Getting started with

RES ONE® Workspace

Relay Servers

Version 10.1.0.0

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

The Relay Server is an infrastructure component that caches information from the Datastore and passes it on to Agents upon request. Therefore, 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. Without Relay Servers, Agents need to connect directly to the Datastore. RES ONE Workspace environments can have a mix of connection methods, with some Agents connecting directly to the Datastore and others connecting to Relay Servers.

Relay Servers offer a number of 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.
- Reduced maintenance on Agents that connect to Relay Servers, as no database driver needs to be installed for the RES ONE Workspace Datastore.

After installing and connecting one or more Relay Servers in a RES ONE Workspace environment, you can switch existing Agents in the same environment to connect to Relay Servers instead of to the Datastore, and you can connect new Agents to Relay Servers during the installation process. It also remains possible to connect existing and new Agents directly to the Datastore.

Relay Servers can be used in environments running RES Workspace Manager 2012 and later/RES ONE Workspace.

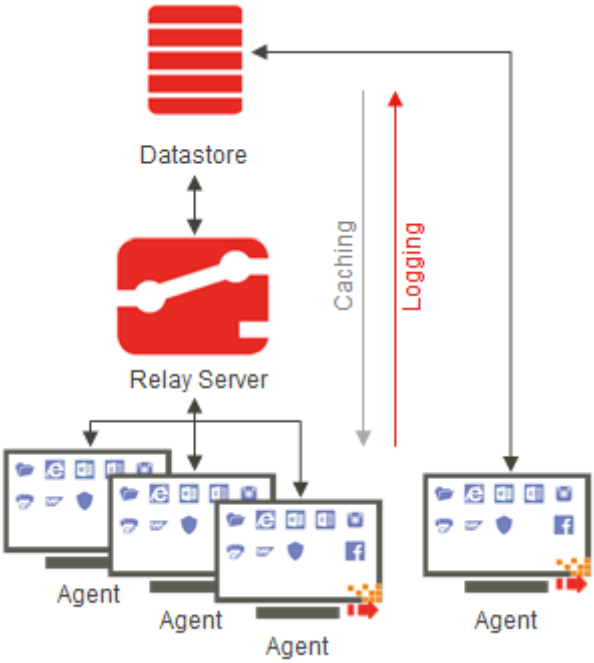
Chapter 2: The benefits of using Relay Servers

2.1 Decreasing Datastore load and increasing scalability

In a single-site topology where many Agents connect to a single Datastore, datastore load can be an issue. Relay Servers can decrease this load considerably, as a single Relay Server can provide a multitude of Agents with information from its cache.

There is also a limit on the number of connections that a Datastore can handle. By using Relay Servers, a single RES ONE Workspace environment can contain more Agents, because the Agents do not need a direct connection to the Datastore.

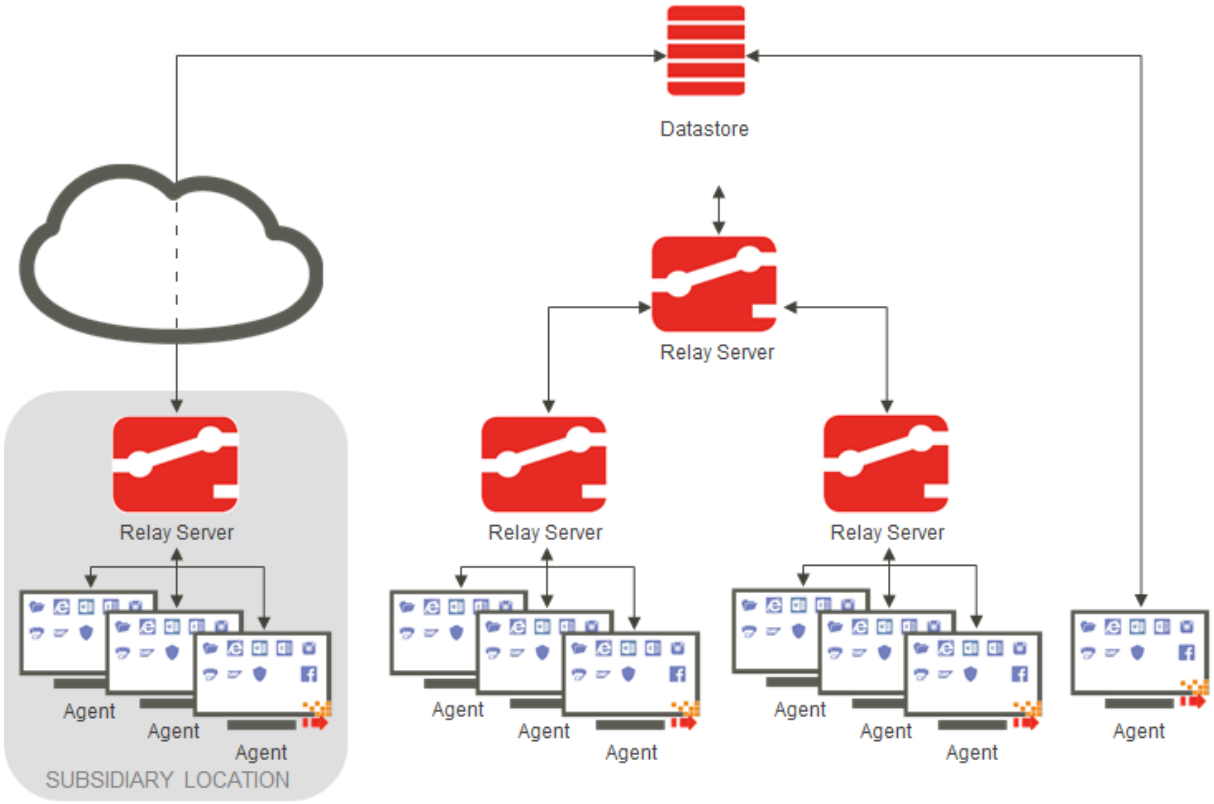
In such sites, configure some or all of the Agents to connect to a Relay Server instead of directly to the Datastore.



2.2 Reducing network traffic in a multiple-site topology

In a multiple-site topology, data connection speed can be an issue. You want as few data transactions across the network or data line as possible, to save bandwidth. In such sites, Relay Servers can reduce network traffic significantly.

Per remote site, configure one or more Relay Servers, which cache information from the central Datastore. Agents requiring information are then no longer dependent on a direct line to the central Datastore. Instead, they can request the necessary information from a Relay Server in the local network.



Chapter 3: Introducing Relay Servers into an existing environment

Take the following steps to start using Relay Servers in an existing RES ONE Workspace environment:

1. In the RES ONE Workspace Console at **Administration > Relay Servers**, on the **Settings** tab, set the environment password.
2. Install the first Relay Server component.
3. Connect the first Relay Server directly to the Datastore of the relevant RES ONE Workspace environment, using the Relay Server Configuration tool.
4. Optionally, install additional Relay Servers on additional machines, and connect them to the relevant environment too. They can connect directly to the Datastore or to other Relay Servers.
5. Configure the behavior of Relay Servers in the RES ONE Workspace Console (fetch change information interval, cache update interval, synchronization policy, and connection password).
6. Connect one or more existing Agents to Relay Server(s) via the RES ONE Workspace Console.

These steps are described in more detail below.

3.1 Installing the Relay Server component

Before installing a Relay Server, make sure you have an existing RES ONE Workspace Datastore. It is not possible to create a new Datastore during the installation of a Relay Server.

The first Relay Server in your environment must connect directly to the Datastore. Subsequent Relay Servers can connect to the Datastore or to parent Relay Servers.

The connections of a specific Relay Server are configured during or after installation of the Relay Server component. The behavior of Relay Servers, such as the interval at which they fetch change information from the Datastore, is configured in the RES ONE Workspace Console at **Administration > Relay Servers**.

Warnings

- We advise against installing a Relay Server on a machine that is also running a RES ONE Workspace Agent, mainly because:
  - If the Agent machine shuts down, the Relay Server would also be unavailable.
  - In sites upgraded from versions prior to RES Workspace Manager 2012, uninstalling the Agent also uninstalls the Relay Server component on that machine.
- The deployment of Relay Servers on 64-bit machines that are directly connected to the Datastore, requires the installation of the 64-bit version of the necessary database drivers on these machines. The other components of RES ONE Workspace use the 32-bit version of these database drivers. It may not be possible to use both versions on the same 64-bit machine simultaneously, so it is not possible to use a Console and a Relay Server on this machine that both point to the same Datastore.

3.1.1 Prerequisites

The following prerequisites apply to machines running the Relay Server component:

- Microsoft .NET Framework 4.5.2 or higher
- Any of the following server operating systems:
  - Microsoft Windows 2008 R2 x64
  - Microsoft Windows 2012 x64
  - Microsoft Windows 2012 R2 x64
- Available hard disk storage space must be at least 500 MB *plus* the current size of the Agent cache. (The size of the "Configuration and state" part of the primary Datastore provides an indication of the current cache size).
- A Relay Server connecting directly to the Datastore needs to have the database client installed for the type of database used for the RES ONE Workspace Datastore. For Microsoft SQL this is not necessary when Windows Authentication and protocol encryption are not used. A child Relay Server connecting to another Relay Server does not need a database client.
- An environment password must be configured in the RES ONE Workspace Console (at the **Relay Servers** node, using the button **Change environment password**). This secures your Relay Servers from unauthorized connections.
- For Relay Servers that are installed on a machine with a Windows Server Operating System, an inbound rule for `RelayServer.exe` must be configured for the machine's firewall. This is needed for successful communication between the Relay Server and Agents.

Notes

- The following operating systems are also supported, but may set a maximum on the number of inbound connections:
  - Microsoft Windows 7 x86/x64
  - Microsoft Windows 8 x86/x64
  - Microsoft Windows 8.1 x86/x64
  - Microsoft Windows 10 x86/x64
- The sizes of different parts of the Datastore are not provided for all database types.
- For MySQL ODBC Driver versions 5.2.2 - 5.2.4, RES ONE Workspace only supports the ANSI version of the driver.

3.1.2 Available installation methods

There are several ways to install the Relay Server component:

- Interactive installation with a wizard, followed by the Relay Server Configuration tool.
- Unattended installation followed by the Relay Server Configuration tool.
- Unattended installation, providing pre-defined connection settings in an XML file.

Regardless of the installation method, use the **RES ONE Workspace Installer** (`RES ONE Workspace Installer 10.1.0.0.exe`) to install the Relay Server.
When selecting the option **Select and install components**, the installation wizard will guide you through the actual installation. The RES ONE Workspace Installer auto-detects whether the 64-bit or 32-bit version of the Relay Server needs to be installed.
When selecting the option **Extract all components**, use the installation file `RES ONE Workspace Relay Server(x64) 10.1.0.0.msi` for 64-bit systems, or `RES ONE Workspace Relay Server(x86) 10.1.0.0.msi` for 32-bit systems.

During an interactive installation, the installation wizard automatically opens the Relay Server Configuration tool.

Unattended installation alone will not connect the newly installed Relay Server to any RES ONE Workspace environment. To configure this connection after the unattended installation, open the Relay Server Configuration tool or use a command line as described in **Connecting a Relay Server using an existing configuration file** (on page 9). The public properties that can be applied to the Relay Server when installing unattended, are described in the next section.

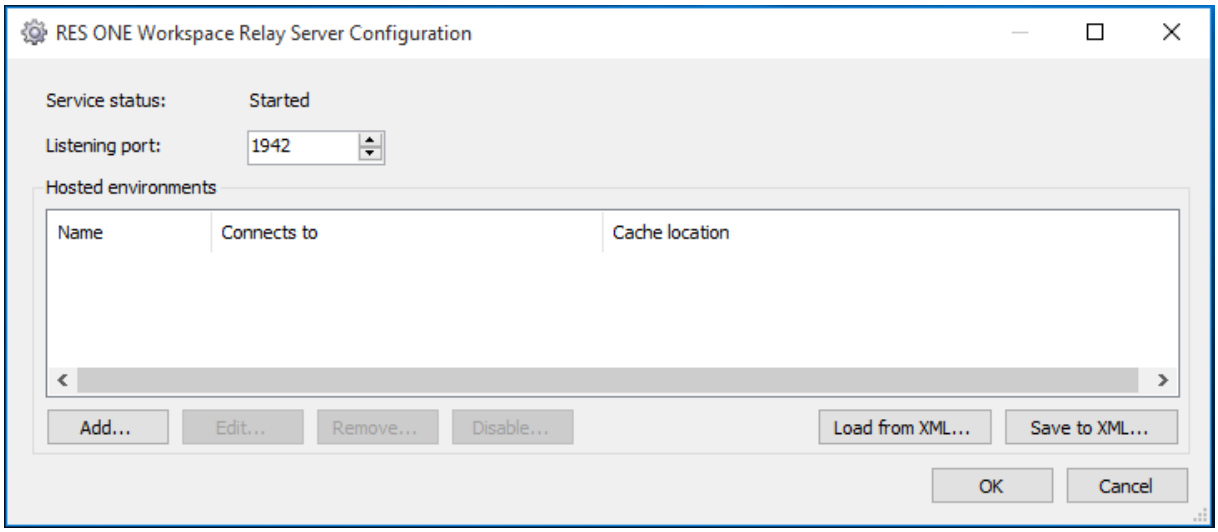
Alternatively, you can use the connection information previously configured for a Relay Server on a different machine. To do so, open the Relay Server Configuration tool on the configured Relay Server and click **Save to XML…**. For the unattended installation of a subsequent new Relay Server, ensure that the XML file is available on a local device (so not on a network share or mapped drive). In the command line for installation, provide the path to the XML file using the public property: `configfile=[path and file name]`.

For example:

```
msiexec /i "C:\temp\RES ONE Workspace Relay Server(x64) 10.1.0.0.msi"
configfile=c:\temp\rls.xml /qn
```

3.1.3 The Relay Server Configuration tool

Use the Relay Server Configuration tool to view and manage the Relay Server's connections to RES ONE Workspace environments.



On a machine running the Relay Server component, the Relay Server Configuration tool is available in the Start Menu. During interactive installation of the Relay Server component, the wizard automatically opens the Relay Server Configuration tool.

- Choose a **Listening port** between `1024` and `65535`, that is not used by any other process on this machine. If a value lower than `1024` is entered, this port number will automatically be changed to `1024` when saving. If a value higher than `65535` is entered, this port number will automatically be changed to `65535` when saving.
  If the Relay Server is installed on a computer that is also a RES ONE Workspace Agent, port `1942` cannot be used as the listening port for the Relay Server.
- You can override the **Default cache location**. Per connected environment, a subfolder created in `%ProgramData%\RES\Relay Server` serves as cache location.
- Choose **Save as XML** to export the list of environments and their settings to an XML file that you can use later when installing another similar Relay Server.

Connecting a Relay Server directly to the Datastore

The first Relay Server in a RES ONE Workspace environment must connect directly to the Datastore. The first Relay Server would normally be connected using the Relay Server Configuration tool. Other Relay Servers can connect directly to the Datastore or to other Relay Servers.

Set an environment password before connecting the first Relay Server. The environment password is set (and can be changed) in the RES ONE Workspace Console, at **Administration > Relay Servers**.

To connect a Relay Server to the Datastore:

- Click **Add** in the Relay Server Configuration tool to open the **Relay Server Connection Wizard**.
- Follow the prompts in the **Relay Server Connection Wizard** to connect the Relay Server to the RES ONE Workspace environment.
  - Choose **Directly to an existing Datastore** as the connection type and provide information about the relevant Datastore.

Security Best Practice

When connecting the Relay Server to a Datastore on a Microsoft SQL Server using Windows authentication, it is recommended to run the Relay Server Service with a **Windows account** instead of the **Local System account**. The Windows account that is used must be a domain account and needs the user right "Log on as a service".

Connecting a Relay Server to other Relay Servers

Instead of connecting directly to the Datastore, subsequent Relay Servers can also connect to parent Relay Servers. A parent Relay Server can have several child Relay Servers.

- Click **Add** in the Relay Server Configuration tool to open the Relay Server Connection Wizard.
- Follow the prompts in the Relay Server Connection Wizard to connect the Relay Server to the RES ONE Workspace environment.
  - Choose **To other Relay Server(s)** as the connection type, then provide servername and listening port of one or more parent Relay Server(s).
  - Since each Relay Server can optionally host multiple environments, you also need to select the relevant environment. For easy reference, the correct environment name is shown in the **Administration > Relay Servers** node in the RES ONE Workspace Console.
  - Provide the environment password that was configured in the RES ONE Workspace Console.

Note

In an environment with cascaded Relay Servers where more than 50,000 transactions exist in the queue of one of the Relay Servers, the Relay Server will not accept new transactions from a RES ONE Workspace Agent or another Relay Server until the queue has been reduced. This is to avoid problems such as that files in the Temporary folder are not cleaned up correctly, or refused transactions are not retried again by an Agent or another Relay Server.

Connecting a Relay Server using an existing configuration file

An existing configuration file can be used in two different ways to connect/configure Relay Servers:

- In the Configuration tool, choose **Load from XML** to import settings that you saved to XML when configuring a previous Relay Server. You can then edit the imported connection if necessary.
- Use a command line:

  ```
  RelayServer.exe /configfile=<file> /silent
  ```

  When using this command line, the Configuration tool will not open after execution. This command line is, for example, useful when current Relay Servers need to be reconfigured. It can be executed by using RES ONE Automation or any other tool.

3.1.4 Public properties for unattended installation

To install the Relay Server unattended from the command line, you can apply the following public properties to the Relay Server MSI file.

Public properties for unattended installation of Relay Server connecting directly to Datastore

Public property	Value	Comments
CONFIGFILE	<FILEPATH>	Specifies the path and filename of a RES ONE Workspace Relay Server configuration stored in an XML file that was generated on a Relay Server that connects directly to the Datastore. In this file, passwords are encrypted to prevent exposure. Create the configuration file from the Relay Server Configuration Tool, by clicking **Save to XML**. Example: CONFIGFILE=C:\TEMP\Configfile.xml
Alternatively, use:		
DBTYPE	MSSQL, DB2, ORACLE, MYSQL or MSSQLAZURE	Specifies the database type. Example: DBTYPE=MSSQL
DBSERVER	<SERVERNAME>	Specifies the database server to which the Relay Server should connect. Example: DBSERVER=SQLServer01
DBNAME	<DATABASENAME>	Specifies the name of the database to which the Relay Server should connect. Example: DBNAME=RESWorkspace
DBUSER	<DBUSERNAME>	Specifies the database user name that the Relay Server should use to connect to the database. Example: DBUSER=RESWorkspaceUser
DBPASSWORD	<DBPASSWORD> or <ENCRYPTED DBPASSWORD>	Specifies the (by default: plaintext) database password the Relay Server should use to connect to the database. Example: DBPASSWORD=RESWorkspaceUserPassword

Public property	Value	Comments
DBPASSWORD_IS_ENCR	YES or NO (default)	Specifies whether the value that is specified at DBPASSWORD is encrypted or not. The encrypted database password can be found in the XML configuration file that was generated on a Relay Server that connects directly to the Datastore. Create the configuration file from the Relay Server Configuration Tool, by clicking **Save to XML**. Example: DBPASSWORD=<ENCRYPTED DBPASSWORD> DBPASSWORD_IS_ENCR=YES
DBPROTOCOLENCRYPTION	YES or NO (default)	Specifies whether protocol encryption should be used when connecting to Microsoft SQL Server.
DBWINAUTH	YES or NO (default)	Specifies whether to use Windows authentication. With Windows authentication you do not specify a SQL account & password, but let the connection use the local Windows credentials to log on to the database.

SERVICEACCOUNTNAME	<DOMAIN>\<USER>	Specifies the account name that should be used as the Relay Server service account when using Windows authentication. The account must have the following permissions:
		• Read/Write permissions for:
		  • the configured cache location
		  • the Temp folder (as configured in the System Environment Variables)
		• Full Control permissions (with inheritance) for HKLM\SOFTWARE\RES\Workspace Manager\RelayServer\
		• Read/Write permissions for the database
		When not using Windows authentication, providing SERVICEACCOUNTNAME is optional. If not provided, the Relay Server service will run under the LocalSystem account.
		Example: SERVICEACCOUNTNAME=MyDomain\RSUser

SERVICEACCOUNTPASSWORD	<PASSWORD>	Specifies the plaintext password that should be used if a service account is specified for SERVICEACCOUNTNAME. Example: SERVICEACCOUNTPASSWORD=RSUserPassword
CACHE_PATH	<CACHEPATH>	Specifies the local cache path on the Relay Server. If not specified, the cache will be stored at %ProgramData%\RES\Relay Server\<Environment ID>. Example: CACHE_PATH=C:\Relay\Cache

Public property	Value	Comments
PORT	<PORTNUMBER>	Specifies the listening port of the Relay Server and must be a value between 1024 and 65535. By default, the listening port is 1942. If the Relay Server is installed on a computer that is also a RES ONE Workspace Agent, port 1942 cannot be used as the listening port for the Relay Server. Example: PORT=21943

Public properties for unattended installation of Relay Server connecting to other Relay Servers

Public property	Value	Comments
CONFIGFILE	<FILEPATH>	Specifies the path and filename of a RES ONE Workspace Relay Server configuration stored in an XML file that was generated on a Relay Server that connects to another Relay Server. In this file, passwords are encrypted to prevent exposure. Create the configuration file from the Relay Server Configuration Tool, by clicking **Save to XML**. Example: CONFIGFILE=C:\TEMP\Configfile.xml
Alternatively, use:		
CACHE_PATH	<CACHEPATH>	Specifies the local cache path on the Relay Server. If not specified, the cache will be stored at %ProgramData%\RES\Relay Server\<Environment ID>. Example: CACHE_PATH=C:\Relay\Cache
PORT	<PORTNUMBER>	Specifies the listening port of the Relay Server and must be a value between 1024 and 65535. By default, the listening port is 1942. If the Relay Server is installed on a computer that is also a RES ONE Workspace Agent, port 1942 cannot be used as the listening port for the Relay Server. Example: PORT=16012

Public property	Value	Comments

SERVICEACCOUNTNAME	<DOMAIN>\<USER>	Specifies the account name that should be used as the Relay Server service account. The account must have the following permissions:
		• Read/Write permissions for:
		  • the configured cache location
		  • the Temp folder (as configured in the System Environment Variables)
		• Full Control permissions (with inheritance) for HKLM\SOFTWARE\RES\Workspace Manager\RelayServer\
		Providing SERVICEACCOUNTNAME is optional.
		If not provided, the Relay Server service will run under the LocalSystem account.
		Example: SERVICEACCOUNTNAME=MyDomain\RSUser

SERVICEACCOUNTPASSWORD	<PASSWORD>	Specifies the plaintext password that should be used if a service account is specified for SERVICEACCOUNTNAME. Example: SERVICEACCOUNTPASSWORD=RSUserPassword
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 servername should be followed by a colon (:) and the listening port. Example: RSLIST=Server1;Server2:2012;Server3.MyDomain.com
RS_ENV_ID	<GUID>	Specifies the GUID that uniquely identifies the RES ONE Workspace environment that the Relay Server should connect to. This GUID can be found in the Management Console, at **Administration > Relay Servers**, on the **Settings** tab. Example: RS_ENV_ID={076FC22E-B7A1-477E-A021-94601893B568}

Public property	Value	Comments
RS_PWD	<ENCRYPTED PASSWORD>	Specifies the encrypted password of the RES ONE Workspace environment that the Relay Server should connect to. This password must already be set in the **Administration > Relay Servers** node in the Management Console. 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**. Alternatively, Technical managers can obtain the encrypted (hashed) version of the Environment password by using one of the following command lines on the machine running the Management Console: • pwrtech.exe /gethashedpassword With Ctrl+C, the hashed password can be copied from the dialog box to the clipboard. • pwrtech.exe /gethashedpassword /f=<full file path> The hashed password is saved in the specified file at the given location.

Examples:

Install Relay Server and connect to Datastore

```
msiexec.exe /i "C:\Install\RES ONE Workspace Relay Server(x64)
10.1.0.0.msi" DBTYPE=MSSQL DBSERVER=SQLSERVER01 DBNAME=RESWorkspace
DBUSER=WorkspaceUser DBPASSWORD=password DBPROTOCOLENCRYPTION=No
CACHE_PATH=C:\Relay\Cache /qn
```

Install Relay Server and connect to Datastore including the Relay Server service account:

```
msiexec.exe /i "C:\Install\RES ONE Workspace Relay Server(x64)
10.1.0.0.msi" DBTYPE=MSSQL DBSERVER=SQLSERVER01 DBNAME=RESWorkspace
DBWINAUTH=Yes DBPROTOCOLENCRYPTION=No
SERVICEACCOUNTNAME=RelayServerServiceAccount
SERVICEACCOUNTPASSWORD=RelayServerServiceAccountPassword
CACHE_PATH=C:\Relay\Cache /qn
```

Install Relay Server and connect to another Relay Server

```
msiexec.exe /i "C:\Install\RES ONE Workspace Relay Server(x64)
10.1.0.0.msi" PORT=1944 RS_LIST=RelayServer.MyDomain.com:1945
RS_ENV_ID={1B084390-9F59-43BA-A601-FC087E681CEE}
RS_PWD=38661621371C7E0C7C10ACA1CAEA1675F8678925 /qn
```

Note

Unattended installation using `msiexec.exe` will only work with parameter `/qn`.

3.1.5 Connection authentication

Encryption

Communication between RES ONE Workspace Agents and Relay Servers and between Relay Servers is encrypted using TLS, version 1.0, 1.1* or 1.2*.
The highest possible TLS version will be negotiated: if TLS 1.2 is not available, first fallback will be to use TLS 1.1. If that is also not available, TLS 1.0 will be used.

* Only available if the Relay Server is installed on a machine that also has .NET Framework 4.5 or higher installed.

Certificates

For the connection between a RES ONE Workspace Agent (RES service) and a Relay Server and between Relay Servers, custom certificates can be used.
To use custom certificates, the following registry values can be used:

- `CustomCertificate`
  Mandatory for using custom certificates.
  Specifies the value that is used to identify the custom certificate by, in the certificate store. By default, the Relay Server will compare this values against 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 following registry values:
- `CustomCertificateFindBy`
  Specifies another property than "Subject name" to identify the custom certificate by, in the certificate store. Possible values are `Thumbprint` and `Serial number`. The values for `Thumbprint` and `Serial number` (provided at `CustomCertificate`) may not contain any spaces.
- `CustomCertificateStore`
  Specifies a different folder than "Personal" in the certificate store to be used by the Relay Server when looking for the custom certificate in the certificate store. For non-English versions of Microsoft Windows, the Microsoft Windows internal folder names must be specified for **Data**. The supported Microsoft Windows internal folder names are specified below:

Microsoft Windows internal folder name	Name of folder on an English Microsoft Windows Operating System
Root	Trusted Root Certification Authorities
CertificateAuthority	Intermediate Certification Authorities
TrustedPublisher	Trusted Publishers
Disallowed	Untrusted Certificates
AuthRoot	Third-Party Root Certification Authorities
TrustedPeople	Trusted People
AddressBook	Other People

All three registry values must be set in the `RelayServer` folder at `HKLM\Software\RES\Workspace Manager`. These registry values can also be found in the RES ONE Workspace Administration Guide which is available from the **RES Success Center**.

Notes

- The "Subject name" on the custom certificate must match the Fully Qualified Domain Name (FQDN) that RES ONE Workspace 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.

Please note that if the registry value `CustomCertificate` (and optionally `CustomCertificateFindBy` and `CustomCertificateStore`) has not been specified, a self-signed certificate will be used for the connection between RES ONE Workspace Agents and Relay Servers, and between Relay Servers.

To disallow the use of a self-signed certificate for the connection between a RES ONE Workspace Agent and a Relay Server, set the following registry value:

- `DoNotAcceptSelfSignedCert` - set this registry value at `HKLM\Software\RES\Workspace Manager` (32-bit) / `HKLM\Software\Wow6432Node\RES\Workspace Manager` (64-bit).

To disallow the use of a self-signed certificate for the connection between Relay Servers, set the following registry value:

- `DoNotAcceptSelfSignedCert` - set this registry value at `HKLM\Software\RES\Workspace Manager\RelayServer`.

Chapter 4: Connecting existing Agents to Relay Servers

All connection information for Agents is stored in the Datastore and can be managed through the RES ONE Workspace Console.

On the **Settings** tab at **Administration > Agents**, you can configure the global default behavior of Agents: **Connect directly to the Datastore** or **Connect through Relay Server**; and if the latter, you can configure how Agents determine which Relay Server to use.

Using the exception tabs ([+]), you can create different default behavior and/or Relay Server connection options for Agents in different Workspace Containers.

By default, each Agent inherits its connection settings (from a Workspace Model or from the global settings). You can edit individual Agents to always connect directly to the Datastore, or to always connect through Relay Servers with specific settings. This is configured on the Agent's **Connection** tab.

4.1 How Agents determine which Relay Server to use

Agents can use a combination of three different methods to determine which Relay Server(s) should be used:

- Automatically discover available Relay Servers in the correct environment; and/or
- Connect to Relay Servers specified in a list; and/or
- Use DNS to resolve the FQDN of a Relay Server. This is particularly useful for identifying a Relay Server that can be reached by Agents connecting from outside the network.

Selected connection methods are handled in order of appearance; and 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 in the RES ONE Workspace Console at **Administration > Agents**, on the **Settings** tab, 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, it will try another Relay Server from the list (in random order). If no other Relay Server can be found, 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, the local cache of the Agent will not be updated.

Notes

- 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 own 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.

Chapter 5: Installing new Agents and connecting them to Relay Servers

There are several ways to install an Agent and connect it to Relay Servers:

- Interactive installation followed by the Connection Wizard.
- Unattended installation using public properties that make the Agent member of a Workspace Container that determines its connection.
- Unattended installation using public properties that give the Agent specific connection settings.

For more detailed information about installing RES ONE Workspace Agents, please refer to **Getting Started with RES ONE Workspace**, which is available for download from the **RES Success Center**.

5.1 Interactive installation followed by the Connection Wizard

During an interactive installation, the Agent installation wizard automatically opens the Connection Wizard, where you can choose to:

- connect to an existing environment, and connect the Agent:
  - directly to the Datastore.
  - to Relay Servers.
- set up a new RES ONE Workspace environment (only available if a full installation of RES ONE Workspace was performed).

Follow the prompts in the Connection Wizard to connect the Agent to Relay Servers.

5.2 Unattended installation during which Agent becomes member of a Workspace Container

By default, Agents inherit their connection type (Relay Server or Datastore) and connection settings from the applicable Workspace Model or from the global settings. Workspace Models are configured per Workspace Container. For example, an environment can use direct Datastore connections as global default, but Agents in the Workspace Container called "Subsidiary" use Relay Servers.

During unattended installation of an Agent, use public properties to provide an initial connection (either to the Datastore or to a Relay Server) *plus*:

- `ADDTOWORKSPACE=<CONTAINERNAME>` to make the newly installed Agent member of a specific Workspace Container.
- `INHERITSETTINGS=YES` to let the Agent inherit its connection settings. The Datastore or Relay Server connection provided with the installation will only be used to establish the initial connection, and will be disregarded afterwards.

An Agent installed in this manner will inherit its connection type and connection settings from the workspace model configured for the specified Workspace Container. Therefore, an Agent installed with `ADDTOWORKSPACE=Subsidiary` will get the Workspace Model that uses Relay Servers.

5.3 Unattended installation using public properties that give the Agent specific connection settings

During unattended installation of an Agent, use the following public properties to set specific Relay Server connection settings for the Agent:

Public property	Value	Comments
RSENVGUID	<GUID>	Specifies the GUID that uniquely identifies the RES ONE Workspace environment that the Agent should connect to. This GUID can be found in the Management Console, at **Administration > Relay Servers**, on the **Settings** tab. Example: RSENVGUID={076FC22E-B7A1-477E-A021-94601893B568}
RSPASSWORD	<PASSWORD> or <HASHED RSPASSWORD>	Specifies the (by default: plaintext) password of the RES ONE Workspace environment that the Agent should connect to. This password must already be set in the **Administration > Relay Servers** node in the Management Console.
RSPWHASHED	YES or NO (default)	Specifies whether the value that is specified at RSPASSWORD is hashed. Technical managers can obtain the hashed version of the Environment password by using one of the following command lines on the machine running the Management Console: • pwrtech.exe /gethashedpassword With Ctrl+C, the hashed password can be copied from the dialog box to the clipboard. • pwrtech.exe /gethashedpassword /f=<full file path> The hashed password is saved in the specified file at the given location. Alternatively, the hashed (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=<HASHED RSPASSWORD> RSPWHASHED=YES
RSDISCOVER	YES or NO (default)	Specifies whether the Agent should discover Relay Server(s) using multicast.
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 servername should be followed by a colon (:) and the listening port. Example: RSLIST=Server1;Server2:2012;Server3.MyDomain.com

Public property	Value	Comments
RSRESOLVE	<RELAY SERVER FQDN>	Specifies the FQDN of a Relay Server to be resolved by DNS. Example: RSRESOLVE=relay.ressoftware.com
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).