Agent 8.7 for Microsoft Windows

Automating Agent Deployment

© Copyright Owner 2018. All Rights Reserved.

The software manufacturer makes no representations or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, the software manufacturer reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of the software manufacturer to notify any person of such revision of changes. All companies, names and data used in examples herein are fictitious unless otherwise noted.

No part of this document may be reproduced, transmitted, transcribed, stored in a retrieval System or translated into any language including computer language, in any form or by any means electronic, mechanic, magnetic, optical, chemical or otherwise without prior written permission.

All other products or company names mentioned in this document are trademarks or registered trademarks of their respective owners.

Acknowledgements: Two encryption methods, DES and TripleDES, include cryptographic software written by Eric Young. The Windows versions of these algorithms also include software written by Tim Hudson. Bruce Schneier designed Blowfish encryption.

"Part of the software embedded in this product is gSOAP software. Portions created by gSOAP are Copyright (C) 2001-2006 Robert A. van Engelen, Genivia inc. All Rights Reserved. THE SOFTWARE IN THIS PRODUCT WAS IN PART PROVIDED BY GENIVIA INC AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE."

The Agent, Agent Console, and Vault applications have the added encryption option of 128/256 bit AES (Advanced Encryption Standard). Advanced Encryption Standard algorithm (named Rijndael, pronounced “Rain Doll”) was developed by cryptographers Dr. Joan Daemen and Dr. Vincent Rijmen. This algorithm was chosen by the National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce to be the new Federal Information Processing Standard (FIPS). See: http://csrc.nist.gov/encryption/aes/round2/r2report.pdf for details.

The Agent and Vault applications have the added security feature of an over the wire encryption method.

Document History

Version	Date	Description
1	December 2018	Initial Automating Agent Deployment guide provided for Windows Agent 8.7*x*.

Contents

1 Automate Windows Agent deployment using Group Policy

You can automate the installation and upgrade of Windows Agents across your organization using Active Directory Group Policy. To do this, you must:

1. Extract .msi and .mst files from the Windows Agent installation kit
2. Specify Agent installation options
3. Push the Agent to systems using Active Directory Group Policy

Important: Beginning in Portal version 8.70, you can provide Windows Agent installers through Portal and upgrade the Agent automatically on computers where Windows Agent version 8.70 or later is installed. For more information, see the Portal documentation.

1.1 Extract .msi and .mst files from the Windows Agent installation kit

Before you can deploy the Windows Agent using Group Policy, you must extract .msi and .mst files from the Windows Agent installation kit. The Windows Agent installation kit is provided in .exe format, and cannot be deployed using Group Policy.

The .msi file is an installation package that can be pushed to systems using Active Directory Group Policy. The .mst file contains settings for the installer, and must be edited before you deploy the Agent. See Specify Agent installation options.

To install and upgrade the Windows Agent automatically on both 64-bit and 32-bit systems, you must extract files from both the 64-bit and 32-bit Windows Agent installation kits using these steps. You can then assign the appropriate .msi and .mst files (64-bit or 32-bit) for each organizational unit (OU) or computer groups.

To extract .msi and .mst files from the Windows Agent installation kit:

1. Make a copy of the Agent installation kit, and name it “setup.exe”.
2. Create a directory for saving the .msi and .mst files (e.g., C:\Temp\MSI).
3. Run the following command:

   ```
   setup.exe /s /b"directory" /v"/qn" [language]
   ```

   Where:

   - *directory* is the directory created in Step 2 for saving the .msi and .mst files (e.g., C:\Temp\MSI).
   - By default, English is used for the .msi file. To specify a language for the Agent, include one of the following language parameters in the command:

     /L1036 – French

     /L1034 – Spanish

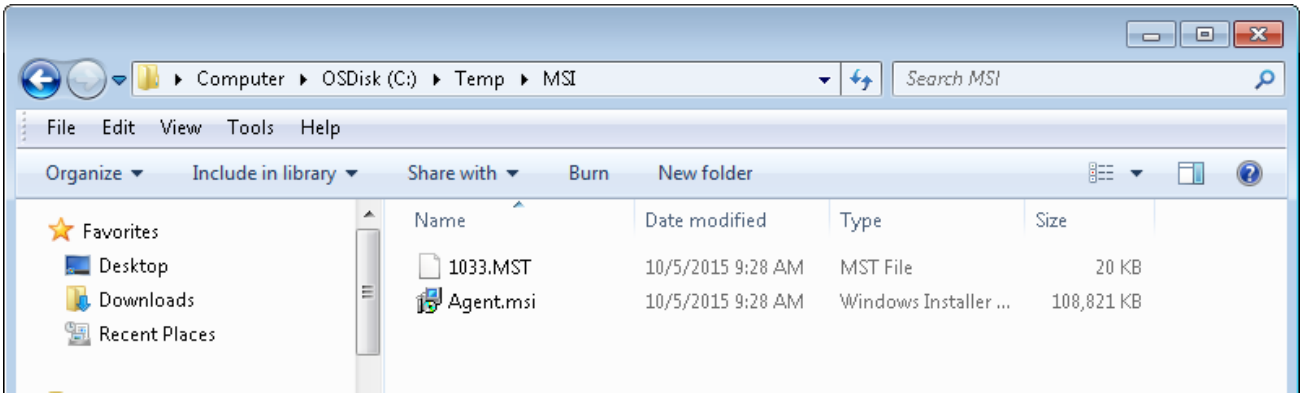
     /L1031 – German

/L1033 – English

For example, the command for extracting an English Agent installer in the C:\Temp\MSI directory would be:

```
setup.exe /s /b"C:\Temp\MSI" /v"/qn"
```

An Agent.msi file and an .mst file is extracted in the specified location. The name of the .mst file corresponds to the specified language.



1.2 Specify Agent installation options

After extracting the Agent.msi and .mst file from the Agent installation kit, you can add and edit properties in the .mst file. Properties in the .mst file provide Portal registration information and specify which plug-ins to install with the Agent.

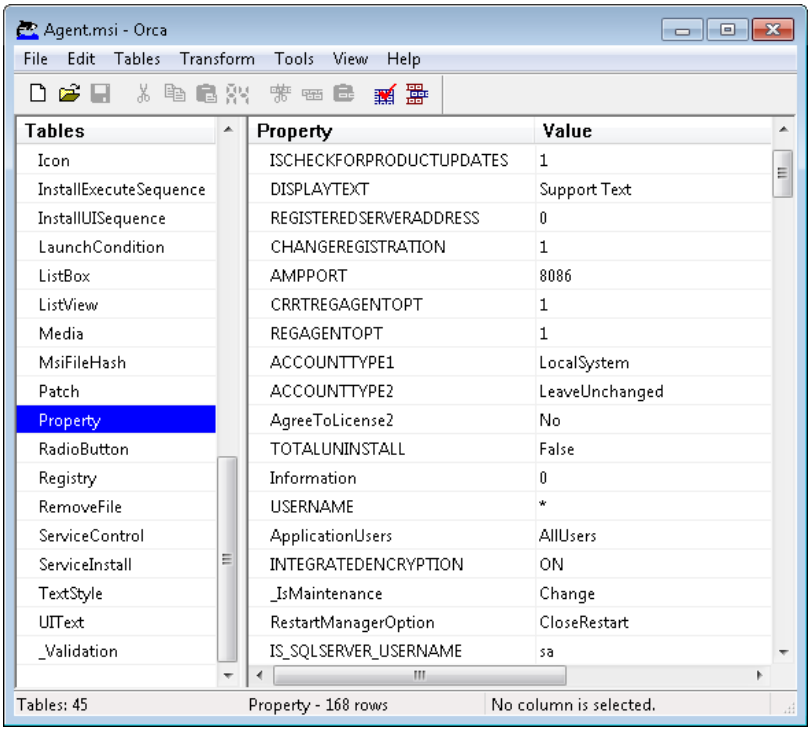
To edit the properties, use Orca: an editor for Windows Installer packages. Orca can be downloaded from Microsoft as part of the Windows Installer SDK.

After editing properties, you can save the new .mst file, and distribute it with the Agent.msi file.

To specify Agent installation options:

1. Using Windows Installer SDK Orca, open the Agent.msi file.
2. Go to **Transform** > **Apply Transform**.
3. In the Open dialog box, select the .mst file, and click **Open**.
4. In the tables list at the left side of the Orca window, click **Property**.

   The right side of the window shows current properties and their values.



5. If you want to register the Agent to Portal, do the following:

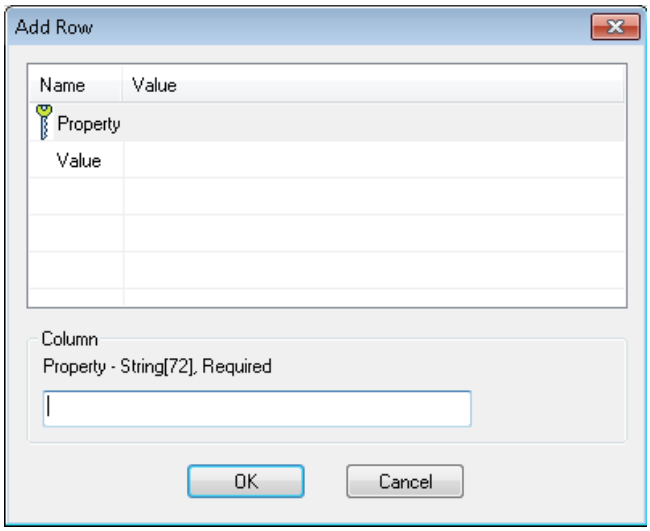
   - Find the REGISTERWITHWEBCC property. Double-click the property's **Value** column, and change the value to TRUE.
   - Add the properties shown in the following table:

Property	**Value**
AMPNWADDRESS	IP address or host name of the Portal for managing the Agent (e.g., portal.company.com)
AMPPORT	(Optional) Port number for the Agent to communicate with Portal. The default port is 8086.
AMPUSERNAME	Name of the Portal user for the Agent (e.g., admin@company.com). The user must be an Admin user or regular user. Typically, the user name is an email address.
AMPPASSWORD	Password of the specified Portal user.

   To add each property, do the following:

   - Right-click the **Property** column, and choose **Add Row**.

     The Add Row dialog box appears.



- In the **Property** row, enter the property name in the **Value** column.
- In the **Value** row, enter the property value in the **Value** column.
- Click **OK**.

6. For each plug-in that you want to install with the Agent, change the plug-in's property value to **ON**.

   The following table shows the property name for each plug-in. By default, plug-ins are not installed with the Agent.

Plug-in	**Property**
Cluster Support Plug-in	`FEATURECLUSTER`
Exchange 2007 DR Plug-in (only available with the 64-bit Windows Agent)	`FEATUREEXCHANGE`
Exchange 2010/2013 DR Plug-in (only available with the 64-bit Windows Agent) *Note:* After the Agent installation, the machine must be restarted before you can share a safeset for restoring individual mailboxes and messages using the Granular Restore for Exchange application.	`FEATUREEXCHANGE2010`
Oracle Plug-in	`FEATUREORACLE`
SQL Server Plug-in *Note:* After the Agent installation, the machine must be restarted before you can share a safeset for restoring individual SharePoint objects using the Granular Restore for SharePoint application.	`FEATURESQL`

Plug-in	Property
Image Plug-in (only available with the 64-bit Windows Agent) *Note:* After the Agent installation, the machine must be restarted before the Image Plug-in can use Changed Block Tracking (CBT) to identify data that has changed since a previous backup. Without CBT, the Agent reads all data for every backup when backing up a volume.	`FEATUREVOLUMEIMAGE`

To change a property value, do the following:

- Find the property for the plug-in.
- Double-click the property's **Value** column.
- Enter **ON**.

7. Go to **Transform** > **Generate Transform**.
8. In the Save Transform As dialog box, specify a new name for the .mst file, and click **Save**.

   You can then push the Agent.msi file and the new .mst file to systems using Group Policy.

1.3 Push the Agent to systems using Active Directory Group Policy

After extracting the Agent installation files and specifying installation options, you can push the Agent to systems using Active Directory Group Policy. For detailed instructions, see information from Microsoft. For a sample procedure, see Example: Pushing the Agent to systems using Active Directory Group Policy.

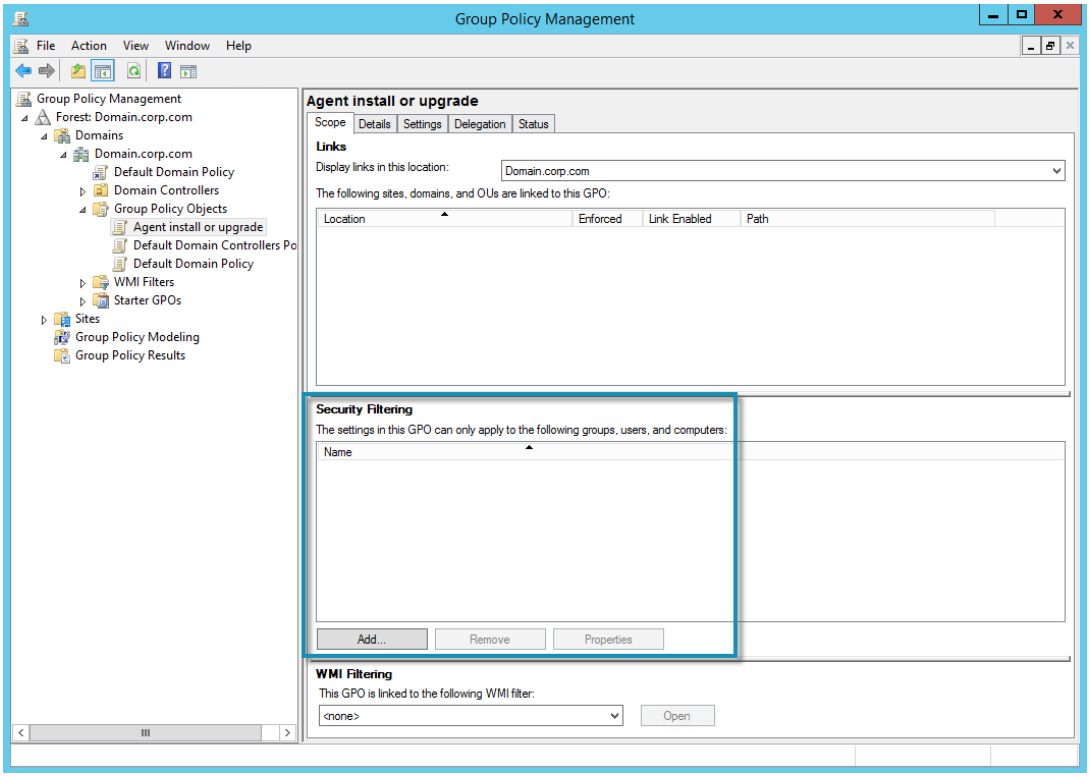
To ensure that the Agent is installed or upgraded correctly, we recommend pushing the files to one system before pushing them to all machines.

1.3.1 Example: Pushing the Agent to systems using Active Directory Group Policy

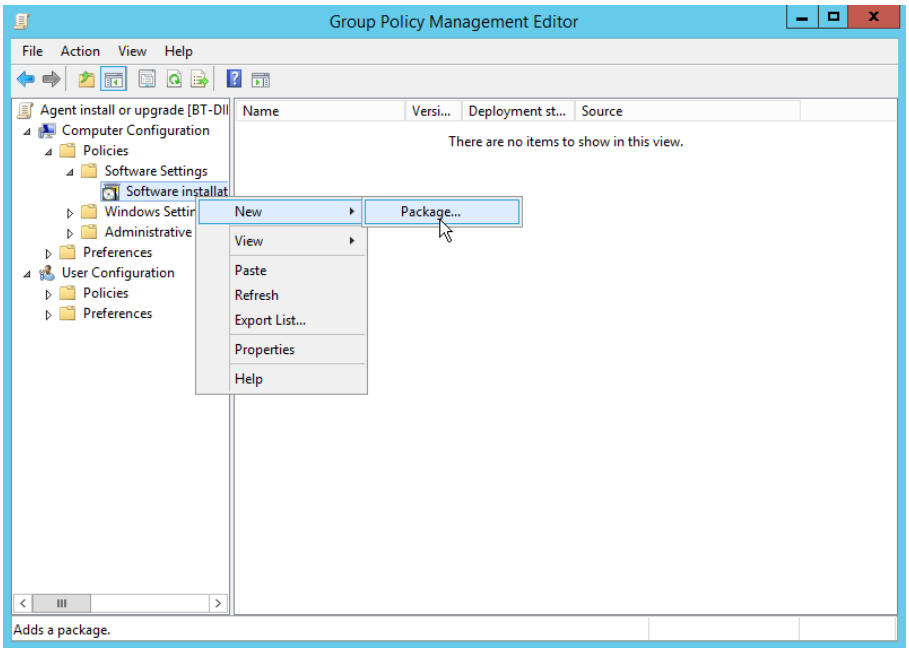
This section describes how to push the Agent to systems using Active Directory Group Policy on Windows Server 2012. This procedure is provided only as an example. For detailed procedures, see information from Microsoft.

1. Create a shared folder (e.g., \\Server\MSI). Ensure that all domain computers have read permission to the UNC share.
2. In the shared folder, save the Agent.msi file and the .mst file that was edited using Orca.
3. On the domain controller, or on a system with Administrative Tools installed, open **Active Directory Users and Computers** from Administrative Tools.

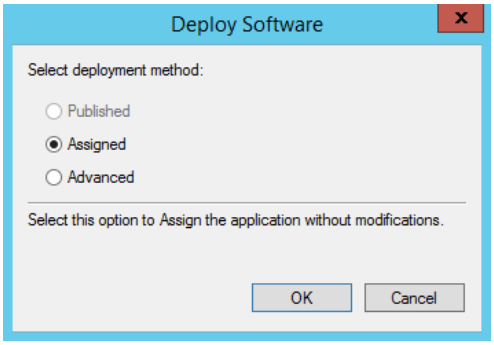
4. Create a new group. In the group, add computers where you want to install or upgrade the Agent.
5. From Administrative Tools, open **Group Policy Management**.
6. Create a new group policy and link it to the domain or OU, as needed.
7. In the **Security Filtering** area, remove the authenticated users, and add the computers or computer groups where you want to install or upgrade the Agent.



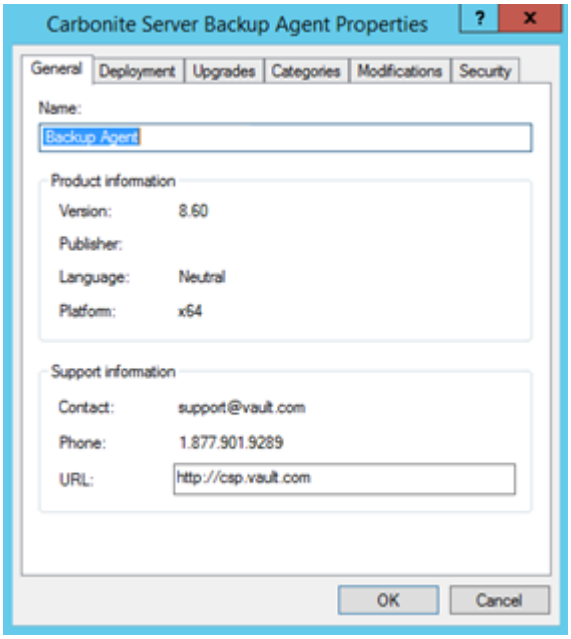
8. Right-click the group policy, and select **Edit**.
9. In the Group Policy Management Editor, go to **Computer Configuration** > **Policies** > **Software Settings** > **Software Installation**. Right-click **Software Installation**, and choose **New** > **Package**.



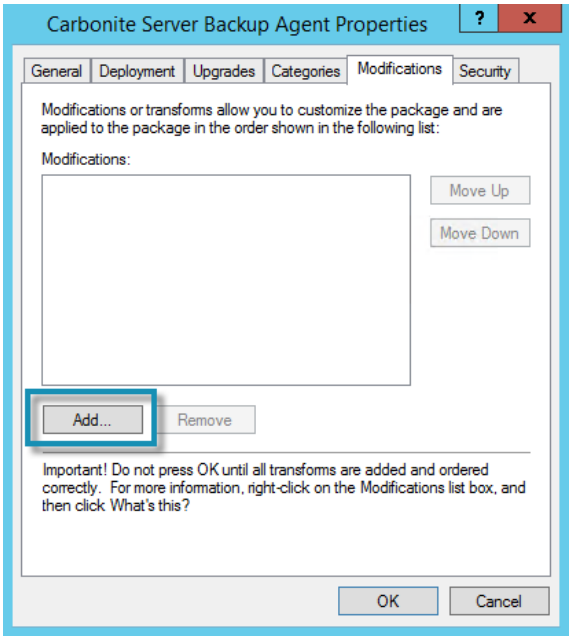
10. In the Open dialog box, navigate to the share path that was created in Step 1 (e.g., \\Server\MSI). Select the Agent.msi file, and click **Open**.
11. In the Deploy Software dialog box, choose **Advanced**, and then click **OK**.



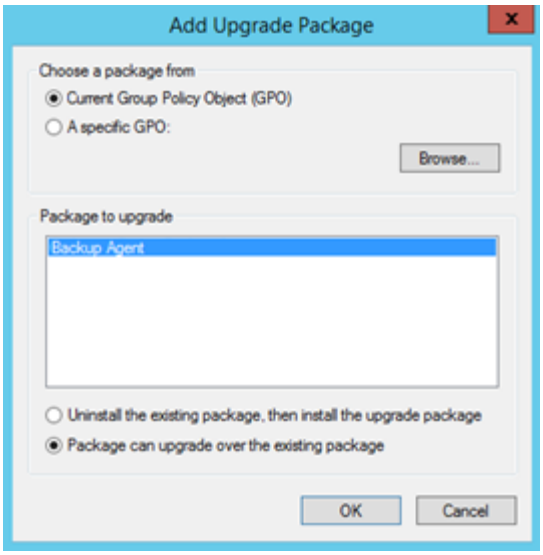
The Properties dialog box appears.



12. In the Properties dialog box, click the Modifications tab. Click **Add**, and add the .mst file from the share path that was created in Step 1 (e.g., \\Server\MSI).



13. If agents will be upgraded on some computers, click the Upgrades tab in the Properties dialog box. Click **Add**. In the Add Upgrade Package dialog box, choose the package that can be upgraded, and select **Package can upgrade over the existing package**. Click **OK**.



14. In the Properties dialog box, click **OK.**
15. Do one of the following:
    - Reboot the domain computers to install or upgrade the Agent.
    - Run the following command to force the group policy:

      ```
      gpupdate /force
      ```