlook 2000.
    - **Lotus Notes Mail**
    - **Microsoft Exchange Online (Office 365)**
    - **Microsoft Exchange Server 5.5 or higher**
      To configure mail profiles for Microsoft Outlook 2016, the option **Use Autodiscover** (requires **Exchange 2007 or higher**) must be selected.
    - **Microsoft LDAP Directory**
    - **Microsoft Mail**
    - **Microsoft Outlook Express**
    - **Nortel CallPilot Desktop Messaging**
    - **Oracle Connector for Outlook**
    - **Outlook Address Book**
    - **Outlook Signature**
      When your Signature is voluntary, the signature is only created when the user starts Microsoft Outlook for the first time. This allows the user to change his signature. You can overwrite this custom signature with the default signature only once, by selecting **Clear history**.
      Signatures can only be edited in Rich Text Format, but when saving the signature, it will also be stored as plain text and HTML.
      You can use environment variables and user properties in the signature.
      You can type user properties directly in the signature field or select them from a list by clicking the **User property** button. When you click this button, you can review whether a specific user property has been assigned a value before deciding to add it to the signature.
      When selecting **Use external editors**, you have to edit each format individually when making changes to the signature. The signature will always be shown in Rich Text Format, even when editing plain text or HTML.
    - **Personal Address Book**
    - **Personal Folders**
    - **Zarafa Groupware Server**
• Select **Create once** to create the mail profile of the user only when the mail application is started for the first time or when a mail profile does not exist.

• If you have selected **Create once** and you want to force an update of the e-mail settings, select **Clear history**. This resets the count, so that the existing e-mail settings are created again throughout the environment, according to the rules selected for **Create once**. This can be useful after migrating to a new mail server or client.

• Click the **Access Control** tab to configure the criteria for **Access Control based on context** (on page 126) of the mail settings.

• Click the **Workspace Control** tab to configure to which **Workspace Containers** (on page 139) the mail settings apply.

**Example: Configuring an Outlook Signature**

• Click the node **Composition > Applications > E-mail Settings**.

• Click **New**. This will open the **New E-mail Settings** window.

• Click the **Properties** tab.

• Enter a name for the E-mail Settings in the **E-mail Settings name** field.

• Optionally enter a note in the **Administrative note** field.

• Select **Outlook Signature** and click **Configure**. This will open the **Configure Feature - Outlook Signature** window, which allows you to configure a signature for all users of Microsoft Outlook (Express). Outlook Signature is typically used to add corporate footers and disclaimers to e-mail messages.

• Enter a name for the signature.

• Select if the signature should be used when replying to or forwarding e-mail messages.

• Specify the behavior. If you select **Signature is voluntary**, the signature will only be created when the user starts Microsoft Outlook for the first time. This allows the user to change his signature.

• Select the appropriate version of Microsoft Outlook from the list.

• Edit the signature on the **New messages** tab. Although you can only edit in Rich Text Format, the signature will also be automatically translated to plain text and HTML. It is stored in these three formats for later use. You can use variables and functions in the signature. With user properties in Outlook Signatures, Outlook can get specific information about the user(s) to which the mail setup applies from Active Directory. You can type user properties directly in the signature field or select them from a list by clicking the **User property** button. When you click the **User property** button, this will open the **Select a user property** window, which will show a list of user properties and their values. This makes it possible to review whether a specific user property has been assigned a value before deciding to add it to the signature.

• Optionally, select **Use external editors** to use external editors. If you select this option, you have to edit each format individually when making changes to the signature. The signature will always be shown in Rich Text Format, even when editing plain text or HTML.

• Select whether the signature should also be used for replies and forwards, and click **OK** to save the configuration settings.

• Click the **Access Control** tab and the **Workspace Control** tab to configure access control and workspace control criteria for the signature.

**Data Sources**

Use the **Data Sources** tab to add an ODBC connection to an application. This allows you to link the application to ODBC-compliant DBMS.

**How to add Data Sources to an application**

1. Open the application and click **Configuration > Data Sources**.

2. Select an available Data Source from the list and click > to add it to the list of Selected Data Sources.

3. Click **Add Data Source** to add a new Data Source. This will open the **Add Data Source** window, which allows you to configure the Data Source. See **Data Sources** (on page 212).
Chapter 7: Composition

Security

The Security section of a Managed Application determines the application's Files Security mode and authorized files; and its Network Security mode and authorized connections.

Authorized Files

Use the Authorized Files tab to configure specific security settings for an application.

When a user starts an application, the application usually needs to access other files and executables to function properly. Access to certain files and folders can be blocked on a global level at Security > Data > Files and Folders. If a certain application needs a file or folder that is blocked on a global level, you could authorize these files and executables on a global level, but this may be undesirable. The alternative approach is to authorize the necessary files and folders for the specific application only. This approach provides the best protection of the user workspace.

- Global authorized files are configured at Security > Global Authorized Files.
- Application authorized files are configured at Managed Applications on the application's Security tab.

Configuration

- To add, edit or remove authorized files and folders for a specific application, open the application at Managed Applications and go to Security > Authorized Files.
- Select Run this application in learning mode if all access to files and folders by this application should be allowed but also logged. Run an application in learning mode for a while to find out which files and executables should be authorized for the application.
- To ensure that a user can only start the application in his Workspace Control session, select Only Workspace Control is allowed to launch this application. This ensures that a user can only use his Start Menu or desktop to start the application, and not e.g. a command prompt or Windows Explorer. This is useful if you want to force license compliance in your organization, because it allows Workspace Control to determine the actual number of application licenses in use. This setting is also useful if certain settings for the application are indispensable (e.g. registry settings). In the following situations, this setting is selected automatically and grayed out:
  - When using concurrent or seat licenses ("Licensing" on page 169) for the application.
  - When adjusting the process priority of the application on the Settings (on page 164) tab.
- The default value for the setting If running application is no longer authorized is configured at Security > Applications. You can change the behavior of the current application so that it does not follow the default anymore.
- You can authorize files and executables by adding a file or executable to the list of authorized files, but you can also authorize a file or executable directly from the log:
  - Click the Log tab. This shows an overview of security events that were caused by the application.
  - Select the file or executable that caused the security event and click Authorize selected incident. This will open the Authorize file window. The Authorized File field will be populated with the values of the incident that you selected.
- Authorized file security can be enhanced by checking the executable's file hash. To check file hashes, the global option Only allow authorized file hashes (at Security > Applications > Managed Applications, on the Settings tab) must be enabled and allowed/denied file hashes must be configured.
- Changes on the Authorized Files tab will not come in effect until you click OK and close the Edit application window.
Tips

• You can easily move authorized files from one application to another; from an application to the global Authorized Files node; and from the global Authorized Files node to a specific application. To do so, right-click one or more selected authorized files and choose Move.
• On the Applications List tab of the Managed Applications node, the column Learning mode shows whether an application is set in learning mode or not.

Example:

The availability of an application can be authorized based on a Zone. Once an application is running in a Workspace Control session, it can remain active if the user shuts down the computer without logging off from the session. Then, if the user logs on from another computer outside of the Zone that authorized the application, the application may still remain active despite its lack of authorization.

This breach of authorization can be prevented with the setting If running application is no longer authorized, [terminate application].

If this is not necessary, Workspace Control can also be configured with If running application is no longer authorized, [do nothing].

The default for this setting is configured at Security > Applications. Different behavior can be set for individual applications by opening the application at Composition > Applications and changing the setting at Security > Authorized Files.

Authorized Connections

Use the Authorized Connections tab in an application’s Security section to allow the application to use network connections that are blocked through the Network Security configured at Security > Network. This may be necessary for database applications, ICA/RDP clients, telnet applications, SSH clients, MSN Messenger, etc.

Configuration

• If you need to determine which network connections should be authorized for the application, but you do not want to disable global Network Security, select Run this application in learning mode. In learning mode, the application can still access unauthorized network connections, but these are logged.
• To convert a Log entry to an Authorized Connection, select the network connection that was logged as a security event, and click Authorize selected incident.

Note

A rule authorizing a Network Connection at application level overrules a rule blocking that same connection at a global level.

Tip

You can easily move authorized connections from one application to another; from an application to the global node Network; and from the global Network node to a specific application. To do so, right-click one or more selected authorized connections and choose Move.
Dynamic Privileges

Use the Dynamic Privileges tab to elevate or restrict rights for applications while maintaining default privileges for the user. This allows you to grant administrative privileges to specific applications that need these privileges (such as proprietary applications, Control Panel applets (using rundll32.exe or control.exe) and applications that allow changes to be made to hardware settings) without granting the user full rights as an administrator. Reducing user privileges may be useful for granting a user that is an administrator an application that should not be run as an administrator, such as a command prompt.

Configuration

Access token:

- **Do nothing** (default) - Does not change any rights for this application.
- **Add administrator rights** - Forces the application to be started with administrator rights.
- **Remove administrator rights** - Forces the application to be started without administrator rights.

Example:

To make a Control Panel applet available create a new application in the Workspace Control Console with `%systemroot%\windows\rundll32.exe` and the appropriate parameter. Add administrator rights to the applet using Dynamic Privileges. For instance:

<table>
<thead>
<tr>
<th>Date &amp; Time Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Module</strong></td>
</tr>
<tr>
<td><strong>Command:</strong></td>
</tr>
<tr>
<td><strong>result:</strong></td>
</tr>
<tr>
<td><strong>Command:</strong></td>
</tr>
<tr>
<td><strong>result:</strong></td>
</tr>
</tbody>
</table>

See [Make Control Panel Applets (CPL files) available as applications](#) (on page 200) for a more extensive list of Control Panel applets and their command lines.

Log

In the Edit application window, in the Security section, use the Log tab to view a list of all security events caused by an application and to authorize files and network connections, if necessary.

Configuration

You can authorize files and network connections with the **Authorize selected incident** button.

- If the event was caused by a file or executable, the Authorized files window will open, which will be populated with the values of the event that you selected.
- If the event was caused by a network connection, the Authorized Connections window will open, which will be populated with the values of the event that you selected.
Diagnostics

- Usage Tracking
  - Usage Tracking Viewer (on page 184) (in the Composition section)
  - Usage Tracking (on page 84) (in the Setup section)
  - Usage Tracking Overview (on page 314) (in the Diagnostics section)
- CPU Optimization (on page 328) (in the Administration section)
- Audit Trail (on page 312) (in the Diagnostics section)
7.1.6 Workspace Control Applications for end users

Access Wizard

It is possible to delegate the task of granting users access to an application to other users. Specific people who are expert users or who are responsible for a certain application can be made Application Managers. In most cases these people are non-IT personnel. Application Managers gain access to the Access Wizard, an application with which they can distribute the application(s) he is responsible for to other users.

Where to find the Access Wizard

<table>
<thead>
<tr>
<th>What</th>
<th>Where</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting Access Control to Controlled by application manager(s)</td>
<td>In the Workspace Control Console: Composition &gt; Applications, on the Access Control &gt; Identity tab of an application</td>
</tr>
<tr>
<td>Access Wizard</td>
<td>In the user’s session: Start menu &gt; Workspace Control settings &gt; Access Wizard</td>
</tr>
</tbody>
</table>

Usage Tracking Viewer

Information gathered by Usage Tracking is presented in the Usage Tracking Viewer. The user can view a list of detailed information, or a graphical representation of it. For reporting purposes, the information can be copied to the clipboard and pasted into a spreadsheet or word processor file.

Notes

- The Usage Tracking Viewer will not display any information about OUs if OU support has not been configured in the Workspace Control Console.
- The Usage Tracking database only stores OU information on the lowest OU level. This means that if the OU structure changes, the information displayed by Usage Tracking will change accordingly.
- On the tabs Details, Sessions and Current Activity in the Usage Tracking Viewer, you can type a search string to search for an object (e.g. user, application, computer or client). Previous search items are retained and using wildcards (*) in your search is allowed.
- Internet Explorer running as a Workspace Extension will not be tracked by Usage Tracking.
- Computer names of extended applications are preceded with an asterisk (“*”) in the Usage Tracking Overview.
- It is also possible to retrieve and analyze Usage Tracking data by using Web services. See Web Service for reporting.

Where to find Usage Tracking

<table>
<thead>
<tr>
<th>What</th>
<th>Where</th>
</tr>
</thead>
<tbody>
<tr>
<td>Usage Tracking</td>
<td>Go to Usage Tracking in the Setup menu</td>
</tr>
<tr>
<td>Usage Tracking Overview</td>
<td>Diagnostics &gt; Usage Tracking Overview</td>
</tr>
<tr>
<td>The Usage Tracking Viewer</td>
<td>In the Workspace Control Console: Diagnostics &gt; Usage Tracking Overview</td>
</tr>
<tr>
<td></td>
<td>In the user’s session: Start menu &gt; Workspace Control settings &gt; Workspace Preferences &gt; Other tab</td>
</tr>
</tbody>
</table>
Chapter 7: Composition

Printing Preferences
The Printing Preferences utility provides users with simple printer-related information and a Printer
Management console. Only user-related printers are shown.

Where to find Printing Preferences
What

Where

Printing Preferences

In the user's session: Start menu > Workspace Control settings >
Printing Preferences

Create a list from which users can choose a printer
It is possible to provide end users with an alternative user interface when connecting to a printer
from Printing Preferences. Usually, the Connect button will show a Microsoft Windows dialog in
which the user can browse the network for the desired printer. However, a geographically oriented
interface would be more intuitive for an average user. To enable this alternative interface,
complete the following procedure:
Create a file with the name "printers.lst". This file consists of sections for each location that
contains lines for each printer on that location. For example:
[USA\Detroit\Building 1\Floor 2\Office
\\fileserver1\printer212|Friendly name
\\fileserver1\printer213|Friendly name
\\fileserver1\printer214|Friendly name

XYZ]
for printer 212
for printer 213
for printer 214

[USA\New York\Office ABC]
\\fileserver8\printer845|Friendly name for printer 845
\\fileserver7\printer713|Friendly name for printer 713
\\fileserver7\printer715|Friendly name for printer 715

The part between square brackets defines the folder structure, where every level is separated by a
slash ("\"). If you want to use a backslash ("\") in the name of a folder, use a double backslash ("\\").
The lines that follow the line with folder names each define a printer that is displayed in that
folder. This line must start with the printershare name ("\\server\share"), optionally followed by a
pipe character ("|") and a friendly name for the printer.
The printers.lst file can be distributed through a User Home Directory Action (in
<HomeDir>\Personal Settings) which allows distribution based on Zones or through Custom
Resources with the class "PowerLaunch \ Printers". The printers.lst file will then look for the
printers.lst file located in "%ProgramFiles%\Ivanti\Workspace
Control\Data\DBCache\Resources\pl_prn".
Note
When distributing the printers.lst file using a User Home Directory Action, the User Settings Central storage
location must be in the User Home Directory. This is the default configuration of the Central storage location (at
Composition > User Settings, on the Settings tab.

Copyright © 2019, Ivanti. All rights reserved. Privacy and Legal.

185


Workspace Preferences

Workspace Preferences is the users' desktop management system. It offers users several options, such as configuring their desktop and their QuickLaunch icons, starting applications automatically, and swapping mouse buttons. But it also provides information that can be useful for troubleshooting (e.g. LDAP entries, Active Directory group membership, current Zones, and the connection state of the machine the user session is running on).

In the Workspace Control Console, you can determine which options should be available in the users' Workspace Preferences. This allows you to make certain options available or unavailable according, for example, to company policies. These user settings are stored in pwruser.ini, located in \Personal Settings in the user's home folder.

Where to find Workspace Preferences

<table>
<thead>
<tr>
<th>What</th>
<th>Where</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workspace Preferences</td>
<td>In the user's session: Start menu &gt; Workspace Control settings &gt; Workspace Preferences</td>
</tr>
</tbody>
</table>

Use User Home Directory Maintenance to change Pwruser.ini

Users can partly determine the behavior of their Workspace Control session by changing settings in their Workspace Preferences tool. These user settings are stored in pwruser.ini, located in \Personal Settings in the user's home folder. The pwruser.ini can also be changed from the Workspace Control Console using Home Directory Maintenance.

Example:

*(partial) contents of a pwruser.ini file*

```
[Preferences]
Printer=\srv-fs01\toshiba
PreviousPrinter=\srv-fs01\prt-oce-groundfloor
DesktopColor=10841658
DesktopForeColor=16777215
SmallIcons=No
LeftRight=No
NoAppguard=Yes
...
```

**NoAppguard**

<table>
<thead>
<tr>
<th>Hide Application Security Management messages in user's session</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Section</strong></td>
</tr>
<tr>
<td><strong>Settings</strong></td>
</tr>
<tr>
<td><strong>Data</strong></td>
</tr>
<tr>
<td><strong>Corresponding option in Workspace Preferences</strong></td>
</tr>
</tbody>
</table>
### NoVistaAppguard

<table>
<thead>
<tr>
<th>Hide extra Vista/2008/w7/2008r2 Application Security Management messages in user’s session when executable is started from Explorer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Section</td>
</tr>
<tr>
<td>Settings</td>
</tr>
<tr>
<td>Data</td>
</tr>
<tr>
<td>Corresponding option in Workspace Preferences</td>
</tr>
</tbody>
</table>

### DesktopColor

Set a different background color for the user’s session (other than the default set in the Workspace Control Console)

| Section | Preferences |
| Settings | DesktopColor |
| Data | [the color code] |
| Corresponding option in Workspace Preferences | Background color on the Background tab |

### DesktopForeColor

Set a different foreground (text) color for the user’s session (other than the default set in the Workspace Control Console)

| Section | Preferences |
| Settings | DesktopForeColor |
| Data | [the color code] |
| Corresponding option in Workspace Preferences | Foreground color on the Background tab |
Chapter 7: Composition

Desktop and DesktopSaveMandatory

Desktop lists the applications that the user has set as voluntary desktop shortcuts. DesktopSaveMandatory lists the applications that are set as mandatory desktop shortcuts.

<table>
<thead>
<tr>
<th>Section</th>
<th>MenuItems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settings</td>
<td>Desktop</td>
</tr>
<tr>
<td></td>
<td>DesktopSaveMandatory</td>
</tr>
<tr>
<td>Data</td>
<td>List of application IDs, separated by vertical bars (</td>
</tr>
<tr>
<td>Corresponding option in Workspace Preferences</td>
<td>Applications on desktop on the Desktop tab</td>
</tr>
</tbody>
</table>

Remarks

These settings are part of the Workspace Control mechanism for handling desktop shortcuts that change from optional to mandatory and vice versa.

DesktopSaveMandatory lists applications that have the setting Desktop: Set mandatory shortcut in the Workspace Control Console (on the application's General tab under Automatic shortcuts). At the start of a user session, Workspace Control checks whether each application in this list still has that setting. If not, the application is removed from the DesktopSaveMandatory list and put in the Desktop list instead. The reverse also happens with optional desktop shortcuts that have become mandatory.

There is not much point in changing these lists manually unless you also change the setting in the Console.

Note

Users can also opt to automatically set desktop shortcuts for all their applications. This is set with the INI file setting ShowAllOnDesktop.

ShowAllOnDesktop

Create mandatory desktop shortcuts for all applications

<table>
<thead>
<tr>
<th>Section</th>
<th>Preferences</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settings</td>
<td>ShowAllOnDesktop</td>
</tr>
<tr>
<td>Data</td>
<td>Yes or No</td>
</tr>
<tr>
<td>Default</td>
<td>No</td>
</tr>
<tr>
<td>Corresponding option in Workspace Preferences</td>
<td>Show all available applications on desktop on Desktop tab</td>
</tr>
</tbody>
</table>

Note

This setting cancels out the settings Desktop (“Desktop and DesktopSaveMandatory” on page 187) and DesktopSaveMandatory (“Desktop and DesktopSaveMandatory” on page 187).
QuickLaunch and QuickLaunchMandatory

<table>
<thead>
<tr>
<th>Section</th>
<th>MenuItems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settings</td>
<td>QuickLaunch</td>
</tr>
<tr>
<td></td>
<td>QuickLaunchMandatory</td>
</tr>
<tr>
<td>Data</td>
<td>List of application IDs, separated by vertical bars (</td>
</tr>
<tr>
<td>Corresponding option in Workspace Preferences</td>
<td>QuickLaunch on taskbar on the QuickLaunch tab</td>
</tr>
</tbody>
</table>

Remarks

These settings are part of the Workspace Control mechanism for handling QuickLaunch shortcuts that change from optional to mandatory and vice versa.

QuickLaunchSaveMandatory lists applications that have the setting QuickLaunch: Set mandatory shortcut in the Workspace Control Console (on the application's General tab under Automatic shortcuts). At the start of a user session, Workspace Control checks whether each application in this list still has that setting. If not, the application is removed from the QuickLaunchSaveMandatory list and put in the QuickLaunch list instead. The reverse also happens with optional QuickLaunch shortcuts that have become mandatory.

There is not much point in changing these lists manually unless you also change the setting in the Console.
### Applications and ApplicationsSaveMandatory

Applications lists the applications that the user has set as voluntary shortcuts in the Start Menu. ApplicationsSaveMandatory lists the applications that are set as mandatory shortcuts.

<table>
<thead>
<tr>
<th>Section</th>
<th>MenuItems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settings</td>
<td>Applications</td>
</tr>
<tr>
<td></td>
<td>ApplicationsSaveMandatory</td>
</tr>
<tr>
<td>Data</td>
<td>List of application IDs, separated by vertical bars (</td>
</tr>
<tr>
<td>Corresponding option in Workspace Preferences</td>
<td>Applications in Start Menu on the Start Menu tab</td>
</tr>
</tbody>
</table>

**Remarks**

These settings are part of the Workspace Control mechanism for handling Start Menu shortcuts that change from optional to mandatory and vice versa.

ApplicationsSaveMandatory lists applications that have the setting Start Menu: Set mandatory shortcut in the Workspace Control Console (on the application's General tab under Automatic shortcuts). At the start of a user session, Workspace Control checks whether each application in this list still has that setting. If not, the application is removed from the ApplicationsSaveMandatory list and put in the Applications list instead. The reverse also happens with optional Start Menu shortcuts that have become mandatory.

There is not much point in changing these lists manually unless you also change the setting in the Console.

---

**Note**

Users can also opt to automatically set Start Menu shortcuts for all their applications. This is set with the INI file setting ShowAllApplication.

### ShowAllApplication

Create mandatory Start Menu shortcuts for all applications

<table>
<thead>
<tr>
<th>Section</th>
<th>Preferences</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settings</td>
<td>ShowAllApplication</td>
</tr>
<tr>
<td>Data</td>
<td>Yes or No</td>
</tr>
<tr>
<td>Default</td>
<td>No</td>
</tr>
<tr>
<td>Corresponding option in Workspace Preferences</td>
<td>Display all available applications in Start Menu on the Start Menu tab</td>
</tr>
</tbody>
</table>

**Note**

This setting cancels out the settings Applications ("Applications and ApplicationsSaveMandatory" on page 189) and ApplicationsSaveMandatory ("Applications and ApplicationsSaveMandatory" on page 189).
Startup

<table>
<thead>
<tr>
<th>List the applications that users can set to be autolaunched</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Section</strong></td>
</tr>
<tr>
<td><strong>Settings</strong></td>
</tr>
<tr>
<td><strong>Data</strong></td>
</tr>
<tr>
<td><strong>Corresponding option in Workspace Preferences</strong></td>
</tr>
</tbody>
</table>

DesktopBackGround

<table>
<thead>
<tr>
<th>Set a specific BMP file as background picture</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Section</strong></td>
</tr>
<tr>
<td><strong>Settings</strong></td>
</tr>
<tr>
<td><strong>Data</strong></td>
</tr>
<tr>
<td><strong>Corresponding option in Workspace Preferences</strong></td>
</tr>
</tbody>
</table>

**Remarks**

The file needs to be placed in the Resources folder in the Workspace Control program directory. Files that are set as background from the Workspace Control Console are placed there automatically. The most convenient way to place other files there is to add the file as a Custom Resource in the Workspace Control Console.

DesktopBackGroundPlacement

<table>
<thead>
<tr>
<th>Location of the background picture (right corner, stretched)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Section</strong></td>
</tr>
<tr>
<td><strong>Settings</strong></td>
</tr>
<tr>
<td><strong>Data</strong></td>
</tr>
</tbody>
</table>
### SmallIcons

**Show small application icons in Start Menu**

<table>
<thead>
<tr>
<th>Section</th>
<th>Preferences</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settings</td>
<td>SmallIcons</td>
</tr>
<tr>
<td>Data</td>
<td>Yes or No</td>
</tr>
<tr>
<td>Default</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Corresponding option in Workspace Preferences**

Use small icons and Use large icons on the Options tab

**Remarks**

Only available in the Workspace Control Shell

### SwapMouse

**Swap the mouse button from right to left**

<table>
<thead>
<tr>
<th>Section</th>
<th>MenuItems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settings</td>
<td>SwapMouse</td>
</tr>
<tr>
<td>Data</td>
<td>Yes or No</td>
</tr>
<tr>
<td>Default</td>
<td>No</td>
</tr>
</tbody>
</table>

**Corresponding option in Workspace Preferences**

Users can swap the orientation of their mouse buttons on the Options tab

**Remarks**

With this setting at No, the mouse button is on the right-hand side. With this setting at Yes, the mouse button is on the left-hand side.

### HideDescription

**Hide balloon pop-up with application description when starting application**

<table>
<thead>
<tr>
<th>Section</th>
<th>Preferences</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settings</td>
<td>HideDescription</td>
</tr>
<tr>
<td>Data</td>
<td>Yes or No</td>
</tr>
<tr>
<td>Default</td>
<td>No</td>
</tr>
</tbody>
</table>

**Corresponding option in Workspace Preferences**

Hide description window on the Options tab

**Remarks**

This option refers to the description balloon that pops up in the bottom right-hand corner of the screen when the mouse pointer hovers over an application in the Start Menu. Only available in the Workspace Control Shell.
### MessageDefaultPrinter

**Display message if default printer is missing**

<table>
<thead>
<tr>
<th>Section</th>
<th>Preferences</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settings</td>
<td>MessageDefaultPrinter</td>
</tr>
<tr>
<td>Data</td>
<td>Yes or No</td>
</tr>
<tr>
<td>Default</td>
<td>Yes</td>
</tr>
<tr>
<td>Corresponding option in Workspace Preferences</td>
<td>Notify me if my default printer is missing or has changed on the Options tab</td>
</tr>
</tbody>
</table>

### LCID

**Set the interface language for Microsoft applications and other Microsoft components (based on installed MUI)**

<table>
<thead>
<tr>
<th>Section</th>
<th>Preferences</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settings</td>
<td>LCID</td>
</tr>
<tr>
<td>Data</td>
<td>[the LCID code]</td>
</tr>
<tr>
<td>Default</td>
<td>[default language in Management Console]</td>
</tr>
</tbody>
</table>

### MLS

**Set interface language of the Workspace Control shell, Workspace Preferences and other Workspace Control components (based on installed Workspace Control Language Pack)**

<table>
<thead>
<tr>
<th>Section</th>
<th>Preferences</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settings</td>
<td>MLS</td>
</tr>
<tr>
<td>Data</td>
<td>[MLS code]</td>
</tr>
<tr>
<td>Default</td>
<td>[default language in Management Console]</td>
</tr>
<tr>
<td>Corresponding option in Workspace Preferences</td>
<td>Language on the Options tab</td>
</tr>
</tbody>
</table>

### HideMyNameInScreensaver

**Suppress user name in the Workspace Control screensaver**

<table>
<thead>
<tr>
<th>Section</th>
<th>Preferences</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settings</td>
<td>HideMyNameInScreensaver</td>
</tr>
<tr>
<td>Data</td>
<td>Yes or No</td>
</tr>
<tr>
<td>Default</td>
<td>No</td>
</tr>
<tr>
<td>Corresponding option in Workspace Preferences</td>
<td>Do not display my name in the screensaver on the Options tab</td>
</tr>
</tbody>
</table>
## HotKeyModifier and HotKeyKey

Define the combination of keys to activate the Start Menu. HotKeyModifier is the first key, HotKeyKey is the second key.

<table>
<thead>
<tr>
<th>Section</th>
<th>Preferences</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settings</td>
<td>HotKeyModifier</td>
</tr>
<tr>
<td></td>
<td>HotKeyKey</td>
</tr>
<tr>
<td>Data</td>
<td>[key]</td>
</tr>
<tr>
<td>Default</td>
<td>Modifier: SHIFT</td>
</tr>
<tr>
<td></td>
<td>Key: ESC</td>
</tr>
<tr>
<td>Options</td>
<td>Modifier: SHIFT, ALT, CTRL or [empty]</td>
</tr>
<tr>
<td></td>
<td>Key: ESC, TAB, F1 up to and including F12 or [empty]</td>
</tr>
<tr>
<td>Corresponding option in Workspace Preferences</td>
<td>Workspace hotkey on the Options tab</td>
</tr>
</tbody>
</table>

## AutoHide

**AutoHide the Taskbar in user session**

<table>
<thead>
<tr>
<th>Section</th>
<th>Preferences</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settings</td>
<td>AutoHide</td>
</tr>
<tr>
<td>Data</td>
<td>Yes or No</td>
</tr>
<tr>
<td>Default</td>
<td>No</td>
</tr>
<tr>
<td>Corresponding option in Workspace Preferences</td>
<td>Auto hide taskbar on the Options tab</td>
</tr>
</tbody>
</table>

## OnTop

**Taskbar always OnTop in user session**

<table>
<thead>
<tr>
<th>Section</th>
<th>Preferences</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settings</td>
<td>OnTop</td>
</tr>
<tr>
<td>Data</td>
<td>Yes or No</td>
</tr>
<tr>
<td>Default</td>
<td>Yes</td>
</tr>
<tr>
<td>Corresponding option in Workspace Preferences</td>
<td>Keep taskbar on top of other windows on the Options tab</td>
</tr>
</tbody>
</table>
## TimeoutScrnSaver

**Set the screensaver timeout (in minutes)**

<table>
<thead>
<tr>
<th>Section</th>
<th>Preferences</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settings</td>
<td>TimeoutScrnSaver</td>
</tr>
<tr>
<td>Data</td>
<td>[value between 1 and 120]</td>
</tr>
<tr>
<td>Corresponding option in Workspace Preferences</td>
<td><strong>Activate screensaver after</strong> on the Options tab</td>
</tr>
</tbody>
</table>

## DoNotShowAgain

**Disable Workspace Control messages based on the option "Do not show again"**

<table>
<thead>
<tr>
<th>Section</th>
<th>DoNotShowAgain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settings</td>
<td>[Application Donotshow again value]</td>
</tr>
<tr>
<td>Data</td>
<td>Yes or No</td>
</tr>
<tr>
<td>Default</td>
<td>No</td>
</tr>
</tbody>
</table>

## NoNetGuard

**Hide Network Security messages in user's session**

<table>
<thead>
<tr>
<th>Section</th>
<th>Preferences</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settings</td>
<td>NoNetGuard</td>
</tr>
<tr>
<td>Data</td>
<td>Yes or No</td>
</tr>
<tr>
<td>Default</td>
<td>No</td>
</tr>
</tbody>
</table>

## RunHistory

**Saves up to 8 commands used in the Run option**

<table>
<thead>
<tr>
<th>Section</th>
<th>RunHistory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settings</td>
<td>[Run1 up to and including Run8]</td>
</tr>
<tr>
<td>Data</td>
<td>command</td>
</tr>
</tbody>
</table>

## Logging

**Generate a Subscriber/Workspace Extender log**

<table>
<thead>
<tr>
<th>Section</th>
<th>SubCon</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settings</td>
<td>Logging</td>
</tr>
<tr>
<td>Data</td>
<td>Yes or No</td>
</tr>
<tr>
<td>Default</td>
<td>No</td>
</tr>
</tbody>
</table>

**Remarks**

The log file subcon.log is generated in \Personal Settings in the user’s Home folder
### Printer

**Save the user’s default printer**

<table>
<thead>
<tr>
<th>Section</th>
<th>Preferences</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settings</td>
<td>Printer</td>
</tr>
<tr>
<td>Data</td>
<td>[printer share]</td>
</tr>
</tbody>
</table>

### NotifyDefaultPrinterChange

**To suppress the notification message when the default printer is changed.**

<table>
<thead>
<tr>
<th>Section</th>
<th>Preferences</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settings</td>
<td>NotifyDefaultPrinterChange</td>
</tr>
</tbody>
</table>
| Data | No *(Notification message will never be displayed when the default printer changes)*  
or  
OncePerLocation *(Notification message is only displayed if the new default printer differs from the default printer that has already been set for this location)* |

### PreviousPrinter

**Previous default printer**

<table>
<thead>
<tr>
<th>Section</th>
<th>Preferences</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settings</td>
<td>PreviousPrinter</td>
</tr>
<tr>
<td>Data</td>
<td>[Printer share]</td>
</tr>
</tbody>
</table>

### PowerPrintView

**Force advanced view in Printing Preferences**

<table>
<thead>
<tr>
<th>Section</th>
<th>Preferences</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settings</td>
<td>PowerPrintView</td>
</tr>
<tr>
<td>Data</td>
<td>Advanced or [empty]</td>
</tr>
<tr>
<td>Default</td>
<td>[empty]</td>
</tr>
</tbody>
</table>

### OutlookNoOpenDialog

**Types of attachments that Microsoft Outlook should open without asking first**

<table>
<thead>
<tr>
<th>Section</th>
<th>Preferences</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settings</td>
<td>OutlookNoOpenDialog</td>
</tr>
<tr>
<td>Data</td>
<td>List of file types, separated by vertical bars (</td>
</tr>
<tr>
<td>Default</td>
<td></td>
</tr>
</tbody>
</table>
### AppguardDump

**Generate an Application Security log**

<table>
<thead>
<tr>
<th>Section</th>
<th>AppguardDump</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settings</td>
<td>AppguardDump</td>
</tr>
<tr>
<td>Data</td>
<td>Yes or No</td>
</tr>
<tr>
<td>Default</td>
<td>No</td>
</tr>
</tbody>
</table>

**Remarks**

The log file `appguardDump_%Servername%.txt` is generated in \Personal Settings.

### NetguardDump

**Generate a Network Security log**

<table>
<thead>
<tr>
<th>Section</th>
<th>NetguardDump</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settings</td>
<td>NetguardDump</td>
</tr>
<tr>
<td>Data</td>
<td>Yes or No</td>
</tr>
<tr>
<td>Default</td>
<td>No</td>
</tr>
</tbody>
</table>

**Remark**

The log file `netguardDump_%Servername%.txt` is generated in \Personal Settings.

### RefreshInterval

**The interval at which information in the Usage Tracking viewer should be refreshed (in seconds)**

<table>
<thead>
<tr>
<th>Section</th>
<th>PwrTrace</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settings</td>
<td>RefreshInterval</td>
</tr>
<tr>
<td>Data</td>
<td>[0 to 30]</td>
</tr>
<tr>
<td>Default</td>
<td>30</td>
</tr>
</tbody>
</table>

**Corresponding option in Usage Tracking viewer**

Refresh interval for "Current activity" on Settings tab.

### NoRecordLimit

**By default, the Usage Tracking viewer displays a maximum of 1000 records. Use the setting NoRecordLimit to disable this maximum and store an unlimited number of records**

<table>
<thead>
<tr>
<th>Section</th>
<th>PwrTrace</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settings</td>
<td>NoRecordLimit</td>
</tr>
<tr>
<td>Data</td>
<td>Yes or No</td>
</tr>
<tr>
<td>Default</td>
<td>No</td>
</tr>
</tbody>
</table>

**Corresponding option in Usage Tracking viewer**

Do not limit output of "Details" and "Sessions" to 1000 records on Settings tab.
Remarks
With this setting at No, a maximum of 1,000 records is stored. With this setting at Yes, an unlimited number of records is stored.

<table>
<thead>
<tr>
<th>NoScreensaver</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hide screensaver data in Usage Tracking results</strong></td>
</tr>
<tr>
<td><strong>Section</strong></td>
</tr>
<tr>
<td><strong>Settings</strong></td>
</tr>
<tr>
<td><strong>Data</strong></td>
</tr>
<tr>
<td><strong>Default</strong></td>
</tr>
<tr>
<td><strong>Corresponding option in Usage Tracking viewer</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ShowFullOUName</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Show full OU names in the Usage Tracking viewer</strong></td>
</tr>
<tr>
<td><strong>Section</strong></td>
</tr>
<tr>
<td><strong>Settings</strong></td>
</tr>
<tr>
<td><strong>Data</strong></td>
</tr>
<tr>
<td><strong>Default</strong></td>
</tr>
<tr>
<td><strong>Corresponding option in Usage Tracking viewer</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ShowOUinReports</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Show OU names in Usage Tracking reports</strong></td>
</tr>
<tr>
<td><strong>Section</strong></td>
</tr>
<tr>
<td><strong>Settings</strong></td>
</tr>
<tr>
<td><strong>Data</strong></td>
</tr>
<tr>
<td><strong>Default</strong></td>
</tr>
<tr>
<td><strong>Corresponding option in Usage Tracking viewer</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ShowEmptyDates</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Show empty dates in Usage Tracking viewer</strong></td>
</tr>
<tr>
<td><strong>Section</strong></td>
</tr>
<tr>
<td><strong>Settings</strong></td>
</tr>
<tr>
<td><strong>Data</strong></td>
</tr>
<tr>
<td><strong>Default</strong></td>
</tr>
</tbody>
</table>

Remarks
Set this setting at No to filter empty columns out of Usage Tracking graphics.
PowerHelp

In most companies, information about available applications and support is not readily at hand for users. In a Workspace Control session, users can get such information from PowerHelp, which provides users with information about application availability, application distribution, and application responsibility.

On the Access information tab, users can see who the Application Manager of an application is, or on what basis they can access an application. This can be useful if they have specific questions about an application, or if they need access to it. The information on this tab is filled automatically.

The Support information tab provides users with additional information about who to contact for technical support. By default, this is a reference to the IT-department. For applications controlled by application managers, the tab shows the names of the application managers and suggests the user could contact one of these.

If Time Restrictions apply to the selected application, Personalize My Workspace includes the Opening times tab where users can see the days and times when the application can be used.

Where to find PowerHelp

<table>
<thead>
<tr>
<th>What</th>
<th>Where</th>
</tr>
</thead>
<tbody>
<tr>
<td>PowerHelp</td>
<td>In the user’s session: Start menu &gt; PowerHelp</td>
</tr>
</tbody>
</table>

Configure Access Control for Workspace Preferences, PowerHelp, Printing Preferences and Refresh Start menu

If you want to configure access control for the Personalize My Workspace, PowerHelp, Printing Preferences and Refresh Start menu options, you need to disable them and offer them as separate applications.

In the Workspace Control Console at Composition > Desktop > Lockdown > Workspace Composer, the options “Always hide PowerHelp”, “Always hide Personalize My Workspace”, “Always hide Refresh in menu”, and “Always hide Workspace Control Settings submenu in menu” should be enabled to disallow access to these applications. Now create the following applications and configure Access Control as needed:

<table>
<thead>
<tr>
<th>Personalize My Workspace</th>
<th>Program</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>%ProgramFiles%\Ivanti\Workspace Control\pfwsmgr.exe</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PowerHelp</th>
<th>Program</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>%ProgramFiles%\Ivanti\Workspace Control\pwrhelp.exe</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Printing Preferences</th>
<th>Program</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>%ProgramFiles%\Ivanti\Workspace Control\setprint.exe</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Refresh</th>
<th>Program</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>%ProgramFiles%\Ivanti\Workspace Control\pwrgate.exe</td>
</tr>
<tr>
<td>parameters:</td>
<td>-2</td>
</tr>
</tbody>
</table>
7.1.7 Make Control Panel Applets (CPL files) available as applications

When the Windows control panel is disabled in Workspace Control, it is impossible for users to access any setting from the control panel. It is possible, however, to enable certain settings from the control panel to users and make them available as application.

Create a new application with rundll32.exe and the appropriate parameter

The following are valid control panel property page and wizard launch statements that will initiate the various control panel applets, and may also include the ability to specify the active tab on multiple-tabbed property pages. Some systems may not have all the control panel applets or related applications installed; those systems executing the statement produce no result.

To make a Control Panel applet available create a new application in the Workspace Control Console with %systemroot%\windows\rundll32.exe and the appropriate parameter.

Examples:

<table>
<thead>
<tr>
<th>Power Management Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Module</strong></td>
</tr>
<tr>
<td><strong>Command:</strong></td>
</tr>
<tr>
<td><strong>parameters:</strong></td>
</tr>
<tr>
<td><strong>result:</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Control Panel</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Module</strong></td>
</tr>
<tr>
<td><strong>Command:</strong></td>
</tr>
<tr>
<td><strong>parameters:</strong></td>
</tr>
<tr>
<td><strong>result:</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Accessibility Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Module</strong></td>
</tr>
<tr>
<td><strong>Command:</strong></td>
</tr>
<tr>
<td><strong>result:</strong></td>
</tr>
<tr>
<td><strong>Command:</strong></td>
</tr>
<tr>
<td><strong>result:</strong></td>
</tr>
<tr>
<td><strong>Command:</strong></td>
</tr>
<tr>
<td><strong>result:</strong></td>
</tr>
<tr>
<td><strong>Command:</strong></td>
</tr>
<tr>
<td><strong>result:</strong></td>
</tr>
<tr>
<td><strong>Command:</strong></td>
</tr>
<tr>
<td><strong>result:</strong></td>
</tr>
</tbody>
</table>
Add New Hardware Wizard

<table>
<thead>
<tr>
<th>Module</th>
<th>SYSDM.CPL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command:</td>
<td>rundll32.exe shell32.dll,Control_RunDLL sysdm.cpl @1</td>
</tr>
<tr>
<td>result:</td>
<td>Runs the Add New Hardware wizard</td>
</tr>
</tbody>
</table>

Safely Remove Hardware

| Command line:  | %windir%/system32/rundll.exe |
| Working Directory: | %windir%/system32 |
| Parameters:    | shell32.dll,Control_RunDLL hotplug.dll |

Add New Printer Wizard

<table>
<thead>
<tr>
<th>Module</th>
<th>SHELL32.DLL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command:</td>
<td>rundll32.exe shell32.dll,SHHelpShortcuts_RunDLL AddPrinter</td>
</tr>
<tr>
<td>result:</td>
<td>Runs the Add New Printer wizard</td>
</tr>
</tbody>
</table>

Note

With Windows NT, it is possible to bring up a predefined Windows Dialog box for connecting to a network printer - the ConnectToPrinterDlg API. However, this dialog is not accessible by Visual Basic programs running under Windows 95. Therefore, you must use a Command line equivalent statement to invoke the “Add Printer Wizard” under Windows 95 as detailed above.

Add/Remove Programs Property Page

<table>
<thead>
<tr>
<th>Module</th>
<th>APPWIZ.CPL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command:</td>
<td>rundll32.exe shell32.dll,Control_RunDLL appwiz.cpl,,1</td>
</tr>
<tr>
<td>result:</td>
<td>Displays the Install/Uninstall tab selected</td>
</tr>
<tr>
<td>Command:</td>
<td>rundll32.exe shell32.dll,Control_RunDLL appwiz.cpl,,2</td>
</tr>
<tr>
<td>result:</td>
<td>Displays the Windows Setup tab selected</td>
</tr>
<tr>
<td>Command:</td>
<td>rundll32.exe shell32.dll,Control_RunDLL appwiz.cpl,,3</td>
</tr>
<tr>
<td>result:</td>
<td>Displays the Startup Disk tab selected</td>
</tr>
<tr>
<td>Module</td>
<td>Command</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>Briefcase</td>
<td>rundll32.exe syncui.dll,Briefcase_Create</td>
</tr>
<tr>
<td>Copy Disk Dialog</td>
<td>rundll32.exe diskcopy.dll,DiskCopyRunDll</td>
</tr>
<tr>
<td>Create New Shortcut</td>
<td>rundll32.exe apwiz.cpl,NewLinkHere %1</td>
</tr>
<tr>
<td>Date &amp; Time Properties</td>
<td>rundll32.exe shell32.dll,Control_RunDLL timedate.cpl,,0</td>
</tr>
<tr>
<td></td>
<td>rundll32.exe shell32.dll,Control_RunDLL timedate.cpl,,1</td>
</tr>
<tr>
<td>Dial Up Networking (DUN)</td>
<td>rundll32.exe rnaui.dll,RnaDial {name of connection to establish}</td>
</tr>
<tr>
<td></td>
<td>rundll32.exe rnaui.dll,RnaWizard</td>
</tr>
</tbody>
</table>
### Display Options (Standard Windows Display Property Page)

<table>
<thead>
<tr>
<th>Module</th>
<th>Command</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>DESK.CPL</td>
<td>rundll32.exe shell32.dll,Control_RunDLL desk.cpl,,0</td>
<td>Displays the Background tab selected</td>
</tr>
<tr>
<td></td>
<td>rudll32.exe shell32.dll,Control_RunDLL desk.cpl,,1</td>
<td>Displays the Screen Saver tab selected</td>
</tr>
<tr>
<td></td>
<td>rudll32.exe shell32.dll,Control_RunDLL desk.cpl,,2</td>
<td>Displays the Appearance tab selected</td>
</tr>
<tr>
<td></td>
<td>rudll32.exe shell32.dll,Control_RunDLL desk.cpl,,3</td>
<td>Displays the Settings tab selected</td>
</tr>
</tbody>
</table>

**Note**

Display options

Your video adapter may install other property pages into DESK.CPL dynamically when selected with its own icon (i.e. an ATI or Matrox control panel icon). Additionally, it also may invoke its own control panel applet mimicking the Windows display options.

### FindFast

<table>
<thead>
<tr>
<th>Module</th>
<th>Command</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>FINDFAST.CPL</td>
<td>rundll32.exe shell32.dll,Control_RunDLL findfast.cpl</td>
<td>Displays the Office FindFast control panel applet (if installed)</td>
</tr>
</tbody>
</table>

### Fonts

<table>
<thead>
<tr>
<th>Module</th>
<th>Command</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>SHELL32.DLL</td>
<td>rundll32.exe shell32.dll,SHHelpShortcuts_RunDLL FontsFolder</td>
<td>Displays the Fonts Folder in Explorer view</td>
</tr>
<tr>
<td></td>
<td>rundll32.exe shell32.dll,Control_RunDLL main.cpl 03</td>
<td>Also displays the Fonts Folder in Explorer view</td>
</tr>
</tbody>
</table>

### Format Drive Dialog (floppy disk only)

<table>
<thead>
<tr>
<th>Module</th>
<th>Command</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>SHELL32.DLL</td>
<td>rundll32.exe shell32.dll,SHFormatDrive</td>
<td>Displays the floppy disk Format Drive dialog. Causes the Drive A to be accessed on showing.</td>
</tr>
</tbody>
</table>
### Game Controllers

<table>
<thead>
<tr>
<th>Module</th>
<th>JOY.CPL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command:</td>
<td><code>rundll32.exe shell32.dll,Control_RunDLL joy.cpl,,0</code></td>
</tr>
<tr>
<td>result:</td>
<td>Displays the Game Controllers General property page</td>
</tr>
<tr>
<td>Command:</td>
<td><code>rundll32.exe shell32.dll,Control_RunDLL joy.cpl,,1</code></td>
</tr>
<tr>
<td>result:</td>
<td>Displays the Game Controllers Advanced property page</td>
</tr>
</tbody>
</table>

### HTML

<table>
<thead>
<tr>
<th>Module</th>
<th>MSHTML.DLL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command:</td>
<td><code>rundll32.exe mshtml.dll,PrintHTML (HTML doc to print)</code></td>
</tr>
<tr>
<td>result:</td>
<td>Sends the passed file to the printer</td>
</tr>
</tbody>
</table>

### Internet Explorer 4 Control Panel

<table>
<thead>
<tr>
<th>Module</th>
<th>INETCPL.CPL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command:</td>
<td><code>rundll32.exe shell32.dll,Control_RunDLL inetcpl.cpl</code></td>
</tr>
<tr>
<td>result:</td>
<td>Displays Internet Properties, General Tab</td>
</tr>
<tr>
<td>Command:</td>
<td><code>rundll32.exe shell32.dll,Control_RunDLL inetcpl.cpl,,0</code></td>
</tr>
<tr>
<td>result:</td>
<td>Displays Internet Properties, General Tab (same as above)</td>
</tr>
<tr>
<td>Command:</td>
<td><code>rundll32.exe shell32.dll,Control_RunDLL inetcpl.cpl,,1</code></td>
</tr>
<tr>
<td>result:</td>
<td>Displays Internet Properties, Security Tab</td>
</tr>
<tr>
<td>Command:</td>
<td><code>rundll32.exe shell32.dll,Control_RunDLL inetcpl.cpl,,2</code></td>
</tr>
<tr>
<td>result:</td>
<td>Displays Internet Properties, Content Tab</td>
</tr>
<tr>
<td>Command:</td>
<td><code>rundll32.exe shell32.dll,Control_RunDLL inetcpl.cpl,,3</code></td>
</tr>
<tr>
<td>result:</td>
<td>Displays the Internet Control Panel, Connection Tab</td>
</tr>
<tr>
<td>Command:</td>
<td><code>rundll32.exe shell32.dll,Control_RunDLL inetcpl.cpl,,4</code></td>
</tr>
<tr>
<td>result:</td>
<td>Displays the Internet Control Panel, Programs Tab</td>
</tr>
<tr>
<td>Command:</td>
<td><code>rundll32.exe shell32.dll,Control_RunDLL inetcpl.cpl,,5</code></td>
</tr>
<tr>
<td>result:</td>
<td>Displays the Internet Control Panel, Advanced Tab</td>
</tr>
</tbody>
</table>

### Joystick Properties (also see Games)

<table>
<thead>
<tr>
<th>Module</th>
<th>JOY.CPL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command:</td>
<td><code>rundll32.exe shell32.dll,Control_RunDLL joy.cpl</code></td>
</tr>
<tr>
<td>result:</td>
<td>Displays the Joystick property page</td>
</tr>
<tr>
<td>Mail and Fax Options</td>
<td>Module</td>
</tr>
<tr>
<td>---------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td></td>
<td>MLCFG32.CPL</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mail Postoffice Options</th>
<th>Module</th>
<th>Command</th>
<th>result</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>WGP0CPL.CPL</td>
<td><code>rundll32.exe shell32.dll,Control_RunDLL wgpocpl.cpl</code></td>
<td>Displays the Microsoft Postoffice Workgroup Admin property page</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Main Group Options/Properties</th>
<th>Module</th>
<th>Command</th>
<th>result</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>MAIN.CPL</td>
<td><code>rundll32.exe shell32.dll,Control_RunDLL main.cpl @0</code></td>
<td>Displays Mouse Properties</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>rundll32.exe shell32.dll,Control_RunDLL main.cpl @1</code></td>
<td>Displays Keyboard Properties, Speed tab</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>rundll32.exe shell32.dll,Control_RunDLL main.cpl @1,,1</code></td>
<td>Displays Keyboard Properties, Language tab</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>rundll32.exe shell32.dll,Control_RunDLL main.cpl @1,,2</code></td>
<td>Displays Keyboard Properties, General tab</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>rundll32.exe shell32.dll,Control_RunDLL main.cpl @2</code></td>
<td>Displays the Printers Folder (including Add Printer)</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>rundll32.exe shell32.dll,Control_RunDLL main.cpl @3</code></td>
<td>Displays the Fonts Folder in Explorer view</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>rundll32.exe shell32.dll,Control_RunDLL main.cpl @4</code></td>
<td>Displays Power Management Properties</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Modem</th>
<th>Module</th>
<th>Command</th>
<th>result</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>MODEM.CPL</td>
<td><code>rundll32.exe shell32.dll,Control_RunDLL modem.cpl,,add</code></td>
<td>Runs the Add New Modem wizard</td>
</tr>
</tbody>
</table>
### Multimedia & Sound Properties

<table>
<thead>
<tr>
<th>Module</th>
<th>Command</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>MMSYS.CPL</td>
<td>rundll32.exe shell32.dll,Control_RunDLL mmsys.cpl,,0</td>
<td>Displays the Multimedia/Audio property page</td>
</tr>
<tr>
<td></td>
<td>rundll32.exe shell32.dll,Control_RunDLL mmsys.cpl,,1</td>
<td>Displays the Multimedia/Video property page</td>
</tr>
<tr>
<td></td>
<td>rundll32.exe shell32.dll,Control_RunDLL mmsys.cpl,,2</td>
<td>Displays the Multimedia/MIDI property page</td>
</tr>
<tr>
<td></td>
<td>rundll32.exe shell32.dll,Control_RunDLL mmsys.cpl,,3</td>
<td>Displays the Multimedia/CD Music property page</td>
</tr>
<tr>
<td></td>
<td>rundll32.exe shell32.dll,Control_RunDLL mmsys.cpl,,4</td>
<td>Displays the Multimedia/Advanced property page</td>
</tr>
<tr>
<td></td>
<td>rundll32.exe shell32.dll,Control_RunDLL mmsys.cpl @1</td>
<td>Displays the Sound Properties page</td>
</tr>
</tbody>
</table>

### Network Properties

<table>
<thead>
<tr>
<th>Module</th>
<th>Command</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>NETCPL.CPL</td>
<td>rundll32.exe shell32.dll,Control_RunDLL netcpl.cpl</td>
<td>Displays the Networks properties, Configuration tab</td>
</tr>
</tbody>
</table>

### ODBC32 Data Source Administrator

<table>
<thead>
<tr>
<th>Module</th>
<th>Command</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>ODBC32.CPL</td>
<td>rundll32.exe shell32.dll,Control_RunDLL odbc32.cpl</td>
<td>Displays the ODBC32 Data Source Administrator properties dialog</td>
</tr>
</tbody>
</table>

### Open With

<table>
<thead>
<tr>
<th>Module</th>
<th>Command</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>SHELL32.DLL</td>
<td>rundll32.exe shell32.dll,OpenAs_RunDLL {drive:\path\filename}</td>
<td>Displays the application/file &quot;Open With&quot; dialog</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Passing the full file drive, path and name as a parameter will cause the dialog to display the line &quot;Click the program you want to use to open the file <code>{filename}</code>&quot;.</td>
</tr>
</tbody>
</table>
### Passwords Properties

<table>
<thead>
<tr>
<th><strong>Module</strong></th>
<th>PASSWORD.CPL</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Command</strong></td>
<td><code>rundll32.exe shell32.dll,Control_RunDLL password.cpl</code></td>
</tr>
<tr>
<td><strong>Result</strong></td>
<td>Displays the Passwords properties, Change Passwords tab</td>
</tr>
</tbody>
</table>

### Power Management Properties

<table>
<thead>
<tr>
<th><strong>Module</strong></th>
<th>POWERCFG.CPL</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Command</strong></td>
<td><code>rundll32.exe shell32.dll,Control_RunDLL powercfg.cpl</code></td>
</tr>
<tr>
<td><strong>Result</strong></td>
<td>Displays the Power Management properties, Power Schemes tab</td>
</tr>
</tbody>
</table>

### Printer

<table>
<thead>
<tr>
<th><strong>Module</strong></th>
<th>SHELL32.DLL</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Command</strong></td>
<td><code>rundll32.exe shell32.dll,SHHelpShortcuts_RunDLL PrintersFolder</code></td>
</tr>
<tr>
<td><strong>Result</strong></td>
<td>Displays the Printers Folder (including Add Printer)</td>
</tr>
</tbody>
</table>

| **Command**      | `rundll32.exe shell32.dll,Control_RunDLL main.cpl @2` |
| **Result**       | Also displays the Printers Folder (including Add Printer) |

### Regional Settings

<table>
<thead>
<tr>
<th><strong>Module</strong></th>
<th>INTL.CPL</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Command</strong></td>
<td><code>rundll32.exe shell32.dll,Control_RunDLL int1.cpl,,0</code></td>
</tr>
<tr>
<td><strong>Result</strong></td>
<td>Displays the Regional Settings property page</td>
</tr>
</tbody>
</table>

| **Command**      | `rundll32.exe shell32.dll,Control_RunDLL int1.cpl,,1` |
| **Result**       | Displays the Numbers property page |

| **Command**      | `rundll32.exe shell32.dll,Control_RunDLL int1.cpl,,2` |
| **Result**       | Displays the Currency property page |

| **Command**      | `rundll32.exe shell32.dll,Control_RunDLL int1.cpl,,3` |
| **Result**       | Displays the Time property page |

| **Command**      | `rundll32.exe shell32.dll,Control_RunDLL int1.cpl,,4` |
| **Result**       | Displays the Date property page |
### Screensaver Installation

<table>
<thead>
<tr>
<th>Module</th>
<th>APPWIZ.CPL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command:</td>
<td><code>rundll32.exe desk.cpl,InstallScreenSaver C:\win\system\Flying Windows.scr</code></td>
</tr>
<tr>
<td>result:</td>
<td>Installs the new screensaver and runs the display/screensaver preview property page</td>
</tr>
</tbody>
</table>

**Note**
Specify a valid path to the screen saver file to install. If you are installing a new screen saver, first copy the screen saver file into the `\windows\system` folder, then execute the above command. This will install the specified saver as the current screen saver. It will not copy the file into the `windows\system` folder. Replace the string above with the name of your actual SCR file.

### System Properties

<table>
<thead>
<tr>
<th>Module</th>
<th>SYSDM.CPL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command:</td>
<td><code>rundll32.exe shell32.dll,Control_RunDLL sysdm.cpl,,0</code></td>
</tr>
<tr>
<td>result:</td>
<td>Displays the General property page</td>
</tr>
<tr>
<td>Command:</td>
<td><code>rundll32.exe shell32.dll,Control_RunDLL sysdm.cpl,,1</code></td>
</tr>
<tr>
<td>result:</td>
<td>Displays the Device Manager property page</td>
</tr>
<tr>
<td>Command:</td>
<td><code>rundll32.exe shell32.dll,Control_RunDLL sysdm.cpl,,2</code></td>
</tr>
<tr>
<td>result:</td>
<td>Displays the Hardware Profiles property page</td>
</tr>
<tr>
<td>Command:</td>
<td><code>rundll32.exe shell32.dll,Control_RunDLL sysdm.cpl,,3</code></td>
</tr>
<tr>
<td>result:</td>
<td>Displays the Performance property page</td>
</tr>
</tbody>
</table>

### Shutdown

<table>
<thead>
<tr>
<th>Module</th>
<th>USER.EXE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command:</td>
<td><code>rundll32.exe user.exe,restartwindows</code></td>
</tr>
<tr>
<td>result:</td>
<td>Forces Windows to perform a proper shutdown, and restart the computer</td>
</tr>
<tr>
<td>Command:</td>
<td><code>rundll32.exe user.exe,exitwindows</code></td>
</tr>
<tr>
<td>result:</td>
<td>Forces Windows to shutdown, and wait either to be turned off, or reset</td>
</tr>
</tbody>
</table>

### Telephony Properties

<table>
<thead>
<tr>
<th>Module</th>
<th>TELEPHON.CPL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command:</td>
<td><code>rundll32.exe shell32.dll,Control_RunDLL telephon.cpl users</code></td>
</tr>
<tr>
<td>result:</td>
<td>Displays the Dialing Properties dialog.</td>
</tr>
</tbody>
</table>
Chapter 7: Composition

Themes
Module: THEMES.CPL
Command: rundll32.exe shell32.dll,Control_RunDLL themes.cpl
result: Displays the Themes control panel app (if installed)

Themes
Module: TweakUI
Command: rundll32.exe shell32.dll,Control_RunDLL tweakui.cpl
result: Displays the TweakUI control panel applet (if installed)

Note
Some dialogs may not work in the Workspace Control shell because they need the presence of explorer.exe.

Disable various tabs on Control Panel applets

It is possible to disable tabs on Control Panel applets to limit the view on these applets. An easy way to do this is to add a Registry Key to the application.

Example:

If you want to make the desk.cpl applet available for your users, but only want the resolution change screen to be available, create a new application in the Workspace Control Console.

Display Options
Module: DESK.CPL
Command: %systemroot%\windows\rundll32.exe shell32.dll,Control_RunDLL desk.cpl,,0
Parameter: shell32.dll,Control_RunDLL desk.cpl

Now add the following Registry keys to this application by editing the (managed) application and selecting Configuration > Actions > User Registry Setting:

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System]
@=""
"NoDispScrSavPage"=dword:00000001
"NoDispBackgroundPage"=dword:00000001
"NoVisualStyleChoice"=dword:00000001
"NoDispAppearancePage"=dword:00000001
"NoColorChoice"=dword:00000001

This will only make the resolution change screen of the DESK.CPL applet visible.

A list of policy settings which can be used to disable various components can be found at http://www.microsoft.com/downloads.
7.1.8  File Types

At Composition > Applications > File Types, you can view all configured File Types. If necessary, you can change the priority of File Types.

Configuration
- You can only create File Types (on page 167) when changing the settings of an application in Applications.
- If you select Show associated applications and a scope applies to your administrative role ("Administrative Roles" on page 317), not all applications may be shown or you may not be allowed to edit all applications.
- When changing the priority of associated applications, the application at the top of the priority list will be used to handle the specified file type. If this application is not accessible to the user, the second application will be used, etc.

7.1.9  E-mail Settings

At Composition > Applications > E-mail Settings, you can view all configured E-mail Settings. E-mail Settings can be configured here or when you create or edit an application. See E-mail Settings (on page 177) for more information.

7.1.10  Data Sources

With Data Sources, you can configure data connections (DSNs) to databases using open database connectivity (ODBC). This allows you to associate DSNs with applications that need access to a certain database.

For example, if a CRM application needs access to a CRM database located on an SQL database server and you would configure this in Microsoft Windows, you would have to configure a DSN link to the database server for each computer on which the CRM application has been installed. If you create a Data Source in Workspace Control, you only need to configure the DSN once to link the CRM application to the CRM database. Each time the application will be used, the database connection will be created automatically.

Configuration

When you have configured the Data Source, you need to associate the Data Source with an application ("Data Sources" on page 179)

- If you select Show associated applications and a scope applies to your administrative role, not all applications may be shown or you may not be allowed to edit all applications.
- Normally, a Data Source is created in a user session when the application to which it is linked is started. This may cause a delay when starting the application. It can therefore be useful to select Create Data Source during logon.

⚠️ Tip

By clicking Workspace Designer, it is possible to use the Workspace Designer to create Data Sources based on your current environment. This enables you to easily transfer from a non-managed environment to a Workspace managed by Workspace Control. For more information, see the Workspace Control Help.
7.2  Actions

Use Actions By Event or Actions By Type to configure global actions. Global actions are executed at the start of the user session (logon), when the user session is refreshed or reconnected, when network connectivity changes, and when the user session is logged off.

The user’s Event Log will be appended with the results of the applied settings. You can view the contents of this Event Log in the Workspace Analysis window of this user.

It is possible to Move and Duplicate settings related to Actions. This makes it possible to:

- duplicate application settings and move them from one application to another
- duplicate application settings and move them to a global level
- duplicate global settings and move them to an application
- move global actions to an application
- move application actions to global

When moving actions from an application to global, the timing changes as displayed in the table below:

<table>
<thead>
<tr>
<th>Timing of application action</th>
<th>Timing of global action</th>
</tr>
</thead>
<tbody>
<tr>
<td>At application start</td>
<td>At logon before other actions</td>
</tr>
<tr>
<td>At application end</td>
<td>At logoff</td>
</tr>
</tbody>
</table>

When moving actions from global to an application, the timing changes as displayed in the table below:

<table>
<thead>
<tr>
<th>Timing of global action</th>
<th>Timing of application action</th>
</tr>
</thead>
<tbody>
<tr>
<td>At logon before other actions</td>
<td>At application start</td>
</tr>
<tr>
<td>At logon after other actions</td>
<td>At application start</td>
</tr>
<tr>
<td>At refresh</td>
<td>At application start</td>
</tr>
<tr>
<td>At reconnect session</td>
<td>At application start</td>
</tr>
<tr>
<td>At logoff</td>
<td>At application end</td>
</tr>
</tbody>
</table>

Please note that executing an action on session reconnect requires that Workspace Control refreshes the session when it reconnects. Therefore, when configuring actions to be executed at session reconnect, make sure the option Do not refresh Workspace when reconnecting to a session is not enabled (at Composition > Lockdown and Behavior, in the Workspace Composer section).
7.2.1 Automation Tasks

Automation Tasks allow you to run specific Automation Tasks in the user workspace, such as the installation of software or the creation of user profiles. Workspace Control will run these Tasks during the logon process of a user.

You can only configure Automation Tasks if you have enabled Automation Integration at Setup > Integration > Ivanti Products > Automation and are connected to a Automation Datastore.

Where to find Automation Tasks

<table>
<thead>
<tr>
<th>What</th>
<th>Where</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global level</td>
<td>Composition &gt; Actions By Type &gt; Automation Tasks</td>
</tr>
<tr>
<td></td>
<td>Composition &gt; Actions By Event &gt; At Logon, select New &gt; Automation Task</td>
</tr>
<tr>
<td>Application level</td>
<td>Open the application at Composition &gt; Applications, go to Configuration &gt; Actions</td>
</tr>
</tbody>
</table>

Configure Automation Tasks

- To configure an Automation Task that should run when a session starts, go to Composition > Actions By Type > Automation Tasks.
- To configure an Automation Task that should run when an application starts, open the application at Composition > Applications and go to Configuration > Actions.
- You can override the global settings of this feature for specific Workspace Containers.
- When configuring an Automation Task, optionally enter a note in the Administrative note field. This is useful to differentiate the Automation Tasks that you configured.
- Click in the Task field to load the available Automation Projects and Modules from the Automation environment that you specified at Setup > Integration > Ivanti Products > Automation. This allows you to select the Automation Projects or Modules that should be part of the Automation Task.
- Skip if application executable was found (only available on application level) when selected, a check will be done whether the application executable is present on the client computer before the task is executed. When the option is not selected, the task is executed as configured when the application is started.
- Workspace Control can detect whether the Automation Task has run before for that user, on that computer, or for the combination of that user on that computer. In the Run once field, you can configure whether the Task should be executed or skipped when a user starts the application:
  - No: the Automation Task will be executed, irrespective of whether it has been executed before.
  - Per user: the Automation Task will be executed once for each user who logs on to the Workspace Control environment.
  - Per computer: the Automation Task will be executed once for each computer in to the Workspace Control environment.
  - Per user per computer: the Automation Task will be executed once for each user who logs on to the Workspace Control environment on a specific computer.
- If you need to repeat an existing Automation Task that has been configured to Run once, select Clear history. This resets the count, so that the existing Automation Task is executed again throughout the environment, according to the rules selected for Run once.
- When you configure a custom message, you can communicate additional information about the Automation Task to the user.
• **Wait for task to finish before continuing** forces Workspace Control to finish the task before continuing with the next Task. Clear this check box to force Workspace Control to continue with the next Task if the Task does not complete. It can be useful to select this option when you have configured a custom message: this allows the user some additional time to read this message. However, if the Automation Task has not started before the specified timeout expires, the Task will be canceled.

• **Run before other actions** makes it possible to specify that the Automation Task should be executed before other configuration Actions (except Environment Variable Actions). At application level, an Automation Task that is configured to **Run before other actions** will appear on top of the list of Actions on the **Actions** tab; The option Run before other actions will automatically be selected or cleared again when moving an Automation Task in the list by using the arrows.

• **Required connection state** specifies the required connection state that allows the Task to be executed. For example, this allows you to configure a Task that only runs if the laptop has an online connection state.

• Click the **Parameters** tab to view which parameters will be used in the Automation Task. This tab is only available if the selected Automation Project or Module contains parameters.

• Click the **Access Control** tab to configure the Access Control criteria of the Automation Task.

• Click the **Workspace Control** tab to configure to which Workspace Container(s) the Automation Task applies.
7.2.2 Environment Variables

Environment Variables are variables set in the memory of the user's workstation or session.

These variables are often used by applications, for example to determine who a user is and what his default path structures are; or what the system date and time is. The option Environment Variables enables you to set or modify environment variables based on various types of access control.

Windows provides several useful variables, such as user name and computer name. You can use these variables in your values by using the percentage character (for example %username% and %computername%).

You can modify the order of execution by setting an order number in the order column. You can change the order by selecting the option Change order of execution.

Where to find Environment Variables

<table>
<thead>
<tr>
<th>What</th>
<th>Where</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global level</td>
<td>Composition &gt; Actions By Type &gt; Environment Variables</td>
</tr>
<tr>
<td></td>
<td>Composition &gt; Actions By Event &gt; At Logon, select New &gt; Environment Variable</td>
</tr>
<tr>
<td>Application level</td>
<td>Open the application at Composition &gt; Applications, go to Configuration &gt; Actions</td>
</tr>
</tbody>
</table>

Configure Environment Variables

- To configure an Environment Variable that should be set when a session starts, go to Composition > Actions By Type > Environment Variables.
- To configure an Environment Variable that should be set when an application starts, open the application at Applications and go to Configuration > Actions.
- At Composition > Actions By Type > Environment Variables, the option Reset Environment Variables on refresh of workspace allows you to reset Environment Variables on a refresh of the user workspace. This ensures that connection state-dependent Environment Variables are resolved correctly.
- You can override the global settings of this feature for specific Workspace Containers.
- When configuring an Environment Variable, optionally enter a note in the Administrative note field. This is useful to differentiate the variables that you configured.
- In the Value field, you can use Microsoft Windows environment variables and the functions $adinfo(<property>), $usershellfolder(<folder>), $substring, $endstring, $replacestring, $lowercase, $uppercase and $autocount.
- When a session starts, the applicable Environment Variables are set in the order in which they appear in this list. If necessary, change the order to ensure the correct processing.
- The Required connection state field specifies the required connection state that allows the setting to be applied. For example, this allows you to configure a setting that will only be applied if a computer has an online connection state.
- Click the Access Control tab to configure the Access Control criteria of the environment variable.
- Click the Workspace Control tab to configure to which Workspace Container(s) the environment variable applies.
Example: %deskpic%

You can use the %deskpic% variable to display a custom desktop picture for a specific (group of) user(s). The variable contains the file name of the picture to be displayed on the desktop, which must exist as desktop image resources. When Workspace Control is started, this variable applies to each user that is member of the Non-management group, and places the Non_mgmnt_back.bmp picture on his desktop.

Example: %PwrGateKeepAlive%

In Windows, when an application such as Outlook needs to open an attachment such as a Word file, the application places the attachment in a temporary location and then starts the associated process (in this case winword.exe). The application then checks whether the process is still running. When it is no longer running, the application removes the attachment file from the temporary location again.

This does not work if an attachment is opened from an application that is managed by Workspace Control because then pwrgate.exe is always started instead of winword.exe, etc. Pwrgate.exe checks the File Types, passes the relevant application (Word) and the file to be opened to the Workspace Composer, and stops. The Workspace Composer then opens Word, with the path to the attachment in the command line.

As soon as pwrgate.exe stops - which is before Word has started - the mail client removes the attachment from the temporary location. As a result, the attachment can no longer be found when Word is actually started through Workspace Control.

Variable

To prevent this, set an environment variable %pwrgatekeepalive% with the value "yes" when the application that needs to open attachments (Word, in this example) is started. This will ensure that the pwrgate.exe process does not stop until Word stops - and so the Word file will not be removed from its temporary location too soon.
7.2.3 **Execute Command**

At the **Execute Command** section you can start external non-Workspace Control tasks or applications when a user logs on or off.

This can be anything from an enterprise-wide questionnaire application to a simple cleanup task.

**Where to find Execute Command**

<table>
<thead>
<tr>
<th>What</th>
<th>Where</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global level</td>
<td>Composition &gt; Actions By Type &gt; Execute Command</td>
</tr>
<tr>
<td></td>
<td>Composition &gt; Actions By Event &gt; At Logon, select New &gt; Execute Command</td>
</tr>
<tr>
<td></td>
<td>Composition &gt; Actions By Event &gt; At Session Refresh, select New &gt; Execute Command</td>
</tr>
<tr>
<td></td>
<td>Composition &gt; Actions By Event &gt; At Session Reconnect, select New &gt; Execute Command</td>
</tr>
<tr>
<td></td>
<td>Composition &gt; Actions By Event &gt; At Logoff, select New &gt; Execute Command</td>
</tr>
<tr>
<td>Application level</td>
<td>Open the application at Composition &gt; Applications, go to Configuration &gt; Actions</td>
</tr>
</tbody>
</table>
Configure commands

- When configuring a command, the option Run Hidden runs the command hidden from the user.
- Workspace Control can detect whether the command has run before for that user, on that computer, or for the combination of that user on that computer. In the Run once field, you can configure whether the command should be executed or skipped depending on this information:
  - Select Run once to execute the command only if it has not yet been executed for the user starting the session.
  - Clear Run once to execute the command regardless of whether it has been executed before.
- If you need to repeat an existing command that has been configured to Run once, select Clear history. If you select Clear history, the history of the command will be cleared and the command will be repeated once.
- If a command has been configured to run at logoff, the option Wait for task to finish before continuing will always be selected. Specify a timeout in seconds to ensure Workspace Control does not wait if the task is unable to finish.
- Required connection state specifies the required connection state that allows the command to be executed. For example, this allows you to configure a command that only synchronizes user files between a laptop and the network if the laptop has an online connection state. See Connection States (on page 145).
- For App-V applications, the option Run outside App-V virtual environment is available. This allows the command that was configured for the application to run outside the App-V bubble of that application.
- On the Script tab you can directly enter script contents. Enter (only) %script% in the command line on the Properties tab, to refer to the script tab content. Note that the correct file extension of the script is entered on the Script tab.
  - It is not possible to execute a Visual Basic- or PowerShell-script in combination with only the %script% variable in the command line. In that case, use the following in the command line:
    - To execute Visual Basic-scripts use cscript.exe %script%.
    - To execute PowerShell-scripts use PowerShell.exe %script%.
- Click the Access Control tab to configure the Access Control criteria of the command.
- Click the Workspace Control tab to configure to which Workspace Container(s) the command applies.

Notes

- The option Execute Command can be Run using Dynamic Privileges. This means that the task will run "elevated", using Administrative Privileges, while maintaining default privileges for the user. The option Run using Dynamic Privileges is part of the functionality of the Security module and therefore is only available if this module is included in your license. For full details, please refer to the Workspace Control Module Capability Matrix available on the Ivanti website.
- When executing PowerShell-scripts with Dynamic Privileges use the following commandline to prevent the profile script from loading: PowerShell.exe -NoProfile %script%
- When configuring a Command as a script, the value entered as Administrative note (on the Properties tab of the Command) will be displayed in the User Event Log (at Diagnostics > User Sessions or at Diagnostics > Workspace Analysis) and in trace files. If no value was entered, %script% will be displayed.
7.2.4 Files and Folders

Drive and Port Mappings

It is possible to create drive and port mappings based on all previously mentioned types of access control.

There may be hundreds of network locations and ports (lpt/com) available: rather than browse a list every time you need a specific one, you can “map” it. This sets your machine to connect to it when you log in and treat it like one of its own disk drives or ports.

Where to find Drive and Port Mappings

<table>
<thead>
<tr>
<th>What</th>
<th>Where</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global level</td>
<td>Composition &gt; Actions By Type &gt; Files and Folders &gt; Drive and Port Mappings</td>
</tr>
<tr>
<td></td>
<td>Composition &gt; Actions By Event &gt; At Logon, select New &gt; Drive and Port Mapping</td>
</tr>
<tr>
<td>Application level</td>
<td>Open the application at Composition &gt; Applications, go to Configuration &gt; Actions</td>
</tr>
</tbody>
</table>
Configure Drive and Port Mappings

Global settings

- **Disconnect all network drives before logging on/off** cleans the user’s profile from user-connected and disabled drives.
- **Skip unmanaged drives** can only be selected when the option **Disconnect all network drives before logging on/off** is enabled. Only network drives that are managed by Workspace Control will be disconnected, all other drives will not be touched. With an unmanaged drive, a drive is meant that has no managed equivalent in Workspace Control. If both a managed and an unmanaged version of a drive exist, the unmanaged version will be replaced by a managed version after logging off/on.
- **Refresh Drive and Port Mappings when network connectivity changes** allows you to refresh Drive Mappings automatically when the network connectivity of a session changes. This ensures that connection state-dependent Drive Mappings become available or disappear correctly.
- Drive and port mappings will not be refreshed if the Lockdown and Behavior option **Do not refresh Workspace when network connectivity changes** is selected (at **Composition > Desktop > Lockdown and Behavior**).
- **Also connect all network drives using VDX plugin**. Drive mappings that are configured for the remote desktop can be set as local drive mappings too. This setting enables the user to access the same drives from local desktop and from virtual desktop using the VDX plugin.
- You can override the global settings of this feature for specific Workspace Containers.

Mapping settings

- Optionally enter a note in the **Administrative note** field. This is useful to differentiate the mappings that you configured.
- **Action**:
  - **Map drive**: Default; perform drive mapping
  - **Disconnect drive mapping**: Disconnect an existing (non-Workspace Control) mapping.
  - **Do not perform mapping operation**: Do not perform the actual mapping, but do set other options, such as setting a friendly name. This setting is also useful when configuring hide drive behavior for existing local drives.
  - **Set RES HyperDrive**: No longer available for new mappings.
- **The Device** field specifies which drive letter should be used for the mapping.
  - If you select **Do not use a drive letter**, Workspace Control will not expose the drive letter when a mapped network resource should be available for the user.
  - If you select **Find first free drive letter**, Workspace Control will find the first available drive letter when mapping a network drive, starting down from "Z:"
- The **Hide drive** field specifies the hide drives behavior of the mapping. Hidden drives are not available to end users and are also blocked in Windows Explorer-type dialogs.
  - If you select **Default**, the default hide drives behavior for Drive and Port Mappings will be applied.
  - If you select **Always hide, but allow access**, the drive will be hidden without blocking it. This can be useful for removable media that cause a delay in application startup or File Open/Save dialogs.
- **Fast connect** allows users to start their sessions faster. Do not select this option if the drive contains applications: until the user accesses the drive, the drive will not be available, which means that any applications on the drive will not be available either.
- When selecting the option **Fast connect**, the option **Wait for task to finish before continuing** becomes unavailable, because the actual mapping will first be performed when the user connects to the drive.
- When clearing the option **Wait for task to finish before continuing** the option **Fast connect** becomes unavailable, because the task will be performed asynchronously.
- The **Required connection state** field specifies the required connection state that allows the setting to be applied. For example, this allows you to configure a setting that will only be applied if a computer has an online connection state.
Click the Access Control tab to configure the Access Control criteria of the mapping.
Click the Workspace Control tab to configure to which Workspace Container(s) the mapping applies.

Notes
- You can use environment variables (for example, %username%).
- For additional security, Drive and Port mappings can also direct the drive mapping to a resource, without the user knowing the username or password.
- Drive and Port Mappings also allow mappings to WebDAV web folders, which start with "http://" or "https://" instead of "\server\share".
- Use the Workspace Analysis window to display an overview of all mappings and their hide drive settings for a specific user.
- When different friendly names are configured for drive letters that are mapped to the same share, the last configured friendly name will be used for all these drive mappings.

Default Hide drives behavior
Hidden drives are also blocked in Windows Explorer-type dialogs.

- Disabled: No default hide drives behavior is configured.
- Never hide any drives: Overrides any hide drive settings in Drive and Port Mappings.
- Do not hide any drives (unless otherwise specified): Default behavior is to show all drives. This setting is overruled by any hidden drives configured with Drive and Port Mappings.
- Hide all drives (unless otherwise specified): Default behavior is to hide all drives. This setting is overruled by any drives configured to be shown with Drive and Port Mappings.
- Never Hide Home Drive is selected by default. If selected, the user's home folder will never be hidden, regardless of the Hide Drives setting of individual mappings.

Create a drive mapping using information from Active Directory
Active Directory stores information about users as user properties, and Active Directory user properties can be looked up using the $adinfo function. This makes it possible, for example, to base a drive mapping on a user's home directory as stored in Active Directory.

To set this up, configure an environment variable that uses the function $adinfo(homedirectory) to set its value based on the user's home directory information in Active Directory, and then map the directory based on this environment variable.

For example:

- At Composition > Actions By Type > Environment Variables, create an environment variable.
  - Give it a name (for example, HomeDrive)
  - In the Value field, enter: $adinfo(HOMEDIRECTORY)
- At Composition > Actions By Type > Files and Folders > Drive and Port Mappings, create a drive mapping
  - In the Share name field, enter: %HomeDrive%

Result: when a user starts a session, the path stored in that user's Active Directory property Home folder is set as the value for the environment variable %HomeDrive%, and then the directory is mapped based on this path as taken from the Active Directory.
Drive Substitutes

For some (legacy) applications it may still be necessary to use a fixed drive letter. You can substitute drives to create the drive needed. You can do this by using the Drive Substitutes option.

You can set the drive substitute to be dependent on connection state. For example, when working with a laptop, the mapping should only be set if the user is connected to the network. This means the required state must be on-line connection. If the mapping is not set to be connection state-dependent, it will be set permanently.

Where to find Drive Substitutes

<table>
<thead>
<tr>
<th>What</th>
<th>Where</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global level</td>
<td>Composition &gt; Actions By Type &gt; Files and Folders &gt; Drive Substitutes&lt;br&gt;Composition &gt; Actions By Event &gt; At Logon, select New &gt; Drive and Port Mapping</td>
</tr>
<tr>
<td>Application level</td>
<td>Open the application at Composition &gt; Applications, go to Configuration &gt; Actions</td>
</tr>
</tbody>
</table>

Configure Drive Substitutes

- At Composition > Actions By Type > Files and Folders > Drive Substitutes, the option Refresh Drive Substitutes when network connectivity changes allows you to refresh Drive Substitutes automatically when the network connectivity of a session changes. This ensures that connection state-dependent Drive Substitutes become available or disappear correctly.
- You can override the global settings of this feature for specific Workspace Containers.
- When configuring a drive substitute, you can optionally enter a note in the Administrative note field. This is useful to differentiate the substitutes that you configured.
- When specifying the hide drives behavior for a drive substitute, the option Always hide, but allow access will hide drives, but they are still available to users that need access to them. This is useful, for example, for local floppy disks. If a local floppy disk is not hidden, this can seriously slow down the initial appearance of Windows Explorer or file dialog windows. You can change the default behavior for all drive substitutes if necessary.
- The field Physical drive and path specifies the physical drive and path to the drive that will be substituted for the virtual drive that you selected in the field Virtual drive.
- The Required connection state field specifies the required connection state that allows the setting to be applied. For example, this allows you to configure a setting that will only be applied if a computer has an online connection state.
- When a session starts, the applicable drive substitutes are set in the order in which they appear in this list. If necessary, change the order to ensure the correct processing.
- Click the Access Control tab to configure the Access Control criteria of the drive substitute.
- Click the Workspace Control tab to configure to which Workspace Container(s) the drive substitute applies.
Folder Redirection

At Composition > Actions By Type > Files and Folders > Folder Redirection, you can configure the redirection of Microsoft Windows User Shell Folders. Folder redirection enables the administrator to redirect the location of certain folders of the user profile to a different path, such as a shared network location. For example, the local folder `C:\Users\<username>\My Documents` can be redirected to a different Target folder location (e.g. `<networkshare>\Users\<username>\My Documents`). Up till now, folder redirection could only be done by creating a User Registry Setting or by defining a GPO. If the folder does not exist in the target location of the user session, it will be created automatically, if possible in the user context.

Some of the advantages of folder redirection are:

- user documents are available from any computer
- helps to reduce logon and logoff times (data is stored outside the user profile)
- reduces the risk of profile corruption
- increased security and availability of user data (safe storage and recovery on network location)

The following folders can be redirected:

<table>
<thead>
<tr>
<th>Folder on Microsoft Windows Vista and higher</th>
<th>Folder on Microsoft Windows XP</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appdata</td>
<td>Application Data</td>
<td>Default location for user application data and binaries (hidden folder)</td>
</tr>
<tr>
<td>Contacts</td>
<td>Not applicable*</td>
<td>Default location for users' Contacts</td>
</tr>
<tr>
<td>Desktop</td>
<td>Desktop</td>
<td>Desktop items, including files and shortcuts</td>
</tr>
<tr>
<td>Documents</td>
<td>My Documents</td>
<td>Default location for all user created documents</td>
</tr>
<tr>
<td>Downloads</td>
<td>Not applicable*</td>
<td>Default location to save all downloaded content</td>
</tr>
<tr>
<td>Favorites</td>
<td>Favorites</td>
<td>Internet Explorer Favorites</td>
</tr>
<tr>
<td>Links</td>
<td>Not applicable*</td>
<td>Contains Windows Explorer Favorite Links</td>
</tr>
<tr>
<td>Music</td>
<td>My Music</td>
<td>Default location for user’s music files</td>
</tr>
<tr>
<td>Pictures</td>
<td>My Pictures</td>
<td>Default location for user’s picture files</td>
</tr>
<tr>
<td>Saved Games</td>
<td>Not applicable*</td>
<td>Used for Saved Games</td>
</tr>
<tr>
<td>Searches</td>
<td>Not applicable*</td>
<td>Default location for saved searches</td>
</tr>
<tr>
<td>Start Menu</td>
<td>Start Menu</td>
<td>Default location for Start Menu</td>
</tr>
<tr>
<td>Videos</td>
<td>My Videos</td>
<td>Default location for user’s video files</td>
</tr>
</tbody>
</table>

* Microsoft Windows XP and before will not recognize these folder redirections.
Configuration of Redirections

- The Redirections tab shows the redirected folders, for example, Favorites may be redirected to `<networkshare>\Users\<username>\Favorites`. If several Folder Redirections have been configured, you can change the order in which the redirections will be carried out by clicking Change order of execution and using the arrow up and down icons.
- Select the Windows folder which must be redirected in the user session. See the table above for possible folders for redirection and the OS version to which they apply.
- Specify for Target folder location, the required type of folder redirection and applicable Root path. When specifying the Root path, keep in mind that this applies to the user session environment. For example, a network location that is accessible to an administrator, is not necessarily also accessible to the user.
  - Redirect to the following location
    - Specify a full network path for Root path. Example: `\\server\Redirection\%username%\<foldername>`.
  - Create a folder for each user under the Root path
    - Specify a network path without `%username%\<foldername>` for Root path. Example: for a redirection of the Documents folder, specifying `\\server\Redirection` for Root path, for user John, this folder will be redirected to `\\server\Redirection\John\Documents`.
  - Redirect to the local user profile location
    - `%USERPROFILE%` is automatically specified for Root path. This value cannot be changed.
  - Move the contents to the new location - Select this option to perform a one-time move of the contents of the specified Windows folder to the Root path (target folder location). When changing the Root path, the content of the current root path will be moved to the new root path. This is also a one-time move. Please note that if this option is selected for an existing folder redirection in a Workspace Control environment without changing the Root path, the one-time move will not be executed for users that logged on, at least once, to a Workspace Control user session. The original content in the Windows folder will remain there. When changing the Root path at a later stage will cause the contents of the redirected folder in the initial root path to be moved to the new root path.
  - Make the contents available offline - Select this option if the contents of the redirected Windows folder should be made available offline (using the Microsoft Windows technology "Offline files and folders"). At session logon, redirected Windows folders are synchronized for offline use to the Offline Files cache. When this option is not selected, Workspace Control will clean up the Offline Files cache for the configured redirected Windows folder. For this option to work correctly, Microsoft Windows must be configured for Offline Files and disk space for the Offline Files cache must be sufficient.
  - The Required connection state field specifies the required connection state that allows folder redirection. For example, this allows you to configure folder redirection that will only take place if a computer is online. See Connection State Settings.
- Click the Access Control tab to configure the Access Control criteria of the Folder Redirection.
- Click the Workspace Control tab to configure to which Workspace Container(s) the Folder Redirection applies.

Configuration of Settings

- Shows whether Folder redirection has been enabled or disabled.
- With the option Use localized names for redirected Windows folders selected, when an Operating System is set to any other language than English, the redirected folder is displayed in the local language of the system the user session is running on.
- You can override the global settings of this feature for specific Workspace Containers.
Notes

- With Folder Redirection, a backup is made of pre-existing folder redirections for that user and this backup is restored at the end of the user session. This is done because otherwise when, for example, a user is placed in a different Workspace Container, he/she could get invalid folder reference(s) due to Folder Redirection.

- When there are User Registry actions that are already configured, enabling Folder redirection will prompt a message that these actions may override Folder Redirections and need to be checked. For example, you may have a registry setting for the Folder Redirection for Citrix Servers, which applies to the Workspace Container Citrix Servers, which may conflict with other Folder Redirections. In this case, you have to be careful configuring a redirection for Citrix Servers in Composition > Actions By Type > Files and Folders > Folder Redirection as it will be overridden by the User Registry action.

- When using Folder Redirection, User Profile Directory Maintenance can no longer be used to manage the contents of these redirected folders, because they are no longer part of the user profile. When a folder is redirected to the user’s home drive, you can use User Home Directory Maintenance to manage the contents of the folder.

- Start Menu will be redirected along with AppData, unless:
  - Start Menu itself has been configured for Folder Redirection
  - Start Menu has already been redirected by means of a GPO to a different path from AppData (also, for Microsoft Windows Vista and later, child shell folders of AppData will also be redirected)

- Not all contents of the original Start Menu folder will be copied to the redirected location. Shortcuts from the section All Users of the local PC Profile will be copied to the redirected Start Menu. The personal part of the profile will, however, not be copied. If you want to keep this, you will have to copy it manually.

- When configuring the Workspace Control option Package delivery mode for Microsoft App-V 5 packages with Minimal (per user) or Full (per user), the feature Folder Redirection for the Windows folder AppData, is not supported.

Examples

Folder Redirection versus User Profile Directory

These can be confusing as both can be used to manage user-dependent files. In most cases, a combination of Folder Redirection and User Profile Directory maintenance will be necessary. For example, an application or application plug-in may need some configuration settings from the local User Profile, but you want to store the user settings on a network drive at logoff for security reasons. Define the file containing the user settings as an object at Composition > Actions By Type > Files and Folders > User Profile Directory. Redirect the AppData folder to a network drive via Composition > Actions By Type > Files and Folders > Folder redirection. This way, the application can start up and the user settings are stored safely.
Folder Synchronization

Users often work from a variety of locations, and in each location they access, create, change and delete files and folders. This may lead to problems if users are unable to find the correct documents because they have different sets of documents, or different document versions, in different workspaces.

Use Folder Synchronization to solve this by synchronizing the files in two designated folders, in order to ensure that the correct set of files and folders is available in the user's workspace.

Folder Synchronization: global or application-based

- Configure global Folder Synchronization actions to synchronize the contents of folders that should be up to date when a Workspace Control session starts, ends, refreshes, reconnects or at specific intervals. Home folders are an example of folders that should be synchronized with a global Folder Synchronization action.
- Configure application Folder Synchronization actions to synchronize the contents of folders that should be up to date when a specific application starts or ends.

Where to find Folder Synchronization

<table>
<thead>
<tr>
<th>What</th>
<th>Where</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global level</td>
<td>Composition &gt; Actions By Type &gt; Files and Folders &gt; Folder Synchronization</td>
</tr>
<tr>
<td></td>
<td>Composition &gt; Actions By Event &gt; At Logon, select New &gt; Folder Synchronization</td>
</tr>
<tr>
<td></td>
<td>Composition &gt; Actions By Event &gt; At Session Refresh, select New &gt; Folder Synchronization</td>
</tr>
<tr>
<td></td>
<td>Composition &gt; Actions By Event &gt; At Session Reconnect, select New &gt; Folder Synchronization</td>
</tr>
<tr>
<td></td>
<td>Composition &gt; Actions By Event &gt; At Logoff, select New &gt; Folder Synchronization</td>
</tr>
<tr>
<td>Application level</td>
<td>Open the application at Composition &gt; Applications, go to Configuration &gt; Actions</td>
</tr>
</tbody>
</table>

Prerequisites

Microsoft Sync Framework 2.1 must be installed on all Agents running user sessions in which folders are to be synchronized. This will be done automatically during installation of Workspace Control. Both folders must be accessible in the user's workspace. For one-way synchronization, the user must have write permissions on the local folder. For two-way synchronization, the user must have write permissions on both folders.
Configure folder synchronization

Global settings

With Default Logging you can configure the level of detail of logging in the User Event Log:

- **Log event details**: A log entry is created for every individual file affected by the Folder Synchronization. This entry states the action (Create, Delete, Rename, Update) that was performed and the path to the file. This is followed by a summary line that contains the totals for each of these actions.

- **Log event summaries**: A log entry is created that contains the totals for each of the actions (Create, Delete, Rename, Update) that was performed by the Folder Synchronization.

Entries in the log are grouped per Synchronization.

You can make exceptions to the Default Logging setting on individual Folder Synchronizations.

Synchronization settings

- **On the Properties tab, you can:**
  - Configure the direction of the Synchronization.
    - **Direction: Both**: two-way synchronization; files deleted in one folder are also deleted in the other location.
    - **Direction: Upload**: single-direction synchronization from local to remote; files deleted locally are also deleted from the remote location.
    - **Direction: Download**: single-direction synchronization from remote to local; files deleted from the remote location are also deleted locally.
  - Configure when the Synchronization is executed. Possible options are Run at: Logon, Refresh, Reconnect session, Interval (configurable) and Logoff.
  - The Required connection state field specifies the required connection state that allows synchronization. For example, this allows you to configure synchronization that will only take place if a computer is on-line.
  - Choose to Exclude read-only files, hidden files and system files.
  - Choose to have files that are overwritten or deleted during the synchronization process Saved to the Recycle Bin, so that they remain available for recovery. This safety measure is enabled by default, but can be turned off if it is not necessary.
  - Configure the level of detail of Logging:
    - **Default** (follows the default configured behavior)
    - **Log event details**
    - **Log event summaries**
  - Optionally, on the Filters tab, you can filter a Folder Synchronization action to include only specific files (for example, RES-ONE.ppt) or file types (for example *.ppt), and/or to exclude specific files, file types and folders.
    - You can use the wildcard characters * and ? in the fields Files to include and Files to exclude.
    - Separate multiple entries in the fields Files to include and Files to exclude with a semi-colon (;).
    - You can specify folders that should be excluded by entering the location in the Folder field and clicking Add. To exclude a folder that is located in another folder, enter the full path. For example, if you only specify temp, the folder temp in the root of the sync folder will be excluded; temp folders in other folders will not be excluded.
  - **Click the Access Control tab to configure the Access Control criteria of the Folder Synchronization.**
  - **Click the Workspace Control tab to configure to which Workspace Container(s) the Folder Synchronization applies.**
Examples

Use Folder Synchronization to:

- synchronize local and network folders. Folder Synchronization will ensure that both folders have the same contents by adding new files and folders, removing deleted files and folders, and overwriting old file versions. This is particularly useful in cases where a user has a home directory on a share as well as a local home directory, for example on a laptop. This is achieved with the Direction: Both.

- download files and folders from the network to local computers. Folder Synchronization will add new files and folders from the network location to the local computer, and will overwrite old file versions. This can be useful for a network folder that users also need to access when they are working locally, for example a folder containing standard forms or presentations. This is achieved with the Direction: Download.

- upload local files and folders to the network. Folder Synchronization will add new files and folders from the local computer to the network location, and will overwrite old file versions. This can be useful if a user creates files locally that need to be made available on the network, for example as output of an authoring application that publishes to a local folder. This is achieved with the Direction: Upload.

For example, the technical writers at <COMPANY> use an authoring tool to create, maintain and publish product documentation. The tool publishes documents to a local folder, and the writers must remember to manually copy the updated output to a central network folder where other people and processes can always access the latest version. This process can be automated using an application-level Folder Synchronization action that uploads the contents of the local folder to the network folder whenever the writer closes the authoring tool.
Directory Maintenance

The Directory Maintenance technology can be used for preparing and maintaining users' home and profile directories.

Directory Maintenance is divided into a User Home Directory node and a User Profile Directory node. Both nodes allow you to configure a model or template of the files and folders that should be present on or copied to the user's home directory and/or the user's profile directory.

**Where to find Directory Maintenance**

<table>
<thead>
<tr>
<th>What</th>
<th>Where</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global level</td>
<td>Composition &gt; Actions By Type &gt; Files and Folders &gt; User Home / Profile Directory</td>
</tr>
<tr>
<td>Application level</td>
<td>Open the application at Composition &gt; Applications, go to Configuration &gt; Actions</td>
</tr>
</tbody>
</table>

**Configure Directory Maintenance**

The User Home Directory and User Profile Directory nodes consist of two tabs:

- The Files tabs: these tabs allow you to configure the model directories of Workspace Control. They provide an Explorer-like view of the model directories, files and subfolders. A model directory contains all folders and resources that you can use when configuring the contents of the user's home directory or profile directory.
- The Actions tabs: these tabs allow you to configure the contents of the user's home directory and profile directory, based on your selection of folders and resources from the model directories.

Specify the user's home directory drive (User Home Directory > Actions)

Select the drive in the Default home drive field on the Settings tab:

- When Resolve home drive from Active Directory is selected, Workspace Control will first try to retrieve the user's home drive letter from the Active Directory User Profile Properties.
- When Use %reshomedrive% if available is selected, Workspace Control will create exceptions to the default Drive to home directory setting by using the %reshomedrive% environment variable.

The Overview in the users Workspace Analysis Details also shows the Home Directory and Profile Directory rules that apply to the user.
Configure Settings (Actions tabs)

- When configuring the settings of a file or folder, you can replace its name with the username. This is useful if you want to copy a file or folder with the same name as the user's logon name to the user's home directory.
- By specifying an alias for the object, the original object name will be overwritten when it is copied to the home directory of a user. This is useful if the home directory of a user should contain a specific object whose values depend on the group membership of the user.
- Select which action should be taken in the Action field, depending on whether you selected a folder or a file. The Object field will be replaced with the username when specifying an Action for a file, the option Set specific values in INI-file allows you to configure INI file values. After configuring INI-file values, select Run once if these values should be set only once.
- Required connection state specifies the required connection state that allows the setting to be applied. For example, this allows you to configure a setting that will only be applied if a computer has an online connection state.

Configure Model Directories (Files tabs)

- Click the Files tab of the User Home Directory or User Profile Directory node, depending on the directory that you want to configure.
- Select the folder to which you want to add a folder or User resource and click New. This will open the Select File(s)/Folder(s) window, which allows you to select and add folders and resources to the model directory.
- Select or browse to the file or folder that you want to add and click OK. The selected file or folder will be added to the Model directory folder of the Home Directory or Profile Directory node, depending on your selection in step 1. You can only use these files and folders to configure the user's Home Directory and Profile Directory.

Examples

Configuration of Actions

- When configuring the settings of a resource, the option Replace with %username% allows you to replace the name of the resource with the username. This is useful if you want to copy a file or folder with the same name as the user's logon name to the user's home directory.

For example, if you want to copy a log file to the home directory of users Jackson, Greene and Smith, make sure that the model directory contains the files jackson.log, greene.log, and smith.log. When these users then log on, the correct files with their login name will be copied to their home directory. This means that you do not need to create an entry for each individual user (jackson.log, greene.log, smith.log), but can create one entry with %username%.log instead.

- By specifying an alias for the resource, the original resource name will be overwritten when it is copied to the home directory of a user. This is useful if the home directory of a user should contain a specific resource whose values depend on the group membership of the user.

The administrator of IvantiDemo has added two INI files to the model directory of Home Directory Maintenance, app_group1.ini and app_group2.ini.

- app_group1.ini has value "green".
- app_group2.ini has value "blue".

- If user petersent logs on, who belongs to group 1, app_group1.ini should be copied to his home directory and renamed to app.ini
- If user williamsj logs on, who belongs to group 2, app_group2.ini should be copied to his home directory and renamed to app.ini

You can configure this by specifying the alias "app.ini" for both files. This ensures that the home directory of user petersent will contain an app.ini file with value "green" and the home directory of user williamsj will contain an app.ini file with value "blue".
7.2.5 **LANDesk**

At Composition > Actions By Type > LANDesk, you can view and configure LANDesk software distributions. This allows you to deploy software in the user workspace.

You can only configure LANDesk software distributions if you have enabled LANDesk in the Setup menu and are connected to a MBSDK Web Service.

**Software distribution Configuration**

To add a software distribution that should run when a session starts, go to Composition > Actions By Type > LANDesk. See Workspace Control Help for configuration settings.

- You can override the global settings of this feature for specific Workspace Containers.

**Configuring software distributions for Applications**

To add a software distribution that should run when an application starts, open the application at Composition > Applications and go to Configuration > Actions. Configuring these software distributions is the same as on global level.

- If the **Wait for action to finish before continuing** has been enabled for a software distribution on an application, a notification is displayed in the user session if a user starts the application and the Package is deployed. This notification window allows the user to select **Dismiss and notify me when done** which allows the user to continue working with already available applications while the Package is deployed.

**Note**

You can easily move Actions from one application to another; from an application to global; and from global to a specific application. To do so, right-click one or more selected Actions and choose **Move**.
7.2.6 Microsoft System Center Configuration Manager Software Distributions

At Composition > Actions By Type > Microsoft ConfigMgr, you can view and configure Microsoft System Center Configuration Manager software distributions. This allows you to deploy software distributions of Applications and Packages in the user workspace.

You can only configure Microsoft Configuration Manager software distributions if you have enabled Microsoft System Center in the Setup menu and are connected to a Microsoft System Center Configuration Management Server.

Software distribution Configuration

To add a software distribution that should run when a session starts, go to Composition > Actions By Type > Microsoft ConfigMgr. See Workspace Control Help for configuration settings.

- You can override the global settings of this feature for specific Workspace Containers.

Configuring software distributions for Applications

To add a software distribution that should run when an application starts, open the application at Composition > Applications and go to Configuration > Actions. Configuring these software distributions is the same as on global level.

- If the Wait for action to finish before continuing has been enabled for a software distribution on an application, a notification is displayed in the user session if a user starts the application and the deployment starts. This notification window presents the user the option to select Dismiss and notify me when done, which allows him to continue working with already available applications while the Software Distribution is deployed.

Note

You can easily move Actions from one application to another; from an application to global; and from global to a specific application. To do so, right-click one or more selected Actions and choose Move.
Chapter 7: Composition

7.2.7 Printers

Depending on the physical location of the desktop or laptop, different printers should be available to the user. You can use Composition > Actions By Type > Printers to achieve this. To configure printers per application, go to the Configuration > Actions tab of the application (at Composition > Applications).

You can set a printer as the default printer for the selected type of access control. It is also possible to define a backup printer for process-critical printing situations. To do this, enable the Failover option.

The Workspace Composer shows a simple list of available printers, and so helps the user to select a default printer or open a Print Status window. The user can even set a default printer based on his work location. You can also allow the user to connect to additional printers.

Please note that with the release of Windows 10 version 1511, Microsoft made a change to the way Windows 10 handles the default printer: the printer that was last used by the user becomes the new default printer.

If the Printers feature is enabled (at Composition > Actions By Type > Printers, on the Settings tab), Workspace Control reverts handling of the default printer to the method Windows 10 used before version 1511, using the Microsoft Windows registry value LegacyDefaultPrinterMode. This registry value impacts not only managed default printers, but also user selected default printers.

Configure printers

• If you select Force mandatory default printer (reset default printer during each logon), the advanced options in the user’s "Printing Preferences" will be disabled. Although the end user will be able to set a different printer as default within a session, the centrally configured default printer will be reset at the start of each new session.

• Allow users to choose default printer per location, based on:
  • IP network address for all Agents - When a default printer is set in a user session, it is stored by Workspace Control based on IP network address.
  • IP network address for laptop Agents, ClientName for all other Agents - When a default printer is set in a user session, for laptops, it is stored by Workspace Control based on IP network address, and for workstations based on Client name.
  • Locations and Devices (use Zones for location based printing) - When a Zone that has been configured for location based printing applies to a Workspace Control session, the user will be allowed to select a default printer for that specific location. For every following Workspace Control session to which this same Zone applies, the previously selected printer is set as default. Enabling this option allows the configuration of location based printing both for managed and unmanaged printers.

Please note, that at least one Zone for location based printing must apply to a user session to enable the user to select a default printer for that location. Zones can be configured for location based printing by enabling the new option Use this Zone for location based printing on the Properties tab of the Zone (at User Context > Locations and Devices). It is recommended that Zones for location based printing are configured in a way, that a user only belongs to one such Zone at a time. If a user belongs to multiple Zones for location based printing at the same time, this may lead to unexpected behavior. Per session only one Zone for location based printing will be taken into account, but the Zone may differ for a next session.

At Diagnostics > Event Log, location based printing entries will be logged (i.e. Zone used for location based printing, Other Zone(s) configured for location based printing, No Zone configured for location based printing).
Also connect default / all printer(s) using VDX plugin also connects printers from the remote session in your local desktop. This allows, for instance to use a printer from your virtual desktop on your local desktop or in an application that is configured as a workspace extension (i.e. that runs from your local desktop). If Connect default printer using VDX plugin is enabled, the default printer of your virtual desktop will be used as default printer in your workspace extensions. If this option is not selected, the default printer of your local desktop will be used.

Disconnect network printers:

- **Before logging off**, Workspace Control will clean the user profile from user-connected and disabled printers. If you clear the check box Disconnect network printers before logging off, these settings will be preserved in the user's profile.
- **Before logging on or on reconnect**, Workspace Control will clean the user profile from user-connected and disabled printers. If you clear the check box Disconnect network printers before logging on or on reconnect, these settings will be preserved in the user's profile.
- **Skip unmanaged printers**: Within Workspace Control, an unmanaged printer is a printer that does not have a managed equivalent in a Workspace Control session. If both a managed and an unmanaged version of a printer exist, the unmanaged version will be replaced by a managed version after logging on. When this option is enabled, only network printers that are managed by Workspace Control will be disconnected before logon/logoff, all other printers will not be touched. The advantage of keeping unmanaged printers is, for instance, when you have defined an unmanaged printer you only use at home, you do not have to reconnect this printer each time you need it.

Refresh printers:

- **On reconnect** causes Workspace Control to reprocess all Network Printers, to determine which printers should be connected when a previously disconnected terminal session is reconnected.
- **On session refresh** causes Workspace Control to reprocess all Network Printers, to determine which printers should be connected when a Workspace refresh occurs.
- **When network connectivity changes** helps workstations and laptops to automatically reconnect printers when switching from offline network connection to online. To work properly, the checkbox Do not refresh Workspace when network connectivity changes at Composition > Desktop > Lockdown and Behavior must be unchecked.

When configuring a network printer, optionally enter a note in the Administrative note field. This is useful to differentiate the Printers that you configured.

- **Fast connect** allows users to start their sessions faster. The Fast Connect option is not available for Printers that are configured for an application.

When selecting the option Fast connect, the option Wait for task to finish before continuing becomes unavailable, because driver checks and permission checks will first be performed when the user actually connects to the printer.

When clearing the option Wait for task to finish before continuing the option Fast connect becomes unavailable, because the task will be performed asynchronously.

When specifying whether printing preferences should be preserved, if you select Default, the default settings as configured in the node Composition > User Settings will be applied. If you select Never save or Always save, this will overrule the default settings as configured in the User Settings node. The option Set as default printer for Printers is mandatory when configuring a printer for an application, but this will not reset the user's preference. The next time the user logs on, the preferred default printer will be restored. The user will also be notified of this event by the "Printing preferences" tool.

- The option Failover allows you to configure a backup printer that the user can connect to if it is not possible to connect to the primary printer, for example because the specified printer driver is unknown or if the print server is unavailable.

- The Required connection state field specifies the required connection state that allows the setting to be applied. For example, this allows you to configure a setting that will only be applied if a computer has an on-line connection state.

- Click the Access Control tab to configure the Access Control criteria of the Printer.
- Click the Workspace Control tab to configure to which Workspace Container(s) the Printer applies.
• When a session starts, the applicable printers are set in the order in which they appear in this list. If necessary, change the order to ensure the correct processing.

Tip

Sometimes the message “Composing default printer” appears in the Startup screen, although a default printer was defined. This is caused by the fact that the workstation cannot access the printer due to missing user credentials. In Workspace Control user credentials cannot be defined for printers. A possible workaround is to define a drive mapping to the same network location (or subdirectory) with the proper user credentials. Any drive letter can be assigned. This will speed up the connection to the printer considerably.
Use Locations and Devices for Printers

Because printers are usually used per location, you can use Zones / Workspace Containers to set up printers. By creating Zones / Workspace Containers you can set up printers per location. It has the advantage that for instance mobile users will automatically connect to the right printer when using a mobile computer at different locations.

Configure Zones for different IP ranges if your users use roaming workplaces or when multiple branches of your company share the same print server.

To configure “location based printing”, make sure the Lockdown and Behavior option Hide advanced options in Printing Preferences (Personalization by end user section) is not enabled.

Location based printing - example

Configuration

Configure Zones for location based printing, based on, for example, IP address range

- At User Context > Locations and Devices, create a Zone “ABC” with the following settings:
  - On the Properties tab, enable Use this Zone for location based printing.
  - On the Rules tab, add a Rule based on Computer IP address range (Computer > IP address > IP address range) between 10.0.0.51 - 10.0.0.60.

- At User Context > Locations and Devices, create a Zone “XYZ”, with the following settings:
  - On the Properties tab, enable Use this Zone for location based printing.
  - On the Rules tab, add a Rule based on Computer IP address range (Computer > IP address > IP address range) between 10.0.0.61 - 10.0.0.70.

Allow users to choose a default printer per location based on Zones

- At Composition > Actions By Type > Printers, on the Settings tab, select Allow users to choose default printer per location, based on.
  - Select Locations and Devices (use Zones for location based printing).

Available printers

- In a Workspace Control session, multiple printers are available.

Result

When a user logs on to a Workspace Control session from a computer with IP address 10.0.0.59, the user can choose a default printer for this location from the list of available printers. This printer will then be the user’s default printer for every session where his computer has an IP address in the range of Zone “ABC” (10.0.0.51 - 10.0.0.60).

When the user logs on to a Workspace Control session from a computer with IP address 10.0.0.62, he can choose a (different) default printer for that location from the list of available printers. This printer will then be the user’s default printer for every session where his computer has an IP address in the range of Zone “XYZ” (10.0.0.61 - 10.0.0.70).

When the user logs on to a Workspace Control session from a computer with IP address 10.0.0.95, he is not able to choose a default printer specifically for that location, but he may choose a default printer for all other locations. This printer will then be the user’s default printer for every session where his computer has an IP address not in the range of Zones “ABC” or “XYZ”. The user may also choose not to register a default printer.

Tip

In a user session, a default printer can be configured at Start > Workspace Control Settings > Printing Preferences, by clicking the Advanced button in the Printing Preferences window.
### 7.2.8 User Registry

With the User Registry technology it is possible to set up registry keys and policies for (groups of) users, based on their specific situations and needs. For example, it is possible to set registry settings based on the selection of the user’s Workspace Control language.

Registry keys (HKCU) can be imported and exported, which facilitates entering or changing registry keys. If you select the Run once option when implementing a registry setting, it will only be applied the first time a user logs on.

Documentation on registry keys can be found at various locations. Registry keys changing Windows settings can be found in the Windows Resource Kit. Documentation on application registry settings may be harder to find, since not all applications provide documentation regarding registry settings. Contact the application vendor for more information.

#### Policies

User Registry also supports Windows policy files (.adm) in the registry section. When adding a new policy template, first select a policy file to base the template on.

#### Where to find User Registry

<table>
<thead>
<tr>
<th>What</th>
<th>Where</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global level</td>
<td>Composition &gt; Actions By Type &gt; User Registry</td>
</tr>
<tr>
<td></td>
<td>Composition &gt; Actions By Event &gt; At Logon, select New &gt; User Registry Setting or User Registry Policy</td>
</tr>
<tr>
<td>Application level</td>
<td>Open the application at Composition &gt; Applications, go to Configuration &gt; Actions</td>
</tr>
</tbody>
</table>

#### Configure Registry Settings

**Configuration**

- Click **New Registry**, this will open the New registry settings window.
- Click the **Properties** tab.
  - Enter the name of the registry setting in the **Name** field.
  - Optionally enter a note in the **Administrative note** field. This is useful to differentiate the registry settings that you configured.
  - To enable the registry setting, select **Enabled**.
  - Select **Run once** to limit implementation of the registry setting to a user’s first startup.
  - Select **Ignore registry redirection (on 64-bit operating systems)** to map the registry value (new or modified) to the path specified by the user. If this option is not selected, the registry value may be mapped to a location under Wow6432Node on a 64-bit operating system.
  - In the **Required connection state** field, select the required connection state that allows the setting to be applied. For example, this allows you to configure a setting that will only be applied if a computer has an online connection state. See Connection State Settings.
  - Right-click HKEY_CURRENT_USER or HKEY_LOCAL_MACHINE and select an action from the Registry section. The first five actions are explained based on an example where HKEY_CURRENT_USER is the subtree, SOFTWARE is the key and Demo is the subkey (HKEY_CURRENT_USER\SOFTWARE\Demo).
How to add a registry subkey

- Right-click HKEY_CURRENT_USER.
- Click Open HKEY_CURRENT_USER. This will open the Pick keys/values from registry window.
- Expand HKEY_CURRENT_USER and SOFTWARE.
- Select Demo and click New.
- Click Close to close the Pick keys/values from registry window.

How to add a new subkey to an existing subkey

- In the New registry setting window, expand HKEY_CURRENT_USER and SOFTWARE.
- Right-click the Demo subkey.
- Point to New and click Key.
- Enter TestSubkey in the folder that is added and press ENTER.

How to add or change a registry subkey value

How to add a new string value

- In the New registry setting window, expand HKEY_CURRENT_USER, SOFTWARE and Demo.
- Right-click the TestSubkey subkey.
- Point to New and click String Value.
- Enter TestString and press ENTER.

How to edit the value of a subkey

- Right-click the value that you just added.
- Click Modify. This opens the Edit String window.
- Enter 1 in the Value data field.
- Enter “This is a test value” in the Administrative Note field. This field can be used to describe the function of the registry value. If you create an Instant Report of the registry setting, any annotations will be included.
- Click OK.

You can add the following registry subkey values:

<table>
<thead>
<tr>
<th>Value</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>String Value</td>
<td>Adds a string value. Most information about hardware components is stored as binary data and shown in hexadecimal format.</td>
</tr>
<tr>
<td>Expandable String Value</td>
<td>Adds a variable-length string value. This data type includes variables that will be resolved when an application or service uses the data.</td>
</tr>
<tr>
<td>Multiple String Value</td>
<td>Adds a multiple string value. In general, this type is used for values that contain lists or multiple values in a form. Separate multiple values with spaces, commas or other marks.</td>
</tr>
<tr>
<td>Binary Value</td>
<td>Adds a binary value. This data type is generated by hardware device drivers and the physical devices it controls. It is shown in hexadecimal format as a binary value.</td>
</tr>
<tr>
<td>DWORD Value</td>
<td>Adds a DWORD value. This data type is a number of 4 bytes long (32-bit integer). Many parameters for device drivers and services are this type and are shown in binary, hexadecimal or decimal format.</td>
</tr>
<tr>
<td>QWORD Value</td>
<td>Adds a QWORD value. This data type is a number that is a 64-bit integer. It is shown as a binary value.</td>
</tr>
<tr>
<td>NONE Value</td>
<td>Adds a value without any particular type. It is written to the registry by the system or applications and is displayed in hexadecimal format as a binary value.</td>
</tr>
</tbody>
</table>
How to rename a registry subkey or value

- Expand HKEY_CURRENT_USER, SOFTWARE and Demo.
- Right-click the TestSubkey key.
- Click Rename.
- Enter Renamed and press ENTER.

How to convert a registry value to a registry value of a different type

- In the New registry setting window, right-click the TestSubkey subkey.
- Point to Convert to and click Expandable String Value. This will convert the TestSubkey from a string value to an expandable string value. You can only convert string values, expandable string values and multiple string values to values of these types.

How to remove a registry subkey or value

How to remove the value from a subkey in the registry

- Expand HKEY_CURRENT_USER, SOFTWARE and Demo.
- Select the Renamed subkey.
- Right-click the TestString value and click Toggle "remove this value". This will remove the value from the registry subkey in the registry.

How to remove a subkey from the registry

- Expand HKEY_CURRENT_USER, SOFTWARE and Demo.
- Right-click the Renamed subkey and click Toggle "remove this value". This will remove the registry subkey and its underlying values from the registry.

How to delete a subkey

- Expand HKEY_CURRENT_USER, SOFTWARE and Demo.
- Select the Renamed subkey.
- Right-click the TestString value and click Delete.
- Click Yes to confirm that you want to delete the value.

Registry Tracing

When you make changes to the preferences of an application, these are usually stored as a registry setting in HKEY_CURRENT_USER. If you want to add these registry settings to Composition > Actions By Type > User Registry manually, you need to know the exact location of these settings in the registry. With the functionality Trace registry changes (available from the Action menu when adding a new User Registry setting), this is not necessary. When tracing the registry changes that are made by an application's process, you can choose the relevant registry setting(s) from a list of logged registry changes and convert them to a User Registry setting. This makes it easier to add registry settings.

You can use registry tracing to configure global User Registry settings, as well as User Registry settings that are set when a user starts an application.

To use Trace registry changes:

- Add or edit a User Registry item (in an application's Configuration section on the Action tab, or at Composition > Actions By type > User Registry).
- Go to Action > Registry > Trace registry changes.
- In the Trace registry changes window, the Process field shows the application's command line. You can change this if necessary, either by typing a process yourself, or by selecting a process that is currently running.
- For processes traced from an application's Configuration section on the Action tab, the button Run now opens the application with the full Workspace Control configuration, including settings, etc. For example, if a command is configured as a setting for the application, then this command will also be executed if you start the application with the Run now button in the Trace registry changes window.
For processes traced from Composition > Actions By Type > User Registry, the Run now button starts the selected process as if from the command prompt.

After clicking Start trace, you can go to the application and make the changes to the preferences you wish to store. The Trace registry changes window will reflect all the registry changes made by the application.

Click Stop trace when you have changed all the settings you needed to change. Select the checkboxes of the changes that you want to set as a User Registry and click Add.

How to import and export registry keys

How to import registry files

- Select the folder in which you want to import or export registry files and click Registry in the menu bar.
- Click Import registry file. This will open the Import Registry File window.
- Select the registry file and click Open. This will open the Import registry file window.
- Select one of the merge options:

<table>
<thead>
<tr>
<th>Item</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Replace existing data</td>
<td>Replaces the existing registry file with the imported registry file.</td>
</tr>
<tr>
<td>Perform incremental merge with existing data</td>
<td>Adds the data in the imported registry file to those in the existing registry file.</td>
</tr>
<tr>
<td>Perform differential merge with existing data</td>
<td>Replaces only those data in the existing registry file that differs from the imported registry file.</td>
</tr>
</tbody>
</table>

How to export registry files

- Select the registry file that you want to export and click Registry in the menu bar.
- Click Export registry file. This will open the Export Registry File window.
- Select the location, enter a name for the file and click Save.

Toggle Remove

In Workspace Control it is also possible to remove specific registry keys and/or values from a user profile, each time User Registry is executed. To achieve this, create a User Registry object that contains the keys and values that should be deleted from the user profile:

- Select the registry key or value you want to delete.
- Right-click the specific key or value.
- Select Toggle - remove this key and subkeys or select Toggle - remove this value.
Language Identity

It is also possible to link a registry key setting to a language setting, allowing an application to start in the user's preferred language (which can be selected on the Options tab of the "Workspace Preferences" tool). This functionality is beneficial for multilingual businesses. However, the application must be able to change a language setting using a registry setting.

Configure registry policies

When you select a policy file, its contents will be displayed and you can set new policies. If a policy requires additional data, a detailed policy window is displayed in which you can type data. When typing textual data in this window, it is possible to use variables such as "%username%" or "%homedrive%".

You can specify the order in which registry files and policies should be processed with the Change order of execution option.

When policies have been set (switched on or off), the menu item View resulting registry in the Policy window enables you to view the registry keys and values that result from the policies. It is also possible to export these keys and values to a registry file for later use.

The policy template will be copied to the Datastore, which allows it to be used at all times and on all servers.

- Click New Policy, this will open the Select ADM file window.
- Select the policy file on which the template will be based. You can select ADM files and ADMX files, which are XML-based.
  - Alternatively, click Add or Remove to add or remove ADM(X) files.
- Click OK. This will open the New registry setting (based on <ADM file>) window.
- Click the Properties tab.
  - Enter the name of the registry setting in the Name field.
  - Optionally enter a note in the Administrative note field.
  - To enable the registry setting, select Enabled.
  - Select Run once to limit implementation of the registry setting to a user's first startup.
  - Expand the contents of the ADM file.
  - Double-click a setting to view its details or right-click the setting and click Explanation to view an explanation of the setting.
- Click the Access Control tab to configure the Access Control criteria of the registry setting.
- Click the Workspace Control tab to configure to which Workspace Container(s) the registry setting applies.
Chapter 7: Composition

7.2.9 Linked Actions

When configuring Actions for applications it is possible to implement the Actions configured for another application. These Actions are called Linked Actions. When adding a linked action, the only configuration to be made is selecting the source application that contains the actions to be used.

This allows, for example, creating an application with a default set of Actions and linking various other applications to that source application, thereby making it unnecessary to create multiple applications and creating the same set of Actions for each application.

Where to find Linked Actions

<table>
<thead>
<tr>
<th>What</th>
<th>Where</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application level</td>
<td>Open the application at Composition &gt; Applications, go to Configuration &gt; Actions</td>
</tr>
</tbody>
</table>

Configure linked actions

It is also possible to implement the Actions configured for another application by adding Linked Actions. When adding a linked action, you only need to select the source application that contains the actions to be used. This makes it possible, for example, to create an application with a default set of Actions and to link various other applications to that source application, thereby making it unnecessary to create multiple applications and the same set of Actions for each application.

Linked Actions Restrictions

- Execution of "Linked Actions" is restricted based on:
  - The Access Control set on the Actions configured for the source Managed Application
  - The Workspace Control set on the Actions configured for the source Managed Application.
  - Access Control configured for the source Managed Application is ignored.
  - Workspace Control configured for the source Managed Application is ignored.
  - Actions with the setting Run Once should only run once for each user, even if several applications reference the same Action.

Linked Actions Relationships

- Managed applications can link to multiple managed source applications.
- Multiple managed Applications (targets) can link to a single managed source application.
- Linked Actions cannot link to any managed application which itself has "Linked Actions" Actions to another managed application.
- Managed Applications cannot link to the same managed source application more than once.
7.3 Desktop

You can configure settings options concerning the appearance and the lockdown of the end user's workspace in the Workspace Control Console at Composition > Desktop.

These settings include:

- **Shell** (on page 244)
- **Background** (on page 244)
- **Lockdown and Behavior** (on page 245)
- **Screensaver** (on page 255)

### 7.3.1 Shell

At the Shell node you can define which shell should be used: the **Workspace Control shell** or the (Workspace Control-managed) **Microsoft Windows shell**. A few of the properties of the Workspace Control shell are:

- Users do not have to attend a course every time Microsoft releases a new version of Windows.
- One company look and feel, regardless of the Windows version used.
- It provides additional menu- and application-related information for the users.
- Upgrading to a new Windows version poses no stress for users and administrators.
- It does not make use of `explorer.exe` which might be needed by some applications, but is less uniform (e.g. it allows the usage of themes).

In the Microsoft Windows Shell, dragging and dropping items on the desktop or in the QuickLaunch area will be detected by the **Workspace Preferences** tool. This enables coexistence of both Workspace Control shortcuts and document shortcuts. Users can customize their shortcuts in the Taskbar Settings window or with the **Workspace Preferences** tool.

When a user switches from the Workspace Control Shell to the Microsoft Windows Shell, all configured settings will be remembered by both shells. When the Workspace Control session ends and the Microsoft Windows Shell was used, all original settings will be restored in the profile of the user.
7.3.2 Background

In the Desktop background picture section you can:

- Select a picture (for example, your company logo) as well as the placement of that picture. The Microsoft Windows Microsoft Shell supports BMP and JPG formats for the desktop. The Workspace Control Shell supports BMP, GIF, ICO, JPG formats. Make sure all bitmaps are available as desktop picture resources. If you do not select a picture, the standard Workspace Control logo will be used.
  - In a session running on an operating system that does not support the configured Picture placement, the system reverts to an alternative picture placement. On Windows 8 and later, the alternative is Center; on Windows Vista and earlier it is Stretched.
  - With the option Use %deskpic% environment variable to determine picture file name, you can configure different desktop pictures in different contexts. See Environment Variables (on page 215) for more information. See the Workspace Control Help for configuration details.
    - The picture that is used with the variable is stored in the resources and is therefore always available.

In the Default desktop colors section you can select a default background and text color for your environment. To force the desktop colors in user sessions, the Lockdown and Behavior option Hide "Change Desktop Colors" in Workspace Preferences (forces default colors) must be selected. By not selecting this option, the desktop colors that the user selects in his Workspace Preferences tool take precedence over the default colors configured at Composition > Desktop > Background.

Note

If the Microsoft Windows Shell is used in combination with a changed Text color at Composition > Desktop > Background, this will not work with Microsoft Windows Vista and higher.
7.3.3   **Lockdown and Behavior**

Once the appearance of the Desktop has been set, you can hide/disable/remove specific settings in order to secure it fully.

Lockdown options can be set related to:

- **Workspace Composer**: hide/disable/remove options related to the Workspace Composer (irrespective of the shell used).
- **Start Menu and Taskbar**: hide/disable/remove specific Start Menu and Taskbar options from either the Windows shell, the Workspace Control shell or both shells.
- **Personalization by end user**: hide/limit specific options in Printing Preferences and Workspace Preferences.
- **Windows Explorer**: hide/disable/remove specific options from the Windows Explorer application.
- **Microsoft Windows Shell**: hide/disable/remove specific options from the Windows Operating System.
- **Workspace Control Shell**: determine specific behavior for the Workspace Control Shell.

Optionally you can enter (part of) a keyword in the **Instant Search** field to find the setting you need.

Certain options in **Lockdown and Behavior** are always evaluated by Workspace Control, even if Lockdown and Behavior is **Disabled**.

- Options marked with 🗝️ are always evaluated and, if selected, applied.
- Options marked with ⏺️ are only evaluated if Lockdown and Behavior is enabled. If Lockdown and Behavior is disabled, these options are grayed out.

The following options are available:

**Workspace Composer**

<table>
<thead>
<tr>
<th>Item</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Always hide &quot;Log Off&quot; in context menu</td>
<td>Hides the context menu options “Sign Out” (on Microsoft Windows 8 and up) and “Log Off” (on prior Windows versions).</td>
</tr>
<tr>
<td>Always hide &quot;Refresh Workspace&quot;</td>
<td>Hides this item in the Start Menu and context menus.</td>
</tr>
<tr>
<td>Ignore “Autolaunch at session start” when starting a published application session</td>
<td>Prevents applications that are configured to &quot;Autolaunch at session start&quot; from starting up when starting a published application session.</td>
</tr>
<tr>
<td>Do not reload user information when refreshing Workspace</td>
<td>Skips reloading user information when a Workspace is refreshed. In situations where it takes a long time to retrieve a user's group membership after a refresh, this option may significantly speed up the refresh of the Workspace. If the option is selected, the option 🔄 (Reload user information) will be added to the <strong>Diagnostics</strong> tab of the user’s <strong>Workspace Preferences</strong> tool. This enables the user to reload this information manually. If you force a refresh of a User Workspace (at <strong>Diagnostics &gt; User Sessions</strong>), the Workspace Composer will always reload the user information, even if the option Do not reload user information when refreshing Workspace is selected.</td>
</tr>
<tr>
<td>Item</td>
<td>Function</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Do not reload Computer OU membership information when refreshing Workspace | Skips reloading computer OU membership information when a Workspace is refreshed. In situations where it takes a long time to retrieve a computer's OU membership after a refresh, this option may significantly speed up the refresh of the Workspace.  
- If you force a refresh of a User Workspace (at Diagnostics > User Sessions), the Workspace Composer will always reload the computer OU membership information, even if the option Do not reload Computer OU membership information when refreshing Workspace is selected.  
- It is recommended to enable this option when there are Zones based on computer OU membership used in your Workspace Control environment. |
| Do not refresh Workspace after resuming from standby or hibernate    | Specifies that the workspace should not be refreshed if resuming from standby or hibernate.                                                                                                               |
| Do not refresh Workspace when display properties change              | Specifies that the workspace should not be refreshed if, for example, an application changes the display properties when starting up. Normally, a refresh is necessary to reflect these changes. |
| Do not refresh Workspace when network connectivity changes           | Specifies that the workspace should not be refreshed if the user disconnects from the network without using the hibernate or stand by options. The availability of applications and settings may depend on the session's network connectivity, for example if an application requires a specific connection state. By default, Workspace Control refreshes the user's Workspace if the network connectivity changes, to re-evaluate the connection state and reflect any resulting changes. |
| Do not refresh Workspace when reconnecting to a session              | Specifies that the workspace should not be refreshed if the user reconnects to an existing session on a Terminal Server. The availability of applications and settings may differ at the new session location, for example as a result of Zones. The default printer may also be different. A refresh is necessary to re-evaluate the location and reflect any resulting changes. |
| Hide main splash screen at session start, end and refresh            | Hides the main Workspace Control splash screen, which is normally shown when a user starts a session, refreshes it, logs off or disconnects. This option is not available when configuring exceptions to the global settings for Workspace Containers; when users start a session, the main splash screen is shown before Workspace Control determines which Workspace Containers apply. |
| Hide mini splash at application start                                | Hides the small splash screen, which is normally shown near the Windows notification area, when a user starts a managed application. This option does not affect the mini splash screens for Automation Tasks and LANDesk or Microsoft ConfigMgr actions that may be invoked by starting an application. |
| Mark window captions red if user has local administrator privileges | Marks title bars if a user is a local administrator.                                                                                                                                                     |
| Maximum number of automatically started applications               | Limits the number of applications the user can select in the Workspace Preferences tool to start automatically at the start of a session.                                                             |
### Chapter 7: Composition

<table>
<thead>
<tr>
<th>Item</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notify user about new applications</td>
<td>Shows a message to the user when new applications have been installed.</td>
</tr>
<tr>
<td>Notify user about not responding applications</td>
<td>Shows a message to the user when applications do not respond.</td>
</tr>
<tr>
<td>Notify user about missing default printer</td>
<td>Shows a message to the user when the default printer cannot be found.</td>
</tr>
<tr>
<td>Refresh Workspace on USB storage device change</td>
<td>Forces a refresh of the workspace of the user when he plugs a different USB storage device into his computer. This option only functions if a rule for a Zone has been configured based on a USB storage device serial number. It is useful if access or applicability of specific applications and/or settings depends on the availability of such a USB storage device serial number. See Adding and editing rules to a Zone.</td>
</tr>
</tbody>
</table>

### Start Menu and Taskbar

<table>
<thead>
<tr>
<th>Item</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Always hide &quot;Log Off&quot; in Start Menu</td>
<td>Hides or grays out the Start Menu options “Sign Out” (on Microsoft Windows 8 and up) and “Log Off” (on prior Windows versions).</td>
</tr>
<tr>
<td>Always hide &quot;PowerHelp&quot; in menu</td>
<td>Hides this item in the Start Menu. This option is enabled by default for new Datastore installations of Workspace Control.</td>
</tr>
<tr>
<td>Always hide &quot;Workspace Control Access Wizard&quot; in menu</td>
<td>Hides this item in the Start Menu.</td>
</tr>
<tr>
<td>Always hide &quot;Workspace Control Console&quot; in menu for other Administrative Roles</td>
<td>Hides this item in the Start Menu for Administrative Roles other than technical manager.</td>
</tr>
<tr>
<td>Always hide &quot;Workspace Control Console&quot; in menu for technical managers</td>
<td>Hides this item in the Start Menu for technical managers.</td>
</tr>
<tr>
<td>Always hide &quot;Workspace Control Settings&quot; submenu in menu</td>
<td>Hides this item in the Start Menu.</td>
</tr>
<tr>
<td>Always hide &quot;Run...&quot; in menu</td>
<td>Hides this item from the Start Menu. The Run command is a quick way to open programs, files, folders, and—when you’re connected to the Internet—websites. This option is only available for technical managers.</td>
</tr>
<tr>
<td>Always hide &quot;Workspace Preferences&quot; in menu</td>
<td>Hides this item in the Start Menu.</td>
</tr>
<tr>
<td>Disable “Shutdown” for all users on all computers</td>
<td>Disables this item from the Start Menu for all users.</td>
</tr>
<tr>
<td>Disable “Shutdown” for end users on workstations</td>
<td>Disables this item from the Start Menu for specific users. If Disable “Shutdown” for all users on all computers has been selected, this option will also be selected and it will not be possible to clear it.</td>
</tr>
<tr>
<td>Disable Recent Documents History</td>
<td>Disables this option from the Start Menu. Recent Documents shows a list of your recently used files on the right side of the Start menu.</td>
</tr>
</tbody>
</table>
### Chapter 7: Composition

<table>
<thead>
<tr>
<th>Item</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hide &quot;Clock&quot; on taskbar and in screensaver</td>
<td>Hides this item from the taskbar and the screensaver.</td>
</tr>
</tbody>
</table>
| Hide "Disconnect" for end users on terminal servers | - If selected, this option will be hidden on Terminal Server sessions and on workstations running Microsoft Windows 7 and later.  
- If not selected, the option will be shown on Terminal Server sessions and on workstations running Microsoft Windows 7 and later.  
- The option is never hidden for Technical Managers. |
| Hide "Exit" in menu and protect "Log off" with password | Hides Exit in the Start Menu and prompts the user for a password when selecting Log Off.  
**NOTE:** If you select this option, please ensure that the option Disable Taskbar Context Menus is cleared (at Desktop Management > Lockdown > Start Menu and Taskbar under Windows Shell only). If both these options are selected, users will not be able to log off. |
| Hide "Lock desktop" icon in system tray           | Hides the icon that is visible by default in the user's system tray. With this button, the user can lock his desktop with one click. |
| Hide "Show tasklist" icon in system tray          | Hides the icon that is visible by default in the user's system tray. With this button, the user can see his active applications and switch between them with one click. |
| Hide Administrative Tools Menu                    | Hides this item in Windows Explorer. Administrative Tools is a folder in Control Panel that contains tools for system administrators and advanced users. The tools in the folder might vary depending on which version of Windows you are using. |
| Hide computername in taskbar popup text           | Hides the computer name from the tooltip that is displayed when hovering over the Tasklist icon in the system tray. |
| Place mouse pointer over Start button after logon  | Places the mouse pointer on the Start button on the task bar when the user logs on. This option is disabled by default. |

### Personalization by end user

<table>
<thead>
<tr>
<th>Item</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hide &quot;Connect/Disconnect printer&quot; in Printing Preferences</td>
<td>Hides this item in the Printing Preferences tool.</td>
</tr>
<tr>
<td>Enable &quot;Find printers&quot; in Printing Preferences</td>
<td>When selected, in a user session, when clicking Connect in the Printing Preferences window, Workspace Control will open the Microsoft Windows Find Printer window to search for and select a network printer from Active Directory. Only available if Hide &quot;Connect/Disconnect printer&quot; in Printing Preferences is not enabled.</td>
</tr>
<tr>
<td>Hide &quot;Change Desktop Colors&quot; in Workspace Preferences (forces default colors)</td>
<td>Hides this item in the Workspace Preferences tool and forces the default desktop colors of Workspace Control in the user's session. If you clear this option, the desktop colors that the user selects in his &quot;Workspace Preferences&quot; tool take precedence over the default colors of Workspace Control. This means that if you change the default desktop colors of Workspace Control in the node Desktop &gt; Background, this will not affect the desktop colors of the user's session.</td>
</tr>
<tr>
<td>Item</td>
<td>Function</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Hide &quot;Change Desktop Background in Workspace Preferences (forces default picture)&quot;</td>
<td>Hides this item in the Workspace Preferences tool. If not selected, users can select a background picture for their desktop using their Workspace Preferences tool.</td>
</tr>
<tr>
<td>Limit “Change Desktop Background” to pre-configured pictures</td>
<td>With this option you can upload pictures and limit the Change Background function in the user’s Workspace Preferences tool to this list of pictures.</td>
</tr>
<tr>
<td>Hide &quot;Change Password&quot; in Workspace Preferences</td>
<td>Hides this item in the Workspace Preferences tool.</td>
</tr>
<tr>
<td>Hide &quot;Do not display my name in the screensaver&quot; in Workspace Preferences</td>
<td>Hides this item in the Workspace Preferences tool.</td>
</tr>
<tr>
<td>Hide &quot;QuickLaunch&quot; in Workspace Preferences</td>
<td>Hides this item in the Workspace Preferences tool.</td>
</tr>
<tr>
<td>Hide &quot;Select applications to display in Start Menu&quot; in Workspace Preferences</td>
<td>If Hide &quot;Select applications to display in Start Menu&quot; in Workspace Preferences is selected, users cannot determine the contents of their Start Menu. Each user’s Start Menu simply shows all the available applications, and the Workspace Preferences tool does not include the Start Menu tab.</td>
</tr>
<tr>
<td>Hide &quot;Pin to Start Menu&quot; in Workspace Preferences</td>
<td>Hides this item in the Workspace Preferences tool.</td>
</tr>
<tr>
<td>Hide &quot;Startup&quot; in Workspace Preferences</td>
<td>Hides this item in the Workspace Preferences tool.</td>
</tr>
<tr>
<td>Hide &quot;Swap left and right mouse button&quot; in Workspace Preferences</td>
<td>Hides this item in the Workspace Preferences tool.</td>
</tr>
<tr>
<td>Hide advanced options in Printing Preferences</td>
<td>Hides this item for all users in the Printing Preferences tool.</td>
</tr>
<tr>
<td>Limit Workspace Preferences to &quot;Change Password&quot; and &quot;Change Desktop Colors&quot;</td>
<td>Removes all other options from the Workspace Preferences tool.</td>
</tr>
<tr>
<td>Never hide client printers in Printing Preferences</td>
<td>When selected, locally configured client printers are displayed in the Printing Preferences tool in the user’s session.</td>
</tr>
</tbody>
</table>

### Windows Explorer

<table>
<thead>
<tr>
<th>Item</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable Add/Remove Programs</td>
<td>Disables this item in Windows Explorer.</td>
</tr>
<tr>
<td>Disable Control Panel</td>
<td>Disables this item in Windows Explorer. You can use Control Panel to change settings for Windows. These settings control nearly everything about how Windows looks and works.</td>
</tr>
<tr>
<td>Disable Context Menu on Desktop and in Windows Explorer</td>
<td>Disables all menus that are displayed when right-clicking an item on the desktop and in Windows Explorer.</td>
</tr>
<tr>
<td>Item</td>
<td>Function</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Hide Computer Management Option</td>
<td>Hides this item in Windows Explorer. Using Computer Management, you can perform many tasks, such as monitoring system events, configuring hard disks, and managing system performance.</td>
</tr>
<tr>
<td>Hide Control panel, Printer and Network Settings</td>
<td>Hides these items in Windows Explorer.</td>
</tr>
<tr>
<td>Hide Internet Explorer Icon</td>
<td>Hides this icon in Windows Explorer.</td>
</tr>
<tr>
<td>Hide My Computer Icon</td>
<td>Hides this icon in Windows Explorer.</td>
</tr>
<tr>
<td>Hide My Documents Icon</td>
<td>Hides this icon in Windows Explorer.</td>
</tr>
<tr>
<td>Hide My Network Places Icon</td>
<td>Hides this icon in Windows Explorer.</td>
</tr>
<tr>
<td>Hide Recycle Bin Icon</td>
<td>Hides this icon in Windows Explorer. Even when the Recycle Bin is hidden, deleted files are still stored there temporarily until you choose to permanently delete them or recover them.</td>
</tr>
<tr>
<td>Remove &quot;Open with...&quot; context menu in Windows Explorer</td>
<td>Removes the option Open with if the user right-clicks a file in Windows Explorer. If you double-click a file in Windows and it opens in the wrong software program, you can choose the program you would prefer to use by selecting the Open with option.</td>
</tr>
<tr>
<td>Remove Map and Disconnect Network Drive Options</td>
<td>Removes this option in Windows Explorer. A network drive is a file folder located on a remote computer that has been configured for sharing over a LAN.</td>
</tr>
<tr>
<td>Remove Properties from My computer</td>
<td>Removes this option in Windows Explorer. You can view a summary of important information about your computer by opening System in Control Panel. You can see basic hardware information, such as your computer's name, and you can change important system settings by clicking the links in the left pane of System Properties.</td>
</tr>
</tbody>
</table>

### Microsoft Windows Shell

<table>
<thead>
<tr>
<th>Item</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatically Place Applications in Programs Menu</td>
<td>Automatically places all application icons in the Programs menu instead of in submenus.</td>
</tr>
<tr>
<td>Disable Drag-and-Drop on the Start Menu</td>
<td>Disables the dragging-and-dropping of Start Menu items.</td>
</tr>
<tr>
<td>Disable Search programs and Control Panel (Windows Vista or later)</td>
<td>Enables the search functionality in the Start Menu. Enables the search of programs and Control Panel items. (i.e. limits the search results to files and folders)</td>
</tr>
<tr>
<td>Disable Taskbar Context Menus</td>
<td>Disables the context menu of the Taskbar.</td>
</tr>
<tr>
<td>Enable Windows 8.1 Start Menu (Windows 8.1 / 2012 R2)</td>
<td>In Microsoft Windows 8.1 / 2012 R2, the Classic view of the Start Menu will be used.</td>
</tr>
</tbody>
</table>

**NOTE:** If you select this option, please ensure that the option Hide "Exit" in menu and protect "Log off" with password is cleared. If both these options are selected, users will not be able to log off.
<table>
<thead>
<tr>
<th>Item</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow user to toggle Windows 8.1 Start Menu in Workspace Preferences</td>
<td>When enabled, the option <strong>Show Windows 8.1 Start Menu</strong> will become available in the users’ <strong>Workspace Preferences</strong>, on the <strong>Options</strong> tab, allowing users to enable or disable the Start Menu.</td>
</tr>
<tr>
<td>Go to the desktop instead of Windows 8 Start screen after logon</td>
<td>In Windows 8, when logging on, users get the Windows 8 Start screen instead of the more familiar desktop. With this option, you can select that users by default go to the desktop instead of the Windows 8 Start screen when logging on.</td>
</tr>
<tr>
<td>Allow user to choose between desktop or Windows 8 Start screen in</td>
<td>When enabled, the option <strong>Go to the desktop instead of Start screen after logon (Windows 8.1 / 2012 R2 and up)</strong> will become available in the <strong>Workspace Preferences</strong> tool, on the <strong>Options</strong> tab, allowing users to enable or disable going to the desktop when logging on.</td>
</tr>
<tr>
<td>Workspace Preferences (Windows 8.1 / 2012 R2 and up)</td>
<td></td>
</tr>
<tr>
<td>Force “Classic Start Menu” (Windows XP or Vista only)</td>
<td>Forces the Classic look.</td>
</tr>
<tr>
<td>Hide Action center from the Taskbar (Windows 7 or later)</td>
<td>Hides the Action Center from the Taskbar. Action Center lists important messages about security and maintenance settings that need your attention.</td>
</tr>
<tr>
<td>Hide desktop icons during session start and session refresh</td>
<td>Shows an empty desktop until all icons are in their correct locations. This eliminates the effect of shifting desktop icons, but it also means that end users cannot start any applications from their desktop until the process has finished.</td>
</tr>
<tr>
<td>Hide Taskbar Settings on the Start Menu</td>
<td>Hides these settings on the Start Menu.</td>
</tr>
<tr>
<td>Remove Active Desktop Options from the Settings Menu</td>
<td>Removes these options from the Start Menu. Active Desktop allows the user to add HTML content to the desktop. (Internet Explorer 4.0 to 6.x)</td>
</tr>
<tr>
<td>Remove Downloads from the Start Menu (Windows 7 only)</td>
<td>Removes this option from the Start Menu. The Downloads folder is the default folder in which downloaded files are stored.</td>
</tr>
<tr>
<td>Remove Games from the Start Menu (Windows 7 only)</td>
<td>Removes this option from the Start Menu. The Games folder is the central repository for games which also offers updates, statistics and news feeds for games.</td>
</tr>
<tr>
<td>Remove Help Option from the Start Menu</td>
<td>Removes this option from the Start Menu. Windows Help is the built-in help system for Microsoft Windows.</td>
</tr>
<tr>
<td>Remove HomeGroup from the Start Menu (Windows 7 only)</td>
<td>Removes this option from the Start Menu. HomeGroup makes it easy to share libraries and printers on a home network.</td>
</tr>
<tr>
<td>Remove My Documents from the Start Menu</td>
<td>Removes this option from the Start Menu. My Documents is the central repository for the user's documents.</td>
</tr>
<tr>
<td>Remove My Favorites from the Start Menu</td>
<td>Removes this option from the Start Menu. Favorites are links to websites that are frequently visited</td>
</tr>
<tr>
<td>Remove My Music from the Start Menu</td>
<td>Removes this option from the Start Menu. My Music is the central repository for the user's music.</td>
</tr>
<tr>
<td>Item</td>
<td>Function</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Remove My Network Places from the Start Menu (Windows XP)</strong></td>
<td>Removes this option from the Start Menu. My Network Places displays shortcuts to shared computers, printers, and other resources on the network.</td>
</tr>
<tr>
<td><strong>Remove My Pictures from the Start Menu</strong></td>
<td>Removes this option from the Start Menu. My Pictures is the central repository for the user’s pictures.</td>
</tr>
<tr>
<td><strong>Remove Network Connections from the Start Menu</strong></td>
<td>Removes this option from the Start Menu. Network Connections provides connectivity between your computer and the Internet, a network, or another computer. Connections are created, configured, stored, and monitored from within the Network Connections folder.</td>
</tr>
<tr>
<td><strong>Remove Personal Folder from the Start Menu (Windows 7 only)</strong></td>
<td>Removes this option from the Start Menu. The Personal folder contains all the user personal folders and libraries.</td>
</tr>
<tr>
<td><strong>Remove Recent Documents from the Start Menu</strong></td>
<td>Removes this option from the Start Menu. Recent documents is a list of recently used files on the right side of the Start Menu</td>
</tr>
<tr>
<td><strong>Remove Recorded TV from the Start Menu (Windows 7 only)</strong></td>
<td>Removes this option from the Start Menu. Recorded TV is the default public library where tv recordings are stored.</td>
</tr>
<tr>
<td><strong>Remove Search link from the Start Menu</strong></td>
<td>Removes this option from the Start Menu. Search allows you to search for files and folders, printers, people, and other computers on your network.</td>
</tr>
<tr>
<td><strong>Remove Set Program Access and Defaults from the Start Menu</strong></td>
<td>Removes this option from the Start Menu. This option specifies default programs for certain activities, such as Web browsing or sending e-mail, and which programs are accessible from the Start menu, Desktop and other locations.</td>
</tr>
<tr>
<td><strong>Remove Start Banner on the Taskbar</strong></td>
<td>Removes the <strong>Click here to begin</strong> banner from the Taskbar.</td>
</tr>
<tr>
<td><strong>Remove Videos from the Start menu (Windows 7 only)</strong></td>
<td>Removes this Library from the Start Menu. The Videos library is used to organize and arrange videos.</td>
</tr>
<tr>
<td><strong>Remove Windows Security on Start Menu (Terminal Server)</strong></td>
<td>Removes this option from the Start Menu. This option allows access to the Windows NT Security menu.</td>
</tr>
<tr>
<td><strong>Restrict Changes to Active Desktop Settings</strong></td>
<td>Prevents changes from being made to the Active Desktop settings. Active Desktop allows the user to add HTML content to the desktop. (Internet Explorer 4.0 to 6.x)</td>
</tr>
<tr>
<td><strong>Use high quality default icons instead of custom icons (Windows Vista or later)</strong></td>
<td>In Microsoft Windows Workspace Control automatically uses the high-quality icons contained in the application executables whenever an application is configured to use the default icon. Check this option to do this for custom icons as well. Note that after an upgrade from a version prior to RES PowerFuse 2010, all icons (including the original default icons) will be treated as custom icons.</td>
</tr>
<tr>
<td><strong>Use Personalized Menus</strong></td>
<td>Allows the use of personalized menus. In a personalized menu, menu items that you have used infrequently are hidden. With an arrow at the bottom a cascade menu is opened that shows you these items.</td>
</tr>
</tbody>
</table>
## Chapter 7: Composition

### Workspace Control Shell

<table>
<thead>
<tr>
<th>Item</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display &quot;Menu&quot; instead of &quot;Start&quot; on Workspace Control Shell taskbar</td>
<td>Renames the Start button to Menu.</td>
</tr>
<tr>
<td>Display AM/PM in clock on Workspace Control Shell taskbar</td>
<td>Changes the time format from 24-hour clock to 12-hour clock.</td>
</tr>
<tr>
<td>Disable single-click on Workspace Control Shell desktop</td>
<td>Disables the possibility to open items on the desktop using a single click.</td>
</tr>
<tr>
<td>Do not show blinking time in Workspace Control Shell</td>
<td>Disables the blinking colon in the time display.</td>
</tr>
<tr>
<td>Do not show welcome message after log on</td>
<td>Disables the welcome message that is normally shown when users start a session. This option is enabled by default for new Datastore installations of Workspace Control.</td>
</tr>
<tr>
<td>Force Microsoft Office Excel to show open workbooks on Workspace Control Shell taskbar</td>
<td>Forces Microsoft Office Excel to show all open workbooks in the taskbar in separate buttons instead of grouping them.</td>
</tr>
<tr>
<td>Force Taskbar on top of full-screen applications</td>
<td>Forces the Taskbar on top of a full-screen application in sessions that use the Workspace Control shell.</td>
</tr>
<tr>
<td>Hide &quot;Start&quot; button on Workspace Control Shell taskbar</td>
<td>Hides the Start button. This is useful if Workspace Control runs in a kiosk or as a Web Portal.</td>
</tr>
<tr>
<td>Protect &quot;Emergency Exit&quot; with password</td>
<td>Protects the emergency exit with a password. The user can access the emergency exit by double-clicking the upper-right corner of his desktop. This allows the user to leave a session immediately.</td>
</tr>
<tr>
<td>Show battery state on Workspace Control Shell taskbar</td>
<td>Shows the battery state on the taskbar. The remaining time of the battery will be shown in a tooltip text (if the laptop works on its battery). The battery state will only be shown if a battery is detected by Workspace Control. This option is disabled by default.</td>
</tr>
<tr>
<td>Show &quot;Hibernate&quot; in &quot;Exit&quot; dialog on workstations</td>
<td>Adds this option to the Exit dialog on workstations. It saves an image of the user's desktop with all open files and documents, before shutting down the computer. When the user starts the computer again, his files and documents will be on his desktop exactly as when he left them. This option does not apply to Terminal Servers.</td>
</tr>
<tr>
<td>Show &quot;Restart&quot; in &quot;Exit&quot; dialog on workstations</td>
<td>Adds this option to the Exit dialog on workstations. It allows the user to end his session, shut down his computer and then restart it again. This option does not apply to Terminal Servers.</td>
</tr>
<tr>
<td>Show &quot;Stand by&quot; in &quot;Exit&quot; dialog on workstations</td>
<td>Adds this option to the Exit dialog on workstations. It reduces the power consumption of a computer by cutting power to hardware components that are not in use. This allows the user to maintain his session, while keeping his computer running on low power with data still in memory. This option does not apply to Terminal Servers.</td>
</tr>
<tr>
<td>Item</td>
<td>Function</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Use Unicode Font to display window captions on Workspace Control Shell taskbar</td>
<td>Uses Unicode Font instead of non-ANSI characters (e.g. Japanese) in windows captions. This option is useful if window captions of application are not shown correctly in the Workspace Control taskbar, but requires the availability of the Unicode font on the target computer.</td>
</tr>
</tbody>
</table>
7.3.4 Screensaver

At the Screensaver section, you can take control of the screensaver in user sessions. A user then cannot change its configuration. Next to that, you can set:

- A screensaver background image. The Microsoft Shell only supports BMP images for the screensaver. The Workspace Control Shell supports BMP and other formats. Make sure all bitmaps are available as screensaver image resources. By clicking the Image button, you can add a picture to the screensaver image resources.
  - A variable screensaver picture. Select the option Use %saverpic% variable... to define via the Workspace Control environmental variable %saverpic% what pictures need to be used for what groups (OUs, Zones, Workspace Containers, etc.).

When a mandatory timeout for the screensaver is set, the user can no longer set this time in his Workspace Preferences tool.

> **Note**

When a VDX session is started from a Workspace Control session, the screensaver of the client will be used by default. It is possible to force the use of the Workspace Control session screensaver by setting the registry value NoAgentScreenSaver.
7.4 User Settings

Workspace Control has a method of preserving and applying user settings independent from the Windows profile called Zero Profile Technology. Zero Profile Technology automatically detects user settings that are being changed by the user. These settings are preserved immediately outside the profile. When these settings are required by the Windows desktop or application, they are applied just in time.

The following assigned Microsoft Windows profile types are supported:

- Local profiles
- Roaming profiles
- Mandatory profiles

Users can change certain settings in a session, such as their default printer, their mouse orientation, and the view in which an application should open. Applications and processes store such user settings in keys and values in the user-specific part of the registry (HKEY_CURRENT_USER), and in configuration files in the user's profile directory.

However, user profile directories and HKEY_CURRENT_USER are not always preserved when the user logs off. This is particularly the case if you use mandatory profiles, or if you use roaming profiles in combination with passthrough applications (see "Set up Instant Passthrough for Citrix XenApp published applications" on page 95) in a Citrix XenApp environment.

With Workspace Control User Settings, you can preserve changes that users make to certain settings, files and folders during a session. These User Settings are preserved in a network location or at a local cache location outside the user profile and are restored automatically when the user logs on again. This is achieved independent of the user's profile.

Please note that for a better user experience, it is recommended to create user settings for an application instead of globally. This can be done by editing the application at Composition > Applications. Global user settings are processed at log on.

7.4.1 Where to find User Settings in the Workspace Control Console

<table>
<thead>
<tr>
<th>What</th>
<th>Where</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global User Settings</td>
<td>Composition &gt; User Settings</td>
</tr>
<tr>
<td>User Settings for an application</td>
<td>Open the application at Composition &gt; Applications, go to User Settings</td>
</tr>
<tr>
<td>Storage location of User Setting data</td>
<td>Composition &gt; User Settings &gt; Central storage location</td>
</tr>
</tbody>
</table>
7.4.2 Zero Profile Modes

- **Capture targeted items on application/session end** (on page 258) - Preserves specified parts of HKEY_CURRENT_USER and of the user profile directory when the session ends or when the user closes an application.

- **Track any changed setting within scope immediately (global)** (on page 262) - Automatically tracks specific trees in HKEY_CURRENT_USER and/or the user profile directory tree and immediately preserves any changes that occur there.

- **Track any setting changed by application immediately (application)** (on page 264) - Automatically tracks specific trees in HKEY_CURRENT_USER and/or the user profile directory tree and immediately preserves any changes that the application's process makes in the registry at HKEY_CURRENT_USER and to files and folders in the user's %appdata% folder.

- **Capture targeted items once, then track further changes** - If this mode is selected User Settings will run once with the Zero Profile mode set to **Capture targeted items on application/session start/end**. The second time the Managed Application is run or the second time a session is started User Settings will run in the Zero Profile mode **Track any setting changed within scope/by application immediately**. By using this option it becomes very easy to use User Settings to migrate personal settings from one machine to another: With the Capture targeted items once, then track further changes mode it is easy to transfer all stored changes that were made on system A and track all new changes on system B with Track any setting changed within scope/by application immediately. Note that you need to specify Targeted items and possibly Excluded items.

**Capture targeted items on application/session end**

Use the Zero Profile modes **Capture targeted items on application/session end** (application) and **Capture targeted items on session end** (global) to preserve a list of specific items, as configured on the Capturing tab. Predefined Templates are available for a select number of applications and Control Panel options. You can use User Settings templates for the following applications:

<table>
<thead>
<tr>
<th>User Settings templates</th>
<th>Windows</th>
<th>Windows Explorer</th>
<th>User Certificates</th>
<th>Windows Messaging Subsystem</th>
<th>Instant Messaging</th>
<th>Internet Browsers</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Windows</strong></td>
<td>Control Panel</td>
<td>Available for all supported Windows versions:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Accessibility Options, Desktop Content, Desktop Icons, Keyboard Settings, Mouse Settings, Regional and Language Options, Screen Saver, Sounds, Taskbar, Themes, Toolbars, Visual Settings, All Control Panel Settings</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows 7 / 2008 R2 only</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Desktop Gadgets, Start Menu</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Windows Explorer</strong></td>
<td></td>
<td>Available for all supported Windows versions:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Folder General, Folder Search, Folder View</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>User Certificates</strong></td>
<td></td>
<td>Available for all supported Windows versions</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Windows Messaging Subsystem</strong></td>
<td></td>
<td>Available for all supported Windows versions</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Instant Messaging</strong></td>
<td>AOL Instant Messenger</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Microsoft Lync</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 2010, 2013</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Skype</strong></td>
<td></td>
<td>Up to and including version 6</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Skype for Business 2013, 2016</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Internet Browsers</strong></td>
<td>Google Chrome</td>
<td>Up to and including version 30</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Internet Explorer</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 9, 10, 11</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### User Settings templates

<table>
<thead>
<tr>
<th>Application</th>
<th>Version Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mozilla Firefox</td>
<td>Up to and including version 25</td>
</tr>
</tbody>
</table>
| Opera                             | • Opera 12 or lower  
• Opera 15 or later |
| **Microsoft Office**              |                   |
| Microsoft Access, Excel, OneNote, | • 2010, 2013, 2016 |
Outlook, PowerPoint, Publisher, Word |
| Microsoft Project, Visio          | • 2010, 2013 |
| Microsoft InfoPath                | • Designer 2010, Designer 2013  
• Filler 2010, Filler 2013 |
| Microsoft SharePoint              | • Designer 2010, Designer 2013  
• Workspace 2010 |
| Microsoft Office Common           | • 2010, 2013, 2016 |
| Microsoft Office Tools            | • 2010, 2013, 2016 |
| **Other Applications**            |                   |
| Adobe Acrobat Professional        | • 6, 7, 8, 9, X, XI, DC |
| Adobe Reader                      |                   |
| Adobe Dreamweaver, Illustrator,   | • CS5, CS6, CC (Compatible with CC, CC 2014, CC 2014.01) |
Photoshop                           |
| FileZilla                         | Up to and including version 3 |
| Foxit Reader                      | • 5, 6, 7 |
| iTunes                            | Up to and including version 11 |
| Quicktime Player                  |                   |
| WinRAR                            | Up to and including version 5 |
| WinZip                            | Up to and including version 17 |

The Start Menu template (under Windows > Vista or later > Control Panel) is only necessary if the option Pin to Start Menu (at Composition > Applications, on the Properties > General tab of an application), is not selected for applications. This template stores the same User Settings.
Chapter 7: Composition

Configuration

The User Settings templates for applications contain predefined Targeted Items for a specific application or Microsoft Windows setting and can assist with configuring User Settings.

**Notes**

- There are some known limitations when using Application Templates:
  - Windows Themes templates are supported on Microsoft Windows Vista and Microsoft Windows 7.
  - Pictures that are saved on a local machine will not be roammed.
  - Custom installed mousepointers will not be roammed, unless they are saved in the folder `\%Local\AppData\%\Microsoft\Windows\Themes\YOURTHEME\cursors` and the `.theme` file is adjusted to take the cursor from that folder.
  - Aero-specific settings will not be applied to non aero-capable sessions (aero-specific settings will be saved).
  - Device/Hardware related settings are not supported.
  - Settings that require administrative privileges are not supported.
  - The Input language template is not supported on Microsoft Windows 7.
  - It is recommended to use the Microsoft Office Common templates on global level.
  - **Composition > Applications > Settings > Disable Active Setup (skips first-time shell init)** should be unchecked for Microsoft Windows settings to function properly.
  - When at **Composition > Applications > Settings > Disable Active Setup (skips first-time shell init)** is selected the following command must be added at **Composition > Actions by Type > Execute Command**: `%SystemRoot%\system32\regsvr32.exe /s /n /i:/UserInstall\%SystemRoot%\system32\themeui.dll`.
  - Windows Themes settings will be captured in Workspace Control sessions on Terminal Servers, but due to technical restrictions on a multi-user platform the Desktop Window Manager will not be notified of these settings.

When adding a User Setting, use one of the following methods:

- Click **New > Templates** to use a predefined template.
- Click **New > Discover User Settings...** to start the User Settings Capture Wizard that discovers which files and registry settings need to be captured as User Settings for applications or processes.
  
  Please note that a full installation of Workspace Control is necessary to run the User Settings Capture Wizard as the wizard makes use of the Workspace Control drivers. Also, to avoid conflicting results, no Workspace Control session may be running on the system on which the User Settings Capture Wizard runs.

- Click **New > Custom** to create your own User Setting.

The following options are available when adding the User Setting (either Custom or by using a Template, or after the User Settings Capture Wizard has finished):

- On the Capturing tab, create a list of all the settings to be preserved. If you use a template or the User Settings Capture Wizard, this list is already pre-populated.
- When adding or editing Captured items:
  - At Limit # of files to, enter the number of User Setting files that must be preserved for the managed application. This setting only applies to: Folder/Folder tree. If the targeted Folder/Folder tree contains more files than specified, only the newest files (based on timestamp of the files) will be preserved.
  - Select Empty target when applying user setting to delete the corresponding User Setting before applying the setting. This setting only applies to: Registry key/Registry tree/Folder/Folder tree. Normally, targeted items are merged into the existing contents of the registry or folder structure of the user's session. This leaves intact any existing settings that are not overwritten by a User Setting. Sometime this is not the desired behavior, for example if an application leaves settings behind that it should have cleaned up. In such situations, enable this option.
  - Optionally, select Show exclusions to add exclusions to the configured settings, so that parts of the settings are not preserved.
• Select **Any file larger than** to determine the maximum size of the User Settings files and folders to be excluded and enter a number in KB, MB, GB. This setting only applies to: Files/Folders/Folder tree.

• Select **Any file unchanged for** to determine the maximum age of the User Settings files and folders to be excluded and enter a number in days or months. This setting only applies to: Files/Folders/Folder tree.

• Click **Add > Import > Flex Profile Kit** to import existing Flex Profile INI files directly into the User Setting.

• When specifying paths and names anywhere in User Settings, you can use:
  - wildcards *, ?, [charlist] and [!charlist].
  - special folders to specify files, folders or folder trees in the user profile directory, as well as the default Microsoft Windows known folders (also called special folders in Microsoft Windows XP and earlier versions of Microsoft Windows) and any other special folder that may exist on the computers in your environment.

---

**Note**

If **Windows Shell shortcut creation** is set to **Replace all unmanaged shortcuts**, this may lead to unpredictable results for global User Settings that preserve information in %desktop%, %startmenu% or %appdata%\Microsoft\Internet Explorer\QuickLaunch. This does not affect application-level User Settings for those folders.

---

**Only applicable to global-level User Settings:**

• For Global User Settings it is possible to capture items exclusively by enabling the option **Automatically exclude these targeted items from all other User Settings** that is available on the **Capturing** tab. In a session where such an “exclusive” User Setting applies, all other User Settings automatically handle the captured items as (hidden) exclusions for the duration of the user session.

• After a certain time, things like registry settings tend to grow large. To save disk space and to improve performance drastically, the User Settings will be compressed. In a new Datastore the setting is enabled by default. There is however a contingency: all Agents must be running on Workspace Control 9.5.2.0 or higher.

---

**Warnings**

• If any of your Agents runs on a version prior to RES Workspace Manager 9.5.2.0, a message appears stating this. You need to update the Agents concerned for the setting to take effect. If an Agent running an older version of the software is added to an existing environment, a more urgent message appears. Such an Agent must be updated immediately, because it cannot load compressed user settings.

• In case of downgrading an Agent, the captured User Settings will not be restored to their previous uncompressed state.

---

**Note**

The compression of User Settings only works when Zero Profile mode is set to **Capture targeted items on session end** at global or application level.
Only applicable to application-level User Settings:

- On the Properties tab, with the option Restore application to default configuration, the end user or Management Console user can revert an application to its original configuration (only available if the Zero Profile mode for the application is set to Capture targeted items on application/session end (on the Capturing tab)).
  - Applying this option will clear or delete all registry values, files and folders configured in the User Settings for the application from the user profile.
  - It is recommended to select the option Empty target when applying user setting for the captured settings (only applicable to Registry key/Registry tree/Folder/Folder tree). This will delete any existing settings that are not overwritten by the User Setting, which can be useful in case the application leaves settings behind that it should have cleaned up.
  - Before enabling the option Restore application to default configuration for an application, it is advised to first test if the application will launch correctly with its default configuration. If this causes problems with the application, you might want to consider only enabling the option Restore settings from previous session(s).
  - When enabling this option for end users, in the user session in the user's Workspace Preferences tool, on the Other tab, the extra option Default configuration will become available in the list of dates for which User Settings can be restored.
  - This option is not available for Microsoft App-V 4.x and ThinApp applications.
  - By default, the settings specified in the application's User Settings are preserved at application end: Capture: After application has ended. Optionally, you can set Capture: After session has ended instead, to preserve the settings later. To change the default configuration, you need to switch to the Advanced User Settings view (Capturing tab).

- The Sampling tab is only available in Advanced User Settings view.
  - If an application in this Zero Profile mode runs in sampling mode, its Sampling tab shows the settings that users did change during the sampled sessions, but that they subsequently lost because those changes did not fall within the scope of the application's Targeted Items.
  - The Sampling ratio controls the number of sessions from which information is logged. A higher ratio results in information from more sessions, and a lower ratio results in information from fewer sessions. With the ratio of 1:1, information is shown from all sessions.
  - On the Sampling tab:
    - settings that are part of a User Setting exclusion are not shown.
    - you can right-click a sampled setting and convert it into a User Setting targeted item or into a User Registry Setting ("User Registry" on page 237).
    - use CTRL+F to search for a specific sampling entry.
    - you can group the information by dragging column headers to the grouping area. To restore the original view, drag the column headers back to the column bar.
  - The value set for the option Start sampling determines when Workspace Control should start sampling data.
    - The default Start sampling: After application has started and is ready to be used is useful if the application loads and processes user-related settings after it has started up. Postponing the sampling until the application is ready for use filters out irrelevant changes from the Sampled data tab. With this option, changes are only sampled if they are made by this specific managed application.
    - Set Start sampling: Immediately when application starts if you want to see sampled data about changes made during the application's startup process. With this option, sampling is active as soon as the session has started. Any changes made by an unmanaged version of this application will also be included in the sampling.
  - Select Use the User Settings from the following application to link an application to the User Settings of another application, rather than giving the application its own User Settings.
Track any changed setting within scope immediately (global)

Use the Zero Profile mode Track any changed setting within scope immediately to preserve all changes made in a tracked registry tree in HKEY_CURRENT_USER, and/or in a tracked folder tree in the user profile directory. This mode is available for global User Settings.

Configuration

- The Sampling and Tracking tabs are only available in Advanced User Setting view.
  - The Sampling ratio controls the number of sessions from which information is logged. A higher ratio results in information from more sessions, and a lower ratio results in information from fewer sessions. With the ratio of 1:1, information is shown from all sessions.
  - In one or both of the fields Registry to track and Folders to track, restrict the User Setting to a single registry tree in HKEY_CURRENT_USER and/or to a single folder tree in the user profile directory.
  - Optionally, use the field Process(es) to track to restrict the User Setting so that it only tracks changes made by one or more specific processes.
    - You can enter just a process name (such as regedit.exe), or you can specify an exact path (such as C:\windows\system32\regedit.exe).
    - Separate multiple entries with a semi-colon (;).
    - If you restrict the User Setting to a process that also uses subprocesses for certain changes, include these subprocesses in the Process(es) to track field.
  - On the Excluded Items tab, create a list of all the settings that should not be preserved.
  - When specifying paths and names anywhere in User Settings, you can use:
    - wildcards *, ?, [charlist] and [!charlist].
    - special folders (see Variables and special folders (on page 277)) to specify files, folders or folder trees in the user profile directory, as well as the default Microsoft Windows known folders (also called special folders in Microsoft Windows XP and earlier versions of Microsoft Windows) and any other special folder that may exist on the computers in your environment.
  - Select Any file larger than to determine the maximum size of the User Settings files and folders to be excluded and enter a number in KB, MB, GB.

Sampling

- If the Sampling Mode is enabled (only available in Advanced User Settings view), the Sampling tab shows the settings that were preserved and/or applied during the sampled sessions.
- On the Sampling tab:
  - settings that are part of an Excluded Item are not shown.
  - right-click a sampled setting and convert it into an Excluded Item or into a User Registry Setting.
  - use Ctrl+F to search for a specific sampling entry.
  - You can group the information by dragging column headers to the grouping area. To restore the original view, drag the column headers back to the column bar.

Note

- If Windows Shell shortcut creation is set to Replace all unmanaged shortcuts, this may lead to unpredictable results for global User Settings that preserve information in %desktop%, %startmenu% or %appdata%\Microsoft\Internet Explorer\QuickLaunch. This does not affect application-level User Settings for those folders.
- If changes handled by a subprocess should be included in the tracking and sampling of a global User Setting in the Zero Profile mode Track any changed setting within scope immediately, the subprocess must be authorized at Security > Global Authorized Files.
- When testing User Settings, please note that manually renaming registry keys may lead to unexpected results. To test User Settings, always use the proper application or Microsoft Windows feature to implement changes.
Track any setting changed by application immediately (application)

Use the Zero Profile mode to preserve all changes that the application's process makes in the registry at HKEY_CURRENT_USER and to files and folders in the user's appdata folder.

Configuration Advanced User Settings

- The Tracking and Sampling tabs are only available in Advanced User Settings view.
  - If an application in this Zero Profile mode runs in sampling mode, its Sampled Data tab shows the settings that were preserved and/or applied during the sampled sessions.
  - The Sampling ratio controls the number of sessions from which information is logged. A higher ratio results in information from more sessions, and a lower ratio results in information from fewer sessions. With the ratio of 1:1, information is shown from all sessions.
  - The value set for the option Start tracking changes determines when Workspace Control should start tracking the changes to be processed.
    - The default Start tracking: After application has started and is ready to be used is useful if the application loads and processes user-related settings after it has started up. Postponing the tracking until the application is ready for use filters out irrelevant changes from the Sampled Data tab. With this option, changes are only tracked if they are made by this specific managed application.
    - Set Start tracking to immediately when application starts if relevant changes are made during the application's startup process. With this option, tracking is active as soon as the session has started. Any changes made by an unmanaged version of this application will also be tracked.
  - On the Tracking tab:
    - Create a list of all the settings that should not be preserved.
    - When specifying paths and names anywhere in User Settings, you can use:
      - wildcards *, ?, [charlist] and ![charlist].
      - special folders (see Variables and special folders (on page 277)) to specify files, folders or folder trees in the user profile directory, as well as the default Microsoft Windows known folders (also called special folders in Microsoft Windows XP and earlier versions of Microsoft Windows) and any other special folder that may exist on the computers in your environment.
    - You can specify any Extra process(es) to track. This can be useful in case applications use subprocesses.
    - Select Any file larger than to determine the maximum size of the User Settings files and folders to be excluded and enter a number in KB, MB, GB.
  - On the Sampling tab:
    - settings that are part of an Excluded Item are not shown.
    - right-click a sampled setting and convert it into an Excluded Item or into a User Registry Setting.
    - use CTRL+F to search for a specific sampling entry.
    - You can group the information by dragging column headers to the grouping area. To restore the original view, drag the column headers back to the column bar.
Notes

- A User Setting for a specific application is never available to users who do not get the application itself. If Access Control and Workspace Control are set on an application-based User Setting, users only get the User Setting if they meet both the criteria for the application and the criteria for the User Setting.
- If the subprocess is listed on the Authorized Files tab of the application's Security section, the subprocess will be processed and, if relevant, sampled as part of the application-level User Setting.
- If the subprocess is listed at Security > Global Authorized Files, changes made through this subprocess will be processed as part of the application-level User Setting, but will not be included in the application's User Setting sampling.
- Application-level Authorized Files are not included in User Setting linking. If an application links to the User Settings of another application, the Authorized Files of the master application must be added to the linked application manually.
- When testing User Settings, please note that manually renaming registry keys may lead to unexpected results. To test User Settings, always use the proper application or Microsoft Windows feature to implement changes.
- With User Settings tracking for applications, in a mixed environment of RES Workspace Manager Console 2012 SR2 or higher and Ivanti Workspace Composer 2012 SR1 or earlier, subfolders of %LOCALAPPDATA%, e.g. %LOCALAPPDATA%\Microsoft, will not be tracked.
7.4.3 Migration settings when switching to another Zero Profile mode

User Settings data is stored in different formats for different Zero Profile modes. When switching an existing global User Setting or application to another Zero Profile mode, use its Migration settings to determine what should happen to data stored in the previous format.

<table>
<thead>
<tr>
<th>Migration Setting &quot;Ignore&quot;</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Effect:</strong></td>
</tr>
<tr>
<td><strong>Other consequences:</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Migration Setting &quot;Remove&quot;</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Effect:</strong></td>
</tr>
<tr>
<td><strong>Other consequences:</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Migration Setting &quot;Apply/Convert and remove&quot;</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Effect:</strong></td>
</tr>
<tr>
<td><strong>Other consequences:</strong></td>
</tr>
</tbody>
</table>
### 7.4.4 Flex Profile Kit INI files

In Citrix and Terminal Server environments, the freeware Flex Profile Kit is sometimes used to store user settings in combination with mandatory profiles. There are, however, several advantages to managing such settings as User Settings in Workspace Control, where they can be managed centrally in a fully supported and enterprise-ready system.

Flex Profile Kit stores information in INI files. The information from such INI files can be imported directly into Workspace Control User Settings.

**Importing Flex Profile Kit settings into User Settings**
- Have the relevant INI file(s) available in an accessible location.
- Create a new User Setting, either at Composition > User Settings or on the User Settings tab of an application at Applications.
- Click Add > Import > Flex Profile Kit and select the relevant INI file. The settings stored in that INI file appear in the User Setting immediately.
- Close the User Setting. The list of User Settings now includes the settings that were previously handled through the Flex Profile Kit.

### 7.4.5 What is saved as part of a Targeted Item

<table>
<thead>
<tr>
<th>A Targeted Item for a:</th>
<th>saves:</th>
<th>but does NOT save:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registry tree</td>
<td>all the keys and subkeys in the specified tree, and the values in those keys</td>
<td>subkeys and their values</td>
</tr>
<tr>
<td>Registry key</td>
<td>the specified key and all the values in it</td>
<td>subkeys and their values</td>
</tr>
</tbody>
</table>
| Registry value         | the specified value | • other values in the same key  
|                        |                     | • subkeys and their values. |
| Folder tree            | all the files and folders in that tree, including subfolders and their files | subfolders and their files |
| Folder                 | the specified folder and its file | subfolders and their files |
| File                   | the specified file | • other files in the same folder  
|                        |                     | • subfolders and the files in them |

**Notes**
- In all cases, parent keys or parent folders will be empty, except for the keys or folders in the path to the User Setting to be stored.
- If you set a registry key as exception to a User Setting, the values in that key will NOT be stored, but any subkeys and their values will.
- If you set a folder as exception to a User Setting, the files in that folder will NOT be stored, but any subfolders and their contents will.
7.4.6 Storage of users’ User Setting data

Storage method

Each User Settings is stored as a separate (compressed) file with a GUID as its file name, and with a file extension that indicates its content type.

If the option Allow users to restore their own settings is enabled, additional files may be created with sequence numbers related to the value set for Number of sessions to keep.

<table>
<thead>
<tr>
<th>Application-level User Settings with “Track specified settings on application start/end”</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>GUID:</td>
<td>GUID of the individual Targeted Item</td>
</tr>
</tbody>
</table>
| File name: | • [GUID].UPR for registry information  
• [GUID].UPF for file and folder information |
| Data for rollback: | Contained in additional files with a sequence number per session:  
• [GUID].UPR_h[n]  
• [GUID].UPF_h[n]  
(where [n] is the session number) |

<table>
<thead>
<tr>
<th>Application-level User Settings with “Track any setting changed by application immediately”</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>GUID:</td>
<td>GUID of the application</td>
</tr>
</tbody>
</table>
| File name: | • [GUID].UPR2 for registry information  
• [GUID].UPF2 for folder tree information |
| Data for rollback: | All data, including rollback data, is contained in a single file. |

<table>
<thead>
<tr>
<th>Global User Settings with “Track specified settings on session start/end”</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>GUID:</td>
<td>GUID of the individual Targeted Item</td>
</tr>
</tbody>
</table>
| File name: | • [GUID].UPR for registry information  
• [GUID].UPF for file and folder information |
| Data for rollback: | Contained in additional files with a sequence number per session:  
• [GUID].UPR_h[n]  
• [GUID].UPF_h[n]  
(where [n] is the session number) |

<table>
<thead>
<tr>
<th>Global User Settings with “Track any changed setting within scope immediately”</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>GUID:</td>
<td>GUID of the User Setting</td>
</tr>
</tbody>
</table>
| File name: | • [GUID].UPR2 for registry information  
• [GUID].UPF2 for folder tree information |
| Data for rollback: | All data, including rollback data, is contained in a single file. |
Central storage location of User Settings and other user-specific information

In a user's session, the central storage location stores the file PWRUSER.ini and other user-specific information. User Settings files are stored in a subfolder (\UserPref) of the central storage location.

The central storage location is defined on the Settings tab at Composition > User Settings, at Central storage location.

The default central storage location is the hidden folder \Personal Settings on the user's homedrive. Its location can be customized to:

- A mapped network drive letter and folder name.
- Any path in UNC format.

Environment variables from both Microsoft Windows and Workspace Control can be used. Always ensure that this path is unique per user, for example by including %username%. (Otherwise, files from multiple users could get mixed together in a single location.) Users need Full control permissions on the folder that is used as Cache location for their User Settings.

You can define different locations for different Workspace Models.

Locally cached User Settings ("User Settings caching" on page 270) files are synchronized to the central storage location automatically at the end of each session.

Note

Support for a UNC path as central storage location was introduced in RES Workspace Manager 2012 SR1 and is not backwards compatible. Should you need to downgrage to a version prior to that, please first ensure that the central storage location refers to a folder on <homedrive> or on a mapped network drive letter.
Migration

When you change the location for Storage of user settings, the value set for Migration Settings (also at Composition > User Settings) determines what will happen to Workspace Control data currently stored in the original location.

<table>
<thead>
<tr>
<th>Option</th>
<th>Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ignore</td>
<td>The stored user settings data remains in the old location, but it is not used or updated. At their next logon, users will initially get the default settings. They will gradually build up a new set of data in the new location. Eventually, two sets of data will exist for each user, in both locations. In that situation, switching the storage location back to previous value results in a switch to the settings that are stored there.</td>
</tr>
<tr>
<td>Copy</td>
<td>The stored user settings data is copied to the new location and is used and updated from there. At their next logon, users get their customized settings as usual. The data also remains in the old location, but it is not used or updated there.</td>
</tr>
<tr>
<td>Move</td>
<td>The stored user settings data is moved to the new location and is used and updated from there. At their next logon, users get their customized settings as usual.</td>
</tr>
</tbody>
</table>

For the options Copy and Move to work as expected, please make sure that:

- Previous storage location is filled in correctly.
- The previous storage location is accessible to users at their next logon, until all stored user settings have been migrated.
User Settings caching

User Settings are always stored centrally, in the central storage location ("Central storage location of User Settings and other user-specific information" on page 268). Optionally, User Settings can also be cached locally.

Locally cached User Settings are available even if the central location is not available, for example on a laptop that is not logged on to a network. Local caching can also improve performance on persistent desktops, as there is no need to copy a User Setting from the central location to the Agent (unless it has changed since the user’s last session). However, cached tracked User Settings are not immediately available across multiple simultaneous sessions. Depending on the configuration of the caching feature, cached files are synchronized at the end of the session.

Caching policy

The User Settings caching policy is determined (per Workspace Model) at Composition > User Settings > User Settings caching:

- Cache locally at logon and logoff, unless otherwise specified.
- Cache locally at logon, during the session, and at logoff, unless otherwise specified.
- Do not cache locally, unless otherwise specified.

On a managed application or on a global User Settings container, use the Advanced User Setting option Override local caching and choose Always cache or Never cache to overrule the User Settings caching policy.

Terminal Servers are automatically excluded from all User Settings caching. All sessions on Terminal Servers use User Setting files from the central storage location.

Cache location

The cache location is determined at Composition > User Settings > Cache location. The default cache location for User Settings is %localappdata%\RES\WM\UserPref. This location is inside the user profile, and is therefore not suitable for environments with mandatory user profiles, or when a fresh user profile is created. In such cases, specify a different path. Always ensure that this path is unique per user, for example by including %username%. (Otherwise, files from multiple users could get mixed together in a single location.) Users need Full control permissions on the folder that is used as Cache location for their User Settings.

A cache location must be a folder on the local hard drive of the Agent running the session. If the folder does not exist, Workspace Control will try to create it. If it fails to create the folder, or if the specified cache location is invalid, User Settings caching is not possible. If available, the User Settings will then be retrieved from the central storage location instead.
Synchronization between central storage location and cache location

The in-built User Settings synchronization process uses a customized synchronization method that is more efficient than other file synchronization methods, as it is optimized for the User Setting mechanism and file structures.

Synchronization between the central drive and the local cache only takes place if the central storage location is available. Without synchronization, User Settings are not uniformly available across sessions on different devices.

The timing of caching is as follows:

- Global User Setting files are synchronized at session start, session end and optionally during the session at defined cache intervals (ranging from 1 minute to 8 hours).
- Application-level User Setting that are preloaded are synchronized in the background at session start, and when the User Settings are stored. Depending on configuration, this can be at application or session end, or during the session at a predefined cache interval.
- Application-level User Setting that are not preloaded are pre-cached in the background at session start and are synchronized when the application starts and when the User Settings are stored. Depending on configuration, this can be at application or session end, or during the session at a predefined cache interval.
7.4.7 Additional User Setting options

Sampling

Sampling is an advanced User Setting and only available in the Advanced User Settings view.

Run a User Setting in sampling mode to obtain information about which settings are changed by users and/or preserved as a User Setting. Sampled information can help you determine:

- which settings users change, but which are lost. You could consider creating User Settings for these settings.
- which changed settings are preserved for users, while they should instead be kept at their default value. You could consider creating User Setting exceptions for these settings, so that users’ changes to these settings are not preserved.
- which settings users always set to specific values. You could consider creating registry setting Actions for these settings to ensure that the desired value is already available for users, depending on their context.

Application-level User Settings

<table>
<thead>
<tr>
<th>Zero Profile mode</th>
<th>Sampled Data</th>
</tr>
</thead>
</table>
| Track any setting changed by application immediately | shows all the registry, file and folder changes that are preserved. Settings that are excluded are not shown.  
  - Right-click an entry and choose Convert selected entry to User Setting exclusion if the setting should not be preserved in future. |
| Track specified settings on application start/end | shows all the changes that are made in user sessions but that are not preserved.  
  - Right-click an entry and choose Convert selected entry to User Setting if the setting should be preserved in future.  
  - Right-click an entry and choose Convert selected entry to PowerLaunch setting if the setting should be set as part of PowerLaunch in future. |

Global User Settings

<table>
<thead>
<tr>
<th>Zero Profile mode</th>
<th>Sampled Data</th>
</tr>
</thead>
</table>
| Track any changed setting within scope immediately | shows all the registry changes that are preserved. Settings that are excluded are not shown.  
  - Right-click an entry and choose Convert selected entry to User Setting exclusion if the setting should not be preserved in future. |
| Track specified settings on session start/end | is not available. |
Sampling ratio

The Sampling ratio controls the number of sessions from which information is logged, and therefore it controls the amount of data shown on the Sampled Data tab. Optionally, set a higher ratio to view information from more sessions, or set a lower ratio to see information from fewer sessions. With the ratio of 1 out of 1, information is shown from all sessions.

The Event Log in a user's Workspace Analysis shows whether sampling was active during a specific session.

Notes

- To include an application subprocess in an application-level User Setting in the Zero Profile mode Track any setting changed by application immediately, the subprocess must be listed as an Authorized File:
  - If the subprocess is authorized on the Authorized Files tab of the application's Security section, the subprocess is included in the application's Sampled Data.
  - If the subprocess is listed at Security > Global Authorized Files, changes made by this subprocess are preserved as part of the application-level User Setting, but are not shown in the application's Sampled Data.
- If files, folders or folder trees containing User Settings are excluded based on size and/or date at Composition > Applications on the User Settings > Tracking tab, these will be added when the application is in sampling mode, but with the note that they will be excluded due to size and/or date.
Linking

If several applications need the same set of User Settings, you do not need to configure this set for each application. Instead, an application can use the User Settings of another application. When the set of User Settings changes, all the applications that use these User Settings will automatically reflect these changes too. This saves configuration and maintenance time, and ensures that multiple applications have identical User Settings.

This is useful, for example, if you need a duplicate of an existing application in order to test out a new version of the application. Another example could be to avoid duplication if multiple applications share the same settings.

- The application with the original set of User Settings cannot itself use the User Settings of another application.
- When you edit linked User Settings, Workspace Control will open the application from which the User Settings originate.
- The application with the original set of User Settings cannot be deleted while other applications still use its User Settings. When you unlink an application, you can choose whether to create a copy of these User Settings for the application.
- When you create a Building Block containing an application that is linked to the User Settings of another application, the Building Block will recreate this link when importing the Building Block again. If necessary, it will also recreate the application from which the User Settings originate.
- If the source application uses Zero Profile mode, you should set Track any setting changed by application immediately with Authorized Files to track changes made by application subprocesses; these Authorized Files must be added to the linked application manually.

On the User Settings > Properties tab of an application, the option Use the User Settings from the following application is available under the Advanced User Settings.

- The option Override settings from linked application allows you to control whether the values stored for the shared User Setting should actually be loaded when the child application is used; and whether changes that the user made while using the child application should be preserved afterwards. This can be useful in specific migration scenarios. The Override option works if only one of the linked applications (either the source application or one of the child applications) is accessible in the user session. In sessions where two or more of these applications are accessible, the User Settings will be applied if one of the linked applications is configured to do so; and preserved if one of the linked applications is configured to do so. Hidden or disabled applications are still considered accessible in the user session.
- The Override option is not supported for any type of virtual application.
Chapter 7: Composition

Allow users to restore their own settings

An application-level or global User Setting becomes available for rollback in the Restore User Settings wizard if the option Allow end users to: Restore settings from previous session(s) is selected for that User Setting AND if the user has actual stored settings for that User Setting.

For applications, if the option Restore application to default configuration is selected, the user can revert the application to its original configuration.

The Restore User Settings wizard is available on the Other tab of the user's Workspace Preferences tool.

The Restore User Settings wizard can also be made available as a separate application in the user's workspace. To do so, create a Managed Application that refers to pwrgate.exe in its command line with the command line parameter -15.

It is also possible to restore a user's User Setting to a previous value from the Workspace Control Console. This allows the administrator to remotely revert a User Setting for a specific user to a previous state, without the user having to use the Workspace Preferences tool. For applications, the administrator can also revert to an application's default configuration for a specific user from the Console.

The wizard can be found at:

- Diagnostics > User Sessions > Context menu
- Diagnostics > Workspace Analysis > Workspace Analysis Details > Composition > User Settings > Context Menu
- Diagnostics > Workspace Analysis > Workspace Analysis Details > Composition > User Settings > View User Setting

Notes

- The option Restore application to default configuration is only available if the Zero Profile mode for the application is set to Capture targeted items on application/session end.
- When reverting to an application's default configuration, all registry values, files and folders configured in the User Settings for the application will be cleared or deleted from the user profile.
- When using the option Restore application to default configuration, it is recommended to select the option Empty target when applying user setting for the captured settings (only applicable to Registry key/Registry tree/Folder/Folder tree). This will delete any existing settings that are not overwritten by the User Setting, which can be useful in case the application leaves settings behind that it should have cleaned up.
- Before enabling Restore application to default configuration for an application, it is advised to first test if the application will launch correctly with its default configuration. If this causes problems with the application, you might want to consider only enabling the option Restore settings from previous session(s).
Save printing preference

If printers are made available through user workspace management, you can set Workspace Control to preserve users’ changes to their default printer settings. To do so, enable this option at Composition > User Settings > Save printing preference.

Workspace Control will handle the technical rules to preserve the correct printer settings for each user.

Applications User Settings

It is possible to change the behavior of the timing of loading User Settings for applications. At Composition > User Settings two options are available for prefetching User Settings:

- **Prefetch in background, check on application start**: this is the default behavior. The User Settings for applications are loaded in the background during session startup. When a user starts an application, Workspace Control checks if the latest User Settings for the application have been prefetched in the background (based on the timestamp of the user settings file). If this is not the case, the latest User Settings are loaded before the application is started.

- **Apply on application start (requires managed shortcut)**: the User Settings are not loaded during session startup, only the first time an application starts its User Settings will be loaded.

- On the User Settings tab of an application, you can choose either setting as the default for that application (i.e. make an exception to the set default) or choose the setting that has the (default) prefix.

- The setting will then be equal to the one set at Composition > User Settings (and will be changed accordingly if the default is modified).

Override local caching

It is possible to change the location where User Settings for applications are stored. The Advanced User Setting Override local caching, allows you to set exceptions for specific applications:

- **Always cache locally** - can be used if local caching is disabled on a Global level, but you want to cache User Settings for this application locally.

- **Never cache locally** - can be used if local caching is enabled on a Global level, but you do NOT want to cache User Settings for this application locally.
Variables and special folders

When specifying paths and names anywhere in User Settings, you can use:

- the wildcards *, ?, [charlist] and [!charlist].
- the default Microsoft Windows known folders (also called special folders in Microsoft Windows XP and earlier versions of Microsoft Windows) and any other special folder that may exist on the computers in your environment.
- the following special folders to specify files, folders or folder trees in the user profile directory:

<table>
<thead>
<tr>
<th>Item</th>
<th>File System Directory</th>
</tr>
</thead>
<tbody>
<tr>
<td>%appdata%</td>
<td>Contains application data for all users. This folder is used for application data that is not user specific.</td>
</tr>
<tr>
<td>%cache%</td>
<td>Common repository for temporary Internet files.</td>
</tr>
<tr>
<td>%cookies%</td>
<td>Common repository for Internet cookies.</td>
</tr>
<tr>
<td>%desktop%</td>
<td>Stores file objects on the desktop.</td>
</tr>
<tr>
<td>%favorites%</td>
<td>Common repository for the user’s favorite items.</td>
</tr>
<tr>
<td>%history%</td>
<td>Common repository for Internet history items.</td>
</tr>
<tr>
<td>%localappdata%</td>
<td>Data repository for local (non-roaming) applications.</td>
</tr>
<tr>
<td>%mymusic%</td>
<td>Common repository for music files.</td>
</tr>
<tr>
<td>%mypictures%</td>
<td>Common repository for image files.</td>
</tr>
<tr>
<td>%myvideo%</td>
<td>Common repository for video files.</td>
</tr>
<tr>
<td>%nethood%</td>
<td>Contains the link objects that may exist in the My Network Places folder.</td>
</tr>
<tr>
<td>%personal%</td>
<td>Stores a user’s common repository of documents.</td>
</tr>
<tr>
<td>%printhood%</td>
<td>Contains the link objects that can exist in the Printers folder.</td>
</tr>
<tr>
<td>%programmenu%</td>
<td>Contains the user’s program groups (which are themselves file system directories).</td>
</tr>
<tr>
<td>%recentfiles%</td>
<td>Contains shortcuts to the user’s most recently used documents.</td>
</tr>
<tr>
<td>%sendto%</td>
<td>Contains Send To menu items.</td>
</tr>
<tr>
<td>%startmenu%</td>
<td>Contains Start menu items.</td>
</tr>
<tr>
<td>%startupmenu%</td>
<td>Corresponds to the user’s Startup program group.</td>
</tr>
<tr>
<td>%templates%</td>
<td>Common repository for document templates.</td>
</tr>
<tr>
<td>%userprofile%</td>
<td>Contains the user profile.</td>
</tr>
</tbody>
</table>
7.4.8 Microsoft App-V applications

Version 4.x

When you create a managed Microsoft App-V 4.x application in Workspace Control based on an OSD file, User Settings are automatically enabled for the application. It will run in the Zero Profile mode Track specified settings on application start/end and it will have a hidden Targeted Item for the folder %APPDATA%\SoftGrid Client\<SGAPPGUID>. This is where the application will store all its user-specific changes, in a PKG file containing deltas as compared to the original App-V package.

If you use an App-V package that contains a set of applications, then all the user-specific data for these applications is stored in the same PKG file. In the default setup, this results in a duplication of stored user settings data, because the same file is stored for each application that uses it. To prevent this, disable User Settings for all the applications in the set. Instead, create a single global User Setting to cover the set of applications.

There is a method to achieve this:

- create a global User Setting in Zero Profile mode Track specified settings on session start/end with a Targeted Item for the specific subfolder of %appdata%\SoftGrid Client where the PKG file of the relevant App-V package is stored; or, if your Workspace Control site includes several App-V packages containing sets of applications, using this option requires a global User Setting for each package.

Ensure that User Settings are disabled for the applications that are covered by the global User Setting.

Version 5.x

The configuration of User Settings for Microsoft App-V 5.x applications is similar to installed applications. All Zero Profile modes and User Settings options are supported.

For Microsoft App-V 5.x applications, when selecting Track any setting changed by application immediately for Zero Profile mode, the Registry to track (on the User Settings > Tracking tab of the application) must be HKEY_CURRENT_USER. If this registry is changed, no User Settings can be tracked for this Microsoft App-V 5 application.

Please refer to User Settings (on page 256) for more information on how to configure User Settings.

<table>
<thead>
<tr>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>- The Zero Profile mode and the Targeted Items can be edited for Microsoft App-V 4.x applications. To view the hidden Targeted Item and its contents, select Show all User Settings and Show Details at Composition &gt; User Settings.</td>
</tr>
<tr>
<td>- When creating Microsoft App-V managed applications, the folder to be captured for Microsoft App-V packages, %appdata%\SoftGrid Client&lt;SGAPPGUID&gt; (specified in the Data column on the Capturing tab after selecting Show details), is predefined and cannot be changed.</td>
</tr>
</tbody>
</table>
Chapter 8: Security

Security restrictions in Workspace Control help you secure the user workspace at different levels:

- **Applications**: prevents the use of unauthorized applications and executables.
- **Removable Disks**: secures the use of removable disks.
- **Files and Folders**: prevents the use of specific file types and folders.
- **Read-Only Blanketing**: renders all local drives on servers and desktops read-only.
- **Global Authorized Files**: allows you to authorize files, folders and drives.
- **Network**: prevents unauthorized network connections.
- **Sessions**: restricts users to a single Workspace Control session at a time.

Except for security restrictions on network level, all security restrictions are based on kernel mode drivers, that offer a high level of security while minimizing the overhead on your system. Security restrictions on network level are based on the NetGuard driver, which is similar to the other drivers, but secures your network connectivity. The RESNFLT driver offers browser independent Website Security.

System processes (such as `svchost.exe`) are also subject to Security. This means that these processes cannot start sub-processes (such as e.g. Windows Media Player or MP3 files) indirectly. **Authorized Files** (on page 294) contains a default rule that allows you to control this behavior.

In general, if security restrictions are enabled, all executables that exist in the user’s Start Menu are accessible to the user. All other executables are inaccessible.

**Search engine on Log tabs**

On the Log tabs, by default, the first 100 log entries are automatically shown when clicking **Search**. When the option **Show last 100 entries only** is not checked, the log view will be cleared. You can then search for the desired log entries.

Except on the **Authorized files > Log** tab, a **More** button is present on the Log tabs. Clicking this button allows you to group your search (**Group By**) or specify a **Date / Time Filter** for your search. The **# incidents** at the bottom of the overview is dynamic.
8.1 Applications

8.1.1 Managed Applications

With security restrictions on Applications, you can prevent unauthorized applications and executables from being used in the user workspace. This prevents potentially harmful applications and executables from causing damage.

- Only applications that are made available to the user through Workspace Control are authorized. All other applications are unauthorized, and are prevented from starting.
- Users are prevented from running executables that they received through e-mail or Internet. This prevents potentially dangerous executables containing viruses, spyware and malware from contaminating the corporate network.
- Users are prevented from using advanced commands in the command box.

You can configure Managed Application Security on a global level at Security > Applications > Managed Application, and on application level at Composition > Applications, on the application's Security > Authorized Files tab.

Notes

- File types other than executables (for example PDF, DOC or VBS) are accessible by default. You can block these file types (and folders) by configuring security restrictions on Files and Folders. See Files and Folders security (on page 291).
- The Workspace Control Agent for Linux and Apple Mac OS X supports the Managed Applications Security feature, providing the capability to allow or block executables in user sessions based on Authorized Files with MD5, SHA-1, and SHA-256 file hashes.

Applications security modes: disabled, learning, enabled

Global level

On global level, there are three modes for the security restrictions on Applications:

- In Disabled mode, users can start applications and executables that are not managed by Workspace Control and no data is logged.
- In Learning mode, attempts to start unauthorized applications and executables will not be blocked, but can be logged. This helps you identify and authorize any executables that are started by authorized applications. When you have fine-tuned your environment sufficiently in Learning mode, you can set Application security to Enabled mode.
- In Enabled mode, only authorized applications and executables can be started. This prevents users accessing any unauthorized file, folder, or executable

Notes

- If you select the option Log security events, security events will be logged if Applications security is in Enabled or Learning mode.
- If you select the option Notify users about security events, users will be notified if Applications security is in Enabled or Learning mode.
- File hashes can only be discovered for Workspace Containers. Managed Application Security must then be set to Enabled or Learning for that Workspace Container. In Learning mode all discovered file hashes are displayed in the log. In Enabled mode, the file hashes for blocked processes and files are not displayed. See the Workspace Control Help for more information.
Application level

If you add a new application, it is not necessary to set Applications security to learning mode on global level, because this jeopardizes the existing security of the user workspace. Instead, it is sufficient to set only the new application to learning mode. The workspace remains secured, because only executables launched by the application will be allowed. Because these executables can be logged as a security event, this allows you to create application-specific exceptions.

If Applications security is enabled, the authorized files configured for a specific application will, by default, be enforced. You can configure authorized files for an application at Managed Applications on the application's Security > Authorized Files tab. See Authorizing files and folders.

Note

If the user is allowed to use the 'cmd' command, any attempts to start executables will be blocked (e.g. a ping command). If necessary, you can authorize additional executables at application level.

Default behavior if running applications are no longer authorized

The availability of an application can be authorized, for example, based on a Locations and Devices zone. Once an application is running in a user session, it can remain active if the user shuts down the computer without logging off from the session. Then, if the user logs on from another computer outside of the zone that authorized the application, the application may still remain active despite its lack of authorization. Similarly, the application may remain active even if the user is no longer a member of the Active Directory group that was the basis for the user's access to that application.

You can configure the default behavior for applications in such situations at Security > Applications.

- With the setting If running application is no longer authorized, terminate application, the application is terminated immediately (and abruptly) as soon a change in circumstances or configuration causes the user's authorization to disappear.
- If this is not necessary or desirable, for example because the application must be closed down correctly in order to prevent data loss, you can choose If running application is no longer authorized, do nothing.
- The option Default behavior if running application is no longer authorized evaluates an application's file hash as well.

To set different behavior for an individual application, open the application at Composition > Applications and change the setting on the tab Security > Authorized Files.
Logging

If Managed Application Security is enabled, the overview on the Log tab shows who accessed which authorized/unauthorized files on which computer. Unauthorized files can be authorized via the context menu on this tab.

With Discover new file hashes enabled (on the Settings tab of a Workspace Container), automatically discovered file hashes will be added to the log.

Select Import file hashes from the context menu to import either a comma delimited CSV file or a tab delimited TXT file.

All Applications security events are logged in the Applications Log (on page 182). This log shows an overview of all events that occurred when users were prevented from starting an unauthorized executable. The log is automatically cleaned up periodically.

Many applications need to start up other, legitimate executables in order to function properly. For example, some application Help features will call on an executable. If that executable is blocked, the user cannot access the Help. You can allow these specific executables to run in your environment by authorizing them from the Applications Log. These specific executables will be set as Global Authorized Files.

The Application Security log file can be exported in XML format via a command line (case insensitive): `PWRTECH.EXE /EXPORTLOG /TYPE=APPLICATION /OUTPUT=<OUTPUT FILEPATH> /START=<START DATE> /END=<END DATE>`. A value for OUTPUT must be specified. START and END are optional values with a YYYYMMDD (optionally YYYYMMDDHHMMSS) format. Data entered for START and END, and timestamps in the export file are all in UTC.

Example:

`PWRTECH.EXE /EXPORTLOG /TYPE=APPLICATION /OUTPUT=C:\LOGS\APPLICATIONLOG.XML /START=20160101082959 /END=20160229`

At least read permission is needed on the Managed Applications node (at Security > Applications > Managed Applications) to export the log. With insufficient access rights, the XML export file will contain no data.
8.1.2 User Installed Applications

At Security > Applications > User Installed Applications you can configure User Installed Applications. User Installed Applications give users the right to install software on specific computers. This can be particularly useful to give expert users a degree of control over their own computer, so that they can install software themselves as and when needed. User Installed Applications are always restricted to specific computers, based on Workspace Containers and/or Zones, and can optionally be further restricted to specific users.

For example, a department may be in the process of developing a new application. They receive new versions several times a week, and each version needs to be installed before it can be tested. It is extremely inefficient for the administrator to have to do this each time. Instead, you can enable User Installed Applications with Access Control set to specific people in that department, and Workspace Control set to a Workspace Container that holds the computers in that department. As a result, the specified users can install the updates on the specified computers.

Similarly, a small number of people might use a highly specialized software package such as AutoCAD. They may well know more about the software than the administrator does, and so it makes more sense to allow them to install the AutoCAD updates or extensions themselves.

Users who are allowed to install User Installed Applications on a computer, get an extra tab in their Workspace Preferences tool, the Other tab. From this tab users can install software using a wizard. With this wizard, they can create shortcuts for these applications in their Start menu, on their Desktop, on their Quick Launch bar and in their Startup items. These applications can also be deleted via the Workspace Preferences tool and be changed.

Configure User Installed Applications

- There are three modes in which the User Installed Applications functionality can run (configured on the Settings tab):
  - **Allow any setup to run** - Any application may be installed by the user if the user has local administrator rights.
  - **Blacklisting** - Any application may be installed by the user, except applications that comply with a set Deny rule. Note that by using Access Control and Workspace Control it is possible to set a global Deny rule in combination with a specific Allow rule (e.g. Deny all software installations by a specific Publisher, but allow this for a specific Group). All Deny rules are checked for a possible match, if a match is found then all Allow rules are checked for possible exception. If no match is found, the user is notified that this setup is not allowed.
  - **Whitelisting** - No applications may be installed, except applications that comply with a set Allow rule. Note that by using Access Control and Workspace Control it is possible to set a global Allow rule in combination with a specific Deny rule (e.g. Allow all software installations by a specific Publisher, but deny this for a specific Group). All Allow rules are checked for a possible match, if a match is found then all Deny rules are checked for possible exception. If a match is found to a Deny rule, the user is notified that this setup is not allowed.

**Note**

In case Administrative Roles are used (at Administration > Administrative Roles), making changes to the setting Software installations is only permitted by Administrative Roles that have Modify access to the Security > Applications > User Installed Applications > Settings tab (on the Settings tab of the Administrative Role).
• User Installed Application Rules (i.e. Allow and Deny rules) can be based on:
  • Publisher in signature
  • Product name in file properties (only in combination with Publisher)
  • Product version in file properties (only in combination with Publisher)
  • Checksum of file (only if no other criteria are selected)
• These values can be entered manually or by browsing to a specific installation file. Note that wildcards are allowed.
• To give a user temporary local administrator rights when installing specified applications, the Software installations mode Whitelisting and Run installation using Dynamic Privileges may be selected. See Dynamic Privileges.

User Installed Applications must always be restricted to specific computers in a Workspace Container or in a Zone. Although you can combine several Workspace Containers and/or Zones, the minimum requirement is one Workspace Container or one Zone.

• Specify the Workspace Container(s) on the Workspace Control tab.
• Specify the Zone(s) on the Access Control tab under Location.
• Optionally, you can restrict the right to install User Installed Applications on the specified computers to specific OUs, groups, users, administrative roles and Identity Director Services. You can specify this on the Access Control tab under Identity.
• Optionally, you can restrict access for a specific time period by specifying a Start and/or End date and time on the Access Control tab under Date and Time.

The Log tab shows who installed or removed what unmanaged applications on which computers.

• You can sort columns by clicking on the column headers. Columns can be moved and resized by dragging and dropping the column headers. In the Options menu, the option Reset all column properties to defaults can be used to restore the columns to their original position and size.
• To filter the view by computer name, select the computer from the Computer drop-down list.
• In the filtered view, click for a list of User Installed Applications on the selected computer.

⚠️ Warning

Users who are allowed to install User Installed Applications on a computer can choose to install any application they like. However, what they install can be monitored (at Security > Applications > User Installed Applications on the Log tab).

💡 Notes

• User Installed Applications do not become available in the Managed Applications node of the Management Console.
• A user can only install unmanaged software if he has the appropriate local privileges to install new software.
• By design, User Installed Applications cannot be installed on Terminal Servers, even if the user session on the Terminal Server complies with all the criteria set for User Installed Applications.

Example

For example, a department may be in the process of developing a new application. They receive new versions several times a week, and each version needs to be installed before it can be tested. It is extremely inefficient for the administrator to have to do this each time. Instead, you can enable User Installed Applications with Access Control set to specific people in that department, and Workspace Control set to a Workspace Container that holds the computers in that department. As a result, the specified users can install the updates on the specified computers.

Similarly, a small number of people might use a highly specialized software package such as AutoCAD. They may well know more about the software than the administrator does, and so it makes more sense to allow them to install the AutoCAD updates or extensions themselves.
8.1.3  Websites

At Security > Applications > Websites, you can enable user specific website filtering based on rules. If Website Security is enabled, it automatically secures the following browsers: Microsoft Edge, Microsoft Internet Explorer, Google Chrome, Mozilla Firefox, and Opera.

There are two methods for using Website Security:

- **Whitelisting** means specific URLs are allowed and all others are denied.
- **Blacklisting** means that specific URLs are denied and all others are allowed.

For fine-tuning purposes, exceptions to the set rules can be made.

**Note**

In case Administrative Roles are used (at Administration > Administrative Roles), making changes to the setting Security method is only permitted by Administrative Roles that have Modify access to the Security > Applications > Websites > Settings tab (on the Settings tab of the Administrative Role).

**Configure Website Security**

- On the Settings tab you may set the feature in learning mode. In Learning mode all rules are applied, but websites are not blocked, only logged.
- You can switch between a Basic and Advanced view on the Settings tab by clicking the Basic Settings / Advanced Settings button. The Basic view presents the most commonly used options, while the Advanced view offers the possibility to secure additional browser processes and logging exclusions, but also allows you to run Website Security in legacy mode instead.
- Additional browsers can be secured by specifying their process names at Additional processes (Advanced setting).
- On the same tab, you can configure the logging of security events:
  - **Log security events** - Enable this option if log entries should be created when Website Security events occur.
    - Click Message to configure security notifications that will be shown if a Website Security event occurs. The security notifications are only shown for http:// events.
    - **Log security events once** - This option only applies to Whitelisting (Security method). When this option is not enabled, please take into account that this will cause a lot of extra log entries.
  - With the option Notify user about security events enabled, in user sessions, to users trying to browse to a blocked website, a notification is displayed (bottom right corner) informing him about the blocked site.
  - **Log all visited websites** - When enabling this option, all visited whitelisted/allowed websites will have the value ALLOW in the Action column on the Log tab, and blacklisted/denied websites the value BLOCK.
    - Please note that enabling this option may produce quite some extra logging in the Datastore.
  - **Specify Logging exclusions** (Advanced setting) to prevent excessive logging. For instance, for white- or blacklisted websites that contain pictures, separate log entries for these pictures might not be desirable. By default, the following extensions are specified as logging exclusions: ICO, JS, CSS, GIF, JPG, PNG and JPEG. This list can be changed.
• Select the Advanced setting Use legacy mode regardless of operating system, to only enable Website Security for Microsoft Internet Explorer 8.
  To enable Website Security for Microsoft Edge, Microsoft Internet Explorer, Google Chrome, Mozilla Firefox, and Opera and any additional processes you specify, do not select Use legacy mode regardless of operating system.
  • The options for Redirected websites, i.e. websites containing iFrames that load a redirected URL in the background, are only applicable for Microsoft Internet Explorer 8 on Operating Systems on which the legacy mode is applied. For Operating Systems for which browser independent website security is enabled, redirected websites are treated like any other, not redirected website.
    • Log security events - Enable this option if log entries should be created for redirected websites that are accessed as a result of iFrames.
    • Notify user with message box - Enable this option to show messages to end users when they are being redirected to another website as a result of iFrames.
• On the Websites tab you may enter allow or deny rules for websites, depending on the method used (configured on the Settings tab).
• Choose the protocol to block (http/https/ftp/all).
• Enter the website to be blocked. Rules may contain an asterisk (*). The asterisks are regarded as wildcards. If an IP address is entered as URL, WebGuard will try to resolve the IP address and the resulting URL will be checked. If you enter a Rule with http://, https:// or ftp://, this prefix will automatically be selected as protocol. If you do not enter a prefix, this must be selected manually. By default this is http://. Sub sites (such as www.res.com/solutions) are supported.
• The default for blacklisting is Allow. Entering only Allow rules therefore, has no effect. Allow rules are exceptions to the Deny rules. A URL is first checked against the Deny rules. If the URL passes this check, i.e. there is no Deny rule for this URL, the web page will be displayed. When a URL has a Deny rule hit, the URL will be checked against the Allow rules. If the URL does match an Allow rule the web page will be displayed despite the matching Deny rule. The Allow rules are used as exceptions to the Deny rules and can be used for fine tuning Websites Security.
• The default for whitelisting is Deny. Entering only Deny rules, therefore, has no effect. Deny rules are exceptions to the Allow rules. A URL is first checked against the Allow rules. If the URL does pass this check, i.e. there is an Allow rule matching the URL, the URL will then be checked against the Deny rules. If the URL has a Deny rule match, the web page will not be shown, despite the matching Allow rule. The Deny rules are used as exceptions to the Allow rules and can be used for fine tuning Websites Security.
• If a Deny rule is configured, you may set a specific Learning mode for that rule:
  • Default learning mode - Use the mode that is selected on the Settings tab.
  • Yes - Always run this rule in Learning mode (indifferent of the setting on the Settings tab).
  • No - Never run this rule in Learning mode (indifferent of the setting on the Settings tab).
• You can configure exceptions to Websites Security, to give specific users on specific locations specific permissions.
• If necessary, you can authorize websites that caused a security event on the Log tab.
• On the Log tab, it is possible to export the log entries to a CSV file.
• You can override the global settings of this feature for specific Workspace Containers.
Notes

- To prevent users from circumventing the applied rules, the following policies are automatically set:
  - **InPrivate browsing.** Internet Explorer 8.0 supports InPrivate browsing mode. When using InPrivate browsing mode, Helper Browser Objects are not active. To prevent users from circumventing WebGuard, the InPrivate mode is disabled. This registry setting can be found at:
    HKCU\Software\Policies\Microsoft\Internet Explorer\Privacy REG_DWORD EnableInPrivateBrowsing
  - **Protected Mode** in Microsoft Internet Explorer 8.0 and higher on Windows 7 should be disabled. This setting is enabled by default. This policy can be found at:\n    Windows Components\Internet Explorer\Internet Control Panel\Security Page\Internet Zone and is by default available in inetres.admx on Microsoft Windows 7 systems.
  - **NoExtensionManagement.** Users should not be able to disable WebGuard. To prevent users from disabling WebGuard the NoExtensionManagement registry setting is set. This registry setting can be found at:
    HKCU\Software\Policies\Microsoft\Internet Explorer\Restrictions REG_DWORD NoExtensionManagement
  - **For Website Security based on whitelisting** to work, at least one rules must be configured.
  - **Prerequisites:** Internet Explorer 9 or higher.
  - **For** https:// **URLs,** Workspace Control filters on the base URL only, i.e. https://www.xxxxx.xxx.

Examples

<table>
<thead>
<tr>
<th>Mode</th>
<th>Rules</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blacklisting</td>
<td>*.com - deny</td>
<td>All .com URLs are denied except news.cnet.com</td>
</tr>
<tr>
<td></td>
<td>news.cnet.com - allow</td>
<td></td>
</tr>
<tr>
<td>Blacklisting</td>
<td>company.* - deny</td>
<td>All company URLs are denied except company.de</td>
</tr>
<tr>
<td></td>
<td>company.de - allow</td>
<td></td>
</tr>
<tr>
<td>Blacklisting</td>
<td>*.google.com - deny</td>
<td>The URL <a href="http://maps.google.com">http://maps.google.com</a> will be allowed.</td>
</tr>
<tr>
<td></td>
<td>Maps.*.com - allow</td>
<td></td>
</tr>
<tr>
<td>Whitelisting</td>
<td>*.google.com - deny</td>
<td>The URL <a href="http://maps.google.com">http://maps.google.com</a> will be denied.</td>
</tr>
<tr>
<td></td>
<td>Maps.*.com - allow</td>
<td></td>
</tr>
<tr>
<td>Whitelisting</td>
<td>*.com - allow</td>
<td>All .com URLs are allowed except news.cnet.com</td>
</tr>
<tr>
<td></td>
<td>news.cnet.com - deny</td>
<td></td>
</tr>
</tbody>
</table>
8.2 Data

8.2.1 Removable Disks security

Removable Disks Security is configured at Security > Data > Removable Disks. With security restrictions on Removable Disks, you can secure the use of removable disks in Workspace Control sessions that run on a local computer. Using Access Control, you can give only specific users on specific locations specific permissions to use removable disks. This allows you to increase the security of your organization by preventing unauthorized users from, for example, copying sensitive corporate data to and from floppy disks, DVD/CD disks, USB sticks, FireWire drives, etc., or accidentally infecting the system network with viruses and other malware.

Standard DVD/CD writing functionality of Microsoft Windows is also managed by Removable Disks Security. Specific DVD/CD writing software and software needed to connect to removable media such as smartphones, can be managed with Managed Applications.

Removable Disks Security supports the use of USB hubs.

Removable Disks security modes: disabled, learning, enabled

There are three modes for the security restrictions on Removable Disks:

- In disabled mode, users can access any removable storage device and no data is logged.
- In learning mode, any user actions will not be blocked, but can be logged. When you have fine-tuned your environment sufficiently in learning mode, you can set Removable Disks security to enabled mode.
- In enabled mode, only authorized removable storage devices can be accessed.

Notes

- If you select the option Log security events, security events will also be logged if Removable Disks Security is in learning mode.
- If you select the option Audit allowed write actions, allowed write actions will also be logged if Removable Disks Security is in learning mode.
- If you select the option Notify users about security events, users will also be notified if Removable Disks Security is in learning mode.
Assign permissions to users

You can give specific users on specific locations specific permissions to use removable storage devices.

Permissions

You can assign different permissions (Read and/or Modify) to Floppy Disks, DVD/CD Disks and Removable Disks (e.g. you can assign Modify permissions to Floppy Disks, Read permissions to DVD/CD Disks, and no permissions to Removable Disks).

Files and folders on removable storage devices are not blocked according to the security restrictions on Files and Folders:

- A user with Modify permissions on a removable storage device can always delete, copy, move and rename the files and folders on that device.
- If certain file types are blocked by the security restrictions on Files and Folders, files of this type on the removable storage device cannot be opened unless they have been authorized. You can authorize these files either on global level (from the Log tab or from Security > Global Authorized Files) or on application level (at Managed Applications on an application’s Security > Authorized Files tab). A blocked file can neither be copied nor moved from the removable storage device to other locations. See Authorizing files and folders.

Access Control and Workspace Control

By combining Access Control criteria and Workspace Control criteria, you can create situations where an authorized user can only access a removable storage device at an authorized location on an authorized computer for a specific period of time.

Drive mappings

If a removable storage device is mapped to a drive, Microsoft Windows remembers this mapping and will try to use it again next time the removable storage device is used. If that drive letter is no longer available, the removable storage device does not become visible. To prevent this, select Map Removable Disk to first available drive letter starting from and provide the drive letter of your preference. If you enable this option, Workspace Control will first try to map the drive to the preferred letter. If this is not available, it will proceed alphabetically until a free letter is found. After Z, it will start at A.
Logging

All Removable Disks security events are logged in the Removable Disks Log. This log shows an overview of all events that occurred when users were prevented from accessing a removable storage device. The list specifies time, file name and location, process, computer, user, session, operation, and action. The log is automatically cleaned up periodically.

You can authorize a blocked file from the Removable Disks Log by selecting it and clicking Authorize selected file. This exception can be Execute and/or Modify. Alternatively, you can authorize the file by right-clicking it and then selecting Authorize selected file from the context menu. It will then automatically be added to the Global Authorized Files.

The Removable Disks Security log file can be exported in XML format via a command line (case insensitive): PWRTECH.EXE /EXPORTLOG /TYPE=REMDISK /OUTPUT=<OUTPUT FILEPATH> /START=<START DATE> /END=<END DATE>. A value for OUTPUT must be specified. START and END are optional values with a YYYYMMDD (optionally YYYYMMDDHHMMSS) format. Data entered for START and END, and timestamps in the export file are all in UTC.

Example:
PWRTECH.EXE /EXPORTLOG /TYPE=REMDISK /OUTPUT=C:\LOGS\REMDISKLOG.XML /START=20160101082959 /END=20160229

At least read permission is needed on the Removable Disks node (at Security > Data > Removable Disks) to export the log. With insufficient access rights, the XML export file will contain no data.
8.2.2 Files and Folders security

With security restrictions on Files and Folders, you can prevent specific file types and folders (such as *.vbs, *.avi, or \server\share\folder\*) from being used in the user workspace.

You can configure Files and Folders Security on a global level at Security > Data > Files and Folders, and on application level at Composition > Applications, on the application's Security > Authorized Files tab.

Files and Folders security Mode: disabled, learning, enabled

There are three modes for the security restrictions on Files and Folders:

- In **disabled** mode, users can use any file or folder and no data is logged.
- In **learning** mode, attempts to use unauthorized files and folders will not be blocked. However, you can choose to log these events in the **Log** file. This allows you to fine-tune the security of your environment by authorizing additional files, if necessary. When you have fine-tuned your environment sufficiently in learning mode, you can set Files and Folders security to **enabled** mode.
- In **enabled** mode, unauthorized files and folders cannot be accessed. You can choose to log security events in the **Log** file.

**Notes**

- If you select the option Log security events, security events will also be logged if Files and Folders security is in learning mode.
- If you select the option Notify user about security events, users will also be notified if Files and Folders security is in learning mode.
- If you configure a blocked resource type, Silent mode on the Settings tab will block the resource, but not log a security event. This can be useful if the resource causes many security events, and you want to filter these events from the Files and Folders Log.

Example: block and authorize files

With Files and Folders security, you can set up a situation in which certain files are blocked for general use, but can be accessed by a specific application.

For example:

- MP3 files and AVI files should be blocked for all users.
- Only managers should be allowed to access MP3 files and only when using Windows Media Player.

This setup can be achieved with the following:

- Configure blocked resources in Files and Folders security for the file types *.mp3 and *.avi.
- Add the application Windows Media Player in the Managed Applications node.
- In the Access Control section of the application window, add Management to the list of selected groups.
- In the Security section, select Only Workspace Control is allowed to launch this application.
- Add an authorized file for the file type *.mp3.
Logging

All Files and Folders Security events are logged in the Files and Folders Log. This log shows an overview of all events that occurred when users were prevented from accessing an unauthorized file or folder. The list specifies time, file, process, computer, user, session, operation and action. Use the drop-down box in the lower part of the screen to sort events by date. The log is automatically cleaned up periodically.

You can authorize a blocked file from the Files and Folders Log by selecting it and clicking Authorize selected file. It will then automatically be added to the Global Authorized Files, and access to it will no longer be prevented.
8.2.3  Read-Only Blanketing

At Security > Data > Read-Only Blanketing you can configure Read-only Blanketing. With Read-Only Blanketing, you can render all local drives on servers and desktops in your environment read-only, without touching Microsoft Windows security permissions on files and folders. This allows you to safeguard data against unauthorized access or modification by Workspace Control users, and secures the user workspace against corruption and loss of information.

Read-Only Blanketing allows you to prevent users from:

- Saving data on local drives. If Read-Only Blanketing is enabled, data can only be saved on network drives.
- Accidentally overwriting or deleting system files and other important files on their desktops.

The following folders are automatically excluded from Read-Only Blanketing:

- The Recycle Bin on each local drive
- %userprofile%, %allusersprofile%
- Tmp and temp locations
- Spool in system32 folder
- Debug\usermode in system32 folder
- The server console

Read-Only Blanketing security Modes: disabled, learning, enabled

There are three modes Read-Only Blanketing:

- In disabled mode, users can access and modify data on local disks and no data is logged.
- In learning mode, attempts to access local disks will not be blocked. However, you can choose to log these events in the Log file. When you have fine-tuned your environment sufficiently in learning mode, you can set Read-Only Blanketing to enabled mode.
- In enabled mode, all local drives on servers and desktops are rendered read-only. You can choose to log security events in the Log file.

<table>
<thead>
<tr>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you select the option Log security events, security events will also be logged if Read-Only Blanketing is in learning mode.</td>
</tr>
<tr>
<td>If you select the option Notify users about security events, users will also be notified if Read-Only Blanketing is in learning mode.</td>
</tr>
</tbody>
</table>

Logging

All Read-Only Blanketing security events are logged in the Read-Only Blanketing Log. This log shows an overview of all events that occurred when users were prevented from accessing an unauthorized file or folder. The list specifies time, file, process, computer, user, session, operation and action. Use the drop-down box in the lower part of the screen to sort events by date. The log is automatically cleaned up periodically.

You can authorize a blocked file from the Read-Only Blanketing Log by selecting it and clicking Authorize selected file. Alternatively, you can authorize the file by right-clicking it and then selecting Authorize selected file from the context menu. It will then automatically be added to the Global Authorized Files, and access to it will no longer be prevented.
8.3 Authorized Files

At Security > Authorized Files you can find Authorized Files, with which you can authorize files and folders in the user workspace, and view a list of all authorized files. Files and folders that are authorized on global level can be accessed by all users, but you can still maintain a high level of security in the user workspace by applying Access Control criteria and Workspace Control criteria to each global authorized file.

Before you authorize a file on global level, always consider if the user workspace is better protected if you authorize the file on application level.

8.3.1 Authorize files and folders

You can make exceptions to the global blocking of files by authorizing access to specific files and folders. Authorization can be global, or it can be provided on an application level.

- Grant global access to specific files either through the Authorized Files section, or by authorizing files from the various security logs.
- Many applications need to start up other, legitimate executables or to access specific files in order to function properly. For example, some application Help features will call on an executable. If that executable is blocked, the user cannot access the Help. You could authorize these files and executables on a global level, but this may be undesirable. Instead, you can grant a specific application (rather than all users) the right to access a specific file. This application is then allowed to access the file, but other applications or users are not. You can set access to a file for an application on the tab Security > Authorized Files for the specific application.
- With the security restrictions on Files and Folders, you can block certain file types. You can still authorize individual files of this type on global level (Security > Authorized Files) or on application level (at Managed Applications on an application's Security > Authorized Files tab).
- Authorized file security can be enhanced by checking the executable's file hash. To check file hashes, the Managed Applications security option Only allow authorized file hashes (at Security > Applications > Managed Applications, on the Settings tab) must be enabled and allowed/denied file hashes must be configured.
  - Files hashes can be added, edited, or deleted for Authorized files on application level (at Composition > Applications, on the Security > Authorized Files tab when selecting an Authorized file) and on global level (at Security > Applications > Managed Applications, from the context menu on the Log tab and at Security > Authorized Files, when editing an Authorized file).
  - File hash calculation is done using the Secure Hash Algorithm "SHA-256".
  - File hashes are not displayed in the Authorized files overview (at Security > Authorized Files), but are returned when searching for specific file hashes. If the option Show all Authorized Files is checked, also the file hashes on application-level are included in the search when searching for a specific file hash.
  - On the Authorized Files tab, select Import file hashes from the context menu to import either a comma delimited CSV file or a tab delimited TXT file. File hashes can also be imported using the command line option Pwrtech.exe /importhashes=<file> /createifnotexists. For <file>, the full path to a CSV (comma delimited) or TXT file (tab delimited) must be specified. See Import file hashes (on page 383) in the Command line Options section for more information and examples of import files.
  - You can easily move authorized files from one application to another; from an application to the Authorized Files node; and from the Authorized Files node to a specific application. To do so, right-click one or more selected authorized files and choose Move.
When adding an authorized file or folder to the Global Authorized Files, use the following formats:

<table>
<thead>
<tr>
<th>Format</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>C:\WINDOWS\inf</td>
<td>File or folder with this name</td>
</tr>
<tr>
<td>C:\WINDOWS\inf\</td>
<td>Only this folder</td>
</tr>
<tr>
<td>C:\WINDOWS\inf*</td>
<td>All files and subfolders in folder</td>
</tr>
<tr>
<td>C:\WINDOWS\inf*.txt</td>
<td>All files with the extension .txt in folder and subfolders</td>
</tr>
<tr>
<td>C:\WINDOWS\inf\readme.txt</td>
<td>Only the file Readme.txt in folder</td>
</tr>
</tbody>
</table>

**Note**

- Authorized Files contains a default rule for the system process `svchost.exe`. In some operating systems, this process causes applications to start when double-clicking a file that is associated with it, even when the application is blocked by a security rule. This security rule determines whether `svchost.exe` is allowed to start other unmanaged applications or file associations (such as e.g. Windows Media Player and MP3 files) indirectly. In new Workspace Control environments, the rule is disabled by default. In environments that are upgraded from a previous version of Workspace Control, the rule is enabled by default.

- If you enable Only allow authorized file hashes (at Security > Applications > Managed Applications, on the Settings tab) and want to make sure that Windows universal apps on Microsoft Windows 10 are blocked by Managed Application Security, do one of the following:
  - Disable the default rule for `svchost.exe`.
  - Enable the default rule for `svchost.exe`, but disable Allow any, except denied hashes (on the File Hashes tab of the rule).
8.4 Network Connections security

With the security restrictions on Network Connections, you can restrict access to resources on the network per user workspace.

If Network Security is enabled and the NetGuard driver is not running on the administrator’s system, a message is displayed on that system to inform you that the NetGuard driver is not found or is not running.

Network Connections security can be configured for the entire user session, or for specific applications assigned to the user. If Network Connections security is enabled, users will not be able to start sessions if the NetGuard driver is not running. To allow users to start sessions on such Agents anyway, select Allow session on computers not running NetGuard.

You can configure Network Connections Security on a global level at Security > Network Connections, and on application level at Composition > Applications, on the application’s Security > Authorized Connections tab.

8.4.1 Network Security Modes: disabled, learning, enabled

Global level

There are three modes for the global settings of the Network Security feature:

- In disabled mode, Network Security allows all network connections, and no data is logged.
- In learning mode, Network Security allows all network connections. However, you can choose to log these events. Use learning mode to monitor and evaluate which network connections are used without restricting users in their work.
- In enabled mode, Network Security is enforced: authorized network connections are allowed and unauthorized connections are blocked. You can choose to log attempts to access blocked connections.

**Notes**

- If you select the option Log security events, security events will be logged if Network security is in enabled or learning mode.
- If you select the option Notify users about security events, users will be notified if Network security is in enabled or learning mode.

Application level

If Network Security is enabled or in learning mode, all configured Authorized Connections will be enforced to all applications. If you need to determine which network connections should be authorized for an application, you can run this application’s Authorized Connections in learning mode so that it can still access unauthorized network connections, but these are logged.

Individual blocked connections

If Network Security is enabled or in learning mode, a new blocked connection is set in learning mode by default. This allows you to monitor the use of this connection, which will be allowed but also logged. If the connection should indeed be blocked, the rule must be set in blocking mode.
8.4.2 Security Method: Whitelisting or Blacklisting

The global Network Security feature has two Security Methods: Whitelisting and Blacklisting.

- **Whitelisting** allows no network connections, except the ones that are listed on the Authorized Connections tab.

  Whitelisting gives you full control over the network connections in your environment. Only authorized connections can be accessed. However, for this approach to work, you do need to know exactly which network connections are required in your environment, so that you can authorize them. If you find out someone is trying to access a new network connection that should be allowed, you add that connection to the list of authorized connections. Optionally, Access Control and Workspace Control can authorize the connection only for certain people or workspaces.

- **Blacklisting** allows all network connections, except the ones that are listed on the Blocked Connections tab.

  Blacklisting allows you to block network connections that you do not want users to access. Blocked connections cannot be accessed, all others can. If you find out people are accessing a new network connection that you do not want them to, you add that connection to the list of blocked connections. Optionally, use Access Control and Workspace Control to block the connection for certain people or workspaces.

**Exceptions to blocked connections when Blacklisting**

With Blacklisting, you can create an exception so that certain people, workspaces or processes can access a connection that is blocked for others:

- To allow a process to access a connection that is blocked on the global level, authorize the connection on the application's Authorized Connections tab.

- To allow certain people and/or workspaces to access a connection that is blocked on the global level, create an Authorized Connection on the Authorized Connections tab at Security > Network. Access Control and Workspace Control on this Authorized Connection must result in a subset of the people and/or workspaces that the global blocked connection applied to.

**Create a Blocked Connection for monitoring purposes in Blacklisting environments**

If Network Security is enabled and uses Blacklisting, you can monitor what connections are actually established by setting up a special blocked connection in learning mode. This blocked connection for monitoring purposes ensures that all connections that are not blocked are logged.

To create a blocked connection for monitoring purposes, create a blocked connection with a wildcard (*) in all the fields, and set it in learning mode. Ensure that the blocked connection appears at the very bottom of the list of blocked connections.
8.4.3 Global Network Security and application-based Authorized Connections

Authorize a specific application to use specific connections

- With Network Security enabled and using Blacklisting, use an application-level Authorized Connection to overrule a blocked connection at the global Network Connection Security level.
- With Network Connection Security enabled and using Whitelisting, use an application-level Authorized Connection to add an additional layer of security: the connection is authorized, but only for the process/application. The connection cannot be accessed from another application. For example, if you authorize connection to a specific server group by an SSH Client application, the connection will only be available if it is accessed from the SSH Client. If any other application or process attempts to set up that connection, Network Connection Security will block or log it, depending on its configuration.

Exempt an application from Network Security Settings

To exempt an application from Network Security settings as configured at Security > Network, select Run this application in learning mode. This allows the application to access all network connections, whether they are blocked or not. In learning mode, these network connections are logged.

This setting is useful if you need to determine which network connections should be authorized for a new application, but you do not want to disable Network Security.

8.4.4 Subnet Masks

Many large network environments are divided into subnets to reflect an internal logic, to lower network traffic and to enhance security. For example, if you have a group of Application servers in your network that are managed by a 3rd party, that group often exists in a separate subnet.

With Network Security, you can use subnet masks to block or authorize connections specifically to a subnet. A subnet is defined through a combination of a network (IP) address (for example 172.16.0.0) with a subnet mask (for example 255.255.255.248).
8.4.5 Examples

Whitelisting

In an environment where Network Security is enabled and uses Whitelisting, Workspace Control does not allow any connections by default. The connections that users need to do their job, must be specifically authorized.

For example, it is not enough to give the administrators of a company's Linux servers an SSH client in their Workspace Control sessions. For the administrators to do their work, the SSH client must be authorized to connect to the Linux servers using TCP/IP over a given port. This can be achieved by creating application-level Authorized Connections for the SSH client, authorizing incoming and outgoing TCP/IP communication over port 22 to the relevant hosts.

Additional restrictions can be added as required. For example:

- Workspace Control on the authorized connection can restrict the authorized connection to a specific set of workstations. The authorized connection will only be available from computers in that Workspace, but not from other computers.
- You can create a separate authorized connection for each Linux server, and restrict each authorized connection to a set of specific administrators, so that, for example, only administrators who work in the London office can access the servers for the London office, while only the French administrators can access the servers for the French office.
- Instead of application-based Authorized Connections, you can create global ones with the relevant Access and Workspace Control.

Note

With Whitelisting, the list of blocked connections is ignored.
Blacklisting

In an environment where Network Security is enabled and uses Blacklisting, Workspace Control allows all connections by default. The connections that could be harmful need to be blocked for all users. Furthermore, connections that should be available but only to specific users need to be blocked for everybody, after which specific users should be excepted using an Authorized Connection.

For example:

- Nobody should be able to transfer information over ports 21 and 22, because these ports are often used for transferring information using FTP.
- Connection to the SQL server holding financial data should be blocked for everyone except staff of the Finance department, provided they are logging on from a computer located in the office, not from home.
- Connection to the Linux servers is blocked for everyone, but authorized for the administrators who manage those servers.

This setup can be achieved with:

- Blocked Connections that apply to all users for:
  - the database server holding the financial data
  - the Linux servers
- Authorized Connections configured for:
  - connection to database server holding the financial data with Access Control set to the members of the Finance department and Workspace Control set to the office computers.
  - connection to the Linux servers, with Access Control set to the administrators.
- An additional blocked connection for monitoring purposes so that the connections that are actually established are logged.

Notes

- With Blacklisting, an authorized connection is only useful if it narrows down a blocked connection. For example, there is no point in blocking all traffic over port 22 but specifically allowing TCP/IP traffic over port 23, as that was already allowed.
- With blacklisting, it is also possible to grant access to a specific connection for a specific group. To do so, create a blocked connection for the specific connection. Set Access Control for this connection to the specific group and select Exclude members of Selected group. Now this connection is blocked for everyone not in the designated group.
8.5 User Sessions security

With the security restrictions on User Sessions, you can restrict users to a single Workspace Control session at a time. This improves the performance of your application servers and allows you to manage license usage. It also prevents issues with locked data in a user's home folder, which sometimes occurs when a user tries to access the same data from two sessions simultaneously.

When users try to start a second Workspace Control session, a message shows that they already have an active session, and are not allowed another session. This message can be configured.

- **Allow end users to log on more than once from the same workstation** allows the user to start different applications that are located at different Terminal Servers in the same Workspace Control session. For example, this allows the user to start Microsoft Office at Terminal Server A and a financial application at Terminal Server B in the same Workspace Control session.

- If the option **Allow end users to end/disconnect an already active session** is enabled, end users can end the previous session and proceed with the logon in the second location. If the option **Show list of applications in the already active session** is enabled, they can see which applications are still open in the active session. This can be useful, because any unsaved data in the active session will be lost.

You can find User Sessions security at Security > User Sessions.

8.5.1 Configure different settings for certain parts of the environment

The security restrictions on Sessions apply to the entire Workspace Control environment. However, in certain situations you may want certain parts of the environment to get different settings.

Exclude certain types of users

There are two options to exclude users from the default security restrictions on Sessions based on an Administrative role. This can be useful, for example, for a system administrator that needs to be able to log on at multiple machines, without being hindered by the security restrictions on Sessions.

- With **Allow any user with assigned Administrative Role to log on more than once**, users with an Administrative Role are excluded from the security restrictions on Sessions, and can start several sessions. This applies to any user who has an Administrative Role, whatever that Administrative Role is.

- With **Allow technical managers to log on more than once**, users who have the Administrative Role of Technical Manager are excluded from the security restrictions on Sessions. Users with other Administrative Roles are not excluded from the security restrictions on Sessions.

Exclude passthrough sessions

Passthrough sessions are sessions that occur when a user starts an application that is located on a remote server from his Workspace Control session. When the user starts the application, a new session is started on the remote server to deliver the application to the user's desktop. This can be a Citrix XenApp published application or a Microsoft TS RemoteApp application. With the option **Always allow passthrough sessions**, you can exclude these sessions from the security restrictions on Sessions.

You can read more about Citrix XenApp published applications and Microsoft TS RemoteApp applications in the chapter Integration.
Configure user-specific settings

Workspace Control stores the Sessions settings in the registry at:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\RES\Workspace Manager\Settings\SessionGuard
```

You can override these settings at user level with Workspace Control Registry Settings (Composition > Actions By Type > User Registry).

The configurable settings are:

- AllowEndSession: Yes/No
- AllowFromSameWorkstation: Yes/No
- AllowPassthrough: Yes/No
- AllowShowApps: Yes/No
- AllowSupport: Yes/No
- AllowTech: Yes/No
- Enabled: Yes/No

**Note**

Please note that overriding the default settings in the registry can make it difficult to troubleshoot your environment. It causes behavior that differs from the settings shown in the Management Console. Alternatively, consider if you can create a Workspace with settings different than the global settings. See Configuring different settings for Workspace Containers.

### 8.5.2 Logging

All Sessions Security events are logged in the Sessions Log. This log shows an overview of all events that occurred when users were prevented from starting a new session. The log also shows which action was taken by the user:

- **Exited on user request.**
- **Retried** (if the user logged off the other session manually, and then retried).
- **Logged off other session on client `<CLIENTNAME>`** (if the user opted to let Workspace Control log off the other session automatically).

The log is automatically cleaned up periodically.
Chapter 9: Diagnostics

9.1 Workspace Analysis

At Diagnostics > Workspace Analysis, you can gather information about the settings that are applied to your users during logon. Workspace Analysis can present this information in a general overview of your users and in a detailed overview of a specific user.

If you configured Management Portal Integration (on page 82), use Launch Management Portal to view the Workspace Analysis data.

9.1.1 General information about users

In the Workspace Analysis node, you can get a general overview of the settings that have been applied to your users by entering search criteria:

- The search is always restricted to a specific Directory Service.
- For a full list of all users (in a particular Directory Service), start a search without a filter or search term.
- Select a filter to find specific kinds of users, for example users who are application manager, who have Administrative Roles, who are locked out, etc.

The users that are shown can have the following statuses:

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal</td>
<td>no immediate attention required.</td>
</tr>
<tr>
<td>Dimmed</td>
<td>this user account is unavailable. This could indicate a password lockout or that the user account has been disabled.</td>
</tr>
<tr>
<td>Flagged</td>
<td>there is something special about this account. This user has abnormal rights like technical manager, or a password that never expires. You can configure the triggers for the attention flag on the Properties tab</td>
</tr>
</tbody>
</table>

Settings tab

On the Settings tab of the Workspace Analysis node, you can configure the conditions that will trigger an attention flag and specify how long event logs should be stored.

By default, each user-specific Workspace Analysis shows event logs for 3 consecutive sessions. To change this number, change the value for Number of event logs to keep. Note that event logs are only cleaned up once per 24 hours, indifferent of the number of event logs to keep. For example, if you have specified that event logs for 3 consecutive sessions should be kept, and the user logs on 4 times within 24 hours, 4 event logs will be kept.
9.1.2  **Detailed information about users**

Besides the basic information that is displayed in the overview, you can gather detailed information about a specific user by double-clicking this user or by clicking **Analyze** from the **Action > Workspace Analysis** menu. The analysis is based on:

- whether the user’s current identity meets the Access Control Identity rules currently set for an application or setting (such as OU and group memberships and Administrative Roles).
- whether the actual date and time of the computer on which the Console user is currently running the Workspace Analysis meets the Date and Time rules set for the application or object.
- whether the computer on which the user logged on most recently, met the **Locations and Devices** rules and the Workspace Control rules currently set for the application or setting.

The **Workspace Analysis Details** window contains detailed information about the user’s settings. It is more or less grouped in the same manner as the tree in the Management Console:

<table>
<thead>
<tr>
<th>User Context</th>
</tr>
</thead>
</table>
| **Locations and Devices**: The accessible Zones are based on the client and server that were used when the user last logged on to a Workspace Control session.  
**Account properties**: All properties of the selected user’s account. This contains all information that is available in the “basic” Workspace Analysis, plus account expiration date, e-mail address, last successful authentication, LDAP user entry, assigned Administrative Roles, (in)direct membership, OU information.  
**Workspace Containers**: The Workspace Containers that are currently active for this user. |

<table>
<thead>
<tr>
<th>Composition</th>
</tr>
</thead>
</table>
| The **Applications** section contains the following information:  
**Applications**: All applications that the user has access to, plus who authorized access to the application (if applicable).  
**File Types**: The File Types configured for this user. That is, for which available applications file associations have been configured.  
**E-mail Settings**: E-mail Settings that are attached to applications to which the user has access. E-mail Settings that are not attached to an application, but that do belong to the scope of the user, will not be displayed.  
**Data Sources**: The Data Sources that are attached to applications to which the user has access. Data Sources that are not attached to an application, but that do belong to the scope of the user, will not be displayed. |

| The **Actions By Event** section contains information on all of the user’s Actions, grouped by the session event that triggers them and listed in the order of execution:  
**At logon**: May contain actions for Environment Variables, Folder Redirection, Automation Tasks, Microsoft ConfigMgr, Execute Command, Drive and Port Mappings, Drive Substitutes, Printers, User Home Directory, Folder Synchronization, User Registry and User Profile Directory.  
**At Session Refresh**: May contain actions for Folder Synchronization and Execute Command.  
**At Session Reconnect**: May contain actions for Folder Synchronization and Execute Command.  
**At Logoff**: May contain actions for Folder Synchronization and Execute Command. |
The Actions By Type section contains the following information:

- **Automation Tasks**: An overview concerning the user's Automation Tasks.
- **Environment Variables**: An overview of the user's Environment Variable Actions.
- **Execute Command**: An overview of the user's Execute Command Actions.

The Files and Folders section contains the following information:

- **Drive and Port mappings**: An overview of the user's Mappings. The last logon is used to determine which language should be used when showing language-based settings.
- **Drive Substitutes**: An overview of the user's Drive Substitutes.
- **Folder Redirection**: An overview of the user's Folder Redirections.
- **Folder Synchronization**: An overview of the user's Folder Synchronizations.
- **User Profile Directory**: An overview of the user's Profile Directory Actions.
- **LANDesk**: An overview concerning the user's LANDesk software distributions.
- **Microsoft ConfigMgr**: An overview concerning the user's Microsoft ConfigMgr Distributions.
- **Printers**: All configured Network Printers for the user.
- **User Registry**: An overview of the user's Registry Settings. When viewing the user's registry settings, double-clicking **End result** (at the bottom of the **Type** column) will merge all configured registry settings and show the end result in the Registry Viewer. To track registry values, the source is shown on the right.
- **User Settings**: All configured User Settings for the user.
  - When clicking **View stored settings** for a User Setting, User Settings for files that contain Unicode or non-Western characters in their name, are displayed with the following text: `<File name contains non-displayable text and formats>`.

The Applications section contains the following information:

- **Managed Applications**: The Applications log for the specific user provides an overview of the applications that were blocked for this user.
- **User Installed Applications**: All User Installed Applications (if applicable).
- **Websites**: The websites log for the specific user provides an overview of all blocked attempts to access websites for this user.

The Data section contains the following information:

- **Removable Disks**: The Removable Disks Access for the specific user provides an overview about the user's access to removable media. The log provides an overview of all blocked attempts to access a removable disk for this user.
- **Files and Folders**: The Files and Folders log for the specific user provides an overview of the files and folders that were blocked for this user.
- **Read-Only Blanketing**: The Read-Only Blanketing log for the specific user provides an overview of all blocked attempts to access a drive that is rendered read-only for this user.
- **Network connections**: The Network Connections log for this user provides an overview of all blocked network connections for this user.
- **User Sessions**: The User Sessions log provides a detailed list of all Sessions security events for this user.
Diagnostics

- **User sessions**: A list of the user's active sessions. Right-click a session in this list to force a refresh of the session, remote control the session, etc.

- **Workspace Model Overview**: An overview of the mode in which each Workspace Control feature is running, including information about any Workspace Container exception that applies to the user.

- **Event Log**: A log of all Action settings that were processed for this user. The Event Log can be used to find problems with a user's settings.

- **Usage Tracking**: Double-click the Details pane to open the Usage Tracking viewer for the selected user.

- **Delegated access control**: The applications of which the user is an application manager. Selecting an application displays all details of the delegated application (users, capacity in use, etc.).

The **Performance** section contains the following information:

- **Access Balancing**: The Access Balancing log provides a detailed list of all Access Balancing events for this user.

- **CPU Optimization**: The CPU Optimization log provides a detailed list of all CPU Optimization events for this user.

- **Instant LogOff**: The Instant LogOff log provides a detailed list of all Instant LogOff events for this user.

- **Memory Optimization**: The Memory Optimization log provides a detailed list of all Memory Optimization events for this user.

---

**Note**

When your Workspace Control environment contains a Relay Server, situations may occur in which the Event Log of certain users has not been updated, because this happens asynchronously. As a result, the Event log may contain an error that a file is missing. This is intended behavior of Workspace Control. The error will disappear again when the Relay Server has processed all data and the Event Log has been updated. The Event Log is available when viewing the detailed Workspace Analysis of a user at Diagnostics > Workspace Analysis.

---

**Tip**

You can minimize the **Workspace Analysis Details** window to the Taskbar, which allows you to browse the Management Console while still having quick access to the Workspace Analysis overview for the selected user.
9.1.3  Workspace Simulation Wizard

The Workspace Simulation Wizard gives you a powerful tool to achieve Desired User State Management. Based on identity, locations and workspace containers you can view the Workspace Analysis of a simulated Workspace. For example, by selecting an OU and a number of groups, locations and workspace containers, you can analyze the contents of a Workspace resulting from the specified context. You can use the wizard to try out various scenarios and to view their impact before applying these to your "live" environment.

The Workspace Simulation Wizard can be started in two ways:

- Prefilled with a user identity:
  - Go to Diagnostics > Workspace Analysis node, select a user and right-click and select Run Workspace Simulation
  - Go to Diagnostics > Workspace Analysis node, select a user and select Action > Workspace Analysis > Run Workspace Simulation

- Without a prefilled user identity:
  - Click the Workspace Simulation button in the Command bar, available at all nodes in Diagnostics
  - Right-click anywhere in the Diagnostics tree view and select Workspace Simulation
  - Select Action > Workspace Simulation, also available throughout Diagnostics

Configuration

The scenario can be based on the following criteria:

- **Identity:**
  - Existing user from the Directory Service
  - OU membership or Group membership
    - You can Search for specific OUs or Groups by entering search criteria. You can use wildcards (e.g. "*team" will yield all OUs/groups containing "team").
    - Click Add manually to select one or multiple Group(s) from the Directory Service. Multiple groups must be separated with semicolons and can be verified for existence by clicking Check.

- **Locations and devices.** One or multiple Zones. If no Zones have been configured, this step will be skipped.

- **Workspace Containers.** One or multiple Workspace Containers. You can preselect the data based on an existing Agent (e.g. if the user logs on from a specific computer). If no Workspace Containers have been configured, this step will be skipped.

  A green check mark indicates that the criteria entered at Identity and/or Zones apply for this Workspace Container. A red cross indicates the criteria do not apply for this Workspace Container. This helps you to decide whether it is useful to include this Workspace Container in the scenario.

- **Time and Connection State.** The day of the week, the time and connection state (Online/Offline) for the workspace you want to preview.

After specifying all criteria, the results of the Workspace Scenario are shown as if the predicted workspace was an actual workspace.

To create an Instant Report of the results, click Action > Create Instant Report. Save or print the report for later comparisons and analysis.
Example:

You want to check whether a user can access a specific application from home and from work on a specific day/time.

You can run two scenarios:

• Location A = Work, Workspace Container defines access on application level, day/time = e.g. Monday, 9:00
• Location B = Home, Workspace Container defines access on application level, day/time = e.g. Tuesday 9:00
• User identity remains the same, Connection state = Online

The result should be that the application is available from both locations and on both days and times.
9.2 User Sessions

With User Sessions, you can gather information about each user that is logged on to your environment.

You can view the following information:

- When was the session started?
- When was the session refreshed?
- What is the idle time of the user?
- What is the state of the user?
- On what client is the user working?
- Which IP address is assigned to the user?
- On what computer is the user working?
- What is the IP address of that computer?
- What Workspace Container is the user working in?
- What is the user's session ID?
- What is the protocol used by the user - ICA, RDP, PCoIP, Blast or Local?
- Is the license in use?
- What is the user's AppGuard mode?
- What is the user's NetGuard mode?
- What is the user's Workspace Composer version?
- What is the user's Workspace Extender version?

**Note**
The Search functionality is case insensitive and will search within the data filled in for Name, User name, and Computer. The search will be based on the entire database of User Sessions and not only on the overview displayed at Diagnostics > User Session.

9.2.1 Where to find User Sessions

<table>
<thead>
<tr>
<th>What</th>
<th>Where</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Sessions</td>
<td>Diagnostics &gt; User Sessions</td>
</tr>
</tbody>
</table>
### 9.2.2 Context menu options

If you right-click a user session, the following options are available from the context menu:

<table>
<thead>
<tr>
<th>Item</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Properties</td>
<td>Displays the user properties.</td>
</tr>
<tr>
<td>Refresh</td>
<td>Refreshes the Active Users list.</td>
</tr>
<tr>
<td>Force refresh of &quot;&lt;user&gt;&quot; now</td>
<td>Refreshes the user's session immediately. This is useful when a refresh is immediately required (e.g. access to a new application was granted or a security rule was added).</td>
</tr>
<tr>
<td>Analyze Workspace of this user</td>
<td>Displays the Workspace Analysis (see Workspace Analysis) details for the selected user.</td>
</tr>
<tr>
<td>Ping the user's workstation</td>
<td>Pings the user's computer to determine the network delay to its computer.</td>
</tr>
<tr>
<td>Remote Control &quot;&lt;user&gt;&quot;</td>
<td>Allows you to remote control the user's session. Remote Control is not possible on Microsoft Windows Server 2012.</td>
</tr>
<tr>
<td>Offer remote Assistance to &quot;&lt;user&gt;&quot;</td>
<td>Allows you to start a Remote Assistance session with the user.</td>
</tr>
<tr>
<td>Send message to &quot;&lt;user&gt;&quot;</td>
<td>Allows you to send a message to the user.</td>
</tr>
<tr>
<td>Log off &quot;&lt;user&gt;&quot;</td>
<td>Allows you to log off the user.</td>
</tr>
<tr>
<td>Reset &quot;&lt;user&gt;&quot;</td>
<td>Resets the user's session.</td>
</tr>
<tr>
<td>Disconnect &quot;&lt;user&gt;&quot;</td>
<td>Disconnects the user's session.</td>
</tr>
<tr>
<td>Restore User Settings</td>
<td>Allows you to restore a user's User Setting to a previous value (from an earlier session) or revert to an application's default configuration.</td>
</tr>
<tr>
<td>Create Instant Report</td>
<td>Creates an Instant Report (see Instant Reports). Depending on your selection, you can also select which items should be included in the Instant report.</td>
</tr>
<tr>
<td>Building Block options</td>
<td>Creates Building Blocks (see Building Blocks). Depending on your selection, you can also select items that should be included in the Building Block(s).</td>
</tr>
<tr>
<td>Help</td>
<td>Opens the Help for the Active Users node.</td>
</tr>
</tbody>
</table>

**Notes**

- It is possible to select multiple users to refresh, send a message, logoff, reset, or disconnect user sessions. Use the CTRL key to select multiple users, use the SHIFT key to select a range of users, or use CTRL+A to select all users in the list.

- The use of these options is subject to NT and/or Citrix permissions.

- If you group the active users list by server, right-click a server to display the option **Send message to all users on server <server name>**. This allows you to send a user-defined message to all users logged on to the selected server. This option is only available in a Terminal Server environment.

- Some options are only available for sessions that are logged on to a Terminal Server.
9.3 Workspace Model Overview

The Workspace Model Overview shows you which features in your environment are active/enabled, which are disabled, and which are set in learning mode. If the global settings of a feature are overridden by exceptions for specific Workspace Containers, these will be shown on separate tabs, per Workspace Container. Each feature shows whether the global settings apply or whether different settings apply to the Workspace Container.

You cannot change a feature's mode directly from Diagnostics > Workspace Model Overview. You can do this from a similar view, at Administration > Workspace Model. It is also possible to change a feature's mode from the relevant node itself, by selecting a feature and clicking ...

### 9.3.1 Where to find the Workspace Model Overview

<table>
<thead>
<tr>
<th>What</th>
<th>Where</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workspace Model Overview</td>
<td>Diagnostics &gt; Workspace Model Overview</td>
</tr>
<tr>
<td>Workspace Model</td>
<td>Administration &gt; Workspace Model</td>
</tr>
</tbody>
</table>
9.4 Audit Trail

The Audit Trail shows detailed information about all modifications in your environment, including the installation of Service Packs (if applicable).

- To view the audit trail of all changes in your environment, go to Diagnostics > Audit Trail.
- To view the audit trail of a specific feature or item, either click the Audit Trail tab of the feature/item or, if this is not available, click in the Command bar.
- If you configured Management Portal Integration (on page 82), use Launch Management Portal to view the Audit Trail data.

9.4.1 Audit Trail options

The following options are available in the Audit Trail node:

- To display the properties of an entry, right-click it and click Properties.
- To refresh the contents of the Audit Trail, click Refresh.
- To copy the contents of the Audit Trail to the clipboard, click Copy.
- To clear the Audit Trail log of all entries or log entries that are older than 90 days, click Clear log.
- To protect the Clear log button with a password, click Security. This opens the Security window, which allows you to enable password protection.
  - If you already configured a password, click Security to change this password. This opens the Verify password window. After entering the correct password, the Security window opens, which allows you to change the password.

Search engine

By default, the first 100 log entries are automatically shown when clicking Search. When the option Show last 100 entries only is not checked, the log view will be cleared. You can then search for the desired log entries.

Clicking the More button allows you to group your search (Group By) or specify a Date / Time Filter for your search. The # incidents at the bottom of the overview is dynamic.
9.5 Agents Overview

Diagnostics > Agents Overview presents a read-only overview of the status, properties and Workspace Container memberships of all the Agents in your environment. Agents are computers on which users can start Workspace Control sessions. You can search for Agents and filter by Workspace Containers. This allows you to easily find Agents in large environments. See Agents (on page 42) for more information.
9.6 Usage Tracking Overview

At Diagnostics > Usage Tracking Overview, you can see the mode in which Usage Tracking is running and open the Usage Tracking Viewer.

See Usage Tracking (on page 84) and Usage Tracking Viewer (on page 184) for more information.

Configuration

To enable Usage Tracking, go to Usage Tracking in the Setup menu.
9.7 Errors

The Errors node shows information about the errors that occurred in your environment:

- To view the properties of an event, right-click it and click Properties in the context menu.
- You can clear the log from the context menu.

Search engine

By default, the first 100 log entries are automatically shown when clicking Search. When the option Show last 100 entries only is not checked, the log view will be cleared. You can then search for the desired log entries.

Clicking the More button allows you to group your search (Group By) or specify a Date / Time Filter for your search. The # incidents at the bottom of the overview is dynamic.

Summarizing repeating entries

- If an error is logged 60 times or more within an hour on a single Agent, logging of the individual occurrences of the error is suspended and the following entry is logged:
  "Start summarizing error <error number> as it was logged 60 times since <time of first occurrence>"
- As long as the error keeps occurring 60 times or more within an hour on that Agent, the following entry is logged once per hour:
  "Summary of error <error number>: logged <amount> times since <time summarizing started or time of previous summary>"
- When the frequency of the error drops below 60 times per hour, the following entry is logged:
  "Stop summarizing error <error number> as it was logged only <amount> times since <time summarizing started or time of previous summary>"
  Logging individual occurrences for that error is then resumed.
- The summarizing mechanism is in place as long as the RES Service is running on the Agent that is generating the errors. If the RES Service is stopped while one or more errors are being summarized, the following entry is logged for each of these errors:
  "Closed summary of error <error number>: logged <amount> times since <time summarizing started or time of previous summary>"

9.7.1 Where to find Errors

<table>
<thead>
<tr>
<th>What</th>
<th>Where</th>
</tr>
</thead>
<tbody>
<tr>
<td>Errors</td>
<td>Diagnostics &gt; Errors</td>
</tr>
</tbody>
</table>
Chapter 10: Administration

10.1 Administrative Roles

Administrative Roles determine which objects a user of the Workspace Control Console is allowed to see and to manage. This enables delegation of control over the Workspace Control site.

Each Administrative Role is defined by the following aspects:

- its permissions determine which nodes and objects are shown in the Workspace Control Console, and whether they can be viewed or edited.
- its Scope Control determines the users and Workspace Containers for whom the Administrative Role can edit objects in the Workspace Control Console. This is based on the Access Control and Workspace Control set on those objects.
- the Access Control and Workspace Control set on the Administrative Role determine which users get the Administrative Role in which locations for which specific time period and Workspace Containers.

Notes

- Administrative Roles can also be selected as part of Access Control on applications and settings. This allows you to use Administrative Roles to create custom groups of users, independent of the groups available in the available Directory Services. Remember to use a very restricted set of permissions for Administrative Roles used in this way.
- You can achieve more granular delegation of control by assigning different permission levels to a node’s list of objects and its settings for Administrative Roles. For example, a role can have 'modify' rights to the Printers tab, but read-only access to the Settings tab and exception tabs for Printers. When upgrading Workspace Control, the same permissions will be applied to both tabs that were assigned to the whole feature, i.e. if Printers had 'Read' rights, both tabs will get 'Read' rights. When downgrading Workspace Control, the lowest rights will be applied, i.e. if the Printers had 'Modify' rights and the Settings tab 'Read', 'Read' rights will be applied to both tabs.
10.1.1 Where to find Administrative Roles

<table>
<thead>
<tr>
<th>What</th>
<th>Where</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defining Administrative Roles</td>
<td>Administration &gt; Administrative Roles</td>
</tr>
<tr>
<td>Setting Administrative Roles as Access</td>
<td>Composition &gt; Applications &gt; the Identity tab in the</td>
</tr>
<tr>
<td>Control criterion on a Managed Application</td>
<td>application's Access Control section</td>
</tr>
<tr>
<td>Setting Administrative Roles as Access</td>
<td>Security &gt; User Installed Applications &gt; Access Control</td>
</tr>
<tr>
<td>Control criterion on User Installed</td>
<td></td>
</tr>
<tr>
<td>Applications</td>
<td></td>
</tr>
<tr>
<td>Setting Administrative Roles as Access</td>
<td>on the Access Control tab of the setting</td>
</tr>
<tr>
<td>Control criterion on a setting</td>
<td></td>
</tr>
<tr>
<td>Viewing your current Administrative Roles</td>
<td>Options menu &gt; Show My Administrative Role(s)</td>
</tr>
<tr>
<td>Viewing the scope of your current</td>
<td>Options menu &gt; Show My Scope</td>
</tr>
<tr>
<td>Administrative Role(s)</td>
<td></td>
</tr>
<tr>
<td>Viewing which users have which</td>
<td>Diagnostics &gt; Workspace Analysis, view the Role column</td>
</tr>
<tr>
<td>Administrative Roles</td>
<td></td>
</tr>
<tr>
<td>Viewing the details of a user's</td>
<td>Diagnostics &gt; Workspace Analysis, select a user and</td>
</tr>
<tr>
<td>Administrative Roles</td>
<td>click ✎</td>
</tr>
</tbody>
</table>

10.1.2 Permissions

By default, all nodes in an Administrative Role have **Deny access** permissions.

If an administrator has several Administrative Roles with different levels of permissions for the same node, the greater permission overrules the lesser permission. In other words:

- **Modify** overrules **Read** and **Deny access**.
- **Read** overrules **Deny access**.

New nodes in the Console get **Deny access** permissions. By default, these new nodes will not be visible for existing Administrative Roles (other than Technical Manager).

10.1.3 Technical Manager

By default, every Workspace Control site has one Administrative Role: **Technical Manager**. This role:

- has **Modify** permissions on all nodes.
- does not have any Scope Control.
- cannot have Access Control based on **Date and Time** restrictions.
- can never be removed, disabled, renamed, or assigned different permissions.

By default, all users have this role, so that every user can open the Workspace Control Console and edit everything.

Applications that are managed by application managers are only shown to users with the administrative role Technical Manager.
10.1.4 Scope Control

Scope Control determines which applications and settings in the Workspace Control Console can be viewed or changed by the Administrative Role, based on the Access Control and Workspace Control of these objects.

With the Scope Control Access Control set to a specific Organizational Unit, for example, the administrator can only modify applications and settings that are assigned to users in that Organizational Unit. Applications and settings that are assigned to users in a different Organizational Unit, or that also have additional different Access Control criteria, cannot be modified.

This makes it possible to give an administrator in a regional office control over the applications assigned to users from that office, but not over applications that are also used in other parts of the Workspace Control site.

- Global settings for which no Access Control applies, such as Shell exceptions, are always shown, irrespective of the scope of an Administrative Role.
- If an object is not exclusive to the scope of the Administrative Role, it is shown as read-only.
- If an administrator has several Administrative Roles with different scopes, the scopes are added up.
- If an administrator has several Administrative Roles with and without Scope Control, the scoped role overrides the role without a scope.
- When a scope is set to a specific Workspace Container, only Workspace Model exceptions are visible that apply to that Workspace Container. It is not possible to add or edit any exception data, even if they are within that scope.

10.1.5 Filters

By default, a filter shows all the objects for which at least one of the specified criteria applies either directly or indirectly. An exclusive filter shows all the objects to which at least one of the criteria applies directly.

10.1.6 Solve a Console lockout

An administrator can only access the Management Console if at least one administrative role has been assigned to him.

If a user is locked out of the Workspace Control Console, Workspace Control can add the user's Windows account to the Technical manager Administrative Role, thus granting the user full access to the Workspace Control Console. To verify that the user is legitimate, the user must provide the correct database credentials for the Workspace Control Datastore. Use of this method, including failed attempts, is reported in the Audit Trail.

Procedure

- Log on with the Microsoft Windows account that needs access to the Workspace Control Console.
- Start the Workspace Control Console with the command line parameter /lockedout. For example: C:\program files\Ivanti\Workspace Control\pwrtech.exe /lockedout
- Provide the correct database login and database password for the Workspace Control Datastore.

If the credentials are correct, the Microsoft Windows credentials of the user are added to the Technical manager role, and user will gain access to the Workspace Control Console.
10.2 Agents

At Administration > Agents, you can view and configure settings for all the Agents in your environment.

Agents are computers on which users can start Workspace Control sessions. Agents get configuration data from the Datastore, either directly or through Relay Servers. See Agents Settings (on page 43) for configuration information.
10.3 Relay Servers

At Administration > Relay Servers, you can configure the default behavior of Relay Servers and you can see which Relay Servers are installed and connected to the current Workspace Control environment.

Relay Servers cache information from the Datastore and pass it on to Agents upon request, so that Agents do not need to contact the Datastore directly. Alternatively, Relay Servers can pass the cached information from the Datastore on to other Relay Servers.

Communication between Agents and Relay Servers, and between Relay Servers is secured using TLS (Transport Layer Security). The highest possible TLS version is negotiated. TLS version 1.2 is preferred, but a fallback to version 1.1 or even 1.0 is available.

For further details about Relay Servers, see the document Getting Started with Workspace Control Relay Servers.

10.3.1 Troubleshoot Relay Servers

When an item in the list of Relay Servers shows the attention flag, a possible cause can be tracked down using the Relay Server Configuration tool and standard Microsoft Windows utilities.

Relay Server Local cache

During the configuration of a Relay Server for a Workspace Control environment you can override the default cache location (%ProgramData%\Ivanti\Relay Server). By default, this cache store closes when there is less than 500Mb of free disk space remaining. The store opens again when the available disk space increases with 10% (to 550 Mb), which takes into account that a cache stage may be needed.

When the cache store is closed the Workspace Control environment will be disabled on that Relay Server and clients will not be able to connect to the Relay Server for their cache data. The environment will be shown as disabled in the Relay Server Configuration Tool.

You can manually configure the value for the amount of free disk space.

- Open the registry editor and go to HKEY_LOCAL_MACHINE\SOFTWARE\RES\Workspace Manager\RelayServer.
- Create a new DWORD Value: MinimumFreeDiskSpace
- Enter a value (Mb).

Relay Server Service

Check if the Workspace Control Relay Server service has been started with an account with sufficient permissions and is running properly. This can be done in the Services node of the Microsoft Server Manager Management Console.

Datstore connection and port

Use the Relay Server Configuration Tool to verify the connection with the Datastore and the listening port.
Event Log

Relay Servers log their information and error events in the Application Log of the Microsoft Windows Event Log. The source name used for these entries is Workspace Control Relay Server.

Performance Monitor

To analyze the performance of a Workspace Control Relay Server, the following Performance counters are available in the Microsoft Windows Performance Monitor.

<table>
<thead>
<tr>
<th>Component</th>
<th>Counter name</th>
<th>Description</th>
<th>Counter type</th>
</tr>
</thead>
<tbody>
<tr>
<td>RES ONE Workspace Caching</td>
<td>#cache cycles</td>
<td>Total number of cache cycles executed</td>
<td>PERF_COUNTER_RAWCOUNT</td>
</tr>
<tr>
<td>RES ONE Workspace Caching</td>
<td>Average time in seconds per cache cycle</td>
<td>Average duration per cache cycle execution, in seconds</td>
<td>PERF_COUNTER_COUNTER</td>
</tr>
<tr>
<td>RES ONE Workspace Transactions</td>
<td># transactions processed</td>
<td>Total number of transactions processed</td>
<td>PERF_COUNTER_RAWCOUNT</td>
</tr>
<tr>
<td>RES ONE Workspace Transactions</td>
<td># transactions queued</td>
<td>Total number of transactions queued</td>
<td>PERF_COUNTER_COUNTER</td>
</tr>
<tr>
<td>RES ONE Workspace Transactions</td>
<td>Average time in seconds per transaction</td>
<td>Average duration per transaction execution, in seconds</td>
<td>PERF_COUNTER_COUNTER</td>
</tr>
<tr>
<td>RES Communication Server</td>
<td>#bytes/sec received</td>
<td>Number of bytes received per second</td>
<td>PERF_COUNTER_COUNTER</td>
</tr>
<tr>
<td>RES Communication Server</td>
<td>#bytes/sec sent</td>
<td>Number of bytes sent per second</td>
<td>PERF_COUNTER_COUNTER</td>
</tr>
<tr>
<td>RES Communication Server</td>
<td>#concurrent connections</td>
<td>Number of concurrent connections</td>
<td>PERF_COUNTER_COUNTER</td>
</tr>
<tr>
<td>RES Communication Server</td>
<td>#connections/sec</td>
<td>Number of connections per second</td>
<td>PERF_COUNTER_COUNTER</td>
</tr>
<tr>
<td>RES Communication Server</td>
<td>#operations/sec</td>
<td>Number of operations per second</td>
<td>PERF_COUNTER_COUNTER</td>
</tr>
<tr>
<td>RES Communication Server</td>
<td>Average connection time in seconds</td>
<td>Average connection time, in seconds</td>
<td>PERF_COUNTER_COUNTER</td>
</tr>
<tr>
<td>RES Communication Server</td>
<td>Average operation execution time in seconds</td>
<td>Average operation execution time, in seconds</td>
<td>PERF_COUNTER_COUNTER</td>
</tr>
<tr>
<td>RES Data Access</td>
<td>#db clients active</td>
<td>Total number of db clients active</td>
<td>PERF_COUNTER_COUNTER</td>
</tr>
</tbody>
</table>

When adding RES ONE Workspace Caching counters to the performance monitor, each Workspace Control environment that is hosted on the Relay Server will be displayed as relay server [<port>]<EnvGuid>, where EnvGuid stands for the unique Environment ID as specified on the Settings tab at Administration > Relay Servers in the Management Console. You can choose to add All instances (= Workspace Control environments) at once, or just add one single environment.
RES ONE Workspace Transactions counters are specified in the same manner. So you can choose to add All instances or just a single environment. The Performance Monitor legend will display relay server[<port>]{<EnvGuid>}. 

RES Communication Server counters can only be added per server. This is shown as: relay server[<port>]. 

The RES Data Access counter is a general-purpose counter that monitors connections to the Datastore. No further selection is required. 

These performance counters can be monitored from both local and remote machines.
10.4 Custom Resources

At Administration > Custom Resources, you can select files and folders and configure them as Custom Resources for your Workspace Control environment.

With Custom Resources you can manage resources that are referenced by other parts of Workspace Control, but which cannot easily be placed on a centrally available file server or which must be available on a computer when it is not connected to the network.

For example, these can be image files used in Outlook signatures, scripts used by commands that are executed, etc.

Custom Resources are locally cached on all computers running Workspace Control. When referencing these resources, use the %rescustomresources% variable, which will be replaced by Workspace Control to point to the actual location of the file. The %rescustomresources% variable will always point to the root of the folder structure.

Configuration

- To configure custom resources, click New to add a custom resource. This will open the Browse for File or Folder window.
- Select a file or folder and click OK. This will display the selected files and folders in the Custom Resources list.

Example:

You have added an image file named corpimage.gif to the root of your Custom Resources (i.e. you have not created a folder structure for your custom resources). If you want this image to be used in your corporate e-mail signature, refer to this image as %rescustomresources%\corpimage.gif.
10.5 Maintenance

Use the node Administration > Maintenance to keep your Workspace Control environment free from outdated information.

Dataport maintenance should be performed at regular intervals. This default maintenance allows you to remove references in the Dataport, to remove users that no longer exist, to check license locks and to clean up or clear log files. Dataport Maintenance can be done from Administration > Maintenance.

- Licenses can be locked due to computer crashes or network connection loss. To unlock them, click Check License lock info.
- By clicking Clean up logs now, all logs older than x days will be cleaned (except for the Error Log, which must be cleaned manually).
  - The x is based on the value specified at Setup > Advanced Settings, for the option # days to keep log files.
- By clicking Clear all logs now, all logs will be cleared entirely (except for the Error Log, which must be cleared manually).
- With Clear Audit Trail log, you clear all entries in the Audit Trail log or only entries that are older than the threshold specified at Setup > Advanced Settings, for the option # days to keep log files. This option is identical to the option Clear log at Audit Trail, which is not available when Management Portal Integration is enabled.
- When you change a Group or User name on NT or Active Directory level, this name will not correspond to the one used in Workspace Control. The name used in Workspace Control can be updated by clicking Rename group or user.
  - At Old name, enter the Group or User name preceded by the Domain name, for example, RESONE\Group1.
  - At New name, you can use to select the Group or User from the Directory Service. If entered manually, the Group or User name must also be preceded by the Domain name, for example, RESONE\Group2.
- To search for non-existing users in the Dataport, click Search for non-existing users. Non-existing users are users who have been removed from the NT Domain or the Active Directory, but who still exist in the Workspace Control Dataport. Click Remove non-existing users if any are found.
- To search for obsolete Citrix Worker Groups in the Dataport, click Search for obsolete Citrix Worker Groups. Obsolete Citrix worker groups are worker groups that exist in the Workspace Control Dataport but are from farms for which the current Workspace Control site does not contain any Agents. The list of obsolete worker groups includes information about where in the Management Console the obsolete worker group is being referenced, i.e. for published applications or on the Defaults tab for Citrix XenApp Publishing Integration. If obsolete worker groups are found, the option Remove obsolete Worker Groups becomes available if the Administrator has write access to both the Citrix XenApp Publishing Integration and the Applications nodes. Clicking this option will remove all reference to the obsolete worker groups in the Management Console and Dataport.
- Verify database integrity - Workspace Control features database integrity, a capability that checks for any errors in the Dataport by closely monitoring all objects, resource types and settings.
  Each time the Management Console starts it will perform this consistency check and show a message if one of the database items is missing or incomplete. Any function that may update such an item will be set to read-only until the issue is resolved.
  Each time the Workspace Control cache checks for changes it will also perform this consistency check; items that are not consistent will not be changed. This ensures the cache contains complete data only.
Within new Workspace Control sites the monitoring of database items is performed for all Workspace Control features by default. Within existing Workspace Control sites the monitoring for individual features starts only when new items are added or existing items are deleted. Execute the **Verify database integrity** action to ensure that database integrity is enforced on all features of an existing site.

**Verify SIDs for groups and users** performs a check to verify each Access Control entry has a valid SID in the Datastore when the option **Account SIDs** is enabled on a Directory Service in **User Context > Directory Services**. Also, a check is performed to verify whether the group and user names still match the actual account in the Directory Service. In case of missing SIDs or incorrect names, an update option can be carried out: **Update SIDs and names**.

**Notes**

- The list created using the option **Search for non-existing users** also specifies which users could not be checked because the related Directory Service was not available. The option **Remove non-existing users** does NOT remove users whose existence could not be checked because their Directory Service was not available.
- Datastore Maintenance does not clean up or clear the Audit Trail.
- For a list of possible errors resulting from the function **Verify Database Integrity** and from the cache update, see [http://support.ressoftware.com/Modules/KnowledgeBase](http://support.ressoftware.com/Modules/KnowledgeBase) "Common errors resulting from the cache update/Database Integrity checks and solutions."
10.6 Performance

The Performance features in Workspace Control help you get the optimal performance out of the available servers in your environment. This can be achieved by spreading the available memory and CPU capacity evenly across the server farm and across logons:

- **Access Balancing** (on page 327) sets a maximum number of simultaneous logons to Workspace Control sessions on servers in a server farm. It is also possible to set different values for specific servers.
- **CPU Optimization** (on page 328) actively lowers the priority of processes with a sustained high CPU usage. This keeps the process running, but with a low priority so that other applications in the system are not hindered anymore. When the process returns to a more acceptable level of CPU usage, its priority is changed back to the original level.
- **Instant LogOff** (on page 330) ensures that user profiles unload correctly, and it disconnects the user when a log off is initiated, which improves the speed of the system as experienced by the user.
- **Memory Optimization** (on page 332) limits the maximum amount of physical memory used per session and sets a maximum number of running applications per session.

10.6.1 Access Balancing

Access Balancing limits the number of session logons that a server is allowed to process simultaneously. This optimizes the speed of logons and stabilizes a server’s overall performance at peak logon times.

If many users log on at once, for example at the start of the working day or after a server reboot, this can impact the speed of session logons and the overall performance of the sessions already running on the server. Access Balancing serves as a throttle on session logons: logons that exceed the set limit are queued until the resources are available for them to be processed. Users whose logons are placed in queue are notified of their position in the queue. As a result, users no longer experience slow logons, at which only an hour glass is shown. Instead, they are informed about what is happening and how many users are ahead of them in the queue.

For example, you can set Access Balancing to allow a maximum of 2 simultaneous logons per server: If 10 users log on to a server more or less simultaneously, the first 2 logons proceed immediately and at a normal speed. Logons 3 to 10 are queued until a logon slot is freed.

![Note](Image)

Administrator logons are not restricted by Access Balancing settings.

Where to find Access Balancing

<table>
<thead>
<tr>
<th>What</th>
<th>Where</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Balancing</td>
<td>Administration &gt; Performance &gt; Access Balancing</td>
</tr>
</tbody>
</table>
Configure user-specific Access Balancing settings

Workspace Control stores the Access Balancing settings in the registry at:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\RES\WorkspaceManager\Settings\AccessBalancing
```

You can overrule these settings at user level with Workspace Control Registry Settings (Composition > Actions By Type > User Registry).

The configurable settings are:

- **Enabled**: Yes/No
- **MaxLogons**: Maximum number of simultaneous logons

```
Note
Please note that overruling the default settings in the registry can make it difficult to troubleshoot your environment. It causes behavior that differs from the settings shown in the Management Console.
```

Logging

The Access Balancing Log shows detailed information about Access Balancing events.

The log also shows additional statistics about all the logons in your environment. This is useful as a basis for determining what limits to configure, but it can also contain valuable information for other purposes, for example, in relation to Service Level Agreements.

For example, the **Average queue length** specifies how many logons are held in queue on average (how many users experience a bottleneck at logon). The **Average delay** specifies how long users were held in the queue.

- If the **Average queue length** is high, while the **Average delay** is short, you can probably allow a higher number of simultaneous logons.
- If the **Average queue length** is high, while the **Average delay** is long, you may need additional server capacity.

```
Note
The higher the number in the field # of logons, the more reliable the statistics.
```
10.6.2 CPU Optimization

Tip
You can use Alerting to configure notifications for CPU Optimization events. You can find Alerting at Setup > Integration > Alerting.

Where to find CPU Optimization

<table>
<thead>
<tr>
<th>What</th>
<th>Where</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU Optimization</td>
<td>Administration &gt; Performance &gt; CPU Optimization</td>
</tr>
<tr>
<td>Exclude an application from</td>
<td>Open the application at Composition &gt; Applications, go to</td>
</tr>
<tr>
<td>CPU Optimization</td>
<td>Properties &gt; Settings, select Exclude from CPU optimization</td>
</tr>
</tbody>
</table>
Multicore machines and hyperthreading CPUs

CPU Optimization settings are independent of the number of processors: multi-CPU systems do not need other settings than single-CPU systems. If the Critical CPU condition is set to 90% on a dual-CPU system, processes will be noticed when they use 45% or more of the total CPU capacity (which is 90% of one CPU).

Workspace Control regards hyperthreading and multicore CPUs as standalone CPUs. This is reflected in CPU Optimization, but also in Zones with a **Hardware Requirement** rule: 1 processor with HyperThreading / 1 dualcore processor is recognized as 2 processors in CPU Optimization and in Locations and Devices zones. As a result:

- 1 processor without HyperThreading = 1 processor in CPU Optimization / Zones
- 1 processor with HyperThreading = 2 processors in CPU Optimization / Zones
- 2 processors without HyperThreading = 2 processors in CPU Optimization / Zones
- 2 processors with HyperThreading = 4 processors in CPU Optimization / Zones
- etc.

**Exclude a specific application from CPU Optimization**

If a lower priority of an application affects its performance or if the application only occasionally has a high CPU utilization, you can exclude it from CPU Optimization. You can configure this by selecting the option **Exclude from CPU Optimization** on the application’s Settings tab.

**Logging**

The CPU Optimization Log shows detailed information about CPU Optimization events.

The default CPU Optimization values are a critical CPU condition of 70% with an escalation period of 5 seconds, and an idle CPU condition of 10% with a probation period of 30 seconds. Use the events displayed in the CPU Optimization log to decide whether these values need to be adjusted.

If a process exceeds the configured CPU Optimization limits, you can view the measured critical CPU load duration in **Usage Tracking**, in the **Critical CPU load duration** column of the Details tab. This allows you to adjust CPU Optimization settings, to pinpoint ’misbehaving’ applications and to notice applications that need to be excluded from CPU Optimization.
10.6.3 **Instant LogOff**

At Administration > Performance you find Instant LogOff. With Instant LogOff, you can manage user profiles that fail to unload during logoff. This behavior can occur if applications do not close their registry handles when they are terminated. This behavior is usually caused by improper coding in either Microsoft software or third-party software.

Instant LogOff performs two separate actions:

- It enumerates all handles to the user registry when a user logs off, and forces them to close if they are not closed automatically. This ensures that user profiles are always unloaded. This prevents problems with the reconciliation of roaming profiles; with the registry size limit; and with the log off process to become slow (with the process remaining at “Saving Settings” for a long time).
- It disconnects users when they log off. The logoff process continues as normal after the disconnect, but users experience a faster logoff.

Microsoft Windows 7 and Windows Server 2008 R2 or higher automatically take care of user profiles that fail to unload. This part of Instant Logoff is not necessary anymore when using these versions of Microsoft Windows.

For Workspace Control sessions running on Citrix XenDesktop 7.x using the ICA protocol, the setting Disconnect user session when logoff is initiated is ignored, except when using the Workspace Control Shell.

**Instant LogOff Modes: disabled, log only, enabled**

There are three Instant LogOff modes:

- In the mode **Disabled (but apply configured disconnect behavior)**, Instant LogOff does not enumerate any registry handles and does not force any to close.
- In the mode **Log only (but apply configured disconnect behavior)**, Instant LogOff log does not enumerate any registry handles and does not force any to close, but it does report any problems that occur with unloading user profiles.
- In **Enabled** mode, Instant LogOff takes action if a user profile fails to unload.

**Note**

The Instant LogOff mode does not affect the behavior for Disconnect user session when log off is initiated. If this option is selected, it is applied even if Instant LogOff is disabled or in log only mode.
Disconnect user session when logoff is initiated

In Terminal Server environments and environments that use Microsoft Windows Vista, the setting **Disconnect user session when log off is initiated** greatly enhances the speed of the system as experienced by the user. It does not affect the actual logoff process, which continues and ends normally in the disconnected session.

Enabling this feature also deactivates the “Saving Settings” message that unexpectedly pops up in Seamless Windows applications.

<table>
<thead>
<tr>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>• If it is configured, <strong>Disconnect user session when log off is initiated</strong> is executed independent of the Instant LogOff mode.</td>
</tr>
<tr>
<td>• You may want to turn <strong>Disconnect</strong> off in test environments where users log off and then on again straight away.</td>
</tr>
<tr>
<td>• After the disconnect, the user remains logged on for a brief period of time while the logoff process continues. This is reflected, for example, in the list of User Sessions in the Management Console, where the user’s name will remain visible until the session is actually logged off.</td>
</tr>
</tbody>
</table>

Configure user-specific Instant LogOff settings

Workspace Control stores the Instant LogOff settings in the registry at:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\RES\Workspace Manager\Settings\InstantLogoff
```

You can overrule these settings at user level with Workspace Control Registry Settings (Composition > Actions By Type > User Registry).

The configurable settings are:

- **AfterSplash**: Yes/No
- **Disconnect**: Yes/No
- **Enabled**: Yes/No
- **Mode**: Active/Log

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Please note that overruling the default settings in the registry can make it difficult to troubleshoot your environment. It causes behavior that differs from the settings shown in the Management Console.</td>
</tr>
</tbody>
</table>
10.6.4 Memory Optimization

Memory Optimization optimizes the physical memory usage of running processes on computers in your environment. With Memory Optimization enabled, Workspace Control automatically releases:

- reserved physical memory that is no longer used by a recently launched application.
- physical memory of applications that have been inactive for a while.

In addition, you can ensure an even spread of memory across sessions on a server by limiting:

- the amount of memory used per session.
- the number of applications that are allowed to run simultaneously in a session.

It is not recommended to use Memory Optimization alongside of other memory optimization features such as Citrix Virtual memory Optimization.

Where to find Memory Optimization

<table>
<thead>
<tr>
<th>What</th>
<th>Where</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory Optimization</td>
<td>Administration &gt; Performance &gt; Memory Optimization</td>
</tr>
<tr>
<td>Exclude an application from Memory</td>
<td>Open the application at Composition &gt; Applications, go to Properties &gt; Settings, select Exclude from Memory Optimization</td>
</tr>
<tr>
<td>Optimization limit on the session's memory usage and the maximum number of applications</td>
<td>Open the application at Composition &gt; Applications, go to Properties &gt; Settings, select Exclude from Memory Optimization Limits</td>
</tr>
</tbody>
</table>
Limit the total memory usage of a session

With the option Limit amount of memory per session, you can restrict the memory usage of each Workspace Control session. As soon as the limit is reached, the user is not allowed to start additional applications. If a user tries to start an additional application, a message shows that memory must be freed up by closing an application. The contents of this message can be configured:

As soon as the session's memory usage drops below the configured limit, the user regains the ability to start applications.

Notes
- The Memory Optimization mode does not affect the options Limit the amount of memory per session and Limit number of running applications per session. If configured, these options are applied, even if Memory Optimization is disabled.
- Workspace Control uses the total memory processes Working Set for the Memory Optimization feature. In the Windows Task Manager, this is shown in the Working Set (Memory) column. By default, this column is not displayed in the Windows Task Manager.

Set Memory Optimization limits
As a rule of thumb, you can use the following procedure to determine a limit for the amount of memory per session:

- Start a Terminal Server without any user sessions.
- Make a note of the amount of available memory (this is the amount of installed RAM, minus the overhead used by the OS).
- Divide the amount of available memory by the number of users who are to use this server.

The resulting number is the amount of memory that you can set per session.
Limit the number of applications running in a session

With the option Limit number of running applications per session, you can restrict the number of applications that are allowed to run in any Workspace Control session. Users are not allowed to start additional applications above the set limit. If a user tries to start an additional application, a message shows that an application must be closed before another one can be started. The contents of this message can be configured:

![Memory Optimization Message](image)

**Notes**

- The Memory Optimization mode does not affect the options Limit the amount of memory per session and Limit number of running applications per session. If configured, these options are applied, even if Memory Optimization is disabled.
- Memory Optimization only affects the number of running applications; not the number of open windows associated with the application.

Exclude a specific application from Memory Optimization

You can exclude an application from Memory Optimization actions:

- With the application option Exclude from Memory Optimization Limits, Memory Optimization will never prevent users from opening this application, even if the set Memory Optimization limits have been exceeded.
- With the application option Exclude from Memory Optimization, Memory Optimization will never release physical memory reserved by this application, even if it is idle. This may be necessary if the application needs its memory for background processes, for example.

Configure user-specific Memory Optimization settings

Workspace Control stores the Memory Optimization settings in the registry at:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\RES\Workspace Manager\Settings\MemoryShield
```

You can overrule these settings at user level with Workspace Control Registry Settings (Composition > Actions By Type > User Registry).

The configurable settings are:

- **Enabled**: Yes/No
- **LimitSessionApps**: Yes/No
- **LimitSessionMemory**: Yes/No
- **SessionAppsLimit**: limit in number of running applications
- **SessionMemoryLimit**: limit in MB

**Note**

Please note that overruling the default settings in the registry can make it difficult to troubleshoot your environment. It causes behavior that differs from the settings shown in the Management Console.
Logging

If a session exceeds the Memory Optimization memory limit, this is recorded in the Memory Optimization Log. This log also records whether Memory Optimization has taken place.

- Optimizations are recorded per session after the user has logged off.
- Limits are recorded per event.

The amount of memory freed up as a result of the Memory optimizations is shown in the Action column of the Memory Optimization Log. This amount is cumulative for the session. For example, if Memory Optimization frees up 5 MB for a specific application, and then frees up another 5 MB at a later stage, only 5 MB of physical memory is freed up at a time, but a total amount of freed up memory is 10 MB, and this total amount is shown in the log.
10.7 Workspace Model

At Administration > Workspace Model, you can view the mode in which each feature is running and change it, if necessary. You can also do so from the relevant node itself. If the global settings of features are overridden by exceptions for specific Workspace Containers, the Workspace Model node shows per Workspace Container which settings apply; either the global settings of a feature or the settings of the exception. More information, see Workspace Model (on page 55).
Chapter 11: Registry settings

The following Registry Settings are available to control the behavior of Workspace Control components.

⚠️ Warning

Careless registry editing can cause irreversible damage! Approach this task with caution, and only after you have made a backup.

ℹ️ Note

If the initial installation of an Agent was RES PowerFuse 2010 or earlier, Registry Settings must be placed in:

- HKLM\Software\RES\PowerFuse (32-bit)
- HKLM\Software\Wow6432Node\RES\PowerFuse (64-bit)

### 11.1 ActiveSetupTimeout

<table>
<thead>
<tr>
<th>ActiveSetupTimeout</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Key</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Value</strong></td>
</tr>
<tr>
<td><strong>Type</strong></td>
</tr>
<tr>
<td><strong>Data</strong></td>
</tr>
</tbody>
</table>

In rare circumstances, Active Setup (which is used to execute an application that is not registered or if the version in the Current User registry is lower than in the Local Machine registry) takes more than 60 seconds to complete. This could result in a timeout at logon. With this registry setting the Active Setup Timeout can be configured.
### 11.2 BlockPicaSvcFix

**Block picasvc.exe**

<table>
<thead>
<tr>
<th>Key</th>
<th>HKLM\Software\RES\Workspace Manager (32-bit)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
</tr>
<tr>
<td>Value</td>
<td>BlockPicaSvcFix</td>
</tr>
<tr>
<td>Type</td>
<td>REG_SZ</td>
</tr>
<tr>
<td>Data</td>
<td>yes</td>
</tr>
</tbody>
</table>

Starting a ThinApp application on a Citrix XenDesktop environment could result in a runtime error generated by `picasvc.exe`. This behavior can be blocked by setting this registry setting.

### 11.3 ChangePasswordTimeout

**Change the default timeout for changing the user's password in the Workspace Preferences tool**

<table>
<thead>
<tr>
<th>Key</th>
<th>HKLM\Software\RES\Workspace Manager (32-bit)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
</tr>
<tr>
<td>Value</td>
<td>ChangePasswordTimeout</td>
</tr>
<tr>
<td>Type</td>
<td>REG_DWORD</td>
</tr>
<tr>
<td>Data</td>
<td>'n' (n in seconds, must be at least 5)</td>
</tr>
<tr>
<td>Default</td>
<td>5</td>
</tr>
</tbody>
</table>

### 11.4 CheckDisabledFolders

**Prevent creation of disabled known folders**

<table>
<thead>
<tr>
<th>Key</th>
<th>HKLM\Software\RES\Workspace Manager (32-bit)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
</tr>
<tr>
<td>Value</td>
<td>CheckDisabledFolders</td>
</tr>
<tr>
<td>Type</td>
<td>REG_SZ</td>
</tr>
<tr>
<td>Data</td>
<td>yes</td>
</tr>
</tbody>
</table>

When User Settings is enabled at Composition > User Settings, default shell folders may be created although they were disabled by the "disable known folders" policy. Workspace Control will no longer create disabled known folders when setting this registry setting.
11.5 CheckShutDown

**Prevent freezes during reboot procedure initiated with Citrix XenApp Advanced Configuration tool**

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKLM\Software\RES\Workspace Manager (32-bit)</td>
<td>CheckShutDown</td>
<td>REG_SZ</td>
<td>yes</td>
</tr>
<tr>
<td>HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

When using the Citrix XenApp Advanced Configuration tool to create a reboot schedule for Citrix Provisioned XenApp servers, the corresponding server sometimes freezes during the reboot. If this occurs, the server no longer responds to any requests and only a hard reset can solve the issue. You can prevent these situations with this registry setting.

11.6 CheckUpdateOSDFile

**Workaround for the automatic SCCM reset, allowing the managed App-V application to launch**

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKLM\Software\RES\Workspace Manager (32-bit)</td>
<td>CheckUpdateOSDFile</td>
<td>REG_SZ</td>
<td>Yes</td>
</tr>
<tr>
<td>HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Please note, it is still possible that launching a managed App-V application fails. This can be a timing-issue: after the workaround was applied, SCCM resets the UpdateOSDfile policy before the managed App-V application was launched.

11.7 ConsoleNoAppIcons

**Don't show application icons in the Console (application list / tree view)**

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKLM\Software\RES\Workspace Manager (32-bit)</td>
<td>ConsoleNoAppIcons</td>
<td>REG_SZ</td>
<td>Yes</td>
</tr>
<tr>
<td>HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Instead of the application's icon, a default icon is displayed indicating the application's type of access (e.g. a globe indicates all users have access to the application). When editing the application, the application icon will be shown. This registry setting is particularly interesting for environments containing more than 1000 applications.
Chapter 11: Registry settings

11.8 CorrectTaskbar

**Force task bar on primary screen in dual screen mode in Citrix environments**

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKLM\Software\RES\Workspace Manager (32-bit)</td>
<td>CorrectTaskbar</td>
<td>REG_SZ</td>
<td>Yes or No (default)</td>
</tr>
<tr>
<td>HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

With this setting at "No" the task bar is stretched across both screens in the Workspace Control Shell.
With this setting at "Yes" the task bar is shown only on the primary screen.
In the Windows shell the task bar is always shown on the primary screen.

11.9 CorrectWorkArea

**Disable icon refresh of Microsoft App-V applications**

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKLM\Software\RES\Workspace Manager (32-bit)</td>
<td>CorrectWorkArea</td>
<td>REG_SZ</td>
<td>Yes</td>
</tr>
<tr>
<td>HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HKCU\Software\RES\Workspace Manager (32-bit)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HKCU\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Under exceptional circumstances, when using the Workspace Control Shell, applications incorrectly change the size of the work area. This behavior can be detected and corrected with this registry setting.

11.10 CTX_PFDesktopUsesPwrstart

**Use pwrstart.exe in the command line of the published application for the Workspace Control desktop**

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKLM\Software\RES\Workspace Manager (32-bit)</td>
<td>CTX_PFDesktopUsesPwrstart</td>
<td>REG_SZ</td>
<td>yes</td>
</tr>
<tr>
<td>HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Create a published application for the Workspace Control desktop previously used pwrstart.exe in its command line. This has been changed to pfwsmgr.exe. This registry setting will revert to the old behavior.
11.11  CTX_PNLaunchUsesFarmName

### Configure Farm Name for PNAgent

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKLM\Software\RES\Workspace Manager (32-bit)</td>
<td>CTX_PNLaunchUsesFarmName</td>
</tr>
<tr>
<td>HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>REG_SZ</td>
<td>- or no or &quot;farmname&quot;</td>
</tr>
</tbody>
</table>

By default, an application is started with the following command:

```
PNagent.exe /QLAUNCH <farmname>:<application name>
```

The farm name is saved with the application when configuring the application in the Workspace Control Console.

- If no value is entered, the application will use the default farm name.
- If the value no is entered, no farm name will be used. The application is started with `PNagent.exe /QLAUNCH <application name>`.
- If a farmname value is entered, this farm name will be used.

11.12  CTX_PublishAppCmdLineFlag

### Use %** parameter list when publishing applications to Citrix

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKLM\Software\RES\Workspace Manager (32-bit)</td>
<td>CTX_PublishAppCmdLineFlag</td>
</tr>
<tr>
<td>HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>REG_SZ</td>
<td>yes</td>
</tr>
</tbody>
</table>

Workspace Control by default publishes applications with a parameter list shaped like %*. Under specific circumstances this might fail. Citrix then advises to use a parameter list shaped like %**.

11.13  DirectoryServiceRetryLimit

### Increase waiting time before Directory Service to become available

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKLM\Software\RES\Workspace Manager (32-bit)</td>
<td>DirectoryServiceRetryLimit</td>
</tr>
<tr>
<td>HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>REG_SZ</td>
<td>Number of seconds (default=15)</td>
</tr>
</tbody>
</table>

In rare circumstances, the Workspace Control Composer reported online while the Microsoft Windows Directory Service was not yet fully available. This could happen for example when connecting via a VPN connection. You can add this registry setting to increase the waiting time for the Directory Service to become available.
11.14 DisableDHCP

Enable or disable an Agent from obtaining Datastore/Relay Server connection information from the DHCP server

<table>
<thead>
<tr>
<th>Key</th>
<th>HKLM\Software\RES\Workspace Manager (32-bit)</th>
<th>HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>DisableDHCP</td>
<td></td>
</tr>
<tr>
<td>Type</td>
<td>REG_SZ</td>
<td></td>
</tr>
<tr>
<td>Data</td>
<td>True or False</td>
<td>Yes or No</td>
</tr>
</tbody>
</table>

You can configure DHCP servers in different locations with information about the Datastore/Relay Server to which Workspace Control Agents should connect in that location. In an environment with multiple Datastores/Relay Servers, this ensures that mobile Agents (such as laptops) always connect to a Datastore/Relay Server that is reachable from their current location. Without the DHCP setup, each Agent always connects to a fixed, preconfigured Datastore/Relay Server.

If the DHCP server holds Datastore/Relay Server connection information, this information is transferred to all computers who log on in the network governed by that DHCP server. Use DisableDHCP=True to exempt specific Agent so they retain their original Datastore/Relay Server connection information instead.

11.15 DisableExternalGroupCheck

Enable or disable Group membership check

<table>
<thead>
<tr>
<th>Key</th>
<th>HKLM\Software\RES\Workspace Manager (32-bit)</th>
<th>HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>DisableExternalGroupCheck</td>
<td></td>
</tr>
<tr>
<td>Type</td>
<td>REG_SZ</td>
<td></td>
</tr>
<tr>
<td>Data</td>
<td>yes</td>
<td></td>
</tr>
</tbody>
</table>

In a multi domain environment, nested group membership cross domain will be discovered by Workspace Control, e.g. DomainA\User is member of DomainA\Group1, which is member of domain local group DomainB\Group2. However, this check may slow down the startup time of the user session.

In cases where the external group membership check is not needed, session startup times can be improved by disabling this check.
### 11.16 DisableFolderSyncLocalCheck

Use network drives in Composition > Files and Folders > Folder Synchronization where normally only local drives are allowed.

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKLM\Software\RES\Workspace Manager (32-bit)</td>
<td>DisableFolderSyncLocalCheck</td>
<td>REG_SZ</td>
<td>yes</td>
</tr>
<tr>
<td>HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HKCU\Software\RES\Workspace Manager (32-bit)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HKCU\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

### 11.17 DisableIconRefresh

Disable icon refresh of Microsoft App-V applications

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKLM\Software\RES\Workspace Manager (32-bit)</td>
<td>DisableIconRefresh</td>
<td>REG_SZ</td>
<td>Yes</td>
</tr>
<tr>
<td>HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

In certain circumstances, icons of active Microsoft App-V applications on the taskbar become blank after a user refreshed the workspace. When the user refreshes the workspace again, the icons return to normal. As a workaround for this issue, you can set this registry hook.

---

### 11.18 DisableTileManagement

Disable the Workspace Control tile management feature

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKLM\Software\RES\Workspace Manager (32-bit)</td>
<td>DisableTileManagement</td>
<td>REG_SZ</td>
<td>Yes</td>
</tr>
<tr>
<td>HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HKCU\Software\RES\Workspace Manager (32-bit)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HKCU\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

As of Workspace Control version 10.2.500.0, it is possible to disable Workspace Control tile management completely, to prevent unwanted side effects on existing tiles. It is possible to manage this registry setting using User Registry actions (at Composition > Actions By Type > User Registry).
11.19 DoNotAllowOverlappedDesktopItems

**Prevent desktop shortcuts to be placed on top of each other after a workspace refresh**

| Key | HKLM\Software\RES\Workspace Manager (32-bit)  
|     | HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)  
| Value | DoNotAllowOverlappedDesktopItems  
| Type | REG_SZ  
| Data | Yes  

This registry value applies to user sessions that contain managed and unmanaged shortcuts on the desktop and for which the setting Windows Shell shortcut creation is set to Merge with unmanaged shortcuts (at Composition > Applications, on the Settings tab).

11.20 DoNotAnalyseDB

**Prevent retrieval of Oracle database size**

| Key | HKLM\Software\RES\Workspace Manager (32-bit)  
|     | HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)  
| Value | DoNotAnalyseDB  
| Type | REG_DWORD  
| Data | 1  

When using an Oracle Database, retrieving the Database size from the Workspace Control Console at Setup > Datastore can take a long time or could even cause the Console to hang. You can prevent this behavior with this registry hook.

11.21 EnableMultipleIE

**Display multiple Microsoft Internet Explorer application shortcuts on Microsoft Windows 8.1 Apps screen**

| Key | HKLM\Software\RES\Workspace Manager (32-bit)  
|     | HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)  
| Value | EnableMultipleIE  
| Type | REG_SZ  
| Data | Yes  

Set this registry value when you configure multiple Microsoft Internet Explorer applications with different Parameters and for which the option Create Start Menu shortcut is selected (on the Properties > Shortcuts tab of the application).

This registry setting is obsolete as of version 10.1, as the behavior is now default. For other executables, a CustomAppUserModellDs.xml file can be created.
11.22 ExcludeProcesses

Exclude a process from the check for running subprocesses that must be ended before a Workspace Control session can end

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>• HKLM\Software\RES\Workspace Manager (32-bit)</td>
<td>ExcludeProcesses</td>
<td>REG_SZ</td>
<td>executables separated by a comma (,). For example: crss.exe,wispetis.exe</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>• HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
<td>ExcludeProcesses</td>
<td>REG_SZ</td>
<td></td>
</tr>
</tbody>
</table>

In a Workspace Control session, Citrix published applications are effectively started as a separate session without a task bar and with the application shown full screen. When the user closes this application, Workspace Control also closes the session. To prevent the session from closing while there are still subprocesses running that were started by the application Workspace Control checks the running processes at the end of the session against a list of the processes that were running at the start of the session. If additional processes are running, the session is not closed.

Some processes are not a reason to keep the session alive. Use ExcludeProcesses to exclude these processes, so the session ends even if those processes are still running.

11.23 ExcludeSubscribedTasks

Suppress taskbar icons of applications that run as Workspace Extension

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>• HKLM\Software\RES\Workspace Manager (32-bit)</td>
<td>ExcludeSubscribedTasks</td>
<td>REG_SZ</td>
<td>&lt;window caption of task to be excluded&gt;,&lt;window caption of other task to be excluded&gt;, etc.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>• HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
<td>ExcludeSubscribedTasks</td>
<td>REG_SZ</td>
<td></td>
</tr>
</tbody>
</table>

Managed applications that run as a workspace extension in a Workspace Control session ("subscribed" tasks) appear with their own icon in the taskbar. Under certain circumstances, this may lead to situations in which the application icon is still shown in the taskbar, but the application is no longer active. As a result, the taskbar icon no longer works. For example, this behavior may occur when tasks with a relative short duration are executed (e.g. 500 ms), such as the windows captions in a Workspace Control session. You can suppress this behavior with this registry hook.
11.24 ForceComputername

<table>
<thead>
<tr>
<th>Change the way Desktop Sampler reads computer/client names</th>
</tr>
</thead>
</table>
| **Key** | • HKLM\Software\RES\Desktop Sampler (32-bit)  
|         | • HKLM\Software\Wow6432Node\RES\Desktop Sampler (64-bit) |
| **Value** | ForceComputername |
| **Type** | REG_SZ |
| **Data** | Yes |

On a VDI/TS environment, the desktop sampler will by default look for the computername of the client connecting to the session. You can change the behavior to look for the hostname of the TS/VM itself with this registry setting.

11.25 ForceDisconnectOnIdle

<table>
<thead>
<tr>
<th>Force a disconnect of workspace session after a certain amount of time</th>
</tr>
</thead>
</table>
| **Key** | • HKLM\Software\RES\Workspace Manager (32-bit)  
|         | • HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)  
|         | • HKCU\Software\RES\Workspace Manager (32-bit)  
|         | • HKCU\Software\Wow6432Node\RES\Workspace Manager (64-bit) |
| **Value** | ForceDisconnectOnIdle |
| **Type** | REG_DWORD |
| **Data** | "n" (n in minutes, at least 1) |
11.26 ForceLogoff

Options to force sessions to log off automatically based on session limit, idle time and disconnected state

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKLM\Software\RES\Workspace Manager (32-bit)</td>
<td>ForceLogoffEnabled</td>
<td>REG_SZ</td>
<td>Yes or No</td>
</tr>
<tr>
<td>HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HKCU\Software\RES\Workspace Manager (32-bit)</td>
<td>ForceLogoffOnIdle</td>
<td>REG_SZ</td>
<td>Yes or No</td>
</tr>
<tr>
<td>HKCU\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
<td>ForceLogoffOnDisconnect</td>
<td>REG_SZ</td>
<td>Yes or No</td>
</tr>
<tr>
<td>ForceLogoffTimeout</td>
<td>REG_SZ</td>
<td>(time in minutes)</td>
<td></td>
</tr>
<tr>
<td>ForceLogoffTimeoutOnDisconnect</td>
<td>REG_SZ</td>
<td>(time in minutes)</td>
<td></td>
</tr>
</tbody>
</table>

**Examples**

To force idle sessions to log off after 30 minutes, set:
- ForceLogoffEnabled: Yes
- ForceLogoffOnIdle: Yes
- ForceLogoffTimeout: 30

To force disconnected sessions to log off after 10 minutes, set:
- ForceLogoffEnabled: Yes
- ForceLogoffOnDisconnect: Yes
- ForceLogoffTimeoutOnDisconnect: 10

**Note**

If ForceLogoffTimeoutOnDisconnect is not set, then ForceLogoffTimeout is used to determine the timeout. If that is not available either, then Workspace Control reverts to the default time out of 1 minute. This means that you can set the same time outs for both mechanisms, or you can set a separate time out for each mechanism.
11.27 ForcePrinterConnections

<table>
<thead>
<tr>
<th>Connect printers restored from User Settings</th>
</tr>
</thead>
</table>
| **Key** | • HKLM\Software\RES\Workspace Manager (32-bit)  
          | • HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit) |
| **Value** | ForcePrinterConnections |
| **Type** | REG_SZ |
| **Data** | yes |

When you are using User Settings only to restore printer connections, you will notice that only the default printer gets connected. If you then check the registry (HKCU\Printers\Connections), you will notice that the printers are restored properly, but not connected. You can force to connect all restored printers with this registry hook.

**Notes**
- Setting this key can cause an increase in logon times depending on how much printers a user has selected. Printers will get connected one by one.
- A User Setting on global level must be in place for capturing the registry tree HKCU\Printers\Connections.

11.28 ForceShutdown

<table>
<thead>
<tr>
<th>Forces a shutdown, power-off or restart when a user logs off from the session</th>
</tr>
</thead>
</table>
| **Key** | • HKLM\Software\RES\Workspace Manager (32-bit)  
          | • HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)  
          | • HKCU\Software\RES\Workspace Manager (32-bit)  
          | • HKCU\Software\Wow6432Node\RES\Workspace Manager (64-bit) |
| **Value** | ForceShutdown |
| **Type** | REG_SZ |
| **Data** | ShutDown or PowerOff or Restart |
### 11.29 IncludeProcesses

Keep user session logged on in case only a system-tray application is launched on the Citrix XenApp server

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKLM\Software\RES\Workspace Manager (32-bit)</td>
<td>IncludeProcesses</td>
<td>REG_SZ</td>
<td>Comma separated list of processes</td>
</tr>
<tr>
<td>HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HKCU\Software\RES\Workspace Manager (32-bit)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HKCU\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

If only a system-tray application is launched in a user session on the Citrix XenApp server, the Workspace Composer does not pick up on the process and will log off the session. The processes of these applications can be listed in this registry value, thus preventing the user session from closing as long as one or more of these processes are running.

### 11.30 Instrumentation

Enable performance metering for pfwsmgr.exe and/or pwrcache.exe

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKLM\Software\RES\Workspace Manager (32-bit)</td>
<td>Instrumentation</td>
<td>REG_SZ</td>
<td>Yes or No (default) or executables (separated by ; )</td>
</tr>
<tr>
<td>HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HKCU\Software\RES\Workspace Manager (32-bit)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HKCU\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Notes**

The log file is called `perfdump_%servername%.txt` and is created in the user's pwrmenu folder and in the `%programfiles%\Ivanti\Workspace Control` folder on every machine.
11.31 InterceptManagedApps

Prevent Workspace Control from modifying the applications' command line.

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKLM\Software\RES\Workspace Manager (32-bit)</td>
<td>InterceptManagedApps</td>
<td>REG_SZ</td>
<td>Yes</td>
</tr>
<tr>
<td>HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

To configure applications for which the command line should not be modified, this registry value must be set in combination with the following settings:

- At Composition > Applications, on the Settings tab, clear the global option Disable process interception for unmanaged shortcuts.
- Configure individual managed applications to intercept their processes if started unmanaged: At Composition > Applications, on the Properties > Shortcuts tab of the application, set If managed shortcut was not used to Intercept new process and apply configuration.

To exclude executables from this behavior, modify the registry value "InterceptManagedApps" to, for example:

Data Yes|Notepad.exe|winword.exe|

This will exclude the applications Notepad and WinWord from the registry value "InterceptManagedApps". Their command lines will be changed when a managed application shortcut is created for these applications in user sessions. The managed shortcut is placed on the desktop, taskbar and/or in the Start Menu. The command line will be changed to "...pwrgate.exe nn" (where nn is the Workspace Control application ID). Microsoft Windows then automatically generates a new AppUserModelID for the application, as it is seen as a new executable.

Note

The AppUserModelID is used for stacking and pinning application shortcut icons on the taskbar and in the Start Menu, generating the list of Recent items in the Start Menu and the Jump Lists. Therefore, the changed command line used by Workspace Control for managed application shortcuts will cause some unwanted side effects and issues.

11.32 KeepSeamlessHostAgent

Allow session sharing for published application started from a Citrix Published Desktop

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKLM\Software\RES\Workspace Manager (32-bit)</td>
<td>KeepSeamlessHostAgent</td>
<td>REG_SZ</td>
<td>Yes</td>
</tr>
<tr>
<td>HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HKCU\Software\RES\Workspace Manager (32-bit)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HKCU\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

When starting a published application from a Citrix Published Desktop, this registry value will allow session sharing.
11.33 KeepSharesWithROB

By default, Read-Only Blanketing deletes all local shares. Use KeepSharesWithROB to keep local shares.

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKLM\Software\RES\Workspace Manager (32-bit)</td>
<td>KeepSharesWithROB</td>
<td>REG_SZ</td>
<td>Yes or No</td>
</tr>
<tr>
<td>HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

11.34 KeepTmpDDEMacros

Start WinWord without Reference manager interfering

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKLM\Software\RES\Workspace Manager (32-bit)</td>
<td>KeepTmpDDEMacros</td>
<td>REG_SZ</td>
<td>yes</td>
</tr>
<tr>
<td>HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

WinWord might not start properly if the “Reference Manager” plugin is used. This can be solved by using this registry setting.

11.35 KeepUnicodePath

Keep original file name (Unicode)

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKLM\Software\RES\Workspace Manager (32-bit)</td>
<td>KeepUnicodePath</td>
<td>REG_SZ</td>
<td>Yes</td>
</tr>
<tr>
<td>HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

By setting this registry value, the original file name will be kept and an 8.3 file name will never be applied in a Workspace Control session. Without this registry value, an 8.3 file name might be applied if a file name contains a lot or special Unicode characters.
11.36 KeepUserDefaultMAPIProfile

**Preserve the default mail profile selected by the user**

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKLM\Software\RES\Workspace Manager (32-bit)</td>
<td>KeepUserDefaultMAPIProfile</td>
</tr>
<tr>
<td>HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
<td></td>
</tr>
<tr>
<td>HKCU\Software\RES\Workspace Manager (32-bit)</td>
<td></td>
</tr>
<tr>
<td>HKCU\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
<td></td>
</tr>
</tbody>
</table>

**Type** REG_SZ  
**Data** Yes

This registry value is useful in the following situations:
- a user creates an additional unmanaged mail profile and makes this profile his default profile.
- if multiple mail profiles are attached to Microsoft Outlook, and the user makes one of these profiles his default profile.

11.37 KeepWordRunning

**Restore auto-correction list of Word**

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKLM\Software\RES\Workspace Manager (32-bit)</td>
<td>KeepWordRunning</td>
</tr>
<tr>
<td>HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
<td></td>
</tr>
<tr>
<td>HKCU\Software\RES\Workspace Manager (32-bit)</td>
<td></td>
</tr>
<tr>
<td>HKCU\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
<td></td>
</tr>
</tbody>
</table>

**Type** REG_SZ  
**Data** Delayed

When the auto-correction list of Microsoft Word cannot be restored with User Settings, you can resolve this with this registry value.
11.38 LingerDisconnectTimerInterval

<table>
<thead>
<tr>
<th>Session Linger for Citrix XenApp 7.x</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Key</strong></td>
</tr>
<tr>
<td><strong>Value</strong></td>
</tr>
<tr>
<td><strong>Type</strong></td>
</tr>
<tr>
<td><strong>Data</strong></td>
</tr>
</tbody>
</table>

The Citrix functionality Session Linger is, via Workspace Control, also possible for Citrix XenApp 7.x on 64-bit systems. When setting the registry value LingerDisconnectTimerInterval, the Citrix session will linger for the specified number of minutes after having closed the last published Citrix application in a user session. After this time, the Citrix session will be disconnected.

**Notes**
- Lingering Citrix XenApp applications started by Workspace Control will not show the status ‘lingering’ on the Citrix server. This is caused by the way Workspace Control starts Citrix published applications.
- To enable Session Linger for Citrix XenApp 7.x, the following registry values can be set:
  - LingerDisconnectTimerInterval
  - LingerTerminateTimerInterval

11.39 LingerTerminateTimerInterval

<table>
<thead>
<tr>
<th>Session Linger for Citrix XenApp 7.x</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Key</strong></td>
</tr>
<tr>
<td><strong>Value</strong></td>
</tr>
<tr>
<td><strong>Type</strong></td>
</tr>
<tr>
<td><strong>Data</strong></td>
</tr>
</tbody>
</table>

The Citrix functionality Session Linger is, via Workspace Control, also possible for Citrix XenApp 7.x on 64-bit systems. When setting the registry value LingerTerminateTimerInterval, Workspace Control will make sure that the Citrix session will linger for the specified number of minutes after having closed the last published Citrix application in a user session. After this time, the Citrix session will be terminated.

**Notes**
- Lingering Citrix XenApp applications started by Workspace Control will not show the status ‘lingering’ on the Citrix server. This is caused by the way Workspace Control starts Citrix published applications.
- To enable Session Linger for Citrix XenApp 7.x, the following registry values can be set:
  - LingerDisconnectTimerInterval
  - LingerTerminateTimerInterval
11.40 LocalCacheOnDisk

Store Workspace Control Agent cache updates in DBcache folder for non-persistent/pooled VDI

| Key | HKLM\Software\RES\Workspace Manager (32-bit)  
     | HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit) |
|-----|----------------------------------------------------------|
| Value| LocalCacheOnDisk                                        |
| Type | REG_SZ                                                  |
| Data | Yes                                                     |

With this registry value, it is possible to make the cache independent of the Operating System’s (OS) registry. Setting this registry value will convert the UpdateGUIDs and policy settings automatically from the OS’ registry to two new XML files in the Workspace Control DBcache folder on the persistent disk: UpdateGUIDs.xml and Settings.xml. The original registry values will not be removed. Once the Agent has finished synchronizing its new cache location with the Datastore, these values can be removed manually. The DBcache folder can be redirected (in this case to the persistent disk) using the registry value LocalCachePath.

Removing the registry value from the Agent, the cache will automatically convert UpdateGUIDs.xml and Settings.xml back into the OS’ registry and the files will be deleted from the DBCache folder.

Setting this registry value will prevent unnecessary network traffic caused by the initial cache update, but may cause some additional disk I/O load on the Workspace Control cache folder when processing changes in the Datastore throughout the day.

11.41 LocalCachePath

Relocate the Workspace Control cache folders

| Key | HKLM\Software\RES\Workspace Manager (32-bit)  
     | HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit) |
|-----|----------------------------------------------------------|
| Value| LocalCachePath                                           |
| Type | REG_SZ                                                  |
| Data | Path in short name, for example: D:\Worksp~1\dbcache    |
| Default| C:\Progra~1\Ressof~1\Worksp~1\data\dbcache               |

The cache files in the original location will not be removed. Once the Agent has finished synchronizing its new cache location with the Datastore, the cache files in the original location can be removed manually. Can be used together with LocalCacheOnDisk.

Note

The local cache path cannot be on a network share.
11.42 LocatePrintersByIP

**Remember the default printer based on Client Subnet ID (instead of Client name)**

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKLM\Software\RES\Workspace Manager (32-bit)</td>
<td>LocatePrintersByIP</td>
<td>REG_SZ</td>
<td>yes (case-sensitive)</td>
</tr>
<tr>
<td>HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Notes**

- This registry value only works when setting the default printer from a client Operating System (e.g. Microsoft Windows 7). When setting the default printer from a server Operating System, the default printer will be saved based on the Client name.
- By setting this registry value, a new section will be added to the pwruser.ini file: RoamingPrintersIP.
- As of RES Workspace Manager 2014 SR3, in the Console, at Composition > Actions By Type > Printers, on the Settings tab, the option IP network address for all Agents replaces the behavior if the option Force mandatory default printer (resets default printer during each logon) has not been selected and the registry value LocatePrintersByIP is present in your Workspace Control environment.
- You may choose to select the option IP network address for all Agents in the Console and remove this registry value from the Agents in your Workspace Control environment or set it to No.

11.43 LogAdapterInfo

**Log additional information about network adapters.**

<table>
<thead>
<tr>
<th>Keys</th>
<th>Value</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKLM\Software\RES\Workspace Manager (32-bit)</td>
<td>LogAdapterInfo</td>
<td>REG_SZ</td>
<td>Yes or No (default)</td>
</tr>
<tr>
<td>HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

By setting this registry value, you can log additional information (description, settings) regarding the network adapters in the User Event Log.
11.44 LogPerformance

Log any function that takes more than 5 seconds, which can be useful for purposes of troubleshooting and performance monitoring.

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKLM\Software\RES\Workspace Manager (32-bit)</td>
<td>LogPerformance</td>
<td>REG_SZ</td>
<td>Yes or No</td>
</tr>
<tr>
<td>HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HKCU\Software\RES\Workspace Manager (32-bit)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HKCU\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

11.45 MSLimitOnProcIDs

Count multiple occurrences of the SAME application only once when calculating memory limits

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKLM\Software\RES\Workspace Manager (32-bit)</td>
<td>MSLimitOnProcIDs</td>
<td>REG_SZ</td>
<td>Yes or No</td>
</tr>
<tr>
<td>HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HKCU\Software\RES\Workspace Manager (32-bit)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HKCU\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Memory Optimization offers the possibility to limit the number of Applications per session. In fact, this limits the number of tasks on the taskbar which is not always equal to the number of Applications. For example, 3 open e-mails in Outlook count for 3, tasks while there is only one application.

With this registry setting it is possible to limit the number of applications, where tasks belonging to the same application count only once.
11.46 **NoAgentScreenSaver**

Force the Workspace Control session screensaver in a VDX session that is started from a Workspace Control session or when the Workspace Extender or Subscriber is detected in a session.

<table>
<thead>
<tr>
<th>Key</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• HKLM\Software\RES\Workspace Manager (32-bit)</td>
<td></td>
</tr>
<tr>
<td>• HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
<td></td>
</tr>
<tr>
<td>• HKCU\Software\RES\Workspace Manager (32-bit)</td>
<td></td>
</tr>
<tr>
<td>• HKCU\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Value</th>
<th>NoAgentScreenSaver</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>REG_SZ</td>
</tr>
<tr>
<td>Data</td>
<td>yes</td>
</tr>
</tbody>
</table>

If this registry value is not set (or it is set to “no”), the screensaver of the client will be used by default.

11.47 **NoFullScreenKiosk**

Ensures that the task bar is always on top and visible in kiosk mode.

<table>
<thead>
<tr>
<th>Key</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• HKLM\Software\RES\Workspace Manager (32-bit)</td>
<td></td>
</tr>
<tr>
<td>• HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Value</th>
<th>NoFullScreenKiosk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>REG_SZ</td>
</tr>
<tr>
<td>Data</td>
<td>Yes or No</td>
</tr>
</tbody>
</table>

11.48 **NoListConcurrentUsers**

Do not show concurrent users when an application starts while no licenses are available.

<table>
<thead>
<tr>
<th>Key</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• HKLM\Software\RES\Workspace Manager (32-bit)</td>
<td></td>
</tr>
<tr>
<td>• HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
<td></td>
</tr>
<tr>
<td>• HKCU\Software\RES\Workspace Manager (32-bit)</td>
<td></td>
</tr>
<tr>
<td>• HKCU\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Value</th>
<th>NoListConcurrentUsers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>REG_SZ</td>
</tr>
<tr>
<td>Data</td>
<td>Yes or No (default)</td>
</tr>
</tbody>
</table>
### 11.49 NoPrecedingSlashInPNFolder

<table>
<thead>
<tr>
<th>Publish application without the PN root folder being preceded by &quot;&quot;.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Key</strong></td>
</tr>
<tr>
<td>- HKLM\Software\RES\Workspace Manager (32-bit)</td>
</tr>
<tr>
<td>- HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
</tr>
<tr>
<td><strong>Value</strong></td>
</tr>
<tr>
<td><strong>Data</strong></td>
</tr>
</tbody>
</table>

If you publish an application via Workspace Control, the PN root folder name can be preceded by a backslash "\". This registry setting prevents this from happening.

### 11.50 OutlookNotificationCheck

<table>
<thead>
<tr>
<th>Always show New Mail Desktop Alerts from Microsoft Outlook</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Key</strong></td>
</tr>
<tr>
<td>- HKLM\Software\RES\Workspace Manager (32-bit)</td>
</tr>
<tr>
<td>- HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
</tr>
<tr>
<td>- HKCU\Software\RES\Workspace Manager (32-bit)</td>
</tr>
<tr>
<td>- HKCU\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
</tr>
<tr>
<td><strong>Value</strong></td>
</tr>
<tr>
<td><strong>Type</strong></td>
</tr>
<tr>
<td><strong>Data</strong></td>
</tr>
</tbody>
</table>

In the Workspace Control Shell not all New Mail Desktop Alerts are shown for several Outlook languages in the Workspace Composer. These New Mail Desktop Alerts will always be shown if this registry value is set. Please note that the transparency and fade effects of the New Mail Desktop Alerts are lost when using this registry value.

### 11.51 PIDoNotSetEnvVars

<table>
<thead>
<tr>
<th>Disable application-level environment variable actions for intercepted processes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Key</strong></td>
</tr>
<tr>
<td>- HKLM\Software\RES\Workspace Manager (32-bit)</td>
</tr>
<tr>
<td>- HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
</tr>
<tr>
<td>- HKCU\Software\RES\Workspace Manager (32-bit)</td>
</tr>
<tr>
<td>- HKCU\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
</tr>
<tr>
<td><strong>Value</strong></td>
</tr>
<tr>
<td><strong>Type</strong></td>
</tr>
<tr>
<td><strong>Data</strong></td>
</tr>
</tbody>
</table>
11.52 PMWAutoAllowFolders

Authorize all executables found in installation folder for application security and read-only blanketing after User Installed Applications

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKLM\Software\RES\Workspace Manager (32-bit)</td>
<td>PMWAutoAllowFolders</td>
<td>REG_SZ</td>
<td>Yes or No</td>
</tr>
<tr>
<td>HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
<td></td>
<td>REG_SZ</td>
<td></td>
</tr>
<tr>
<td>HKCU\Software\RES\Workspace Manager (32-bit)</td>
<td></td>
<td>REG_SZ</td>
<td></td>
</tr>
<tr>
<td>HKCU\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
<td></td>
<td>REG_SZ</td>
<td></td>
</tr>
</tbody>
</table>

11.53 PwrGateAppId

Default AppId for pwrgate.exe

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKLM\Software\RES\Workspace Manager (32-bit)</td>
<td>PwrGateAppId</td>
<td>REG_SZ</td>
<td>&lt;application id to start if arguments are missing&gt;</td>
</tr>
<tr>
<td>HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
<td></td>
<td>REG_SZ</td>
<td></td>
</tr>
</tbody>
</table>

In certain situations, a specific managed application does not start correctly in the user workspace (e.g. when using the Datatrac application). If this behavior is caused by the fact that a 3rd party application starts pwrgate.exe without any arguments, you can set this registry hook.

11.54 PwrGateFileMapping

Enable starting managed applications if called as a process

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKLM\Software\RES\Workspace Manager (32-bit)</td>
<td>PwrGateFileMapping</td>
<td>REG_SZ</td>
<td></td>
</tr>
<tr>
<td>HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
<td></td>
<td>REG_SZ</td>
<td>no</td>
</tr>
</tbody>
</table>

In very rare circumstances Managed Applications will not start if that application is called as a process, e.g. by pressing a specific button in a third-party application. You can prevent this behavior with this registry hook.
11.55 PwrGateSleep

Set pwrgate to sleep for a specified number of seconds after it starts an application, so that pwrgate.exe can be examined with procexp before it exits. This can be useful for purposes of troubleshooting.

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKLM\Software\RES\Workspace Manager (32-bit)</td>
<td>Pwrgatesleep</td>
<td>REG_SZ</td>
<td>[timeout in seconds]</td>
</tr>
<tr>
<td>HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Default: 0

11.56 PwrMapiDelay

Configure a custom delay for starting pwrmapi.exe

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKLM\Software\RES\Workspace Manager (32-bit)</td>
<td>PwrMapiDelay</td>
<td>REG_DWORD</td>
<td>#seconds to wait</td>
</tr>
<tr>
<td>HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

As of Workspace Control 10.2.500.0, the default delay for starting pwrmapi.exe is 5 seconds, to prevent an issue where additional mailboxes and personal folders were not available for users with no existing e-mail profile. This registry sets a custom delay (in seconds) for pwrmapi.exe.

If a custom delay is also configured in the registry UseOutlookName4Profile (on page 373), the value configured for PwrMapiDelay wins.

11.57 RefreshAllMappedDrives (Workspace Control 10.2.0.1 and earlier)

During a workspace refresh, remove all drive mappings before remapping those drive mappings that are valid for the user session

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKLM\Software\RES\Workspace Manager (32-bit)</td>
<td>RefreshAllMappedDrives</td>
<td>REG_SZ</td>
<td>Yes</td>
</tr>
<tr>
<td>HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HKCU\Software\RES\Workspace Manager (32-bit)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HKCU\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

This registry value can be set to bypass the default behavior: during a workspace refresh, only the drives that need to be added or removed because of a context change will be added or removed.
11.58 RefreshAllMappedDrives (Workspace Control 10.2.500.0 and higher)

### During a workspace refresh, remove all drive mappings before remapping those drive mappings that are valid for the user session

<table>
<thead>
<tr>
<th>Key</th>
<th>HKLM\Software\RES\Workspace Manager (32-bit)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
</tr>
<tr>
<td></td>
<td>HKCU\Software\RES\Workspace Manager (32-bit)</td>
</tr>
<tr>
<td></td>
<td>HKCU\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
</tr>
</tbody>
</table>

**Value**: RefreshAllMappedDrives  
**Type**: REG_SZ  
**Data**: No

This registry value can be set to bypass the default behavior: during a workspace refresh only the drives that need to be added or removed because of a context change will be added or removed.

11.59 RemoveStartmenuPinList

### Clear the pin list

<table>
<thead>
<tr>
<th>Key</th>
<th>HKLM\Software\RES\Workspace Manager (32-bit)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
</tr>
</tbody>
</table>

**Value**: RemoveStartmenuPinList  
**Data**: yes

On Microsoft Windows versions prior to Microsoft Windows 7, the pin list was not automatically cleared. With this registry setting, the pin list will be cleared. This will work in Workspace Control sessions using the windows shell, and with Composition > Applications > Properties > Windows Shell shortcut creation set to Replace all unmanaged shortcuts.

11.60 RestoreMappingsAtLogoff

### Skip restore of drive mappings that were available outside of session

<table>
<thead>
<tr>
<th>Key</th>
<th>HKLM\Software\RES\Workspace Manager (32-bit)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
</tr>
</tbody>
</table>

**Value**: RestoreMappingsAtLogoff  
**Type**: REG_SZ  
**Data**: no

At Composition > Drive and Port Mappings > Settings, when you have disabled the settings Disconnect all network drives before logging on/off, all persistent drive mappings that were removed at the start of a Workspace Control session will be restored at logoff. If this is an unnecessary action and you want to skip the restore of drive mappings that were available outside of the Workspace Control session, you can prevent this behavior with this registry hook.
11.61 RunCPUShld

Prevent cpushld.exe from running if CPU optimization is enabled

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKLM\Software\RES\Workspace Manager (32-bit)</td>
<td>RunCPUShld</td>
<td>REG_SZ</td>
<td>No</td>
</tr>
<tr>
<td>HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

At Administration > Performance > CPU Optimization, on the Settings tab, when CPU Optimization was enabled, cpushld.exe still runs on all Agents. To prevent cpushld.exe from running on Agents, this registry setting can be set for each Agent.

When you want to use the CPU Shield, enable CPU Optimization (at Administration > Performance > CPU Optimization, on the Settings tab) and remove the registry setting from the Agents.

11.62 RunWMSync

Prevent the WMSync process to be started immediately at the start of the Workspace Composer

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKLM\Software\RES\Workspace Manager (32-bit)</td>
<td>RunWMSync</td>
<td>REG_SZ</td>
<td>No</td>
</tr>
<tr>
<td>HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HKCU\Software\RES\Workspace Manager (32-bit)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HKCU\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The WMSync process is started immediately at the start of the Workspace Composer to improve local caching of User Settings.

⚠️ Warning

Setting this registry value will prevent local caching from working.
11.63 SCCMDelayBeforeRunningProgram

**Define delay starting SCCM application after successful installation**

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKLM\Software\RES\Workspace Manager (32-bit)</td>
<td>SCCMDelayBeforeRunningProgram</td>
</tr>
<tr>
<td>HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
<td></td>
</tr>
<tr>
<td>HKCU\Software\RES\Workspace Manager (32-bit)</td>
<td></td>
</tr>
<tr>
<td>HKCU\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
<td></td>
</tr>
</tbody>
</table>

Define the method Workspace Control uses to refresh details of Citrix XenApp published applications:

- **SelfService.exe -poll**: Contact the server to refresh application details.
- **SelfService.exe -ipoll**: Same as above, but if no authentication context is available, the user is prompted for credentials.

SelfService.exe -poll (the default method as of Workspace Control version 10.1) is usually considerably faster, but under rare circumstances it can cause Instant Passthrough to fail. Set this registry value to No if you experience this issue. This will change the method to SelfService.exe -ipoll. (only for Workspace Control 10.1.400.0 and higher)

Please note that in Workspace Control version 10.0 and earlier, the default method was SelfService.exe -ipoll.
### 11.65 SessionCheckInterval (RES ONE Workspace 10.0 and earlier)

<table>
<thead>
<tr>
<th>Increase the interval time for RES Operator (resop.exe) to check active sessions</th>
</tr>
</thead>
</table>
| **Key** | • HKLM\Software\RES\Workspace Manager (32-bit)  
| | • HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit) |
| **Value** | SessionCheckInterval |
| **Data** | 60-3600 (seconds) |

By default, the Agent checks once every 60 seconds (and additionally every time the Agent service is restarted) if there are sessions in the Datastore that are not present anymore on the local machine. These are sessions that were not logged off in a normal way (i.e. sessions that were reset) and that may prevent Workspace Control from correctly releasing locked Workspace Control licenses and resetting driver-related session data.

With this registry setting, the interval time for checking session information in the Datastore and, if applicable, releasing locked licenses and reset driver-related session data, can be increased to a maximum of 3600 seconds (60 minutes). Setting a higher interval time will reduce the number of queries to the Datastore.

### 11.66 SessionCheckInterval (Workspace Control 10.1 and higher)

<table>
<thead>
<tr>
<th>Increase the interval time for res.exe to check active sessions</th>
</tr>
</thead>
</table>
| **Key** | • HKLM\Software\RES\Workspace Manager (32-bit)  
| | • HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit) |
| **Value** | SessionCheckInterval |
| **Data** | 60-3600 (seconds) |

By default, the Agent checks once every 60 seconds (and additionally every time the Agent service is restarted) if there are sessions in the Datastore that are not present anymore on the local machine. These are sessions that were not logged off in a normal way (i.e. sessions that were reset) and that may prevent Workspace Control from correctly releasing locked Workspace Control licenses.

With this registry setting, the interval time for checking session information in the Datastore and, if applicable, releasing locked licenses, can be increased to a maximum of 3600 seconds (60 minutes). Setting a higher interval time will reduce the number of queries to the Datastore.
11.67 **ShowSearchFieldAlways**

Always show the Search field on the Application List tab (at Composition > Applications)

<table>
<thead>
<tr>
<th>Key</th>
<th>HKLM\Software\RES\Workspace Manager (32-bit)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
</tr>
<tr>
<td></td>
<td>HKCU\Software\RES\Workspace Manager (32-bit)</td>
</tr>
<tr>
<td></td>
<td>HKCU\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
</tr>
<tr>
<td>Value</td>
<td>ShowSearchFieldAlways</td>
</tr>
<tr>
<td>Type</td>
<td>REG_DWORD</td>
</tr>
<tr>
<td>Data</td>
<td>yes</td>
</tr>
</tbody>
</table>

If this registry value is not set, the Search field will appear automatically when typing in letters on the Application List tab.

11.68 **SilentRefresh**

Turns a refresh caused by a display change, USB change, a reconnect and a ‘force refresh’ from the Console into a silent refresh, where the desktop does not disappear and the splash screen is not shown. The task bar does disappear briefly (in the Workspace Control shell).

<table>
<thead>
<tr>
<th>Key</th>
<th>HKLM\Software\RES\Workspace Manager (32-bit)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
</tr>
<tr>
<td></td>
<td>HKCU\Software\RES\Workspace Manager (32-bit)</td>
</tr>
<tr>
<td></td>
<td>HKCU\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
</tr>
<tr>
<td>Value</td>
<td>SilentRefresh</td>
</tr>
<tr>
<td>Type</td>
<td>REG_SZ</td>
</tr>
<tr>
<td>Data</td>
<td>Yes</td>
</tr>
</tbody>
</table>

11.69 **SkipCloseWFShell**

Prevent unexpected results during logoff from Citrix server

<table>
<thead>
<tr>
<th>Key</th>
<th>HKLM\Software\RES\Workspace Manager (32-bit)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
</tr>
<tr>
<td></td>
<td>HKCU\Software\RES\Workspace Manager (32-bit)</td>
</tr>
<tr>
<td></td>
<td>HKCU\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
</tr>
<tr>
<td>Value</td>
<td>SkipCloseWFShell</td>
</tr>
<tr>
<td>Type</td>
<td>REG_SZ</td>
</tr>
<tr>
<td>Data</td>
<td>Yes</td>
</tr>
</tbody>
</table>

At logoff from a Citrix Server, Workspace Control terminates the WFShell.exe in order to speed up the logoff process. Sometimes this termination leads to unexpected results. You can prevent this situation with this registry value.
### 11.70 SkipCLSID

**Open CSV files from Internet Explorer**

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKLM\Software\RES\Workspace Manager (32-bit)</td>
<td>SkipCLSID</td>
<td>REG_SZ</td>
<td>yes</td>
</tr>
<tr>
<td>HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Under certain circumstances, opening a CSV file from Internet Explorer can fail. You can solve this with this registry hook.

### 11.71 SkipDSWhenOffline

**Decrease logon time**

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKLM\Software\RES\Workspace Manager (32-bit)</td>
<td>SkipDSWhenOffline</td>
<td>REG_SZ</td>
<td>Yes</td>
</tr>
<tr>
<td>HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HKCU\Software\RES\Workspace Manager (32-bit)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HKCU\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

When a user starts a Workspace Control session on an offline device, the session startup may take a very long time. This is caused by the system querying for a domain controller. The long logon time can be decreased with this registry value.

### 11.72 SkipFullNames

**Skip the resolving of full user names**

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKLM\Software\RES\Workspace Manager (32-bit)</td>
<td>SkipFullNames</td>
<td>REG_SZ</td>
<td>Yes</td>
</tr>
<tr>
<td>HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Access Control for applications may be based on groups whose members are users and/or groups from multiple domains. In such situations, determining the full user name may take a long time. This registry value may be set to skip the resolving of full user names, speeding up access to these applications in the Management Console.
11.73 SpecialFoldersFromRegistry

<table>
<thead>
<tr>
<th>Force Workspace Control to resolve the special folders from the registry</th>
</tr>
</thead>
</table>
| **Key** | • HKLM\Software\RES\Workspace Manager (32-bit)  
• HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)  
• HKCU\Software\RES\Workspace Manager (32-bit)  
• HKCU\Software\Wow6432Node\RES\Workspace Manager (64-bit) |
| **Value** | SpecialFoldersFromRegistry |
| **Type** | REG_SZ |
| **Data** | yes |

Under some circumstances folder redirection was properly installed, but not recognized at the time Workspace Control is building up the desktop, start menu and so on. This registry setting forces Workspace Control to resolve the special folders from the registry.

11.74 StartHiddenPexplorer

<table>
<thead>
<tr>
<th>Enable opening UNC paths from another application</th>
</tr>
</thead>
</table>
| **Key** | • HKLM\Software\RES\Workspace Manager (32-bit)  
• HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit) |
| **Value** | StartHiddenPexplorer |
| **Type** | REG_SZ |
| **Data** | yes |

In rare circumstances it might not be possible to open UNC paths in the Workspace Control Shell from within another application (e.g. Microsoft Outlook). This registry setting solves the problem.

11.75 StartWithShortCut

<table>
<thead>
<tr>
<th>Stack Microsoft Office applications on taskbar</th>
</tr>
</thead>
</table>
| **Key** | • HKLM\Software\RES\Workspace Manager (32-bit)  
• HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)  
• HKCU\Software\RES\Workspace Manager (32-bit)  
• HKCU\Software\Wow6432Node\RES\Workspace Manager (64-bit) |
| **Value** | StartWithShortCut |
| **Type** | REG_SZ |
| **Data** | no |

Under rare circumstances, Microsoft Office applications that are started by external applications, do not stack properly on the Windows taskbar within a Workspace Control session. You can prevent this behavior with this registry setting.
Chapter 11: Registry settings

11.76 SuppressShowDesktopButton

<table>
<thead>
<tr>
<th>Suppress Show/Hide Desktop button on taskbar</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key</td>
</tr>
<tr>
<td>• HKLM\Software\RES\Workspace Manager (32-bit)</td>
</tr>
<tr>
<td>• HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
</tr>
<tr>
<td>• HKCU\Software\RES\Workspace Manager (32-bit)</td>
</tr>
<tr>
<td>• HKCU\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
</tr>
<tr>
<td>Value SuppressShowDesktopButton</td>
</tr>
<tr>
<td>Type REG_SZ</td>
</tr>
<tr>
<td>Data yes</td>
</tr>
</tbody>
</table>

For users who use the Workspace Control shell, you can suppress the Show/Hide Desktop button on the taskbar. To do so, use this registry setting.

11.77 SuppressUnknownRequestMessage

<table>
<thead>
<tr>
<th>Suppress &quot;poll to port 1942&quot; informational message from Microsoft Windows Application Event Log</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key</td>
</tr>
<tr>
<td>• HKLM\Software\RES\Workspace Manager (32-bit)</td>
</tr>
<tr>
<td>• HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
</tr>
<tr>
<td>• HKCU\Software\RES\Workspace Manager (32-bit)</td>
</tr>
<tr>
<td>• HKCU\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
</tr>
<tr>
<td>Value SuppressUnknownRequestMessage</td>
</tr>
<tr>
<td>Type REG_SZ</td>
</tr>
<tr>
<td>Data Yes</td>
</tr>
</tbody>
</table>

When using a product that scans ports (for a legitimate reason), a poll to port 1942 will result in an informational message in the Microsoft Windows Application Event Log.

11.78 SyncUserSettingsWhenOffline

<table>
<thead>
<tr>
<th>Prevent synchronizing of User Settings in an offline connection state</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keys</td>
</tr>
<tr>
<td>• HKLM\Software\RES\Workspace Manager (32-bit)</td>
</tr>
<tr>
<td>• HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
</tr>
<tr>
<td>Value SyncUserSettingsWhenOffline</td>
</tr>
<tr>
<td>Type REG_SZ</td>
</tr>
<tr>
<td>Data No</td>
</tr>
</tbody>
</table>

Workspace Control synchronizes User Settings when a network connection is available. With this registry setting, the Workspace Control connection state (instead of network connectivity) is used to determine if User Settings must be synchronized.
Tracing

Enables full tracing of Workspace Control functions, which can be useful for purposes of troubleshooting and performance monitoring.

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKLM\Software\RES\Workspace Manager (32-bit)</td>
<td>Trace</td>
<td>REG_SZ</td>
<td>Yes or No</td>
</tr>
<tr>
<td>HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Value</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>TraceFile</td>
<td>REG_SZ</td>
<td>file name, for example C:\Users\Public\Documents\RESTrace.log</td>
</tr>
<tr>
<td>TraceDetailed</td>
<td>REG_SZ</td>
<td>Yes or No</td>
</tr>
<tr>
<td>TraceFilter</td>
<td>REG_SZ</td>
<td>filter options, separated with semicolon (;).</td>
</tr>
<tr>
<td>TraceClasses</td>
<td>REG_SZ</td>
<td>classes, separated with a vertical bar (</td>
</tr>
</tbody>
</table>

⚠️ Warning

Tracing may affect performance of the user session.

💡 Notes

- Variables are not allowed in the file name or path in versions prior to 2008 SR6.
- All users require modify permissions on the trace file.
11.80 UseClassicLogoff

<table>
<thead>
<tr>
<th>Use the Workspace Control classic logoff</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Key</strong></td>
</tr>
<tr>
<td>• HKLM\Software\RES\Workspace Manager (32-bit)</td>
</tr>
<tr>
<td>• HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
</tr>
<tr>
<td>• HKCU\Software\RES\Workspace Manager (32-bit)</td>
</tr>
<tr>
<td>• HKCU\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
</tr>
<tr>
<td><strong>Value</strong> UseClassicLogoff</td>
</tr>
<tr>
<td><strong>Type</strong> REG_SZ</td>
</tr>
<tr>
<td><strong>Data</strong> Yes</td>
</tr>
</tbody>
</table>

For user sessions running Microsoft Windows 7 or higher, setting this registry value might cause:

- a system power down instead of a restart when the logoff or restart was forced (e.g. when a user executes the **Install updates and restart** option).
- a regular logoff not to be completed correctly. This may result in, for instance, User Settings not being saved.

11.81 UseGetSiteInfo

<table>
<thead>
<tr>
<th>Define the method Workspace Control uses to retrieve Site info when publishing Citrix XenApp applications</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Key</strong></td>
</tr>
<tr>
<td>• HKLM\Software\RES\Workspace Manager (32-bit)</td>
</tr>
<tr>
<td>• HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)</td>
</tr>
<tr>
<td><strong>Value</strong> UseGetSiteInfo</td>
</tr>
<tr>
<td><strong>Data</strong> Yes</td>
</tr>
</tbody>
</table>

As of Workspace Control 10.2, the default method to retrieve Citrix Site info when publishing XenApp applications has changed. The new method allows using a Citrix 'Delivery Group Administrator' account to communicate with Citrix XenApp servers (at Setup > Integration > Application Virtualization > Citrix XenApp Publishing, on the Citrix XenApp 7.x tab).

Set this registry value to **Yes** on the Citrix XenApp server if you want to revert to the previous method.

In that case, the credentials you provided to communicate with the Citrix XenApp server must have 'Full Citrix Administrator' privileges.
11.82 UseMsgBox

<table>
<thead>
<tr>
<th>Show message box when WebGuard blocks URL</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Key</strong></td>
</tr>
<tr>
<td><strong>Value</strong></td>
</tr>
<tr>
<td><strong>Type</strong></td>
</tr>
<tr>
<td><strong>Data</strong></td>
</tr>
</tbody>
</table>

WebGuard has the possibility to show a message box when a URL is blocked. The message box can be configured to disappear automatically after an adjustable timeout. This can be done with this registry setting.

11.83 UseOldShadowing

<table>
<thead>
<tr>
<th>Define the method Workspace Control uses to set up Remote Control</th>
</tr>
</thead>
</table>
| **Key** | • HKLM\Software\RES\Workspace Manager (32-bit)  
• HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit) |
| **Value** | UseOldShadowing |
| **Data** | Yes |

As of Workspace Control 10.2, the default method to set up a Remote Control session that originates from a machine running Microsoft Windows Server 2012 or older, has been changed. Now, MSTSC.EXE /SHADOW is used.

Set this registry value to Yes if you want to revert to the previous method:

Use SHADOW.EXE if available; if not, use MSTSC.EXE /SHADOW.
11.84 UseOnlyComputerNameForShadow

<table>
<thead>
<tr>
<th>Prevent error when remote controlling user session</th>
</tr>
</thead>
</table>
| **Key** | • HKLM\Software\RES\Workspace Manager (32-bit)  
• HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit)  
• HKCU\Software\RES\Workspace Manager (32-bit)  
• HKCU\Software\Wow6432Node\RES\Workspace Manager (64-bit) |
| **Value** | UseOnlyComputerNameForShadow |
| **Type** | REG_SZ |
| **Data** | Yes |

When trying to remote control a user session, this may fail with the error:
"The parameter is incorrect."

You can prevent this error by using this registry setting.

11.85 UseOutlookName4Profile

<table>
<thead>
<tr>
<th>Use 'Outlook' as the name for the e-mail profile, instead of the Display name configured in the Workspace Control E-mail Setting</th>
</tr>
</thead>
</table>
| **Key** | • HKLM\Software\RES\Workspace Manager (32-bit)  
• HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit) |
| **Value** | UseOutlookName4Profile |
| **Type** | REG_SZ |
| **Data** | Yes(#seconds to wait) |

Using 'Outlook' as name of the profile prevents an issue where Microsoft Fixmapi stops working when 'Send to > Mail recipient' was used, in the following scenario:
• A Microsoft Office 2016 version prior to 16.0.8420.100 was used.
• The Microsoft Outlook option Use Cached Exchange Mode was disabled.

Additionally, as of Workspace Control 10.2.500.0, the default delay for starting pwrmapi.exe is 5 seconds to prevent an issue where additional mailboxes and personal folders were not available for users with no existing e-mail profile.

Apart from Yes, the data for UseOutlookName4Profile can also contain a custom delay (in seconds) for pwrmapi.exe.

Example: YES|7

If a custom delay is also configured in the registry PwrMapiDelay (on page 361), the value configured for PwrMapiDelay wins.
11.86 WaitBeforeStart

<table>
<thead>
<tr>
<th>Configurable waiting time before Composer starts</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Key</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Value</strong></td>
</tr>
<tr>
<td><strong>Type</strong></td>
</tr>
<tr>
<td><strong>Data</strong></td>
</tr>
</tbody>
</table>

In certain situations, it may be desirable to have the Workspace Composer wait a few seconds before starting. You can use this registry setting to configure this.

11.87 WaitForUpdatedCache

<table>
<thead>
<tr>
<th>Forcing a cache to be up to date before starting a session</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Key</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Value</strong></td>
</tr>
<tr>
<td><strong>Type</strong></td>
</tr>
<tr>
<td><strong>Data</strong></td>
</tr>
</tbody>
</table>

In certain situations, it is desirable to make sure that the local Workspace Control cache is up to date, before the composer starts the Workspace Control session. If you want the cache to be up to date before the session is started, you use set this registry setting.

- Applying this registry setting bypasses the Fetch change information interval (specified at Administration > Agents, on the Settings tab), after every initial startup or reboot of the computer.
- This registry setting forces an immediate cache update.
- Additionally, applying this registry setting may cause a delay in the logon process.
11.88 XenDesktop7Intercept

<table>
<thead>
<tr>
<th>Intercept unmanaged Citrix XenDesktop\XenApp 7* or Microsoft TS RemoteApp delivered applications</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Key</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Value</strong></td>
</tr>
<tr>
<td><strong>Type</strong></td>
</tr>
<tr>
<td><strong>Data</strong></td>
</tr>
</tbody>
</table>

To intercept unmanaged Citrix XenDesktop\XenApp 7* or Microsoft TS RemoteApp delivered applications:

- Set this registry value on each server that is hosting the applications.
- Enable process interception on the managed application(s) in Workspace Control (only necessary if you want to apply application specific configuration).

* If you use Workspace Control integration with Citrix XenApp Publishing (on page 90), this registry in not needed for Citrix XenApp 7 delivered applications.
Chapter 12: Registry settings for Relay Servers

The following Registry Settings are available to control the behavior of Workspace Control Relay Servers.

12.1 CertificateAlgorithm

| Additional Certificate signing algorithms for Self-Signed Certificates of the Relay Server |
|-----------------------------------------|-----------------------------------------|
| Key                                    | HKLM\Software\RES\Workspace Manager\Relay Server |
| Value                                  | CertificateAlgorithm                    |
| Type                                    | REG_SZ                                  |
| Data                                    | SHA256RSA or SHA384RSA or SHA512RSA     |

A Self-Signed Certificate is used for the TLS (Transport Layer Security) connection between the Relay Server and Workspace Control Agents. The default Certificate signing algorithm used is SHA1RSA.

Please note that after setting this registry value, the Relay Server might not start properly after a reboot. To resolve this, execute the following actions:

- Open a command box with Administrative rights (cmd.exe).
- Enter the following command: `sc config ResRls depend= KeyIso`.

12.2 CertificateKeyLength

| Set the Certificate Key Length for a Relay Server |
|-----------------------------------------|-----------------------------------------|
| Key                                    | HKLM\Software\RES\Workspace Manager\Relay Server |
| Value                                  | CertificateKeyLength                    |
| Type                                    | REG_DWORD                               |
| Data                                    | 512 or 1024 (default) or 2048 or 4096   |

For any other value than the values specified above, the default value will be used.

A key length of at least 1024 is necessary when running Workspace Control sessions on Microsoft Windows 10. On Microsoft Windows 8 / 8.1 / 2012 (R2) and earlier, a key length of 512 suffices.
12.3 CustomCertificate

For the connection between a Workspace Control Agent (RES service) and a Relay Server, and between Relay Servers, custom certificates can be used.

To use custom certificates, the `CustomCertificate` registry value needs to be set. With this registry setting, the value that is used to identify the custom certificate in the certificate store will be specified. By default, the Relay Server will look for the custom certificate's "Subject name" in the "Personal" folder in the certificate store. Optionally, one or both values can be changed by setting the registry values `CustomCertificateFindBy` and `CustomCertificateStore`.

### CustomCertificate

<table>
<thead>
<tr>
<th>Use custom certificates for the connection between the Workspace Control Agent (RES service) and a Relay Server, and between Relay Servers</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Key</strong></td>
</tr>
<tr>
<td><strong>Value</strong></td>
</tr>
<tr>
<td><strong>Type</strong></td>
</tr>
<tr>
<td><strong>Data</strong></td>
</tr>
<tr>
<td><strong>Remark</strong></td>
</tr>
</tbody>
</table>

### CustomCertificateFindBy (optional)

By default, the "Subject name" will be used to identify the custom certificate in the certificate store. With the registry value `CustomCertificateFindBy`, the custom certificate can be identified by its Thumbprint or SerialNumber. When setting this registry value, make sure to specify the correct Data *(i.e. the certificate's thumbprint or serial number)* for the registry value `CustomCertificateFindBy`.

<table>
<thead>
<tr>
<th>Use the certificate's Thumbprint or SerialNumber to identify it in the certificate store</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Key</strong></td>
</tr>
<tr>
<td><strong>Value</strong></td>
</tr>
<tr>
<td><strong>Type</strong></td>
</tr>
<tr>
<td><strong>Data</strong></td>
</tr>
<tr>
<td><strong>Remark</strong></td>
</tr>
</tbody>
</table>
CustomCertificateStore (optional)

By default, the Relay Server will look for the custom certificate in the "Personal" folder in the certificate store. With the registry value CustomCertificateStore, a different folder in the certificate store can be specified. In case a non-English version of Microsoft Windows is being used, the Microsoft Windows internal folder names must be specified for Data. The supported Microsoft Windows internal folder names are specified below:

<table>
<thead>
<tr>
<th>Microsoft Windows internal folder name</th>
<th>Name of folder on an English Microsoft Windows Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root</td>
<td>Trusted Root Certification Authorities</td>
</tr>
<tr>
<td>CertificateAuthority</td>
<td>Intermediate Certification Authorities</td>
</tr>
<tr>
<td>TrustedPublisher</td>
<td>Trusted Publishers</td>
</tr>
<tr>
<td>Disallowed</td>
<td>Untrusted Certificates</td>
</tr>
<tr>
<td>AuthRoot</td>
<td>Third-Party Root Certification Authorities</td>
</tr>
<tr>
<td>TrustedPeople</td>
<td>Trusted People</td>
</tr>
<tr>
<td>AddressBook</td>
<td>Other People</td>
</tr>
</tbody>
</table>

Specify a different folder than "Personal" in the certificate store in which the Relay Server will look for the custom certificate

<table>
<thead>
<tr>
<th>Key</th>
<th>HKLM\Software\RES\Workspace Manager\RelayServer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>CustomCertificateStore</td>
</tr>
<tr>
<td>Type</td>
<td>REG_SZ</td>
</tr>
<tr>
<td>Data</td>
<td>Folder in certificate store the custom certificate is stored in</td>
</tr>
<tr>
<td>Remark</td>
<td>In case a non-English version of Microsoft Windows is being used, the Microsoft Windows internal folder names must be specified for Data.</td>
</tr>
</tbody>
</table>

Notes

- The Subject name on the custom certificate must match the Fully Qualified Domain Name (FQDN) that Workspace Control Agents use to connect to a Relay Server (configured at Administration > Agents, on the Settings tab).
- If the custom certificate cannot be found or is not valid or trusted in some way, an entry will be logged in the Windows event log and connecting to the Relay Server will not be possible.

Disallow use of self-signed certificates

In case the registry value CustomCertificate (and optionally CustomCertificateFindBy and CustomCertificateStore) has not been specified, a self-signed certificate will be used for the connection between the RES service and Relay Server, and between Relay Servers. To disallow the use of a self-signed certificate for these connections, the registry value DoNotAcceptSelfSignedCert must be set. See DoNotAcceptSelfSignedCert (on page 379) for more information.
12.4  **DBCleanupDuration**

<table>
<thead>
<tr>
<th>Specify the duration of the daily cleanup for Relay Servers that are connected directly to the Datastore</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Key</strong></td>
</tr>
<tr>
<td><strong>Value</strong></td>
</tr>
<tr>
<td><strong>Type</strong></td>
</tr>
<tr>
<td><strong>Data</strong></td>
</tr>
</tbody>
</table>

If the duration is not specified, the daily cleanup is not time limited (default behavior) and will continue until finished.

Workspace Control will start (or continue) with the daily cleanup of the Datastore at the time configured at Setup > Advanced Settings (obsolete log files) and Setup > Usage Tracking (obsolete Usage Tracking data).
Chapter 12: Registry settings for Relay Servers

12.5 DoNotAcceptSelfSignedCert

In case the registry value **CustomCertificate** (on page 376) (and optionally **CustomCertificateFindBy** and **CustomCertificateStore**) has not been specified, a self-signed certificate will be used for the connection between a Workspace Control Agent (RES service) and a Relay Server, and between Relay Servers. Set the registry value **DoNotAcceptSelfSignedCert** to disallow the use of a self-signed certificate for these connections.

| Disallow the use of a self-signed certificate for the connection between a Workspace Control Agent and a Relay Server |
|---|---|
| **Key** | HKLM\Software\RES\Workspace Manager (32-bit)  
HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit) |
| **Value** | DoNotAcceptSelfSignedCert |
| **Type** | REG_SZ |
| **Data** | Yes/1/True |

By default, if no custom certificate has been specified, a Workspace Control Agent will connect to a Relay Server that uses a self-signed certificate. Setting this value will prevent this from happening.

| Disallow the use of a self-signed certificate for the connection between different Relay Servers |
|---|---|
| **Key** | HKLM\Software\RES\Workspace Manager\RelayServer |
| **Value** | DoNotAcceptSelfSignedCert |
| **Type** | REG_SZ |
| **Data** | Yes/1/True |
| **Remark** | By default, if no custom certificate was specified, a Relay Server will connect to another Relay Server that uses a self-signed certificate. Setting this value will prevent this from happening. |

By default, if no custom certificate was specified, a Relay Server will connect to another Relay Server that uses a self-signed certificate. Setting this value will prevent this from happening.

**Note**

If the registry value **DoNotAcceptSelfSignedCert** is set without setting the registry value **CustomCertificate**, an entry will be logged in the Windows event log and connecting to the Relay Server will not be possible.
### 12.6 RemoveObsoleteLogFiles

| **Exclude Relay Server from daily cleanup of obsolete log file** |
|---|---|
| **Key** | HKLM\Software\RES\Workspace Manager\Relay Server |
| **Value** | RemoveObsoleteLogFiles |
| **Type** | REG_DWORD |
| **Data** | 0 |

This registry value can only be set for Relay Servers that are connected to the Datastore. In environments where no Agents, but only Relay Servers are connected to the Datastore, please note that by setting this registry value on all Relay Servers, obsolete log files will not be deleted anymore. This may cause an unexpected growth of the Datastore resulting in performance degradation.

### 12.7 RSConnectTimeout

| **Lower the number of seconds of the default connection wait time of 10 seconds** |
|---|---|
| **Key** | • HKLM\Software\RES\Workspace Manager (32-bit)  
• HKLM\Software\Wow6432Node\RES\Workspace Manager (64-bit) |
| **Value** | RSConnectTimeout |
| **Type** | REG_SZ |
| **Data** | 1–9 (number of seconds) |

Every Relay Server that is not available will cause a 10-second delay, because the default connection wait time is 10 seconds.
Chapter 13: Command line Options

13.1 Pwrgate

You can create Managed Applications that start \texttt{pwrgate.exe} with one of the following command line parameters in order to perform an action or start a session.

Workspace Control will perform the specified action or start the specified tool if a user starts the Managed Application.

<table>
<thead>
<tr>
<th>Command line parameters for \texttt{pwrgate.exe}</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-2</td>
<td>Force a session refresh</td>
</tr>
<tr>
<td>-3</td>
<td>Force log off/exit</td>
</tr>
<tr>
<td>-15</td>
<td>Start the \textbf{Restore User Settings} wizard</td>
</tr>
<tr>
<td>-16</td>
<td>Start the \textbf{User Installed Applications Wizard}</td>
</tr>
<tr>
<td>-55</td>
<td>Initiate a graceful restart of a machine from within a Workspace Control session, performing all logoff actions</td>
</tr>
<tr>
<td>-66</td>
<td>Force the Workspace Composer to perform all the actions that it normally does after a refresh. However, this does not refresh the desktop image</td>
</tr>
<tr>
<td>-66 deskpic</td>
<td>Force the Workspace Composer to perform all the actions that it normally does after a refresh, including refreshing the desktop image</td>
</tr>
<tr>
<td>3</td>
<td>Start \textbf{PowerHelp}</td>
</tr>
<tr>
<td>8</td>
<td>Start \textbf{Workspace Preferences}</td>
</tr>
<tr>
<td>15</td>
<td>Start \textbf{Printing Preferences}</td>
</tr>
</tbody>
</table>

The file \texttt{pwrgate.exe} is available in the Workspace Control program directory.
13.2  Pwrtech

13.2.1  Building Blocks and using FIPS compliant security algorithms

When creating a Building Block in a Workspace Control version 10 environment, a password must be specified. When importing this Building Block via the Management Console, this password must be specified again (plain text). When importing this Building Block via a command line with \passwordfips, e.g. pwrtech.exe /ADD c:\folder1\BuildingBlock.xml /passwordfips <Hash of password>, the hash of this password must be specified. Workspace Control version 10 Building Blocks with FIPS enabled can only be imported one by one.

13.2.2  Import file hashes

File hashes can be imported in the Workspace Control Console using a command line option:

Pwrtech.exe /importhashes=<file> /createifnotexists

Specify the full path to a CSV (comma delimited) or TXT file (tab delimited) for <file>. Below more information about the format of CSV and TXT files and several examples.

CSV file

Format: <authorized file name or full path>,<file hash>,<process of authorized file (optional)>,<mode (optional)>,<WorkspaceContainer|WorkspaceContainer (optional)>

Enclose the file name or path in quotation marks if it includes spaces.

To remove files, file hashes, or specific Workspace Containers, the filenames, file hashes, or Workspace Containers in the CSV file must start with a hyphen (-)

TXT file

Format: <Authorized file or application (or the full path to authorized file/application)> <file hash> <process of authorized file (optional)>

<WorkspaceContainer|WorkspaceContainer (optional)>

Enclose the file name or path in quotation marks if it includes spaces.

To remove files, file hashes, or specific Workspace Containers, the filenames, file hashes, or Workspace Containers in the TXT file must start with a hyphen (-)

Examples of when an existing Authorized File matches an imported rule. In the example EXE files are used, other executables files, for example SCR, COM, DLL, are supported as well.

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Authorized File</th>
<th>Authorized Process</th>
<th>Outcome</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full</td>
<td>Notepad.exe</td>
<td>Excel.exe</td>
<td>Existing and imported data match -&gt; update data in</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Workspace Control</td>
</tr>
<tr>
<td>Imported data</td>
<td>Notepad.exe</td>
<td>Excel.exe</td>
<td></td>
</tr>
</tbody>
</table>

No Authorized Process

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Authorized File</th>
<th>Authorized Process</th>
<th>Outcome</th>
</tr>
</thead>
<tbody>
<tr>
<td>Existing data in Workspace Control</td>
<td>Notepad.exe</td>
<td>Allow any process to launch or access this file</td>
<td>Existing and imported data match -&gt; update data in</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Workspace Control</td>
</tr>
<tr>
<td>Imported data</td>
<td>Notepad.exe</td>
<td>Not specified (left blank)</td>
<td></td>
</tr>
</tbody>
</table>

Wildcard in Authorized File path
### Scenario | Authorized File | Authorized Process | Outcome |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Existing data in Workspace Control</td>
<td>*Notepad.exe</td>
<td>Excel.exe</td>
<td>Existing and imported data match -&gt; update data in Workspace Control</td>
</tr>
<tr>
<td>Imported data</td>
<td>*Notepad.exe</td>
<td>Excel.exe</td>
<td></td>
</tr>
</tbody>
</table>

#### Wildcard in existing Authorized File path only

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Authorized File</th>
<th>Authorized Process</th>
<th>Outcome</th>
</tr>
</thead>
<tbody>
<tr>
<td>Existing data in Workspace Control</td>
<td>*Notepad.exe</td>
<td>Excel.exe</td>
<td>Existing and imported data match -&gt; update data in Workspace Control</td>
</tr>
<tr>
<td>Imported data</td>
<td>C:\files\Notepad.exe</td>
<td>Excel.exe</td>
<td></td>
</tr>
</tbody>
</table>

#### Wildcard in imported Authorized File path only

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Authorized File</th>
<th>Authorized Process</th>
<th>Outcome</th>
</tr>
</thead>
<tbody>
<tr>
<td>Existing data in Workspace Control</td>
<td>C:\files\Notepad.exe</td>
<td>Excel.exe</td>
<td>Existing and imported data match -&gt; update data in Workspace Control</td>
</tr>
<tr>
<td>Imported data</td>
<td>*Notepad.exe</td>
<td>Excel.exe</td>
<td></td>
</tr>
</tbody>
</table>

#### Wildcard in Authorized File name only

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Authorized File</th>
<th>Authorized Process</th>
<th>Outcome</th>
</tr>
</thead>
<tbody>
<tr>
<td>Existing data in Workspace Control</td>
<td>Note*</td>
<td>Excel.exe</td>
<td>Existing and imported data match -&gt; update data in Workspace Control</td>
</tr>
<tr>
<td>Imported data</td>
<td>Notepad.exe</td>
<td>Excel.exe</td>
<td></td>
</tr>
</tbody>
</table>

#### Specific existing Authorized File name, wildcard in imported Authorized File name

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Authorized File</th>
<th>Authorized Process</th>
<th>Outcome</th>
</tr>
</thead>
<tbody>
<tr>
<td>Existing data in Workspace Control</td>
<td>Notepad.exe</td>
<td>Excel.exe</td>
<td>Existing and imported data match -&gt; update data in Workspace Control</td>
</tr>
<tr>
<td>Imported data</td>
<td>Note*</td>
<td>Excel.exe</td>
<td></td>
</tr>
</tbody>
</table>

#### No process specified for existing Authorized File, specific process specified for imported Authorized File

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Authorized File</th>
<th>Authorized Process</th>
<th>Outcome</th>
</tr>
</thead>
<tbody>
<tr>
<td>Existing data in Workspace Control</td>
<td>Notepad.exe</td>
<td>Allow any process to launch or access this file</td>
<td>Existing and imported data do not match -&gt; ignore imported data or create new in Workspace Control</td>
</tr>
<tr>
<td>Imported data</td>
<td>Notepad.exe</td>
<td>Excel.exe</td>
<td></td>
</tr>
</tbody>
</table>

#### Process specified for existing Authorized File, no process specified for imported Authorized File

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Authorized File</th>
<th>Authorized Process</th>
<th>Outcome</th>
</tr>
</thead>
<tbody>
<tr>
<td>Existing data in Workspace Control</td>
<td>Notepad.exe</td>
<td>Excel.exe</td>
<td>Existing and imported data do not match -&gt; ignore imported data or create new in Workspace Control</td>
</tr>
<tr>
<td>Imported data</td>
<td>Notepad.exe</td>
<td>Not specified (left blank)</td>
<td></td>
</tr>
</tbody>
</table>

---

**Example scenarios when importing file hashes**

**CSV file format:** `<authorized file name or full path>,<file hash>,<process of authorized file (optional)>,<mode (optional)>,<WorkspaceContainer|WorkspaceContainer (optional)>`
<table>
<thead>
<tr>
<th>Existing configuration in Workspace Control</th>
<th>Imported rules (that match existing configuration)</th>
<th>Result in Workspace Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow hash [XYZ] for Notepad.exe</td>
<td>• Notepad.exe, filehashXYZ,, deny,</td>
<td>Allow hash [XYZ] for Notepad.exe</td>
</tr>
<tr>
<td></td>
<td>• Notepad.exe, filehashXYZ,, allow,</td>
<td></td>
</tr>
<tr>
<td>Allow hash [XYZ] for Notepad.exe</td>
<td>• Notepad.exe, filehashXYZ,, allow,</td>
<td>Deny hash [XYZ] for Notepad.exe</td>
</tr>
<tr>
<td></td>
<td>• Notepad.exe, filehashXYZ,, deny,</td>
<td></td>
</tr>
<tr>
<td>Authorized File for Notepad.exe</td>
<td>• Notepad.exe, , , ,</td>
<td>No Authorized Files for Notepad.exe</td>
</tr>
<tr>
<td>Allow hash [XYZ] for Notepad.exe</td>
<td>• Notepad.exe, filehashPQR,,</td>
<td>Allow hashes [XYZ] and [PQR] for Notepad.exe</td>
</tr>
<tr>
<td>Authorized File for Notepad.exe with</td>
<td>• Notepad.exe, filehashPQR,,</td>
<td>Authorized File for Notepad.exe with Workspace Control set to Workspace Container &quot;Laptops&quot;</td>
</tr>
<tr>
<td>Workspace Control set to Workspace</td>
<td>• Notepad.exe, filehashPQR,,</td>
<td>Authorized File for Notepad.exe with Workspace Control set to Workspace Containers Laptops and Production</td>
</tr>
<tr>
<td>Control set to Workspace Container &quot;Laptops&quot;</td>
<td>• Notepad.exe, , , , ,</td>
<td>Authorized File for Notepad.exe with Workspace Control set to Workspace Container Production</td>
</tr>
</tbody>
</table>

- `/createifnotexists` is an optional value and specifies that the authorized file must be created if it does not yet exist. It will then be created with the specified file hash and process. This value is only applicable for authorized files.

Example:
The CSV file for the authorized file `File_example` contains the following data:

*C:\windows\system32\notepad.exe,56746574657623856,cmd.exe*

Command line option:

`Pwrtech.exe /importhashes=File_example /createifnotexists`

Result:

The file hash `56746574657623856` will be imported for the authorized file `C:\windows\system32\notepad.exe with process cmd.exe`. If the file hash does not yet exist, it will be created for `notepad.exe with process cmd.exe`. If an application and an authorized file for `C:\windows\system32\notepad.exe` exist in the Console, the hash will be added to both the application and the authorized file.

- With CTRL+C, the import of file hashes can be interrupted. In the command box a message will be displayed with the number of files that have been imported until the interrupt.
- When using a command box, processing messages and errors are now displayed. An example of a processing message is how many files hashes were imported. And an error can be, for instance, that the import was not successful.
- In case an error occurs during the import of file hashes, the error level is included with the error. The following errors could be returned:
### Command line Options

#### Error level

<table>
<thead>
<tr>
<th>Error level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>The import of file hashes was completed successfully.</td>
</tr>
<tr>
<td>2</td>
<td>File could not be opened. For instance incorrect syntax or nonexistent file name.</td>
</tr>
<tr>
<td>3</td>
<td>The import of file hashes was interrupted with CTRL+C.</td>
</tr>
<tr>
<td>4</td>
<td>General failure to process the imported file. For instance, the database could not be reached.</td>
</tr>
</tbody>
</table>

#### Error level in case the file could be opened, but the file contents are incorrect

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>401</td>
<td>Incorrect file hash.</td>
</tr>
<tr>
<td>402</td>
<td>Incorrect value for “Type” (allow or deny) for a file hash.</td>
</tr>
<tr>
<td>403</td>
<td>Unknown Workspace for a file hash. Only Workspaces that exist in the Workspace Control Console can be specified in the file.</td>
</tr>
</tbody>
</table>

When importing file hashes for Authorized Files using a CSV or TXT file, please take into consideration the following:

- For each imported rule, the system checks if there are existing Authorized Files (global and application-level) that match the imported combination of authorized executable and additional process.
- If one or more matches are found, then:
  - If the imported file hash is not yet listed in the matching Authorized Files, it is added to them.
  - If the imported file hash is already listed in the matching Authorized Files, and the imported file hash includes a Mode property (= Allow or Deny) then the imported file hash overwrites the Deny/Allow mode of the existing file hash.
    - If the imported file hash does not include a Mode property, then the file hash will be imported with an Allow mode.
  - If the imported rule includes Workspace information, then the specified Workspace Containers are added to or removed from Workspace Control on the matching global Authorized Files.
    - Application-level Authorized Files do not have Workspace Control, so Workspace changes do not take effect there.
    - If multiple Workspace Containers exist with the same name, they are all added or removed as result of the import. Alternatively, specify the Workspace Container GUID in the import rule.
  - Rules in the import are imported and processed top-down, so if the import contains multiple rules that update the same Authorized File or file hash, the end result depends on the order in which the rule appear in the file.
  - An import file that contains a string that is recognized as neither MD5 nor SHA-1 nor SHA-256 will cause the import of the entire file to fail.
13.2.3  Obtain encrypted version of Environment password

Technical managers can obtain the encrypted version of the Environment password by using one of the following command lines on a machine running the Management Console:

- pwrtech.exe /getrspassword
  With Ctrl+C, the encrypted password can be copied from the dialog box to the clipboard.
- pwrtech.exe /getrspassword /f=<full file path>
  The encrypted password is saved in the specified file at the given location.

During an unattended installation of Workspace Control, this password can be provided as an installation parameter (RSPASSWORD) to connect a Workspace Control Agent to a Relay Server.

See also Connect to an existing environment (on page 27).

13.2.4  Process Building Blocks and Custom Resources in batches

You can process Building Blocks and Custom Resources in batches from the Workspace Control Console (pwrtech.exe).

- pwrtech.exe /del <buildingblock file>
  Any object that is in the specified Building Block (<buildingblock file>) will be deleted. Specify the full path to the Building Block for <buildingblock file>
- pwrtech.exe /del /guid={objectguid}
  Delete the object with the GUID as specified between {...}.
- pwrtech.exe /export <filepath> [/type=(type1,type2,...) | /guid={objectguid} ]
  Create Building Block with limited number of features.
  • Specify the specific feature(s) (Type(s)) that need to be included in the Building Block for /type. The list with the different Types can be found below.
  • Separate different Types with a comma (",").
  • If no Types are specified, a Building Block for the entire environment will be created.

Examples:
  pwrtech.exe /export C:\temp\bb.xml /type=printer - > the Building Block bb.xml will be created in C:\temp and will only include data from Type PRINTER.
  pwrtech.exe /export C:\temp\printer_mapping.xml /type=printer,mapping - > Building Block with only data of Types PRINTER and MAPPING will be created.
  Use /guid, to create a Building Block for one specific object. Object GUIDS can be found in the Datastore.
- pwrtech.exe /addresource <resourcefile> /path=Ivanti\Workspace Control [/guid={guid}]
  Add a resource file as a Custom Resource in the specified location.
  • For <resourcefile>, specify the resource file that needs to be added to the Workspace Control environment (full path).
  • For /path, specify the location (full path) where the resource file must be added in the Console (at Administration > Custom Resources).
  • If no path is specified, the resource file will be added as a Custom Resource to the root folder at Administration > Custom Resources.
  • If the specified path does not exist, a new folder will be created in the folder tree at Administration > Custom Resources and the resource file will be added to that folder as a Custom Resource.
Example:
pwrtech.exe /addrres C:\temp\mine.ico /path=\mycustomresources\subfolder - > The resource file mine.ico will be added as a Custom Resource in "subfolder" at Administration > Custom Resources in the MyCustomResources folder.

Giving a value for /guid is optional. /guid can be used to overwrite an existing Custom Resource.

- pwrtech.exe /exportresource /target=<file> [/path=Ivanti Workspace Control | /guid={guid}]

Export a Custom Resource from Workspace Control and place it in the specified location.
- For /target, specify the resource file name and full path the Custom Resource must be exported to.
- For /path, specify the full path to the Custom Resource in the Console.
  - If only a file name is specified, pwrtech.exe will try to extract the Custom Resource from the root folder at Administration > Custom Resources.
  - Specify a value for /guid to extract the Custom Resource with that guid.

Important: Either /path or /guid may be used, not both.

Example:
pwrtech.exe /exportresource /target=C:\temp\dummy.ico /path=mine.ico

The Custom Resource mine.ico will be extracted from the root folder at Administration > Custom Resources and be placed as the resource file dummy.ico at C:\temp.

- pwrtech.exe /delresource [/path=Ivanti Workspace Control | /guid={guid}]

Delete a Custom Resource file from Workspace Control.
- For /path, specify the full path to the Custom Resource file in the Console.
- If only a file name is specified, pwrtech.exe will try to remove the Custom Resource from the root folder at Administration > Custom Resources.
- Specify a value for /guid to remove the Custom Resource with that guid.

Important: Either /path or /guid may be used, not both.

The following Types can be used with /type in the Command line for pwrtech.exe /export:

<table>
<thead>
<tr>
<th>Type</th>
<th>Feature in Management Console</th>
</tr>
</thead>
<tbody>
<tr>
<td>APPLICATION</td>
<td>Composition &gt; Applications</td>
</tr>
<tr>
<td>AUTOMATIONTASK</td>
<td>Composition &gt; Actions By Type &gt; Automation Tasks</td>
</tr>
<tr>
<td>CONFIGMGR</td>
<td>Composition &gt; Actions By Type &gt; Microsoft ConfigMgr</td>
</tr>
<tr>
<td>DATASOURCE</td>
<td>Composition &gt; Applications &gt; Data Sources</td>
</tr>
<tr>
<td>DIRECTORYSERVICE</td>
<td>User Context &gt; Directory Services</td>
</tr>
<tr>
<td>EMAIL</td>
<td>Composition &gt; Applications &gt; E-mail Settings</td>
</tr>
<tr>
<td>EXECUTECOMMAND</td>
<td>Composition &gt; Actions By Type &gt; Execute Command</td>
</tr>
<tr>
<td>FOLDERREDIRECTION</td>
<td>Composition &gt; Actions By Type &gt; Files and Folders &gt; Folder Redirection</td>
</tr>
<tr>
<td>FOLDERSYNC</td>
<td>Composition &gt; Actions By Type &gt; Files and Folders &gt; Folder Synchronization</td>
</tr>
<tr>
<td>HOMEDIRECTORY</td>
<td>Composition &gt; Actions By Type &gt; Files and Folders &gt; User Home Directory</td>
</tr>
<tr>
<td>LOCATION</td>
<td>User Context &gt; Locations and Devices</td>
</tr>
<tr>
<td>MAPPING</td>
<td>Composition &gt; Actions By Type &gt; Files and Folders &gt; Drive and Port Mappings</td>
</tr>
</tbody>
</table>

Example:
pwrtech.exe /addresource C:\temp\mine.ico /path=\mycustomresources\subfolder - > The resource file mine.ico will be added as a Custom Resource in "subfolder" at Administration > Custom Resources in the MyCustomResources folder.

Giving a value for /guid is optional. /guid can be used to overwrite an existing Custom Resource.

- pwrtech.exe /exportresource /target=<file> [/path=Ivanti Workspace Control | /guid={guid}]

Export a Custom Resource from Workspace Control and place it in the specified location.
- For /target, specify the resource file name and full path the Custom Resource must be exported to.
- For /path, specify the full path to the Custom Resource in the Console.
  - If only a file name is specified, pwrtech.exe will try to extract the Custom Resource from the root folder at Administration > Custom Resources.
  - Specify a value for /guid to extract the Custom Resource with that guid.

Important: Either /path or /guid may be used, not both.

Example:
pwrtech.exe /exportresource /target=C:\temp\dummy.ico /path=mine.ico

The Custom Resource mine.ico will be extracted from the root folder at Administration > Custom Resources and be placed as the resource file dummy.ico at C:\temp.

- pwrtech.exe /delresource [/path=Ivanti Workspace Control | /guid={guid}]

Delete a Custom Resource file from Workspace Control.
- For /path, specify the full path to the Custom Resource file in the Console.
- If only a file name is specified, pwrtech.exe will try to remove the Custom Resource from the root folder at Administration > Custom Resources.
- Specify a value for /guid to remove the Custom Resource with that guid.

Important: Either /path or /guid may be used, not both.

The following Types can be used with /type in the Command line for pwrtech.exe /export:

<table>
<thead>
<tr>
<th>Type</th>
<th>Feature in Management Console</th>
</tr>
</thead>
<tbody>
<tr>
<td>APPLICATION</td>
<td>Composition &gt; Applications</td>
</tr>
<tr>
<td>AUTOMATIONTASK</td>
<td>Composition &gt; Actions By Type &gt; Automation Tasks</td>
</tr>
<tr>
<td>CONFIGMGR</td>
<td>Composition &gt; Actions By Type &gt; Microsoft ConfigMgr</td>
</tr>
<tr>
<td>DATASOURCE</td>
<td>Composition &gt; Applications &gt; Data Sources</td>
</tr>
<tr>
<td>DIRECTORYSERVICE</td>
<td>User Context &gt; Directory Services</td>
</tr>
<tr>
<td>EMAIL</td>
<td>Composition &gt; Applications &gt; E-mail Settings</td>
</tr>
<tr>
<td>EXECUTECOMMAND</td>
<td>Composition &gt; Actions By Type &gt; Execute Command</td>
</tr>
<tr>
<td>FOLDERREDIRECTION</td>
<td>Composition &gt; Actions By Type &gt; Files and Folders &gt; Folder Redirection</td>
</tr>
<tr>
<td>FOLDERSYNC</td>
<td>Composition &gt; Actions By Type &gt; Files and Folders &gt; Folder Synchronization</td>
</tr>
<tr>
<td>HOMEDIRECTORY</td>
<td>Composition &gt; Actions By Type &gt; Files and Folders &gt; User Home Directory</td>
</tr>
<tr>
<td>LOCATION</td>
<td>User Context &gt; Locations and Devices</td>
</tr>
<tr>
<td>MAPPING</td>
<td>Composition &gt; Actions By Type &gt; Files and Folders &gt; Drive and Port Mappings</td>
</tr>
</tbody>
</table>
### Type | Feature in Management Console
--- | ---
PRINTER | Composition > Actions By Type > Printers
PROFILEDIRECTORY | Composition > Actions By Type > Files and Folders > User Profile Directory
REGISTRY | Composition > Actions By Type > User Registry
SUBSTITUTE | Composition > Actions By Type > Files and Folders > Drive Substitutes
USERSETTING | Composition > User Settings
VARIABLE | Composition > Actions By Type > Environment Variables

To facilitate these batch scripts, the following error levels are available and will be returned in `%errorlevel%`:

<table>
<thead>
<tr>
<th>Error level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>The command line was executed successfully.</td>
</tr>
<tr>
<td>1</td>
<td>The file was not specified in the command line.</td>
</tr>
<tr>
<td>2</td>
<td>The file was not a valid XML file.</td>
</tr>
<tr>
<td>3</td>
<td>The object was not found in the Datastore.</td>
</tr>
<tr>
<td>4</td>
<td>Saving the Custom Resource in the Datastore failed.</td>
</tr>
<tr>
<td>5</td>
<td>Deleting the object or Custom Resource failed.</td>
</tr>
<tr>
<td>6</td>
<td>The /guid has an invalid guid specified.</td>
</tr>
<tr>
<td>7</td>
<td>The object specified with /guid does not exist.</td>
</tr>
<tr>
<td>8</td>
<td>The Custom Resource specified with /guid does not exist.</td>
</tr>
<tr>
<td>9</td>
<td>Insufficient rights, the caller belongs to an administrative role which does not have modify permissions for the object type or Custom Resources.</td>
</tr>
<tr>
<td>10</td>
<td>Required command line options not specified.</td>
</tr>
<tr>
<td>11</td>
<td>The path specified for /path does not exist.</td>
</tr>
<tr>
<td>12</td>
<td>Importing a Building Block via the command line with /passwordfips failed, because the file name contains a wildcard (* or ? or</td>
</tr>
<tr>
<td>14</td>
<td>Importing a Building Block via the command line failed, because no /passwordfips is provided or the password is incorrect.</td>
</tr>
</tbody>
</table>
13.2.5 Republish a published application

You can republish a published application with the following command line:

```
%respfdir%/pwrtech.exe /republishusers {AppID | AppGUID}
```

This command line is useful in situations where access to a published application is based on, for instance, OU membership or Identity Director Service (configured on the Access Control > Identity tab of an application). For example, using this command line in the workflow of the Identity Director Service that gives users access to the application, will trigger an immediate republish of the application when the user requests it. Without this command line, the user could request the published application, but the published application could not yet be accessed through Citrix. Republishing the application is necessary for this.

Examples

Command line with AppID: `%respfdir%/pwrtech.exe /republishusers 167`

Command line with AppGUID: `%respfdir%/pwrtech.exe /republishusers {3F634F83-5048-46E4-9D2B-61CCF3761A4A}`

13.3 Setprint

<table>
<thead>
<tr>
<th>Command line parameters for setprint.exe</th>
</tr>
</thead>
<tbody>
<tr>
<td>/allowconnect</td>
</tr>
</tbody>
</table>

13.4 Network Security Log

You can export the Network Security log file in the interchangeable XML format using the following command line.

```
Pwrtech.exe /exportlog /type=network /output=<output filepath> /start=<start date> /end=<end date>
```

Example:

```
Pwrtech.exe /exportlog /type=network /output=C:\outputlog.xml /start=20160101 /end=20160229
```

You must set the value for output. The values for start and end need to be set in the YYYYMMDD (optionally YYYYYMMDD HHMMSS) format and are not mandatory.

Note

At least read permission on the Network Connections node (at Security > Network Connections) is needed to export this log successfully. With insufficient access rights, the XML export file will contain no data.
## 14.1 The order of events when a session starts

<table>
<thead>
<tr>
<th>Event</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Load language settings</td>
<td></td>
</tr>
<tr>
<td>2. Initialize MLS</td>
<td></td>
</tr>
<tr>
<td>3. Identify the computer/client and its properties:</td>
<td>By default, a computer’s connection state is “online” if it can reach the IP address of the local network connection. Advanced connection state settings may apply for specific Zones, as configured at User Context &gt; Connection States in the Management Console.</td>
</tr>
<tr>
<td>- Name</td>
<td></td>
</tr>
<tr>
<td>- IP address</td>
<td></td>
</tr>
<tr>
<td>- Session ID</td>
<td></td>
</tr>
<tr>
<td>- Operating System type and version</td>
<td></td>
</tr>
<tr>
<td>- Connection state</td>
<td></td>
</tr>
<tr>
<td>4. Determine primary Directory Service and OU and group memberships</td>
<td></td>
</tr>
<tr>
<td>5. Determine accessible Zones</td>
<td></td>
</tr>
<tr>
<td>6. Determine accessible Workspace Containers</td>
<td>If the option Let user decide which accessible Workspace Container to use is selected for a managed application, user is prompted to choose a Workspace Container.</td>
</tr>
<tr>
<td>7. Determine accessible Workspace Containers</td>
<td></td>
</tr>
<tr>
<td>8. Set:</td>
<td>Environment Variables are set in the order in which they appear in the list at Composition &gt; Actions By Type &gt; Environment Variables in the Management Console.</td>
</tr>
<tr>
<td>- Managed Applications Properties</td>
<td></td>
</tr>
<tr>
<td>- Desktop &gt; Lockdown and Behavior</td>
<td></td>
</tr>
<tr>
<td>- Desktop &gt; Background</td>
<td></td>
</tr>
<tr>
<td>9. Set Security for:</td>
<td></td>
</tr>
<tr>
<td>- Applications</td>
<td></td>
</tr>
<tr>
<td>- Removable Disks</td>
<td></td>
</tr>
<tr>
<td>- Files and Folders</td>
<td></td>
</tr>
<tr>
<td>- Read-only Blanketing</td>
<td></td>
</tr>
<tr>
<td>- Global Authorized Files</td>
<td></td>
</tr>
<tr>
<td>- Network</td>
<td></td>
</tr>
<tr>
<td>10. Set shell</td>
<td></td>
</tr>
<tr>
<td>11. Access Balancing</td>
<td></td>
</tr>
<tr>
<td>12. Set Environment Variables</td>
<td></td>
</tr>
<tr>
<td>13. User Settings storage location</td>
<td>Map Drive or connect Full path.</td>
</tr>
</tbody>
</table>
### Event Order in Workspace Control Sessions

<table>
<thead>
<tr>
<th>Event</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>13. Set Folder Redirections</td>
<td>If configured, certain folders of the user profile (e.g. Appdata, Documents, etc.) are redirected to a different path, such as a shared network location. If possible, target folders are created. A backup is made of pre-existing folder redirections.</td>
</tr>
<tr>
<td>14. Execute Automation Tasks</td>
<td>If configured with the option <strong>Run before other actions</strong>.</td>
</tr>
<tr>
<td>15. Execute Microsoft ConfigMgr software distributions</td>
<td>If configured with the option <strong>Run before other actions</strong>.</td>
</tr>
<tr>
<td>16. Execute LANDesk software distributions</td>
<td>If configured with the option <strong>Run before other actions</strong>.</td>
</tr>
</tbody>
</table>
| 17. Execute Commands | • If configured with the option **At logon before other actions**.  
   • Commands are executed asynchronously, in the order in which they appear in the list at Composition > Actions By Type > Execute Command in the Management Console. |
| 18. Set Drive and Port Mappings | • If fast connect is enabled, the actual mappings are not established until the moment of use.  
   • Drive and Port Mappings are processed asynchronously if the option **Wait for task to finish before continuing** is cleared.  
   • If the User Settings storage location could not be mapped directly after Environment Variables, then it is mapped now. |
| 19. Set Drive Substitutes | |
| 20. Check/create Folder Redirection target folders | |
| 21. Set Sessions Security + check passthrough | |
| 22. Printers | • If fast connect is enabled for printers, the actual printer connections are not established until the moment of use.  
   • Printers are processed asynchronously if the option **Wait for task to finish before continuing** is cleared. |
| 23. Build User Home Directory | |
| 24. Perform Folder Synchronization actions | |
|  • determine sampling mode | |
|  • load settings | |
| 26. Set User Registry settings | |
| 27. Build User Profile Directory | |
| 28. Execute Commands | • If configured with the option **At logon after other actions**.  
   • Commands are executed asynchronously, in the order in which they appear in the list at Composition > Actions By Type > Execute Command in the Management Console. |
| 29. Execute Automation Tasks | |
### Chapter 14: The order of events in Workspace Control sessions

<table>
<thead>
<tr>
<th>Event</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>30. Execute Microsoft ConfigMgr software distributions</td>
<td></td>
</tr>
<tr>
<td>31. Execute LANDesk software distributions</td>
<td></td>
</tr>
<tr>
<td>32. Set default printer</td>
<td></td>
</tr>
<tr>
<td>33. Load language settings and mappings</td>
<td></td>
</tr>
</tbody>
</table>
| 34. Data Sources | • Remove existing Data Sources  
| | • Create Data Sources configured with the option **Create Data Source during logon**. (By default, Data Sources are created when the linked application is started.) |
| 35. Load settings for: | • Usage tracking  
| | • CPU Optimization  
| | • Instant LogOff  
| | • Memory Optimization  
| | • Desktop/Screensaver  
| | • Web Portal  
| 36. Create Start Menu items | The Start Menu is created asynchronously. |
| 37. Initialize Process Interception | |
| 38. Set Security for: | • Applications  
| | • Removable Disks  
| | • Files and Folders  
| | • Read-only Blanketing  
| | • Global Authorized Files  
| | • Network  
| 39. Remove existing File Associations and create new ones | |

At this point, the session has started and the user’s workspace is available. In the meantime, application-level User Settings are processed in the background:

- determine sampling mode
- load settings

⚠️ **Tip**

In a user’s Workspace Analysis, the Event Logs show full details of each logged session.
### 14.2 The order of events at a session refresh

<table>
<thead>
<tr>
<th>Event</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Query local IP of Subscriber/Desktop Extender client</td>
<td></td>
</tr>
<tr>
<td>2. Determine refresh mode</td>
<td>(silent yes/no)</td>
</tr>
<tr>
<td>3. Restart Guardian process</td>
<td></td>
</tr>
<tr>
<td>4. Set process priority of <code>pfwsmgr.exe</code> to Normal</td>
<td></td>
</tr>
<tr>
<td>5. Query for license on client through virtual channel</td>
<td></td>
</tr>
<tr>
<td>6. If not silent refresh, hide desktop/taskbar</td>
<td></td>
</tr>
<tr>
<td>7. Reload license info</td>
<td></td>
</tr>
<tr>
<td>8. Close desktop process</td>
<td></td>
</tr>
<tr>
<td>9. Unload application menus</td>
<td></td>
</tr>
<tr>
<td>10. Reload language settings</td>
<td></td>
</tr>
<tr>
<td>11. Initialize MLS</td>
<td></td>
</tr>
<tr>
<td>12. Re-load user context</td>
<td>(username, group membership, OU membership, Zones, workspace containers, etc.)</td>
</tr>
<tr>
<td>13. Load language specific actions</td>
<td>(registry, etc.)</td>
</tr>
<tr>
<td>14. Check for valid license on client through virtual channel</td>
<td></td>
</tr>
<tr>
<td>15. Reload application menus</td>
<td></td>
</tr>
<tr>
<td>16. Initialize Process Interception</td>
<td></td>
</tr>
<tr>
<td>17. Load desktop items</td>
<td></td>
</tr>
<tr>
<td>18. Set screensaver timeout</td>
<td></td>
</tr>
<tr>
<td>19. Set Security for:</td>
<td></td>
</tr>
<tr>
<td>• Applications</td>
<td></td>
</tr>
<tr>
<td>• Removable Disks</td>
<td></td>
</tr>
<tr>
<td>• Files and Folders</td>
<td></td>
</tr>
<tr>
<td>• Read-only Blanketing</td>
<td></td>
</tr>
<tr>
<td>• Global Authorized Files</td>
<td></td>
</tr>
<tr>
<td>• Network</td>
<td></td>
</tr>
<tr>
<td>20. Remap removable disks</td>
<td></td>
</tr>
<tr>
<td>21. Configure network security</td>
<td></td>
</tr>
<tr>
<td>22. Start desktop</td>
<td></td>
</tr>
<tr>
<td>23. Load quicklaunch/taskbar items</td>
<td></td>
</tr>
<tr>
<td>24. Configure instant file associations</td>
<td></td>
</tr>
<tr>
<td>25. Refresh mappings, substitutes</td>
<td></td>
</tr>
</tbody>
</table>
### Chapter 14: The order of events in Workspace Control sessions

<table>
<thead>
<tr>
<th>Event</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>26. Reconnect printers at refresh</td>
<td></td>
</tr>
<tr>
<td>27. Run folder sync tasks at refresh</td>
<td></td>
</tr>
<tr>
<td>28. Run external tasks at refresh</td>
<td></td>
</tr>
<tr>
<td>29. Run autolaunch items</td>
<td></td>
</tr>
<tr>
<td>30. Show desktop/taskbar</td>
<td></td>
</tr>
<tr>
<td>31. Check for new apps in menu (and display message if needed)</td>
<td></td>
</tr>
<tr>
<td>32. Check autolaunch new apps on refresh</td>
<td></td>
</tr>
<tr>
<td>33. Check running apps &amp; terminate if needed</td>
<td></td>
</tr>
<tr>
<td>34. Reset process priority for pfwsgr.exe to High</td>
<td></td>
</tr>
<tr>
<td>35. Save user event log (Actions (/PowerLaunch) log)</td>
<td></td>
</tr>
</tbody>
</table>

At this point, the session has started and the user’s workspace is available. In the meantime, application-level User Settings are processed in the background:

- determine sampling mode
- load settings

**Note**

In sessions running on Microsoft Windows 8, 8.1, 2012 R2, or 10, changes to tiles on the Start screen are not executed at a session refresh. Microsoft’s architecture on these Operating Systems does not allow a smooth addition or deletion of tiles.
## The order of events when a session ends

<table>
<thead>
<tr>
<th>Event</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Disconnect session</td>
<td>• If Instant Logoff is enabled</td>
</tr>
<tr>
<td></td>
<td>• &quot;Before Workspace Control splash screen appears&quot; is enabled</td>
</tr>
<tr>
<td></td>
<td>for Disconnect user session when log off is initiated</td>
</tr>
<tr>
<td>2. Save User Settings</td>
<td>User Settings are processed synchronously.</td>
</tr>
<tr>
<td>3. Run folder sync tasks at logoff</td>
<td></td>
</tr>
<tr>
<td>4. Execute Commands</td>
<td>Commands are executed synchronously, in the order in which they appear</td>
</tr>
<tr>
<td></td>
<td>in the list at Composition &gt; Actions By Type &gt; Execute Command in the</td>
</tr>
<tr>
<td></td>
<td>Management Console.</td>
</tr>
<tr>
<td>5. Save Memory Optimization statistics</td>
<td></td>
</tr>
<tr>
<td>6. Unload taskbar</td>
<td></td>
</tr>
<tr>
<td>7. Release VDX license</td>
<td></td>
</tr>
<tr>
<td>8. Release any application</td>
<td></td>
</tr>
<tr>
<td>concurrent licenses</td>
<td></td>
</tr>
<tr>
<td>9. Release Workspace Control license</td>
<td></td>
</tr>
<tr>
<td>10. Remove Sessions Security (SessionGuard) lock</td>
<td></td>
</tr>
<tr>
<td>11. Remove drive mappings</td>
<td></td>
</tr>
<tr>
<td>12. Restore persistent drive</td>
<td></td>
</tr>
<tr>
<td>mappings</td>
<td></td>
</tr>
<tr>
<td>13. Save default printer</td>
<td></td>
</tr>
<tr>
<td>14. Save printer preferences</td>
<td></td>
</tr>
<tr>
<td>15. Remove printer connections</td>
<td></td>
</tr>
<tr>
<td>16. Remove File Types (Instant File Associations)</td>
<td></td>
</tr>
<tr>
<td>17. Remove policies</td>
<td></td>
</tr>
<tr>
<td>18. Remove webtop</td>
<td></td>
</tr>
<tr>
<td>19. Close security for:</td>
<td></td>
</tr>
<tr>
<td>• Applications</td>
<td></td>
</tr>
<tr>
<td>• Removable Disks</td>
<td></td>
</tr>
<tr>
<td>• Files and Folders</td>
<td></td>
</tr>
<tr>
<td>• Read-only Blanketing</td>
<td></td>
</tr>
<tr>
<td>• Global Authorized Files</td>
<td></td>
</tr>
<tr>
<td>• Network</td>
<td></td>
</tr>
<tr>
<td>and</td>
<td></td>
</tr>
<tr>
<td>Close Process Interception</td>
<td></td>
</tr>
<tr>
<td>20. Cleanup Folder Redirections</td>
<td>Folder redirections for the user that started the session are restored.</td>
</tr>
<tr>
<td>21. Synchronize User Settings</td>
<td></td>
</tr>
<tr>
<td>Event</td>
<td>Remarks</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>22. Disconnect session</td>
<td>If &quot;After Workspace Control splash screen disappears&quot; is enabled for Disconnect user session when log off is initiated</td>
</tr>
</tbody>
</table>
Chapter 15: Compatibility Matrix Workspace Control

The compatibility matrix for Workspace Control is now maintained at https://forums.ivanti.com/s/article/Workspace-Control-Maintained-Platform-Matrix-10-3-x
Chapter 16: Feature deprecation

In a next version of Workspace Control, the following features are no longer supported. Most of these features have already been removed. The remaining features on this list are scheduled to be removed from the product in a next release.

✔ = Supported
☑ = Available, not supported
☒ = Removed, end of support

<table>
<thead>
<tr>
<th>Product Name / Feature</th>
<th>2015*</th>
<th>2016*</th>
<th>v10</th>
<th>v10.1</th>
<th>v10.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Windows XP</td>
<td>✔</td>
<td>✔</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
</tr>
<tr>
<td>Microsoft Windows Vista</td>
<td>✔</td>
<td>✔</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
</tr>
<tr>
<td>Microsoft Server 2003</td>
<td>✔</td>
<td>✔</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
</tr>
<tr>
<td>Microsoft Server 2008</td>
<td>✔</td>
<td>✔</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
</tr>
<tr>
<td>Microsoft SCCM 2007 SP2</td>
<td>✔</td>
<td>✔</td>
<td>☒*</td>
<td>☒*</td>
<td>☒*</td>
</tr>
<tr>
<td>Microsoft SCCM 2007 R3</td>
<td>✔</td>
<td>✔</td>
<td>☒*</td>
<td>☒*</td>
<td>☒*</td>
</tr>
<tr>
<td>Microsoft Windows NT Domains</td>
<td>✔</td>
<td>✔</td>
<td>☒*</td>
<td>☒*</td>
<td>☒*</td>
</tr>
<tr>
<td>Microsoft App-V 4.x</td>
<td>✔</td>
<td>✔</td>
<td>☒*</td>
<td>☒*</td>
<td>☒*</td>
</tr>
<tr>
<td>Novell Directory Services</td>
<td>✔</td>
<td>✔</td>
<td>☒*</td>
<td>☒*</td>
<td>☒*</td>
</tr>
<tr>
<td>Citrix XenApp 6.0</td>
<td>✔*</td>
<td>✔*</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
</tr>
<tr>
<td>Citrix XenDesktop/XenApp 5.x</td>
<td>✔*</td>
<td>✔*</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
</tr>
<tr>
<td>Citrix Presentation Server (all)</td>
<td>✔*</td>
<td>✔*</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
</tr>
<tr>
<td>Citrix Application Streaming</td>
<td>✔*</td>
<td>✔*</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
</tr>
<tr>
<td>RES HyperDrive</td>
<td>✔*</td>
<td>✔*</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
</tr>
<tr>
<td>E-mail Setting: HP OpenMail</td>
<td>✔</td>
<td>✔</td>
<td>☒*</td>
<td>☒*</td>
<td>☒*</td>
</tr>
</tbody>
</table>
## Chapter 16: Feature deprecation

<table>
<thead>
<tr>
<th>Product Name / Feature</th>
<th>Workspace (Control) versions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2015*</td>
</tr>
<tr>
<td>E-mail Setting: IMAP (Outlook XP only)</td>
<td>✔️</td>
</tr>
<tr>
<td>E-mail Setting: Internet Mail</td>
<td>✔️</td>
</tr>
<tr>
<td>E-mail Setting: Lotus Notes Mail</td>
<td>✔️</td>
</tr>
<tr>
<td>E-mail Setting: Microsoft Mail</td>
<td>✔️</td>
</tr>
<tr>
<td>E-mail Setting: Microsoft Outlook Express</td>
<td>✔️</td>
</tr>
<tr>
<td>E-mail Setting: Nortel CallPilot</td>
<td>✔️</td>
</tr>
<tr>
<td>E-mail Setting: Oracle Connector for Outlook</td>
<td>✔️</td>
</tr>
<tr>
<td>E-mail Setting: Zarafa Groupware Server</td>
<td>✔️</td>
</tr>
<tr>
<td>IBM DB2</td>
<td>✔️</td>
</tr>
</tbody>
</table>

*Note: The referenced RES ONE Workspace 2015 and RES ONE Workspace 2016 include all ‘Service Releases’, ‘Feature Packs’ and ‘Minor’ releases.

**“Best Effort” Support: “Best Effort” means that if something used to work correctly and stopped working, Ivanti will try to make it work as before. This does not mean that Ivanti will add new functionality to unsupported products or provide support for unsupported products (the 3rd party product was not supported in the major release).**
Chapter 17: Index

A
About Workspace Control • 4
Access Balancing • 327
Access Control • 157, 174
Access Control based on context • 126, 174, 179
Access Control on Workspace Containers • 141
Access principle • 147
Access Wizard • 184
Actions • 175, 176, 213
ActiveSetupTimeout • 338
Add and remove Citrix XenApp Servers using the command line • 101
Add/Update Applications and Delete Applications • 65
Additional User Setting options • 273
Administration • 317
Administrative roles • 66
Administrative Roles • 212, 317
Advanced Settings • 122
Agents • 44, 314, 320
Agents Overview • 314
Agents Settings • 44, 320
Alerting • 76, 90
Allow users to choose a configuration set based on Workspace Container • 142
Allow users to restore their own settings • 276
AppguardDump • 197
Application level • 282, 297
Application List tab • 149
Application Managers • 127, 170, 171, 172
Application Virtualization • 91
Applications • 148, 149, 162, 281
Applications and ApplicationsSaveMandatory • 190
Applications security modes
  disabled, learning, enabled • 281
Applications User Settings • 277
Architecture • 5
Architecture Overview • 14
Assign permissions to users • 290
Associated items • 66
Audit Trail • 183, 313
Audit Trail options • 313
Authorize a specific application to use specific connections • 299
Authorize files and folders • 295
Authorized Connections • 181
Authorized Files • 180, 280, 295
AutoHide • 194
Automation • 116
Automation Tasks • 214
Availability • 145
B
Background • 244, 245
Blacklisting • 301
BlockPicaSvcFix • 339
Building Blocks • 63
Building Blocks and using FIPS compliant security algorithms • 383
C
Capture targeted items on application/session end • 258
Central storage location of User Settings and other user-specific information • 269, 271
CertificateAlgorithm • 376
CertificateKeyLength • 376
Change language of Management Console • 70
ChangePasswordTimeout • 339
Check the connection settings of an Agent to a Datastore or Relay Server • 48
CheckDisabledFolders • 339
CheckShutDown • 340
CheckUpdateOSDFile • 340
Citrix XenApp Integration • 138
Citrix XenApp Publishing • 89, 91, 375
Command line Options • 382
Command line parameters • 67
Communication Model • 10
Compatibility Matrix Workspace Control • 398
Components • 5
Composition • 148
Computer Control • 141
Configuration • 157, 175
Configuration Wizard • 38
Configuration Wizard for existing Workspace Control site • 38, 71
Configure a Citrix XenApp published application • 99
Configure a managed application as Citrix XenApp published content • 101
Configure Access Control for Workspace Preferences, PowerHelp, Printing Preferences and Refresh Start menu • 200
Configure Agent connection after installation • 33
Configure Agents • 34
Configure Automation Tasks • 214
Configure commands • 219
Configure different settings for certain parts of the environment • 302
Configure Directory Maintenance • 230
Configure directory services • 136
Configure Drive and Port Mappings • 221
Configure Drive Substitutes • 223
Configure Environment Variables • 216
Configure folder synchronization • 228
Configure linked actions • 243
Configure printers • 234
Configure registry policies • 242
Configure Registry Settings • 238
Configure the Datastore • 37
Configure the Datastore dynamically • 39, 43
Configure the Workspace Composer as a Citrix XenApp Published Application • 94, 96
Configure User Installed Applications • 284
Configure user-specific Access Balancing settings • 328
Configure user-specific Instant LogOff settings • 332
Configure user-specific Memory Optimization settings • 335
Configure user-specific settings • 303
Configure Web Portal styles • 121
Configure Website Security • 296
Configure Workspace Extensions • 161
Connect to an existing environment • 28, 33, 387
Connection States • 146, 219
Connections • 72
ConsoleNoAppIcons • 340
Context menu options • 311
CorrectTaskbar • 341
CorrectWorkArea • 341
CPU Optimization • 183, 327, 329
Create a Blocked Connection for monitoring purposes in Blacklisting environments • 298
Create a drive mapping using information from Active Directory • 222
Create a list from which users can choose a printer • 185
Create a new application with rundll32.exe and the appropriate parameter • 201
Create a new Datastore • 26
Create and edit Applications • 157
Create Building Blocks • 64
CTX_PFDesktopUsesPwrstart • 341
CTX_PNLaunchUsesFarmName • 342
CTX_PublishAppCmdLineFlag • 342
Custom Resources • 324
CustomCertificate • 377, 380
Customize the contents and presentation • 61
Data • 289
Data Sources • 175, 179, 212
Datastore connection and port • 321
Datastore Management • 72
Datastore Migration Wizard • 72, 74
Datastore Split/Join Wizard • 75
Date and Time • 135
DBCleanupDuration • 379
Default behavior if running applications are no longer authorized • 282
Default behavior of Microsoft Windows 10 affecting Workspace Control • 154
Default Hide drives behavior • 222
Defaults for new applications • 156
Desktop • 244
Desktop and DesktopSaveMandatory • 188
Desktop Sampler • 54
Desktop Transformation • 54
DesktopBackGround • 191
DesktopBackGroundPlacement • 191
DesktopColor • 187
DesktopForegroundColor • 187
Detailed information about users • 305
Diagnostics • 157, 183, 304
Directory Maintenance • 230
Directory Services • 136
DirectoryServiceRetryLimit • 342
Disable various tabs on Control Panel applets • 211
Disabled Features • 70
DisableDHCP • 343
DisableExternalGroupCheck • 343
DisableFolderSyncLocalCheck • 344
DisableIconRefresh • 344
DisableTileManagement • 344
Disconnect user session when logoff is initiated • 332
Distributed environment • 16
Do not passthrough if available locally • 102
DoNotAcceptSelfSignedCert • 378, 380
DoNotAllowOverlappedDesktopItems • 345
DoNotAnayliseDB • 345
DoNotShowAgain • 195
Drive and Port Mappings • 220
Drive mappings • 290
Drive Substitutes • 223
Dynamic Datastore configuration for Agents • 28, 39
Dynamic Privileges • 182
Dynamic Relay Server configuration • 43
E
Edit references to external files • 68
E-mail Settings • 175, 178, 212
EnableMultipleIE • 345
Environment Variables • 216, 245
Errors • 316
Event Log • 322
Example • 40, 285
allow a user to choose a pre-set application configuration • 143
allow a user to choose a pre-set session configuration • 143
block and authorize files • 292
force a session to start in a particular, exclusive Workspace Container • 144
Use a USB device for authentication purposes • 129, 135
Examples • 226, 229, 231, 288, 300
Examples multiple Directory Services • 139
Exceptions to blocked connections when Blacklisting • 298
Exclude a specific application from CPU Optimization • 330
Exclude a specific application from Memory Optimization • 335
Exclude certain types of users • 302
Exclude passthrough sessions • 302
ExcludeProcesses • 346
ExcludeSubscribedTasks • 346
Execute Command • 218
Exempt an application from Network Security Settings • 299
Feature deprecation • 64, 138, 399
File Types • 157, 168, 212
Files and Folders • 220
Files and Folders security • 281, 292
Files and Folders security Mode disabled, learning, enabled • 292
Filter Criteria and Filter Types • 59
Filtering • 58
Filters • 319
Flex Profile Kit INI files • 267
Folder Redirection • 224
Folder Synchronization • 227
ForceComputername • 347
ForceDisconnectOnIdle • 347
ForceLogoff • 348
ForcePrinterConnections • 349
ForceShutdown • 349
General • 157
General Functionality • 58
General information about users • 304
Global level • 281, 297
Global Network Security and application-based Authorized Connections • 299
GUIDs • 68
Hide this workspace container if user needs to select one • 144
HideDescription • 192
HideMyNameInScreensaver • 193
HotKeyModifier and HotKeyKey • 194
Identity • 127
Identity Director • 117
Import Building Blocks • 64
Import Building Blocks into a specific workspace • 66
Import file hashes • 295, 383
IncludeProcesses • 350
Individual blocked connections • 297
Information excluded from Building Blocks • 67
Information excluded from Instant Reports • 62
Install the Desktop Sampler • 55
Install Workspace Control Agent Service under different account • 20, 21
Installation • 17, 19
Installation public properties • 23, 33
Instant LogOff • 327, 331
Instant LogOff Modes disabled, log only, enabled • 331
Instant Report format • 61
Instant Reports • 61
Instrumentation • 350
Integrate Automation Tasks • 116
Integrate Citrix XenApp Publishing • 92
Integrate File Types with Workspace Extensions • 161
Integrate Identity Director services • 117
Integrate Microsoft App-V • 104
Integrate Microsoft TS RemoteApp • 108
Integration • 89
InterceptManagedApps • 351
Introduction to the Workspace Control Administration Guide • 1
Ivanti Products • 116
Ivanti Support • 3
Ivanti Training • 2
Keep Workspace Control up to date • 49
KeepSeamlessHostAgent • 351
KeepSharesWithROB • 352
KeepTmpDDEMacros • 352
KeepUnicodePath • 352
KeepUserDefaultMAPIProfile • 353
KeepWordRunning • 353
Known limitations of Workspace Control on Microsoft Windows 8.1, 2012 R2, and 10 • 156
LANDesk • 89, 112, 232
Language Identity • 127, 242
Languages • 70, 147
Languages Example • 147
Nodes excluded from filtering • 60
NoFullScreenKiosk • 358
NoListConcurrentUsers • 358
NoNetGuard • 195
NoPrecedingSlashInPNFolder • 359
NoRecordLimit • 197
NoScreensaver • 198
Notifications • 157, 174
NotifyDefaultPrinterChange • 196
Novell Directory Services • 138
NoVistaAppguard • 187

O
Obtain encrypted version of Environment password • 387
OnTop • 194
Order of processing • 145
OutlookNoOpenDialog • 196
OutlookNotificationCheck • 359
Override local caching • 277

P
Pattern matching in Zones • 134
Performance • 327
Performance Monitor • 322
Permissions • 318
PIoNotSetEnvVars • 359
PMWAutoAllowFolders • 360
PowerHelp • 200
PowerPrintView • 196
Prerequisites • 17, 227
PreviousPrinter • 196
Printer • 196
Printers • 234
Printing Preferences • 185
Process Building Blocks and Custom Resources in batches • 387
Process interception for unmanaged shortcuts • 150, 152
Properties • 157
Publish Citrix XenApp Applications • 99, 174
Publish Citrix XenApp applications manually • 101
Publishing • 157, 174
Pwrgate • 382
PwrGateAppId • 360
PwrGateFileMapping • 360
PwrGateSleep • 361
PwrMapiDelay • 361, 373
Pwrtech • 383

Q
QuickLaunch and QuickLaunchMandatory • 189

R
Read-Only Blanketing • 294
Read-Only Blanketing security Modes
disabled, learning, enabled • 294
Recommended Configuration when using Microsoft Windows 10 • 155
RefreshAllMappedDrives (Workspace Control 10.2.0.1 and earlier) • 361
RefreshAllMappedDrives (Workspace Control 10.2.500.0 and higher) • 362
RefreshInterval • 197
Registry settings • 338
Registry settings for Relay Servers • 376
Relay Server Local cache • 321
Relay Server Service • 321
Relay Servers • 41, 321
Removable Disks security • 289
Removable Disks security modes disabled, learning, enabled • 289
RemoveObsoleteLogFiles • 381
RemoveStartmenuPinList • 362
Reporting Services for Workspace Control • 88
Republish a published application • 390
RestoreMappingsAtLogoff • 362
RSConnectTimeout • 381
RunCPUShld • 363
RunHistory • 195
RunWMSync • 363
S
Sampling • 273
Save printing preference • 277
Scalability and performance • 13
SCCMDelayBeforeRunningProgram • 364
Scope Control • 319
Screensaver • 244, 256
Security • 157, 180, 280
Security Method Whitelisting or Blacklisting • 298
Select Workspace Control Modules • 76, 79, 80
SelfServicePoll (Workspace Control 10.1.400.0 and higher) • 364
Server-based Computing • 34, 35
SessionCheckInterval (RES ONE Workspace 10.0 and earlier) • 365
SessionCheckInterval (Workspace Control 10.1 and higher) • 365
Set Memory Optimization limits • 334
Set up Alerting • 90
Set up Instant Passthrough for Citrix XenApp published applications • 94, 97, 99, 257
Set up Instant Passthrough for TS RemoteApp applications • 110
Set up Microsoft App-V applications • 105
Set up Microsoft TS RemoteApp applications • 109, 174
Set up Remote Assistance • 113
Set up the Datastore • 37
Set up Usage Tracking • 86
Setprint • 390
Settings • 157, 165, 180
Settings tab • 149
Setup • 71
Shell • 244
Shortcuts • 157, 162
ShowAllApplication • 190
ShowAllOnDesktop • 188
ShowEmptyDates • 198
ShowFQName • 198
ShowQOUInReports • 198
ShowSearchFieldAlways • 366
SilentRefresh • 366
SkipCloseWFSShell • 366
SkipCLSID • 367
SkipDSWhenOffline • 367
SkipFullNames • 367
SmallIcons • 192
Solve a Console lockout • 319
SpecialFoldersFromRegistry • 368
Specify a different application icon, Outlook signature or Registry setting • 68
Specify a different desktop background image • 69
Specify a different Policy settings file • 69
Specify a different screensaver image • 69
Start a Remote Assistance session • 113
Start Menu tab • 148
StartHiddenPexplorer • 368
Startup • 191
StartWithShortcut • 368
Storage method • 268
Storage of users’ User Setting data • 268
Subnet Masks • 299
SuppressShowDesktopButton • 369
SuppressUnknownRequestMessage • 369
SwapMouse • 192
SyncUserSettingsWhenOffline • 369
T
Technical Manager • 318
The Management Portal • 5
The order of events at a session refresh • 394
The order of events in Workspace Control sessions • 391
The order of events when a session ends • 396
The order of events when a session starts • 391
The structure of Building Blocks • 68
The Usage Tracking Viewer • 87
The Workspace Composer • 9
The Workspace Control Agent Cache • 12
The Workspace Control Agent Service and its subprocesses • 11
The Workspace Control Agents • 6
The Workspace Control Console • 5
The Workspace Control Datastore • 5
TimeoutScrnSaver • 195
Toggle Remove • 241
Tracing • 370
Track any changed setting within scope immediately (global) • 258, 263
Track any setting changed by application immediately (application) • 258, 264
Troubleshoot Relay Servers • 321

U
Unattended Installation • 20, 22, 78
Usage Tracking • 86, 183, 315
Usage Tracking Overview • 183, 315
Usage Tracking Viewer • 183, 184, 315
Use Locations and Devices for Printers • 237
Use User Home Directory Maintenance to change Pwruser.ini • 186
Use Workspace Containers to configure exceptions to the global settings of a feature • 145
Use Workspace Control to create different configurations for an application or the user session • 142
UseClassicLogoff • 371
UseGetSiteInfo • 371
UseMsgBox • 372
UseOldShadowing • 372
Use Only Computer Name For Shadow • 373
User Context • 126
User Installed Applications • 284
User Registry • 238, 262
User Sessions • 310
User Sessions security • 302
User Settings • 157, 257, 279
User Settings caching • 269, 271

V
Variables and special folders • 263, 264, 278
VDX • 118
VDX Licensing • 83
VMware ThinApp • 89, 111

W
WaitBeforeStart • 374
WaitForUpdatedCache • 374
Web Portal • 120
Websites • 286
What is saved as part of a Targeted Item • 267
Where to find Access Balancing • 327
Where to find Access Control • 126
Where to find Administrative Roles • 318
Where to find Alerting • 90
Where to find Automation Tasks • 214
Where to find Building Blocks in the Workspace Control Console • 63
Where to find Citrix XenApp Publishing • 91
Where to find CPU Optimization • 329
Where to find Directory Maintenance • 230
Where to find Drive and Port Mappings • 220
Where to find Drive Substitutes • 223
Where to find Environment Variables • 216
Where to find Errors • 316
Where to find Execute Command • 218
Where to find Filtering • 58
Where to find Folder Synchronization • 227
Where to find Instant Reports • 61
Where to find Linked Actions • 243
Where to find Memory Optimization • 333
Where to find Microsoft App-V • 103
Where to find Microsoft Remote Assistance • 113
Where to find Microsoft TS RemoteApp • 108
Where to find PowerHelp • 200
Where to find Printing Preferences • 185
Where to find the Access Wizard • 184
Where to find the Workspace Model Overview • 312
Where to find Usage Tracking • 184
Where to find User Registry • 238
Where to find User Sessions • 310
Where to find User Settings in the Workspace Control Console • 257
Where to find Workspace Containers • 140
Where to find Workspace Extensions • 161
Where to find Workspace Preferences • 186
Where to find Zones • 128
Whitelisting • 300
Windows Authentication for Management Portal's Datastore connections to Microsoft SQL Servers • 85
Windows authentication with designated account • 37, 74
Workspace Analysis • 304
Workspace Branding • 125
Workspace Containers • 140, 179
Workspace Control and Microsoft Windows 8.1, 2012 R2, and 10 • 154
Workspace Control Applications for end users • 184
Workspace Control Modules • 51, 72, 76
Workspace Control Relay Servers • 8
Workspace Designer • 54, 56
Workspace Extensions • 159, 161, 168
Workspace Model • 54, 57, 337
Workspace Model Overview • 312
Workspace Preferences • 186
Workspace Simulation Wizard • 308

X
XenDesktop7Intercept • 375

Z
Zero Profile Modes • 258
Zone Members
Nest Zones • 134
Zone rules • 128