Troubleshooting client-side policy merging

ManageSoft knowledge base article 100619

Introduction

This document describes how to perform debugging and developer tracing to help diagnose problems with ManageSoft client-side merging. It also includes details of troubleshooting locked down computers. In addition, this article details of a number of tools that you can use when diagnosing problems with Active Directory.

Note: The information is intended for use by ManageSoft Professional Services Engineers and advanced customers who are involved in setting administrative policies for Active Directory.

Debugging and developer tracing

If the troubleshooting recommendations in *ManageSoft Reference: System Reference* do not generate enough information to troubleshoot the problems, additional debugging information can be obtained using developer tracing. This form of problem diagnosis is very low-level, and is generally only useful to a ManageSoft consultant with access to ManageSoft source code. It is best suited to diagnosing obscure policy merging failures.

For developer tracing to work, an **ndplc.ini** file containing the trace settings is also required. This file must be placed in the current working directory for **ndpolicy.exe**. So if policy merging is being run from a scheduled task, you will need to set the **Start in** field of the task to the directory in which **ndplc.ini** resides (usually **Program Files\ManageSoft\Policy Client**).

Alternatively, you can copy the **ndplc.ini** file to the **$System32** directory, which is the default working directory for scheduled tasks.

If you are manually running **ndpolicy.exe** via a run command or via packages for updating Machine Policy and schedules (as described in ***Error! Reference source not found.*** on page **Error! Bookmark not defined.**, then the **ndplc.ini** file must reside in the Policy Client folder under Program Files\ManageSoft\Policy Client.

This file provides developer tracing, which can be extremely useful. For client-side merging, you can trace all activity, although the output is quite extensive. The file contains filtering information, if you do need to filter out data.

Important: In the configuration settings in the **ndplc.ini** file, the second line points to the output of the tracing, and the directory structure of this path must already exist on the managed device for the file to be created. In the sample **ndplc.ini** text below, the path is **C:\Temp\ndplc.trc.** If the C:\Temp directory does not exist on the managed device, no trace (.trc) file will be created.

A sample **ndplc.ini** file is contained below. This sample traces all developer files (A-z) in all five libraries (NDPANTRACE to EMSTRACE)

```
[environment]
NDTRACEFILE=c:¥temp¥ndplc.trc
NDPANTRACE=ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz
NDPOLTRACE= ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz
NDPMTRACE= ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz
NDAUDTRACE= ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz
EMSTRACE= ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz
```

Contact your local ManageSoft support representative for help with tracing.

Troubleshooting machine policy update by a locked-down user

Because machine policies and schedules can only be executed under **System** context or by a local machine administrator, troubleshooting Machine Policies for managed devices that are locked-down users is a unique problem.

However using the capabilities of ManageSoft, you can provide your help desk personnel with a ManageSoft package which can be initiated by a locked-down user and will update a machine policy and schedule.

This section describes a straightforward method of allowing restricted users to update computer and user policies and schedules on demand or as instructed by help desk personnel.

Before you start, you should become familiar with the policy agent (ndpolicy.exe) and its use as a command line tool. For details, see *ManageSoft Reference: System Reference*.

It is important to note that while it is always possible to apply the user policy and schedule via **ndpolicy**, for NT4, W2K and XP, application of the computer policy and schedule can only be performed by administrators and the local system account. This is a security measure put in place to stop restricted users from interfering with machine operations. However because the ManageSoft installation agent can run commands using the system context, this can be overcome by using the following method.

Method

To apply the computer policy and schedule, it is necessary to do so with elevated privileges. ManageSoft has the ability to run external commands using either the current user or local system context, so it is possible create packages that allow restricted users to update their computer policy and schedule.

While application of the user policy and schedule does not require elevated privileges, packages that accomplish this have been added for completeness.

Following is a description of how to create ManageSoft packages that apply policies and schedules for both user and computer.

Important:

- 'ndpolicy' command lines have **-t User** and **-t Machine** for user policy/schedule and computer policy/schedule respectively
- 'ndpolicy' command lines have **–o AllowedPkgTypes=Schedule** when applying only the schedule referenced in policy

- ‘ndpolicy’ command lines specify **–o UserInteractionLevel=Status** to display the ManageSoft installation agent ‘Status’ user interface
- ManageSoft packages must be authored to run ‘ndpolicy’ with current user privileges for user operations and full access privileges for computer operations

These packages can be installed by manually running the package OSD file, via a batch file or script or by the creation of shortcuts on the desktop whereby users can manually run the shortcut.

To create a package that applies computer policy:

1. Create a basic ManageSoft package.
2. Expand the **Project** node for the new package.
3. Right-click **Application Details** and select **Properties**. The **Application Details Properties** dialog is displayed.
4. Select the **Permissions** tab.
   a. Deselect the **Allow installing user to decide which profile to use** option.
   b. Click **OK** to close the dialog.
5. From the **Project** node, expand the **External Installer** node to display the **All External Installers** node.
6. Right-click **All External Installers** and select **New External Installer**. The **New external installer Properties** dialog is displayed.
   a. For the **Installer used to pack the application**, select **Other Installer Technology** from the drop-down list.
   b. To apply computer policy from the last known location, set the external installer command line to:

      ```
      ndpolicy.exe -t Machine -o UserInteractionLevel=Status
      ```

      Or:

      To apply computer policy without a last known location, set the external installer command line to:

      ```
      ndpolicy.exe -t Machine -o UserInteractionLevel=Status  -s
      http://server/<deploymentshare>/Policies/Merged/Machine/$(MachineID).npl
      ```

      Note: On ManageSoft, the default <deploymentshare> is **ManageSoftDL**. $(MachineID) will automatically calculate the current **Machine Policy Name**.

   c. Select the **Optional Settings** tab and select the **Full Access Privileges** radio button.
   d. Click **OK** to close the dialog.
7. Right-click the **Project** node and select **Save** to save the package.

To create a package that applies user policy:

1. Create a basic ManageSoft package.
2. Expand the **Project** node for the new package.
3. Right-click **Application Details** and select **Properties**. The **Application Details Properties** dialog is displayed.
4. Select the **Permissions** tab.
   a. Deselect the **Allow installing user to decide which profile to use** option.
   b. In the **Install this application for:** field, select the **The user installing the application (current user)** radio button.
   c. Click **OK** to close the dialog.
5. From the **Project** node, expand the **External Installer** node to display the **All External Installers** node.
6. Right-click **All External Installers** and select **New External Installer**. The **New external installer Properties** dialog is displayed.
   a. For the **Installer used to pack the application**, select **Other Installer Technology** from the drop-down list.
   b. To apply user policy from the last known location, set the external installer command line to:

      ```
      ndpolicy.exe -t User -o UserInteractionLevel=Status
      ```

      Or:

      To apply user policy without a last known location, set the external installer command line to:

      ```
      ndpolicy.exe -t User -o UserInteractionLevel=Status -s
      http://server/<deploymentshare>/Policies/Merged/User/$(UserID).npl
      ```

      Note: On ManageSoft, the default <deploymentshare> is **ManageSoftDL**. $(UserID) will automatically calculate the current **User Policy** name
   c. Select the **Optional Settings** tab and select the **Current User Privileges** radio button.
   d. Click **OK** to close the dialog.
7. Right-click the **Project** node and select **Save** to save the package.

To create a package that applies computer schedule:

1. Create a basic ManageSoft package.
2. Expand the **Project** node for the new package.
3. Right-click **Application Details** and select **Properties**. The **Application Details Properties** dialog is displayed.
4. Select the **Permissions** tab.
   a. Deselect the **Allow installing user to decide which profile to use** option.
   b. Click **OK** to close the dialog.
5. From the **Project** node, expand the **External Installer** node to display the **All External Installers** node.
6. Right-click **All External Installers** and select **New External Installer**. The **New external installer Properties** dialog displays.
   a. For the **Installer used to pack the application**, select **Other Installer Technology** from the drop-down list.
   b. To apply a computer schedule from the last known location, set the external installer command line to:

      ```
      ndpolicy.exe -t Machine -o UserInteractionLevel=Status -o AllowedPkgTypes=Schedule
      ```

      Or:

      To apply a computer schedule without a last known location, set the external installer command line to:

      ```
      ndpolicy.exe -t Machine -o UserInteractionLevel=Status -o AllowedPkgTypes=Schedule
      -s http://server/<deploymentshare>/Policies/Merged/Machine/$(MachineID).npl
      ```

      Note**:** On ManageSoft, the default <deploymentshare> is **ManageSoftDL**. $(MachineID) will automatically calculate the current **Machine Policy** name.
   c. Select the **Optional Settings** tab and select the **Full Access Privileges** radio button.
   d. Click **OK** to close the dialog.
7. Right-click the **Project** node and select **Save** to save the package.

To create a package that applies user schedule:

1. Create a basic ManageSoft package.
2. Expand the **Project** node for the new package.
3. Right-click **Application Details** and select **Properties**. The **Application Details Properties** dialog is displayed.
4. Select the **Permissions** tab.
   a. Deselect the **Allow installing user to decide which profile to use** option.
   b. In the **Install this application for:** field, select the **The user installing the application (current user)** radio button.
   c. Click **OK** to close the dialog.
5. From the **Project** node, expand the **External Installer** node to display the **All External Installers** node.
6. Right-click **All External Installers** and select **New External Installer**. The **New external installer Properties** dialog is displayed.
   a. For the **Installer used to pack the application**, select **Other Installer Technology** from the drop-down list.
   b. To apply a user schedule from the last known location, set the external installer command line to:

      ```
      ndpolicy.exe -t User -o UserInteractionLevel=Status -o AllowedPkgTypes=Schedule
      ```

      OR

      To apply a user schedule without a last known location, set the external installer command line to:

      ```
      ndpolicy.exe -t User -o UserInteractionLevel=Status -o AllowedPkgTypes=Schedule -s
      http://server/<deploymentshare>/Policies/Merged/User/$(UserID).npl
      ```

      Note**:** On ManageSoft, the default <deploymentshare> is **ManageSoftDL**. $(UserID) will automatically calculate the current **User Policy** name
   c. Select the **Optional Settings** tab and select the **Current User Privileges** radio button.
   d. Click **Ok** to close the dialog.
7. Right-click the **Project** node and select **Save** to save the package.

Active Directory group policy tools

A number of tools are available from the Windows 2000 Professional Resource Kit. A summary of these tools, and references to additional documentation are provided in *ManageSoft Reference: System Reference*.

This article describes the following tools in further detail:

- Group Policy Results tool (GPResult.exe)
- Group Policy Verification tool (GPOTool.exe)

These tools both read group policy information. The key difference is that GPResult reads data from the local Registry, while GPOTool attempts to make a connection to your domain controllers to calculate group membership and policy information.

GPOTool also compares the group policy information from the various domain controllers to verify that replication of the group policy information is accurate. You can also use this tool to target group policy information from a particular domain controller.

GPResult

GPResult provides useful debugging information, including:

- Operating system information
- User information: Name and location in AD, domain, site, security group membership, security privileges
- Computer information: Name and location in AD, domain, site
- Group policy information:
  - Last time policy was applied, and the domain controller that applied policy
  - Applied group policy objects.

From this, the following diagnosis can be performed:

1. **Domain controllers:** If the domain controller that applied native policy is different from the domain controller that applied ManageSoft policy, then AD replication may be the cause of the problem. Try forcing replication, or waiting for a period of time, before running another policy merge.

2. **Applied Group Policy objects:** If the applied group policy objects through *native policy* are different from those applied through *ManageSoft policy*, possible causes are:

   - AD replication. See point 1.

- Security group membership changes. ManageSoft determines security group membership dynamically, while native group policy uses the security token as established at logon. For this reason, native group policy requires a logoff and logon to pick up security group membership changes that affect the applied group policy objects.

Local Group Policy Information

Windows2000 will calculate its group policy information and store this information locally in the Registry, in keys stored under:

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Group Policy
```

And

```
HKEY_CURRENT_USER¥Software¥Microsoft¥Windows¥CurrentVersion¥Group Policy
```

It is important to realize that tools such as GPResult simply use this information for reporting and as such will only report their last known policy information. This does not test any connectivity to the AD domain controller but is still valuable information.

How to use GPResult

The following is an excerpt from Microsoft's TechNet article **Troubleshooting Group Policy in Windows 2000.**

Group Policy Results Tool (GPResult.exe)

This command line tool tests Group Policy.

Note: Make sure you run this tool on the computer on which you wish test Group Policy.

To run GPResult:

1. From the **Start** menu, select **Run** and enter **cmd** to open a command window.
2. Type **gpresult** and redirect the output to a text file as shown in Figure 1 below:

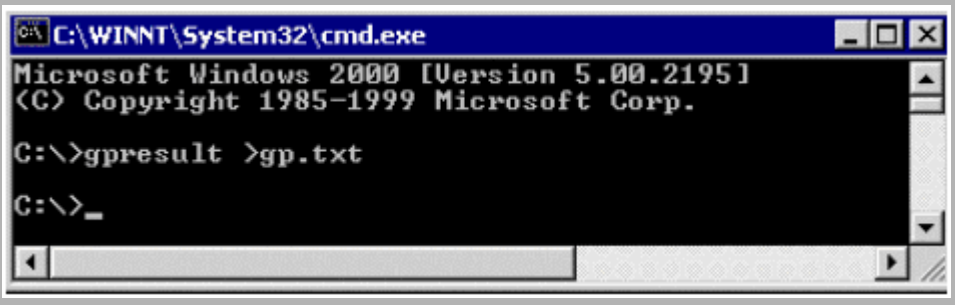

Figure 1 Directing GPResult data to a text file

- Enter **notepad gp.txt** to open the file.

GPResult provides the following general information:

- **Operating System information**
  - Type (Professional, Server, Domain Controller).
  - Build number and Service Pack details.
  - Whether Terminal Services is installed and, if so, the mode it is using.
- **User Information**
  - User name and location in the Active Directory™ service (if applicable).
  - Domain name and type (Windows 2000 or Windows NT®).
  - Site name.
  - Whether the user has a local or roaming profile and location of the profile.

- Security group membership.
- Security privileges.

- **Computer Information**
  - Computer name and location in Active Directory (if applicable).
  - Domain name and type (Windows 2000 or Windows NT).
  - Site name.

Policy Application Information

GPResult also provides the following information about Group Policy:

- The last time policy was applied and the domain controller that applied policy, for the user and computer.
- The complete list of applied Group Policy objects and their details, including a summary of the extensions that each Group Policy object contains.
- Registry settings that were applied and their details.
- Folders that are redirected and their details.
- Software management information detailing assigned and published applications.
- Disk quota information.
- IP Security settings.
- Scripts.

Using GPResult in different modes

GPResult can deliver varying levels of detail as shown in Table 1 below.

Table 1 GPResult Syntax

Mode	Description	Enter
Verbose mode	Adds: List of user's security privileges. Group Policy object details including globally unique identifier (GUID), friendly name, version, and source. Details for the following Group Policy extensions: • Administrative Templates (Registry-Based Policies) • Application Management • Disk Quotas • Folder Re-direction • IP Security • Scripts	gpresult /v
Super verbose mode	Delivers all the above plus: • Binary values of binary Registry settings when applicable. • A detailed list of which applications will be displayed in Add/Remove Programs. • Both version numbers of a Group Policy object —the version number of the Group Policy Container (GPC) and the version number of the Group Policy Template (GPT) including binary Registry values.	gpresult /s
Computer settings only	Restricts results to computer settings.	gpresult /c
User settings only	Restricts results to user settings.	gpresult /u

Availability

GPResult ships with the Windows 2000 Resource Kit and is also available as a free download on the Windows 2000 Web site at http://www.microsoft.com/windows2000/techinfo/reskit/tools/existing/gpresult-o.asp. For more detailed information about interpreting GPResult, see the **readme** file included with the download.

GPOTool

The following is an excerpt from Microsoft's TechNet article **Troubleshooting Group Policy in Windows 2000**.

GPOTool

GPOTool can:

- **Check Group Policy object consistency.** Reads mandatory and optional directory services properties, version, friendly name, extension, globally unique identifiers (GUIDs) and SYSVOL data (Gpt.ini), compares directory services and SYSVOL version numbers, and performs other consistency checks. Functionality version must be **2** and user/computer version must be **greater than 0** if the extensions property contains any GUID.
- **Check Group Policy object replication.** Reads the Group Policy object instances from each domain controller and compares them [selected Group Policy Container (GPC) properties and full recursive compare for the Group Policy Template GPT)].
- **Display information about a particular Group Policy object**. Includes properties that can't be accessed through the Group Policy snap-in such as functionality version and extension GUIDs.
- **Browse Group Policy objects.** Searches policies based on friendly name or GUID. A partial match is also supported for both name and GUID.
- **Use preferred domain controllers.** By default, all available domain controllers in the domain will be used; this can be overwritten with the supplied list of domain controllers from the command line.
- **Provide cross-domain support.** A command line option is available for checking policies in different domains.
- **Run in verbose mode.** If all policies are fine, the tool displays a validation message; in case of errors, information about corrupted policies is printed. A command line option can turn on verbose information about each policy being processed.

Availability

GPOTool.exe ships with the Windows 2000 Server Resource Kit and is also available as a free download at http://www.microsoft.com/windows2000/techinfo/reskit/tools/existing/gpotool-o.asp.

GPOTool options

To display command line options for GPOTool, enter the following command at the MS-DOS prompt:

```
Gpotool.exe /?
```

This command displays the following output.

```
Group Policy Object verification tool

Usage: gpotool [options]

Options:
/gpo:GPO[,GPO...] Preferred policies. Partial GUID and friendly name
                  match accepted. If not specified, process all policies in the
                  domain.
/domain:name      Specify the DNS name for the domain hosting the policies. If
                  not present, assume current domain.
/dc:DC[,DC...]    Preferred list of domain controllers. If not specified, find
                  all controllers in the domain.
/checkacl         Verify sysvol ACL. For faster processing, this step is skipped by default.
/verbose          Display detailed information.
```

A common option is to redirect the output of this tool to a text file using a command such as:

```
Gpotool.exe /domain:managesoft.com >gpotool.txt
```

The results can indicate whether there are any domain controllers available.

Sample results when no domain controller exists

```
gpotool: e    ERROR: GetDCList: DsBindW: hr=8007054b: The specified domain either does not exist or
could not be contacted.

gpotool:      +  File:d:¥nt¥private¥ctpolprf¥common¥polutil¥polutil.cxx: Line:728

gpotool: e   ERROR: GetDCList: GetDCList failed: hr=8007054b: The specified domain either does not
exist or could not be contacted.

gpotool:     +  File:d:¥nt¥private¥ctpolprf¥common¥polutil¥polutil.cxx: Line:644

Error: get DC list
```

Sample results when a domain controller is available

```
Validating DCs...
Available DCs:
machine1.lab3.headoffice.mycompany.com
Searching for policies...
Found 5 policies
=====================================================
Policy {0AFEDBFF-F294-4CD5-8E54-9C1D1C881452}
Policy OK
=====================================================
Policy {0FED227C-0966-42AC-8415-29168C7C40F3}
Policy OK
=====================================================
Policy {31B2F340-1234-11D2-945F-00C04FB984F9}
Policy OK
=====================================================
Policy {6AC1786C-016F-1201-8415-00C04FB984F9}
Policy OK
=====================================================
Policy {D8E6F75A-4C16-49ED-9382-5E92E103DE86}
Policy OK

Policies OK
```

Sample results when a domain controller is available (verbose option)

```
Domain: lab3.headoffice.mycompany.com
Validating DCs...
foxbat.lab3.headoffice.mycompany.com: down
machine1.lab3.headoffice.mycompany.com: OK
Available DCs:
machine1.lab3.headoffice.mycompany.com
Searching for policies...
Found 5 policies
=====================================================
Policy {0ADFEDFF-F294-4CD5-5E55-8D1D1C881452}
Policy OK
```

```
Details:
------------------------------------------------------------

DC: machine1.lab3.headoffice.mycompany.com
Friendly name: Test
Created: 1/22/2002 6:51:23 PM
Changed: 1/28/2002 5:47:06 PM
DS version:     0(user) 1(machine)
Sysvol version: 0(user) 1(machine)
Flags: 0
User extensions: not found
Machine extensions: [{6DA1C122-05CD-4B9A-9671-91B70CCBF530}{6DC1A488-45BA-4F4F-9671-90B70CBCF530}]
Functionality version: 2
------------------------------------------------------------

============================================================
Policy {0ABC227C-6906-42DE-8415-29168C7C40F3}
Policy OK
Details:
------------------------------------------------------------

DC: machine1.lab3.headoffice.mycompany.com
Friendly name: Global Packages Policy
Created: 1/22/2002 4:39:37 PM
Changed: 1/28/2002 8:42:17 PM
DS version:     0(user) 3(machine)
Sysvol version: 0(user) 3(machine)
Flags: 0
User extensions: not found
Machine extensions: [{4FADB488-04BA-4A9F-9671-90B70CBCF530}{6DADE444-04BA-4A9F-9671-90B70CBCF530}]
Functionality version: 2
------------------------------------------------------------

============================================================
Policy {22B4F540-056D-1552-935F-02C04BD984F9}
Policy OK
Details:
------------------------------------------------------------

DC: machine1.lab3.headoffice.mycompany.com
Friendly name: Default Domain Policy
Created: 9/5/2000 7:26:39 PM
Changed: 1/28/2002 5:44:51 PM
DS version:     1(user) 4(machine)
Sysvol version: 1(user) 4(machine)
Flags: 0
User extensions: [{3123F8D0-7020-11D2-842D-00C04FA372D4}{3123F8CE-7020-11D2-842D-00C04FA372D4}]
Machine extensions: [{58329AAC-683F-4515-A89A-00C04FBBCFA2}{58329A1B-2488-11D1-A28C-
00C04FB94F17}][{6DA1C488-04BA-4A9F-1029-30B70FDDE530}{5FE1C488-04BA-4B9A-9671-
90B70CBCF530}][{123D319E-6CEA-11D2-A4EA-00C04F79F83A}{102E14A0-B4FB-11D0-A0D0-
00A0C90F574B}][{A2AE8D72-6CEA-11D2-A4EA-00C04F79F83A}{3506AC1D-2488-11D1-A28C-00C04FB94F17}]
Functionality version: 2
------------------------------------------------------------

============================================================
Policy {6AC1786C-016F-11D2-945F-00C04FB984F9}
Policy OK
Details:
------------------------------------------------------------

DC: machine1.lab3.headoffice.mycompany.com
Friendly name: Default Domain Controllers Policy
Created: 9/5/2000 7:26:39 PM
Changed: 1/28/2002 7:02:39 PM
```

```
DS version:     0(user) 6(machine)
Sysvol version: 0(user) 6(machine)
Flags: 0
User extensions: not found
Machine extensions: [{103A429A-6EAC-4039-A4EA-00C04F79F83A}{192A14F0-C2CF-11D0-A0D0-00A0C90F574B}]
Functionality version: 2
------------------------------------------------------------
============================================================
Policy {D8E6F74E-4C16-49ED-9618-5E92E103DE86}
Policy OK
Details:
------------------------------------------------------------
DC: machine1.lab3.headoffice.mycompany.com
Friendly name: Stamfird Policy
Created: 1/22/2002 1:04:48 PM
Changed: 1/28/2002 5:47:02 PM
DS version:     1(user) 4(machine)
Sysvol version: 1(user) 4(machine)
Flags: 0
User extensions: [{2AE1F584-04BA-4A9F-9671-90B70CBCF530}{6CA1C488-14BA-4A9F-9671-90B70CBCF530}]
Machine extensions: [{6DA1C488-04BA-4A9F-9671-90B70CBCF530}{6CA1C434-23EB-4A9F-9671-90B70CBCF530}]
Functionality version: 2
------------------------------------------------------------

Policies OK
```