

Getting Started with

RES ONE®

Workspace

Agents for Linux and Apple Mac OS X

Version 10.0.1.0

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

Disclaimer

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

Contents

Chapter 1:	Introduction	1
<hr/>		
Chapter 2:	What's new	2
<hr/>		
Chapter 3:	Prerequisites and General Guidelines	3
<hr/>		
Chapter 4:	Install Agent for Linux	5
<hr/>		
Chapter 5:	Install Agent for Apple Mac OS X	7
<hr/>		
Chapter 6:	Directory Structure of Agent	9
<hr/>		
Chapter 7:	Configuration Files	10
<hr/>		
Chapter 8:	Log Files	13
<hr/>		
Chapter 9:	Retrieving and using file hashes for the Agent	14
<hr/>		
Chapter 10:	Known Limitations Agent for Linux	15
<hr/>		
Chapter 11:	RES Support	16
<hr/>		
Chapter 12:	RES Training	17
<hr/>		

Chapter 1: Introduction

The RES ONE Workspace Agents for Linux and Apple Mac OS X Operating Systems were introduced with RES ONE Workspace 2015 and have now been enhanced further. On supported systems, these Agents provide enhanced workspace security and protection from malicious threats through advanced file hash-based application security (whitelisting). Access Control that is based on the location where and/or the device on which the user session is started can now also be configured.

The Agents establish an encrypted connection to a RES ONE Workspace 2015 or higher Relay Server, authenticate to a RES ONE Workspace environment, and access the configured list of Authorized Files with their associated SHA-256 hash values. If Access Control is configured, then the user session must meet the rules that are configured based on location and/or device.

When appropriately configured, the Agents will prevent the execution of unauthorized applications, which are not in the list of authorized file hash values or if the user session was started on a location or device for which no access control was granted.

This document guides you through the installation of the RES ONE Workspace Agents for Linux and Apple Mac OS X and explains you how to configure them.

Chapter 2: What's new

In this release of the Agents for Linux and Mac OS X you find the following new feature supported:

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

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

You can configure zone rules in the RES ONE Workspace Console at **User Context > Locations and Devices**.

Chapter 3: Prerequisites and General Guidelines

Prerequisites

Product	Prerequisite
RES ONE Workspace	<ul style="list-style-type: none"> • RES ONE Workspace 10.0.400.0 or higher environment • RES ONE Workspace 10.0.400.0 or higher Relay Server for Windows • All Authorized Files and hashes for the target Linux or Apple Mac OS X system must be imported in the RES ONE Workspace Console
Linux	<ul style="list-style-type: none"> • One of the following Linux Operating Systems, with <ul style="list-style-type: none"> • Linux Kernel version 2.6.18-398: <ul style="list-style-type: none"> • CentOS Linux 5.11 <ul style="list-style-type: none"> • Software installation package <code>res-workspaceagent-10.1.0.401965.x86_64-centos-5.11.rpm</code> • RHEL 5.11 <ul style="list-style-type: none"> • Software installation package <code>res-workspaceagent-10.1.0.401965.x86_64-redhat-5.11.rpm</code> • Linux Kernel version 3.10.0-327: <ul style="list-style-type: none"> • CentOS Linux 7.2-1511 <ul style="list-style-type: none"> • Software installation package <code>res-workspaceagent-10.1.0.401965.el7.x86_64-centos-7.2.rpm</code> • RHEL 7.2 <ul style="list-style-type: none"> • Software installation package <code>res-workspaceagent-10.1.0.401965.el7.x86_64-redhat-7.2.rpm</code> • Linux Kernel version 3.10.0-229: <ul style="list-style-type: none"> • CentOS Linux 7.1-1503 <ul style="list-style-type: none"> • Software installation package <code>res-workspaceagent-10.1.0.401965.el7.x86_64-centos-7.1.rpm</code> • RHEL 7.1 <ul style="list-style-type: none"> • Software installation package <code>res-workspaceagent-10.1.0.401965.el7.x86_64-redhat-7.1.rpm</code> • Linux Kernel version 3.10.0-123: <ul style="list-style-type: none"> • CentOS Linux 7.0-1406 <ul style="list-style-type: none"> • Software installation package <code>res-workspaceagent-10.1.0.401965.el7.x86_64-centos-7.0.rpm</code> • RHEL 7.0 <ul style="list-style-type: none"> • Software installation package <code>res-workspaceagent-10.1.0.401965.el7.x86_64-redhat-7.0.rpm</code> • Linux Kernel version 2.6.32-642: <ul style="list-style-type: none"> • RHEL 6.8 <ul style="list-style-type: none"> • Software installation package <code>res-workspaceagent-10.1.0.401965.el6.x86_64-redhat-6.8.rpm</code>

Product	Prerequisite
	<ul style="list-style-type: none"> Linux Kernel version 2.6.32-573: <ul style="list-style-type: none"> RHEL 6.7 <ul style="list-style-type: none"> Software installation package <code>res-workspaceagent-10.1.0.401965.el6.x86_64-redhat-6.7.rpm</code> Linux Kernel version 2.6.32-504: <ul style="list-style-type: none"> RHEL 6.6 <ul style="list-style-type: none"> Software installation package <code>res-workspaceagent-10.1.0.401965.el6.x86_64-redhat-6.6.rpm</code> <p>IMPORTANT: Only the specified Operating Systems and Service Pack versions are supported. The Linux Kernel version must match exactly.</p>
Apple Mac OS X	<ul style="list-style-type: none"> Apple Mac OS X Version 10.8.5 up to Version 10.11 <ul style="list-style-type: none"> Software installation package <code>res-workspaceagent-10.1.0.401965-Mac-10.8-to-10.11.pkg</code> Apple Mac OS X Version 10.12 <ul style="list-style-type: none"> Software installation package <code>res-workspaceagent-10.1.0.401965-Mac-10.12.pkg</code> <p>IMPORTANT: Only the specified Operating Systems are supported. The version must match exactly.</p>

Settings	Prerequisite
Account	<ul style="list-style-type: none"> Root privileges (Linux) or Superuser rights (Apple) to install software on the target computer
Network	<ul style="list-style-type: none"> IPv4 network connection to a RES ONE Workspace 2015 or higher Relay Server Network routers and firewalls must be configured to allow communication between the target Linux/Apple Mac OS X system and the Relay Server
RES ONE Workspace Relay Server Connection Information	<ul style="list-style-type: none"> Relay Server network host name or IPv4 address Relay Server network port number
RES ONE Workspace Environment credentials	<ul style="list-style-type: none"> Environment GUID Hashed Password for Environment <p>Note: To obtain the hashed password, on the Windows system with the RES ONE Workspace Console installed, run the command <code>"%respfdir%\pwrtech.exe" /gethashedpassword</code> and use Ctrl+C to copy it to the clipboard.</p>

Chapter 4: Install Agent for Linux

To install the RES ONE Workspace Agent package for Linux, follow these steps:

1. Make sure you are running as the root user.


```
# id
uid=0(root) gid=0(root) groups=0(root)
```
2. Transfer the RPM file to the target machine.
3. Install the RPM package. Run the command below to install the package from the folder in which the package is located (one version given as an example):


```
CentOS: rpm -ivh res-workspaceagent-10.1.0.401965.el7.x86_64-centos-7.2.rpm
Redhat: rpm -ivh res-workspaceagent-10.1.0.401965.el7.x86_64-redhat-7.2.rpm
```
4. Configure the Agent to start automatically by using the command


```
chkconfig --add reswmd
```

 And then follow these steps:
 - a) Once added to the configuration, the auto start of the Agent can be toggled with the command


```
chkconfig reswmd on
```
 - b) The auto start can be disabled with the command


```
chkconfig reswmd off
```
5. To configure the Agent service, modify the files in `/etc/res`.
 - a) Use the command `cd /etc/res`
 - b) Copy `/etc/res/reswmd.conf.example` to `/etc/res/reswmd.conf`.
Modify the contents of the configuration file with the connection information for your RES environment.

Note: lines that begin with the comment character (#) are ignored.

```
#
# Example connection configuration file for RES ONE Workspace
service: reswmd
#
# Remove the comment marker from the front of each line and
substitute your connection information.
# The file should be renamed "/etc/res/reswmd.conf"
#
# RSENGUID={489E9C23-11E7-4A4F-B56E-2D6F3DF3A241}
# RSPASSWORD=650CABD8A997B36733D5A652DEDC2305511D292E
# RSPWHASHED=yes
# RSLIST=192.168.1.9:1942
```

6. To configure Agents, go to the RES ONE Workspace Console, at **Administration > Agents**.
 - For instance:
 - to configure an Agent to run automatically, in the Management Console at **Administration > Agents** on the **Agents** tab, set the option **Run Workspace Composer** to **Automatic** for the specified Agent.
 - to configure an Agent to run in **Learning** mode, in the Management Console, at **Security > Applications > Managed Applications**, on the **Settings** tab, select **Learning** for **Managed Application Security**.

7. The Agent will start automatically when you use the command `chkconfig reswmad on` and restart the target machine.
If required, you can choose to start the Agent service manually with the command `/etc/rc.d/reswmad start`.
8. You can stop the Agent service at any time by issuing the command `/etc/rc.d/reswmad stop`.
Please note that the Agent service will restart at the next machine reboot unless the command `chkconfig reswmad off` is also executed.

The Agent for Linux will appear as a registered Agent in the RES ONE Workspace Console after successful initial contact with the Relay Server. Agents for Linux can be configured and edited via the Management Console. The `/etc/res/resauthd.conf` configuration file is no longer needed.

Chapter 5: Install Agent for Apple Mac OS X

To install the RES ONE Workspace Agent package for Apple Mac OS X, follow these steps:

1. Transfer the PKG file to the target system.
2. Install the package. There are two methods:
 - a) Use **Finder** to open the package file and execute the installation via the graphical user interface. You will be asked for your password to allow the installation.
 - b) Use the `sudo` command line to install the package in the **Terminal** application:
Apple Mac OS X: `sudo installer -pkg res-workspaceagent-10.1.0.401965-Mac-10.8-to-10.11.pkg -target /`
Apple Mac OS X 10.12: `sudo installer -pkg res-workspaceagent-10.1.0.401965-Mac-10.12.pkg -target /`

You may be asked for your password to allow the installation.

3. Configure the Agent software by modifying the file in `/etc/res` directory.
Use the command `cd /etc/res`
4. Copy `/etc/res/reswmad.conf.example` to `/etc/res/reswmad.conf`.
Modify the contents of the configuration file with the connection information for your RES environment.

Note: lines that begin with the comment character (`#`) are ignored.

```
#
# Example connection configuration file for RES ONE Workspace service:
reswmad
#
# Remove the comment marker from the front of each line and substitute
your connection information.
# The file should be renamed "/etc/res/reswmad.conf"
#
# RSENVGUID={489E9C23-11E7-4A4F-B56E-2D6F3DF3A241}
# RSPASSWORD=650CABD8A997B36733D5A652DEDC2305511D292E
# RSPWHASHED=yes
# RSLIST=192.168.1.9:1942
```

5. To configure Agents, go to the RES ONE Workspace Console, at **Administration > Agents**.
 - For instance:
 - to configure an Agent to run automatically, in the Management Console at **Administration > Agents** on the **Agents** tab, set the option **Run Workspace Composer** to **Automatic** for the specified Agent.
 - You can also configure the setting `AUTORUNCOMPOSER=yes` in the configuration file `reswmad.conf`.
 - to configure an Agent to run in **Learning** mode, in the Management Console, at **Security > Applications > Managed Applications**, on the **Settings** tab, select **Learning** for **Managed Application Security**.

6. The Agent will start automatically when the target machine is restarted. If required, you can choose to start the Agent without restarting the machine by using the following optional commands:

- `sudo launchctl load /Library/LaunchDaemons/com.ressoftware.reswmd.plist`
- `sudo launchctl load /Library/LaunchDaemons/com.ressoftware.resauthd.plist`

The Agent for Apple Mac OS X will appear as a registered Agent in the RES ONE Workspace Console after successful initial contact with the Relay Server. Agents for Apple Mac OS X can be configured and edited via the Management Console. The `/etc/res/resauthd.conf` configuration file is no longer needed.

Chapter 6: Directory Structure of Agent

The Agents for Linux and Apple Mac OS X consist of three logical components: two service daemons, one kernel (extension) module.

- Service daemons

- `reswmad`

This service:

- communicates with the RES ONE Workspace Relay Server for Windows or the Portable Relay Server
- authenticates to the RES ONE Workspace environment
- accesses the Authorized Files list.
The Authorized Files list is saved in the file
`/etc/res/workspace/dbcache/objects/sec_globauth.xml`.
- accesses Agent Workspace Container information.
The Workspace Container information is saved in the files
`/etc/res/workspace/dbcache/objects/workspaces.xml` and
`/etc/res/workspace/dbcache/objects/respf_agents.xml`.
- accesses information specific to each individual Agent.
This Agent-specific information is saved in the files
`/etc/res/workspace/agentinfo.xml`, `/etc/res/workspace/unique_id`, and
`/etc/res/workspace/globalupdateguid`.

The service daemon `reswmad` continuously monitors the Relay Server for updates in the Authorized Files list and applies the updates to the Agent.

- `resauthd`

This service applies the cached authorized files rules (found in `/etc/res/workspace/dbcache/objects/sec_globauth.xml`) to the running Agent using the `resmod` kernel module (see below).

The service daemon `resauthd` runs independently of the `reswmad` service daemon and continues to apply the cached rules even if the `reswmad` service daemon does not have contact with the Relay Server.

- Transactions between the Agent and the Relay Server are stored at `/etc/res/workspace/transactions`. These transactions are generated by `resauthd` and submitted to the Relay Server by `reswmad`.

- Kernel module for Agent for Linux

- `resmod`

Under the direction of the `resauthd` service daemon, the RES kernel module monitors all attempts to execute programs and blocks them if they are not permitted by the current rule set.

The kernel module is automatically inserted and activated every time the `resauthd` service daemon is started.

- Kernel extension module for Agent for Apple Mac OS X

- `RESKext.kext`

Under the direction of the `resauthd` service daemon, the RES kernel extension module monitors all attempts to execute programs and blocks them if they are not permitted by the current rule set.

The kernel extension module is automatically inserted and activated every time the `resauthd` service daemon is started.

Chapter 7: Configuration Files

It is recommended to configure the Agent settings in the RES ONE Workspace Console. However, to configure the Agent service, use the configuration file `reswmad.conf`, that is located in the `/etc/res` directory.

Important: Make sure only the **root user** may access and modify the `/etc/res` directory and the configuration file by setting the permissions accordingly.

Please note that files that are executed by the users “root”, “bin”, and “daemon” are never blocked. The filenames may not contain the characters “\” (backslash), newline, or tab. File path entries in the Authorized Files list that begin with `\\` or `X:\` (where `X` is a drive letter) are assumed to be Microsoft Windows paths and are ignored by the Agent for Linux and Apple Mac OS X.

If the configuration file `resauthd.conf` is present on the Agent system, the settings related to **Managed Application Security**, for instance `LearningMode`, are always taken from that configuration file. For all other Agent settings, after Agents had a successful initial contact with a Relay Server, the settings from the RES ONE Workspace Console overrule the settings in this Agent's configuration file.

Below, the settings in the `reswmad.conf` configuration file you need to configure or think about. These settings are needed for the initial installation of the Agents for Linux and Apple Mac OS X.

- **/etc/res/reswmad.conf**

This is the configuration file for the `reswmad` service daemon. It provides the information that is needed to contact the Relay Server and to obtain the Authorized Files list.

These settings need to be configured in this file:

Name	Type	Value
RSENVGUID	String	{ }

The RES environment GUID.

Example

```
{12345678-90AB-CDEF-1234-567890ABCDEF}
```

RSPASSWORD	String	Hexadecimal value: 0-9 A-F (40 characters)
------------	--------	--

The hashed password of the RES ONE Workspace environment. See the **Prerequisites** section for the command to obtain this hashed password. The value (hexadecimal letters) must be specified in upper case.

Example

```
650CABD8A997B36733D5A652DEDC2305511D292E
```

RSPWHASHED	Boolean	yes
------------	---------	-----

yes = password is hashed. Currently, the value no (password is *not* hashed) is not supported.

RSLIST	String	
--------	--------	--

The upstream Relay Server. Use the Relay Server's IPv4 address or host name and include the port number. When no port is specified, the default port (1942) is used. In this version, a single upstream Relay Server is supported.

Example

```
192.168.1.1:1942
```

LOGLEVEL	String	Info (default) / Debug
----------	--------	------------------------

The minimum severity for log messages to be logged. If set to `DEBUG`, many additional log messages will be generated. The `DEBUG` value should only be used for troubleshooting setup issues. After that, set it back to `INFO`.

AUTORUNCOMPOSER	Boolean	yes / no (default)
-----------------	---------	--------------------

This setting determines if the Agent starts automatically.

- yes = The Agent starts automatically
- no = The Agent is stopped

Please note that the behavior of the option **Run Workspace Composer** for Agents for Linux and Apple Mac OS X is different from the behavior of this option for Agents for Windows.

INHERITSETTINGS	Boolean	yes / no (default)
-----------------	---------	--------------------

This setting specifies whether the Agent should revert to inherited settings after establishing its initial connection to the Relay Server.

- yes = The Agent initially connects to the Relay Server with the configured settings from the Agent's configuration files, but will then be set to inherit its connection settings from the global Agent settings configured in the RES ONE Workspace Console.
- no (or INHERITSETTINGS not provided) = the connection settings in the Agent's configuration files are set specifically for the Agent, overruling inheritance.

- **/etc/res/workspace/...**

These files are generated by the `reswmad` daemon service and *should not be edited*. It provides the list of rules to the `resauthd` daemon service. To make changes to the contents of these files, use the RES ONE Workspace Console. Please note that manual edits to the file might be lost when a change is made in the RES ONE Workspace Console.

Chapter 8: Log Files

The Agents for Linux and Apple Mac OS X each generate three log files. They are all located in the `/var/log` directory.

- `/var/log/reswmad.log`

This file contains the log messages from the `reswmad` service. It contains information related to contacting the RES ONE Workspace Relay Server and obtaining the Authorized Files list. This trace file has a maximum size of 4 MB which cannot be configured differently. Only the most recent trace entries are kept.
- `/var/log/resauthd.log`

This file contains the log messages from the `resauthd` service. It contains information related to the Authorized Files list. This trace file has a maximum size of 4 MB which cannot be configured differently. Only the most recent trace entries are kept.
- `/var/log/res_unauthorized.log`

This file contains a log message for each attempt to run an unauthorized file. Each attempt generates a line in the log file. As this is a security log that contains all attempts to run unauthorized files per user, all entries are kept. New entries are added at the end of the log.

Chapter 9: Retrieving and using file hashes for the Agent

Hashes for the Agent can be added to the RES ONE Workspace environment in several ways.

File hashes are available in the RES ONE Workspace Console at **Security > Applications > Managed Applications**, on the **Log** tab. On the **Log** tab, file hashes can be added to your RES environment. Open the context menu by right-clicking the line you want to add and choose **Authorize selected file...** or **Authorize file hashes...** from the menu.

You can also generate file hashes by using the command `openssl dgst -sha256` directly on the Agent system. For example, the command `openssl dgst -sha256 /bin/ls` might produce the following output:

```
SHA256 (/bin/ls)=  
5d03750ae764cb93b2fa541158eea815ebb76623fe96358944e28def59e0f506
```

With the retrieved files hashes you can create a CSV or tab-separated TXT file that can be used to import the file hashes into the RES ONE Workspace Console. To import this file, in the Management Console go to **Security > Authorized Files**, right-click in the overview section (on **Authorized Files** tab) and select the option **Import file hashes...** from the context menu and select your CSV or TXT file.

An example tab-separated TXT file might look like the following:

```
/bin/bash  
05fa593bb1247e5f73e21e8951c2215e4c83f60047167aad5e4371947587cce7 *  
/bin/cat  
9f9b36ec79b9fcaf649e17f2f94c544dd408c2ab630e73d7c62a7a43f1bc7b1d *  
/bin/chmod  
772fa71ce0bcebd1fa76ea0aa0c0c3ed1f3a601471756bf9a9b6266f6888349f *  
/bin/cp c7ce85716b98f30acbb8b9dd1f244d0b337064493383ee4365fe2fd003684cd9  
*  
/bin/csh  
1c57b082ddc89659df67bcd8045c86bd687bec8c1258ee0fec9e5a908c823e0f *  
/bin/date  
7cbba457df4c02d6a7fb93046fea0e869732c65a2225bee6f2e8ec290d38c57b *  
/bin/dd d8ee28d9f5596a0acad28bebc140d3954d40324f19b21100105de3cc62480bc8  
*  
/bin/df 60b03106cf89c8ca4d2ebe9126cb555f0a33fbede14b280cbb7c8e506b583b67  
*
```

Chapter 10: Known Limitations Agent for Linux

RES has identified the following limitations of the RES ONE Workspace Agent for Linux:

- CentOS Linux 7.1-xxxx and RHEL 7.1
 - The RES ONE Workspace Agent for Linux can fail to connect to the Relay Server under the following circumstances:
 - Network is not set to automatically connect at startup.
 - Solution: Set network to connect automatically at startup.
 - Network is configured for DHCP with no host information for the Relay Server specified on the Agent.
 - Solution: Specify the host name and IP address of the Relay Server in the Agent's hosts file.
 - `reswmad.conf` is using machine name instead of IP address.
 - Solution: Use the Relay Server's IP address in `reswmad.config` instead of the machine name/hostname.

Chapter 11: RES Support

At RES, our core business is to help heighten productivity in your organization. RES Support helps us to achieve this goal, and has been embedded in the core principles of our company since it was founded. RES is dedicated to supporting everyone who uses or wants to use its proven products with RES 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 (**Success Center > Support**) or you can contact RES Support directly (**Success Center > Click Contact Us**).

Product Upgrades and Service Releases - To upgrade your version of RES ONE Workspace to the latest standard, you can install Product Upgrade Packs from <http://www.res.com> and Service Releases from the **Success Center > Downloads**. The supporting documentation consist of Online Help (available via F1 in the Console), Release Notes and Administration Guide (**Success Center > Downloads**).

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.

Early Adopter Program - Participants of the Early Adopter Program are actively involved in taking RES 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.

RES Community - RES invites you to become part of our community to share best practices and tips with fellow IT professionals, find solutions and more (**Success Center > Q&A**).

Please visit the **RES Success Center** (<http://success.res.com>) for more information on **Support**.

Chapter 12: RES Training

RES 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 the Academy at RES Success Center (<http://success.res.com>) or go to <http://res.com/support/training> to find more information on Training.

RES Academy - RES Academy provides an engaging way to learn about RES 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 RES product.

Workshops - For customers and partners RES 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, RES has developed several technical courses that deal with the installation and configuration of RES ONE Workspace, RES ONE Automation and RES ONE Service Store. These technical courses are offered by RES Authorized Learning Centers (RALCs).

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