Best Practices for Agent Configuration and Deployment (BKM)

Revision 1.00

Don White

Dec 10, 2009
# Table of Contents

Table of Figures .................................................................................................................. 4

Introduction ......................................................................................................................... 5

Hot links to main document sections .................................................................................. 5

Scope ................................................................................................................................... 5

Assumptions ......................................................................................................................... 5

What’s New in 9.0 ................................................................................................................ 5

Core Server Prerequisites .................................................................................................... 6

Agent Configuration Objectives .......................................................................................... 6

Agent Configuration Settings .............................................................................................. 6

Launching the Agent configuration process ......................................................................... 6

Initial Windows Agent configuration .................................................................................... 12

Security and Compliance screens ....................................................................................... 26

Creating agents for non-Windows environments ................................................................. 30

Customizing the Agent Installation ..................................................................................... 31

Adding Commands to the Agent INI using Mergeini.exe .................................................. 32

Agent Deployment Objectives ............................................................................................. 34

Methods of deployment ....................................................................................................... 34

Advance Agent Deployment Method .................................................................................. 34

Creating an Advance Agent ................................................................................................. 37

Deploying the Advance Agent as a Push ............................................................................ 37

Deploying the Advance Agent as a Group Policy Object .................................................... 38

Deploying a GPO with an associated software package ...................................................... 45

Scheduler Service ............................................................................................................... 54

Conclusion .......................................................................................................................... 56

About LANDesk Software .................................................................................................... 57
Table of Figures
Figure 1: Launching Agent configuration from the Tools menu .......................................................... 7
Figure 2: Launching Agent configuration from the left menu pane .................................................... 7
Figure 3: Default Agent configurations list ......................................................................................... 8
Figure 4: Agent configuration annotated tools ..................................................................................... 9
Figure 5: Part A: Windows agent configuration .................................................................................. 10
Figure 6: Part B: Windows agent configuration .................................................................................. 10
Figure 7: Standard LANDesk Windows agent ..................................................................................... 12
Figure 8: Inventory scanner parameter setup ...................................................................................... 13
Figure 9: Schedule-driven scan setup ................................................................................................. 14
Figure 10: Local scheduler configuration ........................................................................................... 15
Figure 11: Agent configuration for alerting ......................................................................................... 16
Figure 12: Bandwidth detection and control ....................................................................................... 17
Figure 13: Software usage monitoring setup ...................................................................................... 19
Figure 14: Set up any custom data forms ............................................................................................ 20
Figure 15: Software distribution methods .......................................................................................... 21
Figure 16: Policy-based software distribution ..................................................................................... 22
Figure 17: Software Launchpad ........................................................................................................ 23
Figure 18: Software Portal ................................................................................................................ 23
Figure 19: Client Remote control management ................................................................................... 24
Figure 20: End user options permitted ............................................................................................... 25
Figure 21: Remote control client side indicators and settings .............................................................. 26
Figure 22: Security and compliance .................................................................................................... 27
Figure 23: Spyware detection .............................................................................................................. 28
Figure 24: Application Blocker setup .................................................................................................. 29
Figure 25: Agent watcher setup .......................................................................................................... 30
Figure 26: Linux agent configuration .................................................................................................. 31
Figure 27: Advance Agent configuration ............................................................................................ 36
Figure 28: Advance Agent push .......................................................................................................... 38
Figure 29: Group Policy Management in Administrative tools .............................................................. 39
Figure 30: GP Management console .................................................................................................. 40
Figure 31: Create new GPO ................................................................................................................ 41
Figure 32: “Name that GPO” ............................................................................................................. 43
Figure 33: Group Policy Object Editor ............................................................................................... 45
Figure 39: GPO Software Package Properties .................................................................................... 46
Figure 40: Package locations browsing ............................................................................................... 47
Figure 41: MSI packages location ........................................................................................................ 48
Figure 42: List of MSI’s available .......................................................................................................... 49
Figure 43: MSI is selected .................................................................................................................... 50
Figure 44: Package deployment method .............................................................................................. 51
Figure 45: Selecting Users, Computers or Groups ............................................................................. 52
Figure 46: Select computers only ....................................................................................................... 53
Figure 47: Select a target machine ...................................................................................................... 53
Figure 48: GPO summary .................................................................................................................... 54
Figure 49: Configure Services information for the Scheduler .............................................................. 56
Introduction

Client configuration and deployment are at the heart of LANDesk Management Suite functionality. Managed desktops and servers are configurable and controllable using a wide range of manageability tools, but only if an agent has been installed.

We will first overview the manageability functions of clients with agents installed, and then look in detail how to configure agents for various operating environments. Lastly we will discuss the deployment of those agent configurations to devices that are to be managed.

There are many factors that influence what the “correct” configuration for an environment is. Some of the factors that need to be considered are network infrastructure, number of sites, available bandwidth, business needs, and company policies. As you configure a client for the target machine and operating system, you will be making decisions about these settings. The configuration section of this guide will help you make those choices.

In the second part of the document we will discuss several methods that can be used to deploy agent packages you have decided to use. Decisions as to how best accomplish this will be seen to depend on the operating system you are deploying on and security considerations driven by the latest versions of, in particular, Microsoft operating systems.

Hot links to main document sections
Agent Configuration Objectives
Agent Deployment Objectives

Scope
This document explains the steps necessary to configure agents for LDMS 9.0 and then shows how these agent configurations can be deployed. We explore the necessary prerequisites that must be established before configuration and deployment can take place.

Assumptions
This paper assumes that the reader has a working knowledge of LANDesk Management Suite 8.7 and/or 8.8, its functionality, and how a Core Server deployment takes place. Since 9.0 agent configuration and deployment is not much different in 9.0 versus earlier releases, knowledge of 9.0 is not necessary.

What’s New in 9.0
During the discussion we will point out places where menus and processes have changed from the 8.8 release of the product.

In general most agent manipulations have remained the same, some menu items and parameters have been moved to different locations in the menu tree, and some past configuration options have been removed. We will be sure to point these out in context.

Some changes in agent operations have been emphasized in order to accommodate the more robust security of Windows Vista, Windows 2008 and Windows 7.
Core Server Prerequisites
The core server must be configured to support the deployment of agents with the correct security settings. Otherwise you may not be able to effect a successful agent installation on the target machines.

Agent Configuration Objectives
The agent configuration recommended is designed to accomplish the following:

- Daily inventory scan
- Inventory scan on IP address change
- Daily policy based software distribution
- Remote control
- Daily vulnerability scan

The following configuration can be used as a guide. Changes may be needed to meet the requirements of an environment.

Agent Configuration Settings
The following configuration shows the agent configuration changes that are needed. Any setting that is not shown as modified is recommended to remain as the default. If a screenshot is not shown below, the default settings are recommended.

The first settings you need to consider are found in the configure Settings process used to set up many parameters for the core server. Since Agent configuration and deployment take place on and from the core server, it will be necessary for you to set up several items there.

Launching the Agent configuration process
In the LANDesk console you initiate the agent configuration process by selecting Tools | Configuration | Agent configuration or by clicking on the left pane configuration group.
Figure 1: Launching Agent configuration from the Tools menu

Figure 2: Launching Agent configuration from the left menu pane
Once open you see that Agent configuration has several pre-defined selections for various operating systems such as Windows, Linux, or Macintosh.

![Image of Agent configuration interface]

**Figure 3 Default Agent configurations list**

You can define your own configurations by selecting a location for it in Public or My configurations or Public configurations. You cannot create an agent in All configurations, because that is a read-only list. Here is a screen shot explaining all the icons on the tool bar. You can see you have numerous ways to create agents. There are also some deployment tools that we will discuss later.
In order to illustrate agent configuration processes, we will investigate the creation of a windows agent, since that provides the richest set of features at your disposal.

When the agent configuration panel opens you see the following. (We have included two screen shots so you can see the full set of menu items expanded.)
Figure 5 Part A: Windows agent configuration

Figure 6 Part B: Windows agent configuration
You will notice a number of options that let you configure your agent’s set of included components. The right pane shows which components will be installed, including the ability to remote control the agent from the core, ability to install antivirus and power management features, and so on. We will now discuss some of the more important features in detail.

LDMS 9 alert: There are additional entries in the left pane from the 8.8 version. You will notice that Security and Compliance is now in place of Security and patch scan because AV and Agent Watcher are moved under Security and Compliance, and a new sub-head Patch and compliance scan inserted. In the component list LANDesk Trust Agent has been decommissioned and Real-time inventory and Monitoring added, since the older separate Server and system manager has been subsumed in the LDMS agent setup. Also note that Extended Device discovery is now a sub-item in the Start menu.

When you create your own configuration you can modify a pre-assigned configuration, but it is normally best to not change the default configurations. When you make your own you will give it a name in the Configuration name box. Then you will select the desired components keeping in mind that you normally want Remote control and you should install Antivirus and software distribution if you have plans to update desktops with application packages. At the bottom of the screen you can request a full inventory scan as soon as the agent installation is done. If you wish to not show end users the Start menu shortcuts for running various agent programs, then uncheck Show start menu on end user device.
Initial Windows Agent configuration

This screen shows you the core server certificate that will be used for agent authentication. The name of the core server is visible and the Test button lets you check your connectivity to the core server.

The Core Server name can be specified as an FQDN, host name or IP address. Use the test button to verify that the console can find the core by the specified value. The FQDN is the recommended setting, unless the end nodes are unable to resolve the FQDN correctly. The Management Gateway does NOT support using the IP address in the agent configuration. If the Agent will be communicating through the Management Gateway use the FQDN, or Host name of the Core Server.

NOTE: The Core Server specified in the Default Agent configuration will be the default Core Server and will be used by software distribution for status updates.

Set the Path (Location) if Active Directory or eDirectory are not used (optional field).
This screen is somewhat different from the 8.8 version since the section Run inventory scans is more descriptive. The inventory scanner is configured to run from the Local Scheduler. The scanner is set to run a daily scan and when the IP address changes. The local scheduler task will run every 24 hours or at the first time the agent is available after the 24 hours. When the task starts it will select a random time in the next hour in which to process the scan. This randomization flattens the network load. In 9.0 you now have the option to set a delay that applies to any scan sent in at user logon. This can help avoid a sudden crush of inventory scans flooding the core server.
Figure 9 Schedule-driven scan setup

Notice that scans can now be scheduled to run if certain events happen (user logon and change of IP address) as well as by schedule-driven events. Here a time range for the scan can be specified. Please be aware that if you do not pick a time interval, it is possible for the scan inception time to drift, because of the random nature of the Max random delay in the previous screen. So if you need to make sure that a scan only runs when someone is at lunch, set the proper hour interval in the Time range.
Figure 10 Local scheduler configuration

This determines how the client will invoke the local scheduler task to see if tasks need to be performed as well as probe the available bandwidth.
The ability to monitor and alert on agent conditions is now part of the standard LDMS agent. This functionality was only available in the previously released Server manager product. There is no longer a separate server oriented product. In this screen you set up any additional alerting rule sets that you want to distribute. Use this for computers that you feel are critical, so you can monitor their health.

This screen is new to the LANDesk 9 release
Internet Control Message Protocol (ICMP) bandwidth detection is recommended and requires that ICMP packet forwarding is enabled on routers. If ICMP forwarding is disabled on the routers then select PDS (Ping Discovery Service).
If the Device is not rebooted after the agent installation, some components may not function correctly.
Figure 13 Software usage monitoring setup

If you want to monitor and manage licenses check the box.
Figure 14 set up any custom data forms

If you wish to gather any additional client configuration or inventory data that is not found in the normal inventory scans, you can specify that the user must input any such information at a time of your choosing such as at user logon or when an inventory scan runs.

The data to be sent is defined in Tools | Configuration | custom data forms and can include any data input you need as defined by your company policy. For example, you can ask the user to input the location of the machine as he logs in.
Figure 15 Software distribution methods

If you selected the software distribution component, this screen allows you to specify the modes and policy controls you will permit.
Figure 16 Policy based software distribution

This screen is much like the Local Scheduler control we saw earlier, except it controls when the client interrogates the core server for any new policy-based tasks that should run to update inventory information.
Figure 17 Software Launchpad

Figure 18 Software Portal
These two features are components of the LANDesk Desktop Manager. They allow you to present menus to the end user that let them install applications that you control. See other documentation for extended features and functionality.

![Agent configuration](image)

**Figure 19 Client Remote control management**

Remote control is a powerful feature that allows the system admin to remote into any computers where the agent is installed that selected RC. The Permissions and Indicators are used to set up what parts of remote control are enabled and how they are presented to the end user.

This indicates the type of security that is required for the remote control viewer to connect to the end node. Integrated Security is the recommended configuration.

Local template does not require any viewer authentication.
Windows NT security / local template - the viewer validates the remote control operator with the Local group “Remote control Operators”.

Certificate based /local template - the viewer contacts the Core Server requesting that the Core Server contact the client and validates the remote control operator is a LANDesk user and the machine is in the user scope. Then the core server requests that the Client launch the remote control client allowing the viewer to connect. This option is not supported with the LANDesk Management Gateway.

Integrated Security validates the remote control operator with the Core Server and then connects the viewer.

![Agent configuration](image)

**Figure 20 End user options permitted**

Here we set up what RC features are presented to the administrator and what control the end user has.
Remote Control settings should be set to reflect the corporate security and privacy policies.

Security and Compliance screens
Figure 22 Security and compliance

Because of the scope and breadth of this part of the agent setup, we are going to ask you to consult the extensive documentation in the Help section of the console as well as other white papers. In general this section configures how the security scanner is launched and how it will act on the managed device.

The vulnerability scanner is configured to run from the Local Scheduler. The Scanner is set to run a daily scan. The local scheduler task will run every 24 hours, or at the first time the agent is available after the 24 hours. When the task starts it will select a random time in the next hour in which to process the scan.

Global settings are recommended only for client configurations that are used on mission critical systems. These settings could impede an emergency patch process.

Default Scan and Repair settings are recommended. Refer to the Best Known Methods for Patch Manager and Security suite for additional configuration information.
Figure 23 Spyware detection

If the users are allowed to install software select “If an application is not recognized as spyware, require user’s approval before it can be installed”. This prompts that the application is being installed. If this option is not selected then users will not be prompted and the application is not installed.
Figure 24 Application Blocker setup

Selecting the box “Notify user when an application has been blocked” will alert the user that the file executed is denied. If this option is not selected the user will not receive an indicator that the application was blocked. It will appear as if the application just never launched.
Agent Watcher allows proactive monitoring of selected LANDesk agent services and files. Agent Watcher can be enabled and agent watcher settings deployed with an initial device agent configuration. It can also be updated at any time without having to perform a full agent configuration.

Creating agents for non-Windows environments
We saw earlier that agents can also be configured for non-Windows operating environments. These include the Linux RedHat, Ubuntu and Souse, as well as HP-UX and Macintosh. Since these are of somewhat limited usage for many LANDesk customers, we will merely point out their availability. To illustrate just one of these configurations we will show the screen used to configure Linux agents.
Linux options include the ability to scan and repair vulnerabilities and to implement monitoring and alerting. The Inventory scanner screen is very simple, giving you the choice of when to run the scan Daily, Weekly or Monthly.

**Customizing the Agent Installation**

The agent installation is controlled by an INI file. This file is created from the NTstacfg.INI when the agent configuration is created. The settings for the agent behavior are contained in an MSI that is created when the Agent is created. The MSI settings can be modified using the agent configuration interface. If the Agent configuration requires customization, changes can be merged into the Ntstacfg.ini. A scheduled update will only redeploy the MSI and the settings contained within, customizations to the INI are not redeployed.

The following example shows how to change the local scheduler tasks by adding commands lines to the INI. (Local scheduler tasks are created by default in the MSI and have the same settings as shown below.)
Adding Commands to the Agent INI using Mergeini.exe

The following steps will need to be completed.
Create an INI file.
Create a registry key.
Restart the Inventory service

Creating an INI file

In order to use the Mergeini.exe, create an INI file that contains the additional commands that will be added to the Agent configuration INI file. By making these settings in a separate file, LANDesk® Management Suite patches and services packs can modify or replace the Ntstacfg.ini file without overwriting custom modifications. Place the INI file in the Idlogon directory. Create the custom INI with the following commands:

[Policy Management Post Copy]
EXEC10001=%DEST%\LOCALSCH.EXE /del /taskid=777
EXEC10002=%DEST%\LOCALSCH.EXE /del /taskid=555
EXEC10003=%DEST%\LOCALSCH.EXE /del /taskid=600
EXEC10004=%DEST%\LOCALSCH.EXE /taskid=777 /exe="%DEST%\LDIScn32.EXE" /cmd="/RSTART=60 /NTT=CORESERVER:5007 /S=CORESERVER /l=HTTP://CORESERVER/Idlogon/IdappI3.ldz /NOUI" /freq=86400 /start="06 Jan 2006 16:56:20" /tod="0|11"
EXEC10005=%DEST%\LOCALSCH.EXE /taskid=555 /exe="%DEST%\vulScan.exe" /cmd="/RSTART=60" /freq=86400 /start="06 Jan 2006 17:56:20" /tod="0|11"
EXEC10006=%DEST%\LOCALSCH.EXE /taskid=600 /exe="%DEST%\AMCLIENT.EXE" /cmd="/apm /s /retry=3 /tspan=60 /Rstart" /freq=86400 /start="06 Jan 2006 18:56:20" /tod="0|11"

Edit the INI file for the specific environment with the following information:
1. Change CORESERVER to reflect the name of the Core Server.
2. Random start time /rstart=60. 60 is a variable and can be modified if needed, based on network bandwidth and number of clients.
4. tod – The (time of day) filter limits the hours in which a task can run. (optional)

Creating the Registry String Value

Once the INI file has been saved, create a new string value in the registry that contains the full path to the INI file under the following registry key:
HKEY_LOCAL_MACHINE\SOFTWARE\LANDESK\ManagementSuite\Stamping\Files.
The string name is of your choosing.
Note: If the path name contains a space be sure to use quotes around the full path

Importing the custom INI to the Template

To import the settings from the INI file to the Ntstacfg.in# file, Stamper.exe needs to be run. Restart the inventory service to run Stamper.exe. Execution of Stamper.exe is part of the inventory service starting.

Import Setting to Agent INI

Build the Agent configuration or run “Rebuild All” to update all existing client configurations.
Agent Deployment Objectives
There are many factors that influence what the “correct” deployment method for an environment is. Some of the factors that need to be considered are network infrastructure, number of sites, available bandwidth, and company policies. The objective is to maximize the number of clients that are installed while minimizing the network impact.

Methods of deployment
There are numerous methods provided for deploying the LANDesk® agent. The following are some of the common methods and uses. Combinations of different methods may be used to install the agent in a given environment.

- **Manual**: Map a drive to the ldlogon Folder and run Wscfg32.exe. This is used for single client installs and testing.
- **Push**: Schedule a push of the full agent. This deploys a cab to the client machine using the scheduler service credentials. The push is a set of RPC commands that are executed on the client machine from the Core Server.
- **Self Contained EXE**: Creates an EXE that can be installed. The EXE contains all client files and settings. This can be used manually, posted on web site or deployed using LANDesk® Software Distribution.
- **Login Script**: Agents can be installed using login scripts, the batch file IPsetup.bat can be added to the login script. This method requires that the users have administrative rights.
- **LdDiscover**: Self Contained program that can discover machines and issue NT RPC commands. This can be used to discover nodes and issue RPC commands.
- **Advance Agent**: This is a two stage process. The advance agent consists of a small MSI and a self contained EXE. The MSI is deployed to the client and then the MSI downloads and installs the EXE. This allows for bandwidth friendly downloads.
- The Advance agent is the preferred method for deploying the agent in most environments. Advance agent leverages the LANDesk® bandwidth options during the agent installation. It also avoids the issue with pushing to windows 2008, vista and windows 2007 where restricted permissions may not let a normal agent push work correctly.

Advance Agent Deployment Method
Advance agent has been created to leverage LANDesk® bandwidth friendly technology during the agent deployment. The Advance agent can reduce the amount of network bandwidth used for Windows-based agent configuration. The Advance agent is a two stage deployment method. The Advance agent is an MSI file that is deployed in advance of the full agent. The MSI installs and then initiates the download and install of the full agent exe package.

A bit of an explanation for the name “Advance Agent.” Advance Agent uses a method of deploying agent software by first placing an advance agent (a small agent that goes down ”in advance” of the full agent. The Advance Agent is a service that runs and copies down the full agent in two parts: an msi that copies down the self-contained exe that actually installs the agent software.
The Advance agent MSI is a 500 KB MSI package. When this package runs on a device it installs the LANDesk® Advance agent service. The Advance agent service downloads the associated full agent configuration package and initiates the install. When creating an Advance agent the dialog prompts for a path and name for the Advance agent configuration. The path and name of the agent configuration are coded in the MSI along with the hash value of the EXE. The Advance agent service will use the name and hash to determine the package to download and install. In the Advance agent configuration window bandwidth-friendly distribution options can be configured. All settings configured in the Advance Agent dialog are included in the Advance agent MSI and are used by the Advance agent service after the MSI is installed.
Figure 27 Advance Agent configuration

When creating an Advance agent configuration, it takes a few seconds to create the full agent configuration package. The Advance Agent package (<configuration name>.msi) and the full agent configuration package (<configuration name>.exe) are placed in the Core Server's Idlogon\AdvanceAgent folder. Each time the Advance agent dialog is run a new set of agent files are created. The MSI and EXE are recreated NOT updated. The MSI will only download and install the EXE that is created at the same time it is created. The MSI contains the hash, file name and path of the EXE that it should download and install. The path specified in the Advance agent configuration can be any share that the clients will be able to access. The EXE needs to be manually moved to the specified location. By default the files are placed in the AdvanceAgent folder on the Core Server. After creating an agent configuration package, the MSI portion can be installed on devices by using any of the following methods:

- Schedule a push distribution of the Advance Agent
Configure a login script or Group Policy Object to install the MSI
- Run the **MSI** manually on each device

When deployed, the advance agent downloads the agent configuration listed in the configuration window. The agent runs silently on the device, without showing any dialogs or status updates. The Advance agent service uses the bandwidth preferences specified in the Advance Agent configuration.

The Advance agent works independently from the Core Server once installed. It downloads the full agent configuration but does not report status to the Core Server. If a device disconnects from the network before the agent configuration finishes downloading, the advance agent automatically resumes the download where it left off when the device reconnects to the network. After the **MSI** installs, downloads and configures the full Agent on a device, the Advance agent service is set to manual. After the install of the agent the Advance Agent service is removed. Registry keys are placed such that the **MSI** will not reinstall. This allows the **MSI** to be used in a login script or GPO. The full agent configuration package is placed in the sdmcache folder so that it can be downloaded by peer machines.

**Creating an Advance Agent**

To create an Advance agent configuration

1. Create a Windows-based agent configuration (**Tools | Configuration | Agent configuration**).
2. Right-Click the desired agent configuration, click Advance Agent.
3. Select the desired download option:
   - **Standard**: This attempt to download the **EXE** from the local cache, peers and then the path specified in the configuration.
   - **Peer Download**: This option attempts to download the **EXE** from the local cache, and then peers. If using this option, the **EXE** has to be staged to a peer in every subnet. If the **EXE** is not staged to the **sdmcache** of a peer, the download fails.

4. If relocating the associated agent configuration package (the **EXE** file), change the path for the agent configuration package.

5. Select desired bandwidth options

6. Click **OK**.

7. If necessary, copy the associated **EXE** file from the **Idelogon\AdvanceAgent** folder to the distribution server share.

Make sure the path to the agent configuration executable matches the path specified in the Advance agent configuration window. Leave the **MSI** package on the Core Server in the default location. Otherwise, the package won't be visible for the Advance agent push distribution.

**Deploying the Advance Agent as a Push**

To set up an Advance agent push distribution
1. From the Console Click (Tools | Configuration | Agent configuration)

2. In the Agent configuration window, click the Schedule a push of an Advance Agent configuration toolbar icon.

3. The Advance Agent push window lists the agent configuration MSI's found in the \Idlgon\AdvanceAgent folder. Click to highlight the Advance Agent configuration to distribute and click OK.

4. The Scheduled Tasks window opens with the Advance Agent task selected. The task name is "Advance Agent <configuration name>".

5. Add target devices to the task by dragging them from the Network view or Unmanaged Device Discovery and dropping them on the task in the Scheduled Tasks window.

6. Right-Click the Advance Agent task and click Properties and schedule the task. The MSI distribution progress can be monitored in the Scheduled tasks window. There are no status updates on the full agent configuration once the MSI distribution completes. Status information in the task is regarding the distribution of the Advance Agent MSI.

**Deploying the Advance Agent as a Group Policy Object**

With the Advance Agent an MSI of 500Kb is created and this allows the Advance Agent to be deployed as a Group Policy Object.

Microsoft Group Policy objects are only supported in an Active directory domain. Once you have such an entity set up you will be able to invoke the GPO construction tools.
Invoke the GPO Management console by double clicking on the Group Policy Management tool. That opens the following window:
Now right click on the Group Policy Objects menu item and name your New GPO:
Figure 31 Create new GPO

Assign your GPO a name and any template that it might use as a basis
Create a GPO or determine which existing GPO can have the Software assigned to it.
Give the GPO a name.

![New GPO dialog box]

**Figure 32 “Name that GPO”**

Now right click your object and edit it.
Select the GPO right click and select Edit. This will open the Group Policy Editor:
There are two broad categories of policies that can be specified in a GPO: Computer and User configurations. Each contains literally hundreds of polices.

In the figures below we will illustrate just one of the many policies that can be enabled. Our goal is to have a policy sent to a set of machines that will install the Windows agent via an Advance Agent package associated with the policy.

**Deploying a GPO with an associated software package**

Our purpose is to show you how to implement a GPO that includes the installation of an Advance Agent package in the form of an MSI (Windows Installer package).

However, before we can link a policy to an installation package such as an Advance Agent MSI, we need to let the GP Manager know where our advance agent packages are. This is done in the following screens.

As before create a GPO and name it something like “Deploy-adv-agent-via-GPO”—policy. As illustrated below in computer configuration | Policies | Software Settings | Software Package, right click and select Properties.
Expand this screen and browse to the location of your agent packages.
Expand Network and select the machine where you have your Advance Agents, typically in Program files\LANDesk\ManagementSuite\ldlogon\advanceagent. In the screen below you see that the UNC path is entered: (\<Core server name\>\ldlogon share\>).
Be sure to select Assign under New packages. Now click OK and select the desired MSI.
Figure 37 List of MSI's available

Click the MSI you want and then notice it is associated with the selected policy.
Figure 38 MSI is selected

Now that we have selected the MSI to associate with the software installation of this policy, close the GPM editor and select your GPO under Group Policy Objects.

Next we need to specify the deployment method for the package. Right click on the package name in the right pane and select Properties.
Now select Assigned under the Deployment tab, Deployment type as shown above.

We have now set up the package parameters, and need to now specify the targets for the policy object.

Close the GPM Editor and select the GPO policy we have been working with in the Group Policy Management console as seen next.
Figure 40 Selecting Users, Computers or Groups

Now we need to select the targets for the GPO. In particular, for our example, select the computer that will get the policy pushed to it. Do this by right-clicking the object and under the Scope tab select the Add button below the Security Filtering pane. The Select Users, Computer, or Group window appears. For our example we will select a computer by checking only Computers as seen in the next screen.
Now we enter the name or names of computers we want this policy to apply to. The next time that policies are synced or a user logs on, the software package will be installed.

Fill in the first part of a computer name and click Check names and the name is filled in.
The software should be deployed as Assigned software. This will cause the MSI to be installed the next time deployed polices are invoked on the client is updated.

**Scheduler Service**

To install LANDesk® agents on unmanaged devices, the scheduler service needs to be able to connect to devices with administrative permissions. The default account the scheduler service uses is LocalSystem. If devices are in a domain, a domain administrator account must be specified on the Scheduler service. Use the Change login window (click Change login on the Scheduler tab) to change the default scheduler login. Alternate credentials can be specified for the scheduler service to try when it needs to execute a task on unmanaged devices. Alternate credentials may consist of other domain administrators, cross domain administrators or local administrator accounts. The primary scheduler service login must have Core Server administrative rights (run as a Service). Alternate credentials do not require Core Server administrative rights; they are used only for administrative rights on clients. The scheduler service will try the default credentials and then use each credential specified in the Alternate credentials list until successful or all credentials have failed. Credentials
specified are securely encrypted and stored in the core server's registry. Set the following options for the default scheduler credentials:

- **Username**: Enter the default domain\username or username for the scheduler to use.
- **Password**: Enter the password for the credentials specified.
- **Confirm password**: Retype the password to confirm it.

Set the following options for additional scheduler credentials:

- **Add**: Adds a username and password to the alternate credentials list.
- **Remove**: Removes the selected credentials from the list.
- **Modify**: Modifies the selected credentials allows for password changes.

When adding alternate credentials, specify the following:

- **Username**: Enter the username.
- **Domain**: Enter the domain for the username specified.
- **Password**: Enter the password for the credentials specified.
- **Confirm password**: Retype the password to confirm it.
Conclusion
This is a best practice guide based upon the objectives outlined. Additional Resources: Online help, LDMSusers guide, whitepapers (available under Downloads at www.LANDesk.com), and the LANDesk Knowledge base (kb.landesk.com).
About LANDesk Software

The foundation for LANDesk’s leading IT management solutions was laid more than 20 years ago. And LANDesk has been growing and innovating the systems, security, service and process management spaces ever since. Our singular focus and our commitment to understanding customers’ real business needs—and to delivering easy-to-use solutions for those needs—are just a few of the reasons we continue to grow and expand.

LANDesk pioneered the desktop management category back in 1993. That same year, IDC named LANDesk the category leader. And LANDesk has continued to lead the systems configuration space: pioneering virtual IT technology in 1999, revolutionizing large-packet distribution with LANDesk® Targeted Multicast™ technology and LANDesk® Peer Download™ technology in 2001, and delivering secure systems management over the Internet and hardware-independent network access control capabilities with LANDesk® Management Gateway and LANDesk® Trusted Access™ Technology in 2005.

In 2006, LANDesk added process management technologies to its product line and began integrating the systems, security and process management markets. LANDesk also extended into the consolidated service desk market with LANDesk® Service Desk, and was acquired by Avocent to operate as an independent division.

Today, LANDesk continues to lead the convergence of the systems, security, process and service management markets. And our executives, engineers and other professionals work tirelessly to deliver leading solutions to markets around the globe.