TECHNICAL DOCUMENTATION

SPECOPS DEPLOY / APP

4.7   DOCUMENTATION

Contents

1. Getting Started

This page will walk you through the setup of Specops Deploy and help you deploy your first software package.

It is possible to conduct an entire evaluation on a single computer if a larger testing environment is unavailable, although the computer has to be a member of an Active Directory Domain and at least one Group Policy Object (GPO) is required, which applies to the computer and or user account being utilized for testing which can be edited.

In a single computer test, the computer will have the server software, admin tools and the client side extension installed locally.

1.1 Specops Deploy Supported Configurations

Operating System	Specops Deploy Server	Client Side Extension
Windows XP	✘	✔
Windows Vista	✘	✔
Windows 7	✘	✔
Windows 8	✘	✔
Windows Server 2003	✔	✔
Windows Server 2003 R2	✔	✔
Windows Server 2008	✔	✔
Windows Server 2008 R2	✔	✔
Windows Server 2012	✔	✔

2. Specops Deploy and Active Directory

- *NOTE: Although Specops Deploy integrates into Active Directory,* **it does not edit or extend the Active Directory Schema.**

- An Active Directory Service Account is required to run the Specops Deploy Service. This account should be setup and configured in advance and granted administrative rights to the deploy server or servers being used for Specops Deploy.

- Active Directory administrative rights are required to modify and apply group policy.

3. Specops Deploy Prerequisite Components

3.1 Windows Server Operating System

The Specops Deploy Server requires Windows Server 2003 or higher installed to host the Specops Deploy Server components. This can be an existing server or a dedicated server.

3.2 Microsoft .Net Framework

The Specops Deploy Setup Assistant requires that Microsoft .Net Framework 3.51 or 4.0 is installed on the server where the Setup Assistant is started. If it is not installed it can downloaded from Microsoft

3.3 Microsoft Management Console

Specops Deploy requires the Microsoft Management Console version 3.0 installed on the computers where Specops Deploy will be managed.

3.4 Microsoft Group policy Management Console

The Specops Deploy Admin Tools requires that Microsoft Group Policy Management console be installed on the computer where the admin tools need to be used.

3.5 Microsoft SQL Server

An instance of Microsoft SQL Server is required to host the Specops Deploy Database. This is used to store the feedback information that the clients send during and after software operations. The SQL Server does not have to be running on the same computer as the Specops Deploy Server and any SQL server instance can be used.

Specops Deploy uses a database called **Specops3**.

Specops Deploy Setup Assistant will create the database if no database with that name exists. The database will use default values for location on disk and other settings and the initial size will be 50 MB with a transaction log of 20 MB. If special requirements exist for location, size etc. for the database files then the database can be created manually before the Specops Deploy Assistant is started. All versions of SQL above Microsoft SQL 2005 SP3 are supported with Specops Deploy / App

4. How to Setup Specops Deploy

Specops Deploy ships as one binary file. When extracted it launches a program called Specops Deploy Setup Assistant. This Setup Assistant will help an administrator install Specops Deploy in an Active Directory environment.

The Setup Assistant should be run for the first time on the computer intended to be used for the Specops Deploy server. The Setup Assistant guides the administrator through four different steps that should be performed in the following order to get started as fast as possible:

▪ **Server installation** – This will install the Specops Deploy Database and Server Service software on the local computer.

▪ **Client installation** (on a single computer) – Installs the Specops Deploy Client Side Extension (CSE) on the local computer. This method of installation should only be used when installing during evaluation, for a live installation, see the Client Deployment tab.

▪ **Admin tools installation** (on a single computer) – Installs the Specops Deploy Administrative Tools on the local computer.

▪ **Client deployment**: Will guide an administrator through the process of deploying the Specops Deploy Client Side Extension to all the client computers via native group policy. It is recommended the during testing of Specops Deploy that administrators start with the manual installation and then use this method when ready to deploy the client side extension to a large number of computers in the organization.

For organizations with an existing version of the Specops Deploy Client Extension (CSE) installed it is recommended that the correct upgrade path be configured by utilizing the Specops Deploy setup assistant.

   ▪ *NOTE: Hovering over any fields of the Specops Deploy Consoles will display help on what information is required for those fields.*

4.1 Deploy Server Installation

- Select the Server installation tab once the Specops Setup Assistant has been launched
- Verify that the Operating System, Local Permissions, .Net Framework version and Microsoft SQL Server Prerequisites Pass.
- Enter the Service Account created as part of the Prerequisites step by selecting the "Select account button". This account should be a local administrator on the server where Specops Deploy is being installed.
- Create the required security group "Specops Deploy Feedback Users" by selecting the Create button.
- Install the Specops Deploy Server by selecting the "Install" button.

4.2 Client Installation (For Local Testing on the same computer)

- Select the Client installation tab
- Verify that the.Net Framework Prerequisites are met.
- Install the Specops Deploy Client Side Extension by selecting the "Install" button.

4.3 Admin Tools Installation

   o *NOTE! The Specops Deploy Admin tools can be installed on any computer being used to administer Specops Deploy.*
- Select the Admin tools installation tab once the Specops Setup Assistant has been re-launched
- Verify that the .Net Framework version and MMC Version Prerequisites Pass.
- Install the "Specops Deploy Admins Tools" by selecting the "Install" button

4.4 Client Deployment (Recommended)

NOTE: For machines older than Windows Vista .NET Framework 2.0 is required to run the Specops Client Side Extension.

- Select the Client deployment (Optional) tab once the Specops Setup Assistant has been re-launched
- Select Group Policy Object by selecting the "Select GPO" button. This dialog will allow an administrator to Select an existing GPO or create a new GPO to utilize for deploying the client side extension.
   o *It is recommended that a new clean GPO be used for this purpose as this can then be linked to a test OU without impacting existing group policies that are currently in used.*
- Select a network share by selecting the "Select Share" button. This dialog will allow an administrator to automatically create a share on the deployment server locally or select a share manually. This can be an existing file server used for hosting software or a DFS share.
- Begin editing the newly created GPO by selecting the "Start GPOE" button.
- Create a new package by selecting the New->Package menu item from the "Computer Configuration->Software Settings->Software installation node.
- Browse to the share created in a previous step that contains the Windows Installer file for Specops Deploy GPO Extension, SpecopsDeployClientSideExtension-x86.msi on the server share or DFS location where the client side extension files have been loaded \\SpecopsDeploy, this will install the client side extension for 32 bit computers.
- Select Advanced in the "Deploy Software" dialog and then press OK.
- Open the deployment tab and select the "Advanced" button
- Ensure the package is not deployed to 64-Bit computers by unchecking the options "Make this 32-Bit X86 applications available to Win64 machines."
- Click OK on all dialogs. The Specops Deploy Client Side Extension should now appear in the "Software Installation" list

- Browse to the share created in a previous step that contains the Windows Installer file for Specops Deploy GPO Extensions, SpecopsDeployClientSideExtension-x64.msi on the server share or DFS location where the client side extension files have been loaded, this will install the client side extension for 64 bit computers.
- Select Advanced in the "Deploy Software" dialog and then press OK.
- Click OK on all dialogs. The Specops Deploy Client Side Extension should now appear in the "Software Installation" list
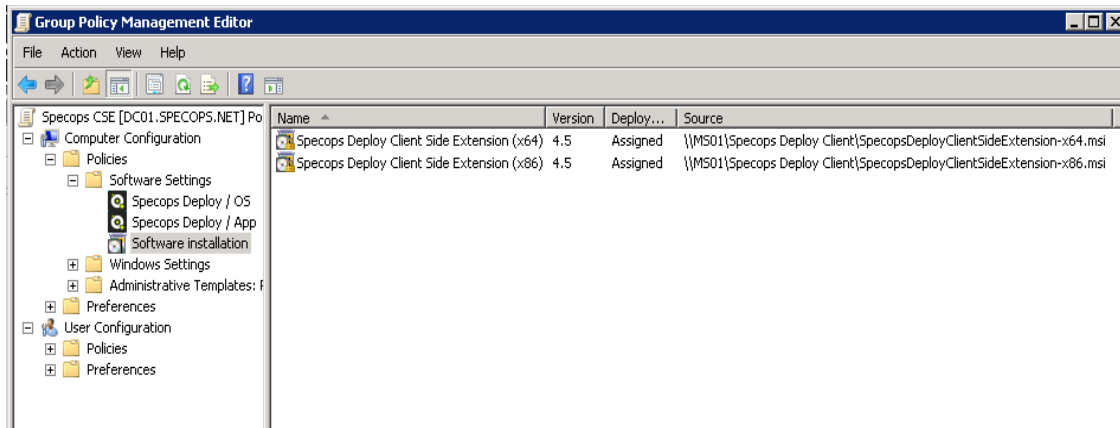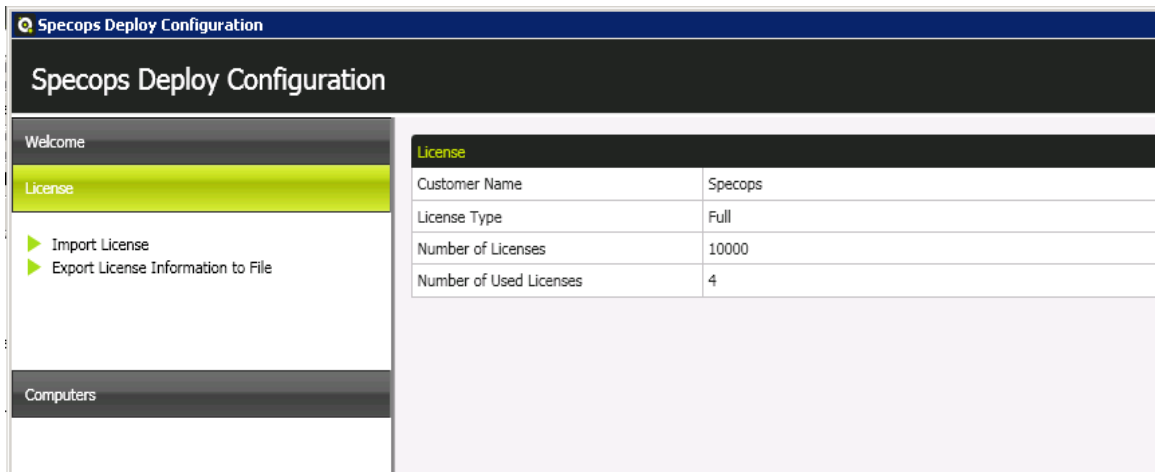

- Once all steps have been completed and machines affected by the GPO are rebooted the new Client Side Extension will be installed and administrators can now begin deploying Software using Specops Deploy.

5.License management in Specops Deploy

Specops Deploy tracks the number of installed and active client side extensions installed in an environment. As a result, license management and computer management is performed via the Specops Deploy Configuration tool. Before Specops Deploy can be used an administrator must import a Specops Deploy license using the Specops Deploy Configuration Tool.

5.1 Using the Specops Deploy Configuration Tool to manage computers

All clients with an active Specops Deploy Client Side Extension (CSE) will send a heartbeat to the central Specops Deploy Server. These will then be counted as an active license in Specops Deploy. Machines with a Client Side Extension heartbeat greater than 6 months will not be counted as active or consume a license and can be removed for the Specops Deploy Database using the Specops Deploy Configuration Tool. This can also be used to export a list of computers from the database based on filter criteria.

6.How to Deploy Software using Specops Deploy

Specops Deploy comes with two UI's to manage Specops Deploy; these are Specops Deploy Control Center and the Specops Deploy GPMC Snap-in, the latter integrates into the Microsoft Group Policy Management Console (GPMC) and is intended for administrators that already have knowledge of Group Policy and use it to administer Group Policy within Active Directory environments. Specops Deploy Control Center hides some of the complexity of the underlying Group Policy infrastructure and is primarily intended for administrators that are not used to working with Group Policy. Both tools support fully functionality of Specops Deploy and can be used to edit the same GPOs.

In this section it is assumed that Specops Deploy Control Center is used. However, any differences between the two tools will also be explained.

7.How to Deploy Software using Specops Deploy Control Center

Specops Deploy Control Center can be started from the Setup Assistant when the installation has been completed or from the start menu on a system where the admin tools have been installed. From within the Setup Assistant click the Start button in the Start Specops Deploy Control Center section.

From the start menu navigate to All Programs>Specops Software> Specops Deploy>Specops Deploy Control Center

NOTE: When the Control Center is started for the first time a dialog will be displayed where you are asked to select or create a new GPO. It is recommended that a new GPO be used for testing purposes which is targeted at a test OU containing either users or computers.

7.1 Select a GPO for Specops Deploy

Specops Deploy stores all information about software deployments in Group Policy Objects. When working in the Specops Deploy Control Center administrators are always working within the context of one GPO. Make sure that the scope of the GPO contains all the computers and users that administrators wish to manage software for.

▪ Click on the Create and select a new Group Policy Object link.

▪ In the New Group Policy object dialog, enter a name for the new GPO for example Specops Deploy Applications with Control Center.

▪ Select an Organizational Unit (OU) that contains the computers or users administrator intend to manage software for. It is recommended that an OU be created for testing of Software Deployments and those computers and or users be moved to this OU for testing. It is recommended that administrators do not modify the Default Domain Policy or target applications at the root of a Domain unless extensive testing has been performed on the application prior to deployment

▪ *NOTE: When a GPO itself targets an OU, only the computers in this OU where the Specops Deploy Client Side Extension has been installed will actually receive advertisements.*

▪ Click OK.

The GPO will now be created and linked to the selected OU and is ready to use. Another GPO can be selected at any time from within the Control Center from the Options section.

NOTE: Although Control Center works with a single GPO it is possible to use any number of GPOs to manage software with Specops Deploy. If more than one GPO is used, it may be easier to use the

Specops Deploy GPMC Snap-in since GPMC is more suited for switching between several different GPO's

7.2 How to Deploy a Package Using Specops Deploy Control Center

When deploying software using Specops Deploy there are three basic terms which are important to know.

- **Package** – Information about the software that is to be deployed. Such as name, version and path to the setup files.

- **Target** – The computers or users that should receive the package. Such as All Windows 7 Computers

- **Deployment** – A package and target combined with additional deployment parameters such as when and how the package will be deployed. The desired deployment also has a state such as deploying or un-deploying.
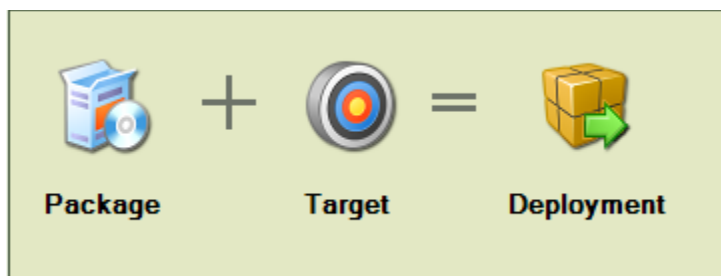
7.3 Make the software package available on the network

In order to deploy a package the administrator will need to determine the original source location of the application. This may be located on the Specops Server itself, a network share or DFS.

Specops Deploy can deploy many file types such as

- o Windows Installer setup files (msi)
- o Executable files (exe)
- o Batch Files (bat)
- o Windows Installer Patches (msp)
- o Windows Store (Also known as Modern UI style applications)

The application Specops Active Directory Janitor will be used to show the steps required to deploy a Windows Installer setup file to client computers.

- Find or create a new subdirectory on a server share or DFS path that will be used to host applications to be deployed in the environment. In this share create a new sub directory for each setup package; use the name of the application for the folder name, for example Active Directory

Janitor. Copy the setup file(s) to the new directory and ensure the folder is shared so that all users have access to the source files.

NOTE: It is recommended to use a Distributed File System (DFS) share to store setup files. For testing purposes any share can be utilized.

- **Start the Deploy Package Wizard**
  On the Welcome page for Specops Deploy Control Center, click on the Start Deploy Package Wizard link.
- **Create a package**
  Click the "Create new Package" button on the first page of the wizard. Select *Windows Installer Package* in the *Package type* dialog.

  > ### NOTE: Windows Installer and Legacy Setups
  > *Windows Installer is a Microsoft technology that is built into the operating system and defines a common standard for the setup of packages. Specops Deploy natively manages Windows Installer packages and retrieves more detailed information from the setups than most other tools.*
  > *Legacy Setup is a common name for older types of setup packages that is started from a program such as Setup.exe or equivalent. Specops Deploy can be used to install this type of package to both computers and users, even to computers where the logged on user does not have administrative permissions. Legacy Setups is often used for hardware driver installations.*

- Deploy Package Wizard (1/6). This window displays information relating to existing package in the infrastructure or offers the ability to create a new package. Select the "Create new package" button and select "Windows Installer Package"
- In the Package Category field. Select the "New" button to create a new Package Category. In the Package Category, enter a name and description, for example *Specops Active Directory Janitor and "*Specops Active Directory Janitor Deployment". Select OK.

  > **NOTE:** It is not necessary to select a package category for the package, as it does not affect the actual deployment, but it makes it easier to sort and view the deployments when the number of deployments increases.

- Select Browse in the "*Network path to install file"* and navigate to the UNC path or DFS location where the install files are located
  > **NOTE:** The path to the source files must be in the UNC format, e.g. \\<server name>\<sharename>\path or an AD integrated DFS path \\<domain name>\<DFS root name>\<Share name>\Path. Mapped drive letters cannot be used.
- The Package Properties for MSI packages will automatically be updated with the information found in the selected Windows Installer package. For non-MSI packages this will need to be populated manually.
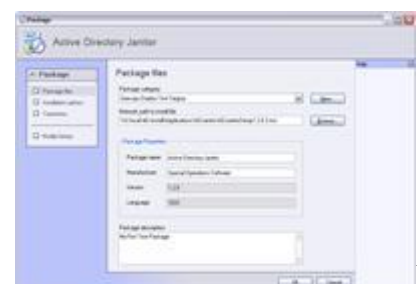
5

Figure 1

- Enter a description for the package in the description field. Although this information is not necessary, it is useful especially if more than one administrator is working with the same package. The package window should now look something like Figure 1.
- Select the Installation options in the menu box to display the Installation options page. The following settings can be edited here:

▪ **Install command** – Only used for Legacy setups. For Windows Installer packages this will always say Windows Installer.

▪ **Additional Windows Installer properties** – Some Windows Installer packages can be customized using Windows Installer properties. Any properties entered here will be used during installation. This option is only used during installation and not advertisements.

▪ **Pre installation commands and parameters** – Offer administrators the ability to perform specific functions prior to execution of the main package e.g. Stop a Service

▪ **Post installation commands and parameters** – Offer administrators the ability to perform specific functions after execution of the main package e.g. Start a Service

▪ **Transforms** – Offer administrators the ability to define an MST package for use with the package.

▪ **Advanced options** – Offer administrators the ability to configure the package to reboot computers if required or publish the package via an internal URL

  o **NOTE**: Using a HTTP URL as the package source requires that there only be one binary file in the source directory. Multiple files cannot be copied to clients from a HTTP source.

▪ Click OK to save the new package.
  - **Select a Target**
    o Once the package has been created it can then be configured for deployment using the targeting criterion functionality that has been built into Specops Deploy. A target contains one or more criteria that define which computers or users will get the deployment.
  - Select the Create new target button. Select Computer target in the Target Type dialog.
  - Enter a name for the target, e.g. *My Specops Deploy Test Computers* and optionally enter a description in the description field.
  - Select *Target criteria*. In this page one or more criteria can be added to the target. A computer or user must meet all the criteria of the target to be reached by the target.
    o For this test do not add any criteria, only select the checkbox *All computers*. This will make the target reach all the computers within the scope of the current GPO.
  - Select OK.

NOTE: Computer and User targets differ in that packages deployed to a Computer target will install software to a specific set of computers while a User target will install on any computer where the users, which are reached by the target, log on.

- Select *Next >* to continue.

- **Select installation type** -- For Windows Installer there is two types of installations:
  - o **Install** – A full installation that completely installs the package on the computer.

  - o **Advertise only** – The package is prepared for installation but the files are not installed. Shortcuts are mounted on the start menu so when a user clicks on one of the shortcuts the installation is completed. This is only available with MSI packages.

  - o **Publish in Add/Remove programs**? – Publishes the application in the available programs list in Add / Remove Programs

- Uninstall the package if the deployment falls "Out of the Scope of Management" determines what happens if the target is not valid anymore or if the actual GPO no longer applies. For example, if the user or computer has been moved to another OU in Active Directory where the GPO is not linked.
- Select Next

7.4 Select Deployment Options

- **Installation Time**
  Specops Deploy can deploy application "As soon as possible" or Administrators can schedule operations to occur after a set date and time. In which case the first group policy refresh after the set date and time will cause the installation to occur.

- **Installation Options**
  Administrators may also specify if operations should be performed during the following times.
  - o Only install during computer start or user logon
  - o Only install after the computer has been started or the user has logged on
  - o Both

  NOTE: Default is to, always install after the computer is booted or after the user has logged on. This will optimize boot and logon times.

- **Source File Options**
  Depending on network topology and/or client disk capacity, Administrators can determine where the source files for the application can be installed from.
  - o Download and install, leave source files in cache
  - o Download and install, remove source files in cache
  - o Install from the network

NOTE: Before deploying applications to an organization careful consideration should be given to the effects of the applications cache or source files on Network Performance and Client Disk capacity. Installing multiple large applications from a network share may seriously degrade network performance.

7.5 End User Interaction

Administrators can define how deployments are displayed on end users computers. This allows end users to have some flexibility with regards to how deployments affect them.

- **Installation popup dialog**
  - o **None**
    - No popups will be displayed to the end users
  - o **Display popup**
    - Administrators can display a popup dialog and countdown time prior to the deployment.
  - o **Allow user to postpone**
    - Allows the end users to postpone the deployment until another time thus allowing them to complete unfinished tasks. This will continue at each group policy refresh until the application is installed.
  - o **Use Custom end user message**
    - Allows administrators to define a custom message for end users containing more information in relation to the deployment. If no message is entered the end user will only be notified by a default text that describes the package.

- Select the checkbox "Use custom end user message" and enter e.g. "*This is a Specops Deploy Test Package*".
- Click Ok

NOTE: The deployment is now underway and detailed deployment can be viewed under Objects>Deployments

7.6 Testing Deployment on End User machines

Logon to a test client and ensure that the Specops Deploy Client Side Extension has been successfully installed. This can done by checking in the add/remove program menu item.

- **NOTE:** Default Group Policy processing occurs every 90 minutes with a random offset of 0 to 30 minutes, but this cycle can be forced to occur immediately by entering the following command in a command prompt on Windows XP, Windows Vista, Windows 7, Windows 2003 or Windows 2008
    - GPUpdate or Gpupdate /force

A group policy processing cycle will begin and once completed an icon will appear in the System tray that indicates that new applications are ready to be installed.

- Double click the icon and select the *Start now* button. The deployment will begin based on the options set in the deployment configuration steps.

7.7 Deployment Feedback

Administrators can view the status of current deployments in the environment through the Specops Deploy Control Center under Objects>Deployments.

Detailed information on a specific deployment can be viewed by selecting the deployment and selecting ''Deployment feedback''.

7.8 Specops Deploy Control Center Options

- **Select group policy object**
    - Allows administrator to open and modify a different Group Policy being used for deployment within the infrastructure.
- **Import/Export**
    - Provides support for migration of Specops Deploy settings between GPO's
    - Provide support to allow administrators to bulk modify all applications in the environment or allow settings to be exported to another Specops Deploy infrastructure with needing to re-create all deployments from scratch.

8.How to Deploy Software using the Group Policy Management Console

All functions described in the Section How to Deploy Software using Specops Deploy Control Center can be accomplished directly in Group Policy Management Editor (GPMC). This allows administrators greater flexibility in managing multiple policies in the environment.

The Group Policy Management Console which is installed as part of the Windows Administrative Tools is used to manage Group Policy in an Active Directory environment. It can be started from the Administrative Tools folder on the Start menu or in the Control Panel. Once opened individual group policies may be viewed or edited by selecting edit which will open the Group Policy Management Editor

GPMC information
NOTE: When a group policy for Specops Deploy is edited using the Group Policy Management Editor, Specops Deploy setting are viewed in two separate locations depending on whether a Computer Target or Used Target is being used. These locations are

- *Group Policy Name>Computer Configuration>Software Settings>Specops Deploy*
- *Group Policy Name>User Configuration>Software Settings>Specops Deploy*

 NOTE: It is recommended that a new GPO be used for testing purposes which is targeted at a test OU containing either users or computers.

8.1 Create and edit a new GPO for Specops Deploy

- Open Group Policy Management and expand the tree **Forest>Domains>Domain-Name**.

- Select the OU to be used for testing, right click and select **"Create a GPO in this domain and link it here"**

- Enter a name for the new GPO for example **"Specops Deploy Applications with Group Policy"**

- In the New Group Policy object dialog, enter a name for the new GPO for example Specops Deploy Applications.

NOTE: When a GPO itself targets an OU, only the computers in this OU where the Specops Deploy Client Side Extension has been installed will actually receive Deployment.

- Click OK.

8.2 How to Deploy a Package Using Specops Deploy snap-in for Group Policy Management Editor

When deploying software using Specops Deploy there are three basic terms which are important to get to know. They are:

▪ **Package** – Information about the software that is to be deployed. Such as name, version and path to the setup files.

▪ **Target** – The computers or users that should receive the package. Such as All Windows 7 SP1 Computers

▪ **Deployment** – A package and target combined with additional deployment parameters such as when and how the package will be deployed. The desired deployment also has a state such as deploying or un-deploying.
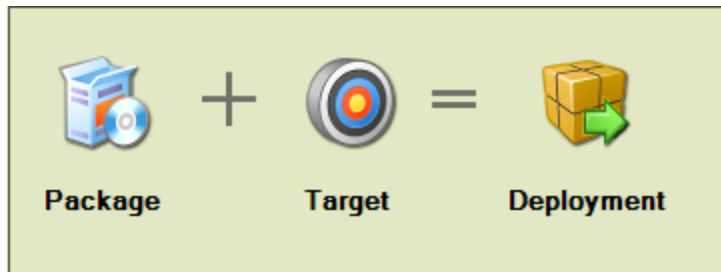
8.3 Make the software package available on the network

In order to deploy a package the administrator will need to determine the original source location of the application. This may be located on the Specops Server itself, a network share or DFS.

Specops Deploy can deploy many file types such as

- o   Windows Installer setup files (msi)
- o   Executable files (exe)
- o   Batch Files (bat)

The application Specops Active Directory Janitor will be used to show the steps required to deploy a Windows Installer setup file to client computers.

- Find or create a new subdirectory on a server share or DFS path that will be used to host applications to be deployed in the environment. In this share create a new sub directory for each setup package, use the name of the application for the folder name, for example Active Directory Janitor. Copy the setup file(s) to the new directory.

NOTE: It is recommended to use a Distributed File System (DFS) share to store setup files. For testing purposes any share can be utilized.

- Edit the Group Policy **"Specops Deploy Applications with Group Policy"** by right clicking on the policy in the Group Policy Management console and selecting edit.
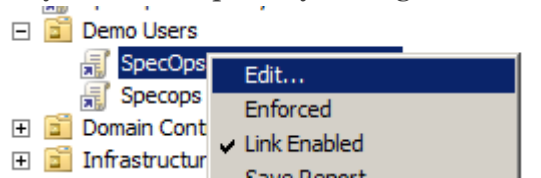
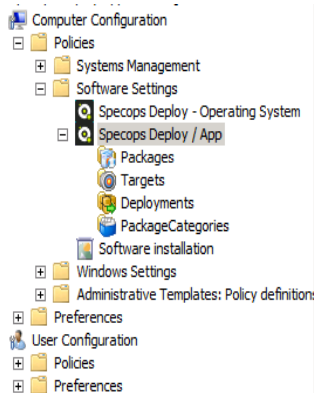
- Navigate to **"Specops Deploy Applications with Group Policy >*Computer Configuration>Software Settings>Specops Deploy"***
- Under this location each of the sections associated with deploying applications is available for use.

- Select the "Click here to deploy a package" and then select "New Package"
- Select Windows Installer Package
    - ***NOTE: Windows Installer and Legacy Setups***
      Windows Installer is a Microsoft technology that is built into the operating system and defines a common standard for the setup of packages. Specops Deploy natively manages Windows Installer packages and retrieves more detailed information from the setups than most other tools.
      Legacy Packages are based on setup programs such as setup.exe and as such there are some limitations when using legacy packages. There are no standards governing the behavior of these types of packages thus some automated functions found in MSI packages cannot be accomplished. Consult the product documentation and test the installation manually prior to deployment using Specops Deploy.

- In the Package Category field. Select the "New" button to create a new Package Category. In the Package Category, enter a name and description, for example "*Specops Active Directory Janitor" and* Select OK.
  - **NOTE:** It is not necessary to select a package category for the package, as it does not affect the actual deployment, but it makes it easier to sort and view the deployments when the number of deployments increases.
- Select Browse in the "*Network path to install file"* and navigate to the UNC path or DFS location where the install files are located
  - **NOTE:** The path to the source files must be in the UNC format, e.g. *\\<server name>\<share name\path* or an AD integrated DFS path *\\<domain name>\<DFS root name>\<Share name>\Path.* Mapped drive letters cannot be used.

- The Package Properties will automatically be updated with the information found in the selected Windows Installer package.

- Enter a description for the package in the description field. Although this information is not necessary, it is useful especially if more than one administrator is working with the same package.
- Select the Installation options in the menu box to display the Installation options page. The following settings can be edited here:
- **Install command** – Only used for Legacy setups. For Windows Installer packages this will always say Windows Installer.

- **Additional Windows Installer properties** – Some Windows Installer packages can be customized using Windows Installer properties. Any properties entered here will be used during installation. This option is only used during installation and not advertisements.

- **Pre installation commands and parameters** – Offer administrators the ability to perform specific functions prior to execution of the main package e.g. Stop a Service

- **Post installation commands and parameters** – Offer administrators the ability to perform specific functions after execution of the main package e.g. Start a Service

- **Transforms** – Offer administrators the ability to define an MST package for use with the package.

- **Advanced options** – Offer administrators the ability to configure the package to reboot computers if required or publish the package via an internal URL

    - **NOTE**: Using a HTTP URL as the package source requires that there only be one binary file in the source directory. Multiple files cannot be copied to clients from a HTTP source.

- Click OK to save the new package.

8.4 Select a Target

Once the package has been created it can then be configured for deployment using the targeting criterion functionality that has been built into Specops Deploy. A target contains one or more criteria that define which computers or users will get the deployment.

- Select the Targets node in Group Policy Management Editor and then select the New target, button. Select Computer target in the Target Type dialog.
- Enter a name for the target, e.g. *My Specops Deploy Test Computers* and optionally enter a description in the description field.
- Select *Target criteria*. In this page one or more criteria can be added to the target. A computer or user must meet all the criteria of the target to be reached by the target.
    - For this test do not add any criteria, only select the checkbox *All computers*. This will make the target reach all the computers within the scope of the current GPO.
- Select OK.

8.5 Configure the Deployment

- Select the Deployment node in Group Policy Management Editor and then select the New Deployment. On the select package Windows select the newly created package for Specops Active Directory Janitor. Select Ok
- On the Deployment Window under the General Settings select the newly created Target
- **Select installation type** -- For Windows Installer there is two types of installations:

  - **Install** – A full installation that completely installs the package on the computer.

  - **Advertise only** – The package is prepared for installation but the files are not installed. Shortcuts are mounted on the start menu so when a user clicks on one of the shortcuts the installation is published to the client computer.

  - **Publish in Add/Remove programs**? – Publishes the application in the available programs list in Add / Remove Programs

  - Uninstall the package if the deployment falls "Out of the Scope of Management" determines what happens if the target is not valid anymore or if the actual GPO no longer applies. For example, if the user or computer has been moved to another OU in Active Directory where the GPO is not linked.

  - Select Next

8.6 Select Deployment Options

- **Installation Time**
  Specops Deploy can deploy application "As soon as possible" or Administrators can schedule operations to occur after a set date and time.

- **Installation Options**
  Administrators may also specify if operations should be performed during the following times.
  - Only install during computer start
  - Only install after the computer has been started.
  - Both

  NOTE: The default is to always install after the computer is booted or after the user has logged on. This will optimize boot and logon times.

  - **Source File Options**
    Depending on network topology and/or client disk capacity, Administrators can determine where the source files for the application can be installed from.
    - Download and install, leave source files in cache
    - Download and install, remove source files in cache
    - Install from the network

NOTE: Before deploying applications to an organization careful consideration should be given to the effects of that applications cache or source files on Network Performance and Client Disk capacity. Installing multiple large applications from a network share may seriously degrade network performance.

NOTE: Uninstall the package if the deployment falls "Out of the Scope of Management" determines what happens if the target is not valid anymore or if the actual GPO no longer applies. For example, if the user or computer has been moved to another part of Active Directory where the GPO is not linked.

- Leave the default and Select **End User Interaction.**

8.7 End User Interaction

Administrators can define how deployments are displayed on end users computers. This allows end users to have some flexibility with regards to how deployments affect them.

- **Installation popup dialog**
  - **None**
    - No popups will be displayed to the end users
  - **Display popup**
    - Administrators can display a popup dialog and countdown time prior to the deployment.
  - **Allow user to postpone**
    - Allows the end users to postpone the deployment until another time thus allowing them to complete unfinished tasks. This will continue at each group policy refresh until the application is installed.
  - **Use Custom end user message**
    - Allows administrators to define a custom message for end users containing more information in relation to the deployment. If no message is entered the end user will only be notified by a default text that describes the package.
- Select the checkbox Use custom end user message and enter e.g. *This is a Specops Deploy Test Package*.
- Click Ok

NOTE: The deployment is now underway and detailed deployment information can be viewed under "**Specops Deploy Applications with Group Policy >*Computer Configuration>Software Settings>Specops Deploy / App>Deployments*"**

8.8 Testing Deployment on End User machines

Logon to a test client and ensure that the Specops Deploy Client Side Extension has been successfully installed. This can done my checking in the add/remove program menu item.

- **NOTE:** Default Group Policy processing occurs every 90 minutes interval with a random offset of 0 to 30 minutes, but this cycle can be forced to happen immediately by entering the following command in a command prompt on Windows XP, Windows Vista, Windows 7, Windows 2003 or Windows 2008 or Windows 2008 R2
    - GPUpdate or Gpupdate /force

A group policy processing cycle will begin and once completed an icon will appear in the System tray that indicates that new applications are ready to be installed.

- Double click the icon and select the *Start now* button. The deployment will begin based on the options set in the deployment configuration steps.

8.9 Deployment Feedback

Administrators can view the status of Deployment in the environment by selecting Deployment Feedback in the Group Policy Management Editor under the following locations

- *Group Policy Name>Computer Configuration>Software Settings>Specops Deploy / App>Deployments*
- *Group Policy Name>User Configuration>Software Settings>Specops Deploy /App>Deployments*

Detailed information on a specific deployment can be viewed by selecting the deployment and selecting ''Deployment feedback''.

9. Working with Windows Store applications

Windows 8 and Windows Server 2012 are able to use a new class of applications made in what is known as the "Modern UI style".

Specops Deploy has full support for working with Modern UI style applications; however, the package type is currently referred to as "Windows Store". This term is subject to change if Microsoft decides to change their long-term naming strategy for this type of application.

When working with Windows Store applications that are not actually downloaded from the Windows store (and thus not signed by Windows Store) the computers need to enable something called *sideloading*.

More information on Windows Store Applications can be found here:

http://technet.microsoft.com/en-us/library/hh852635.aspx

9.1 Enabling Side-loading

As Specops Deploy knows when it is about to deploy a Windows Store application the Client-Side Extension is able to automatically enable side-loading on the client machine. This is done by adding the following registry key:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Appx\AllowAllTrustedApps = 1
```

9.2 Packaging and Signing Windows Store Apps

Before you can deploy your Windows Store App you need to package and sign it.

This is done by using the App Packager (MakeAppX.exe) and SignTool (SignTool.exe) executables shipped with Visual Studio 2012 and the Windows 8 SDK.

During the signing process it is vital that you are using a certificate which is trusted by your client computers. Failure to use a trusted certificate will prevent Windows 8 from starting your Windows Store application.

More information about these tools can be found here:

http://msdn.microsoft.com/en-us/library/hh446767(v=vs.85).aspx

9.3 Windows App Certification Kit

In order to test your Windows Store Applications you can use the Windows App Certification Kit, which is included in the Windows 8 SDK.

Testing the application is a good way of ensuring that it is compatible with Windows 8 and that it follows the rather strict set of rules which apply to Windows Store applications.

More information about the Windows App Certification Kit can be found here:

http://msdn.microsoft.com/en-us/library/windows/apps/hh694081.aspx

10. Support and Troubleshooting

Please visit the Specops Forum for support and help with troubleshooting at:

http://community.specopssoft.com

For Tips and Tricks in Relation to Specops Deploy visit our blog at

http://blogs.specopssoft.com

For support and help with troubleshooting go to:

http://www.specopssoft.com/about-specops/contact

Urgent requests for support may be submitted to:

http://www.specopssoft.com/support