Table of Contents

1 Welcome

AutoAdministrator 2.4.0 is a Windows WinXP / Vista / Win2k8 / Windows 7/8 application that allows common system administration tasks to be executed on multiple computers simultaneously. The intuitive GUI interface simplifies complex tasks.

The following administration tasks are supported:

- Password updates
- Remote shutdown / reboot
- Services maintenance
- Registry maintenance
- Network ping
- Remote file management
- Remote file information
- Logged on user information
- Execute processes locally or remotely
- WMI queries
- ODBC maintenance

Questions regarding AutoAdministrator should be directed to

- Webform
- support@netikus.net

AutoAdministrator is free software.

Please take a moment now to review the Read This First page.

The **NETIKUS.NET ltd** team.

2 Read This First

Please read this CAREFULLY before using AutoAdministrator

AutoAdministrator can help automate many tasks and save significant amounts of time, but it can also **wreak havoc** on networks. This tool is **only recommended for experienced system administrators and network professionals**.

AutoAdministrator is no different than other system utilities that modify system settings in that respect, except for one key difference: AutoAdministrator **can make changes to potentially hundreds of computers with the click of a button**.

> Many of the actions performed with
> AutoAdministrator cannot be undone!

In general, any action performed by AutoAdministrator should be assumed to be able to cause a irreversible side-effect. Only those actions specifically designated as "**read-only**" in this manual should be considered safe. **The actions listed below are designed to make changes to multiple remote systems and cannot be undone**. Other actions (e.g. "Execute Process") may alter remote systems

depending on user input.

ODBC Update: Updating ODBC drivers can potentially corrupt the ODBC setup on the remote machine and might require reinstalling the respective ODBC driver. "Attempt to copy driver files" and "Copy additional drivers" should only be selected if the files the ODBC driver(s) require are known. AutoAdministrator does not provide a mechanism to undo a "Delete DSN" operation.

Password Update: When changing passwords make sure to remember the new password.

Service Update: Removing a service cannot be reversed, especially when also removing the service file.

Shutdown / Reboot: When shutting down or rebooting servers, a timeout of 5 minutes or more is recommended so that users or administrators on those machines have enough time to abort the action, if necessary.

Registry Update: Deleting keys or values on multiple machines can render those installations unusable. Even adding keys and values to the registry can create undesirable behavior. Extreme caution should be exercised when making any kind of registry change to multiple computers.

File Management: If "Overwrite existing files" is selected then remote files will be silently overwritten. Care must be taken to ensure that files are not accidentally overwritten. "Delete files" will delete files on the remote system. This action cannot be undone.

3   Requirements

Operating Systems (Installation)

AutoAdministrator can be installed on the following operating systems:

- Windows XP, Windows Server 2003
- Windows Vista, Windows Server 2008 (R2)
- Windows 7
- Windows 8 / 8.1
- Windows 2012 (R2)

Operating Systems (Remote)

AutoAdministrator can manage the following operating systems on remote hosts:

- Windows NT 4, 2000 (not tested)
- Windows XP, Windows Server 2003
- Windows Vista, Windows Server 2008 (R2)
- Windows 7
- Windows 8 / 8.1
- Windows Server 2012 (R2)

Additional Requirements

Remote Registry Access
The "Remote Registry" service must be running on the remote host(s) for any feature that accesses the remote registry (e,g, Registry, Logons) to work correctly.

User Account Control
Even though most features of AutoAdministrator technically wouldn't require elevated privileges on Microsoft Vista and later, AutoAdministrator has been configured to always require elevated permissions to work correctly. This is to avoid problems with the functionality of the product and to ensure that all included features can be utilized to its full extent.

4   Overview
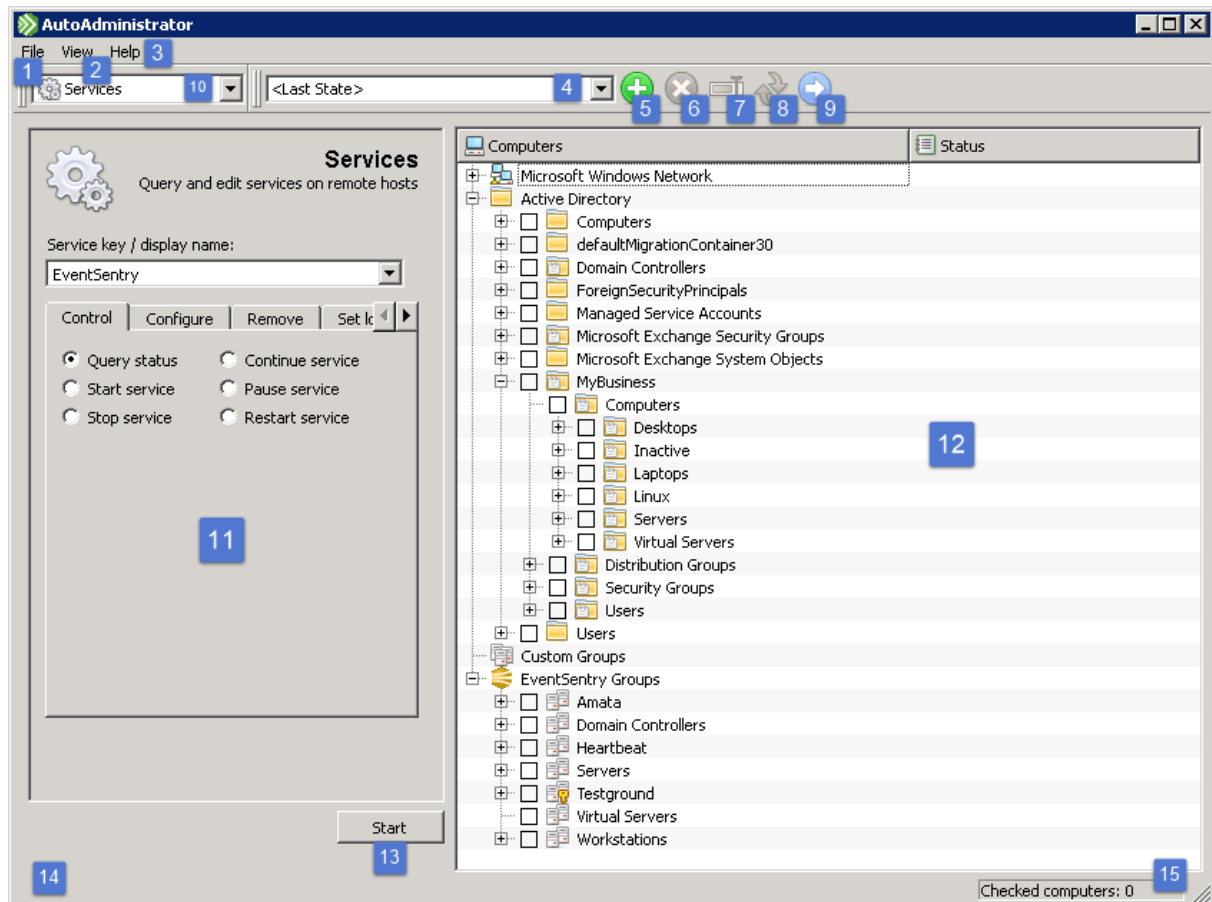
Window Components

1	**File menu**
2	**View menu**
3	**Help menu**
4	**Preset selector**
5	**Add new preset** Creates a new preset based on the AutoAdministrator's current state.
6	**Delete current preset** The current preset is removed. Not available for built-in presets *<Last State>* and *<Default>*.
7	**Rename current preset**
8	**Update current preset** Changes the current preset to current state of the application. Not available for built-in presets *<Last State>* and *<Default>*
9	**Apply current preset** Changes the current state of application to the current preset.
10	**Feature selector**

11 **Feature options panel**
Contains all feature-specific options.

12 **Network tree view**
Allows selection of hosts for update. Selecting a group will automatically select all hosts within that group. Update results are displayed in the status column.

13 **Start/Stop update**
The text of this button will change from "Start" for a non-destructive operation to "Update" for a potentially destructive operation to "Stop" while an update is in progress.

14 **Update summary**
Following an update, a summary of the number of hosts affected and the time it took is displayed here.

15 **Checked computer count**
The number of hosts currently selected for update. The actual number of updated hosts may be less, as this number does not check for duplicate hosts.

Basic Use-Case
Performing an action involves the following steps:
1) Use the network tree view to select the hosts to which the update should be applied.
2) Use the Feature selector to select the action to be performed.
3) Specify options with the feature options panel, as needed
4) Apply the update by clicking on the *Update* button.
5) Results are displayed in the status column for each computer. Red text indicates a failure, while green text indicates success.

Custom Groups
Custom groups allow computers to be grouped in an arbitrary fashion. This can be useful, e.g., if there is a subset of a domain that is commonly updated.

Computers can be added to custom groups via the following means:
- Drag-and-drop from the *Windows Networking* or *Active Directory* lists
- Context menu for the *Windows Networking* or *Active Directory* lists
- Context menu for a custom group
- Manually entered names need not exist in *Windows Networking* or *Active Directory*

4.1 General Options
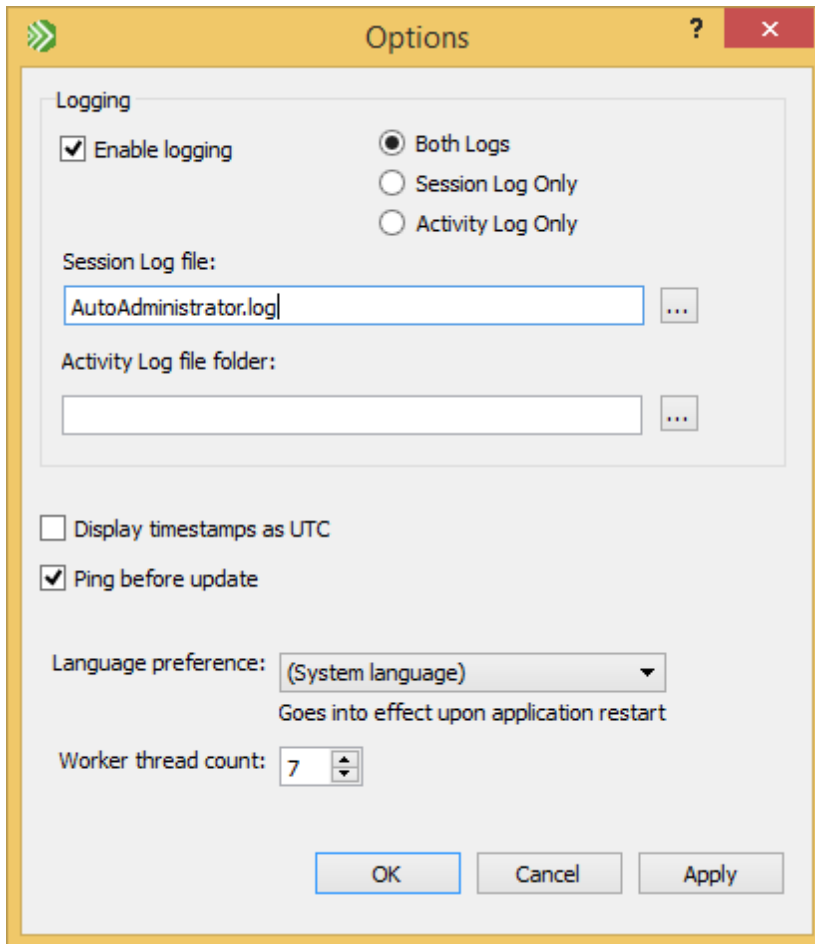
Logging
If logging is enabled, a detailed log of all activity is written to one or more log files, depending on which log file options are selected.

Session Log
The session log records detailed information about any action performed, including:

- Date/Time when action was performed
- User who performed action
- Source computer
- Details about action performed (dialog settings)
- Output
- Summary information, including total duration and average processing time

There is only one session log, and multiple sessions are appended to the same file.

Example session log:

```
========================================================
AutoAdministrator Activity Log
Date Start: Fri Feb 19 12:44:42 2010
```

```
User: DOMAIN.LOCAL\john.smith
Computer: WORKSTATION01
----------------------------------------------------------
Feature: Execute Processes
Executable: C:\Tools\plink.exe
Arguments: -l root -pw canttellyou! $HOSTNAME "uname -a"
Process timeout (s): 120
netbsd.unix.local : Exit code: 0  Elasped time (s): 0.76804 NetBSD  5.0 NetBSD 5.0
(GENERIC) #0: Sun Apr 26 18:50:08 UTC 2009  builds@b6.netbsd.org:/home/builds/ab/
netbsd-5-0-RELEASE/i386/200904260229Z-obj/home/builds/ab/netbsd-5-0-RELEASE/src/sys/
arch/i386/compile/GENERIC i386  Using keyboard-interactive authentication.
freebsd.unix.local : Exit code: 0  Elasped time (s): 0.72804 FreeBSD freebsd71.unix-
dev.netikus.local 7.1-RELEASE-p6 FreeBSD 7.1-RELEASE-p6 #0: Tue Jun  9 16:26:47 UTC
2009    root@i386-builder.daemonology.net:/usr/obj/usr/src/sys/GENERIC  i386  Using
keyboard-interactive authentication.
openbsd.unix.local : Exit code: 0  Elasped time (s): 1.0111 OpenBSD openbsd45.unix-
dev.netikus.local 4.5 GENERIC#0 i386
========================================================
AutoAdministrator Activity Log Summary
Duration: 3 second(s)
Average Time: 1 second(s)
========================================================
```

<u>Activity Logs</u>
Unlike the session log, activity logging creates one or more CSV files (separated with the | character) that contain the feature output. The CSV file contains the following information:

- Timestamp
- Host Name
- Result Summary
- Result

Activity logging creates at most one log file per day and feature, with a file name of `YYYY-MM-DD_<Feature>.log`, for example `2010-02-03_Services.log`.

Example activity log, after running "uname" through plink.exe:

```
Timestamp|Host Name|Result Summary|Result
Fri Feb 19 13:00:55 2010|freebsd.unix.local|Ok|Exit code: 0  Elasped time (s): 0.59003
FreeBSD  Using keyboard-interactive authentication.
Fri Feb 19 13:00:55 2010|netbsd.unix.local|Ok|Exit code: 0  Elasped time (s): 0.78905
NetBSD  Using keyboard-interactive authentication.
Fri Feb 19 13:00:55 2010|openbsd.unix.local|Ok|Exit code: 0  Elasped time (s): 0.89405
OpenBSD
```

Ping Before Update
This option attempts to ping remote machines before applying updates. If the ping fails the machine is skipped. This is useful for updating machines that may not be online, as the ping will fail faster than an update attempt would.

Language Preference
Allows the user to change the language preference. This change will not go into effect until the application is restarted. The list is initialized based on *.qm* files found at program initialization. AutoAdministrator currently supports the following languages for the user interface:

- English (default)

· German.

Worker Thread Count
The number of updates that may be pending at any one time. Once this limit is reached no additional updates will begin until a pending update has completed.

5   Features

AutoAdministrator provides support for automating many common administrative tasks on remote computers including:

· Ping

· ODBC Update
  · Copy DSN
  · Delete DSN
  · Query DSN

· Password Update
  · Change Password
  · Reset Password
  · Verify Password

· Shutdown / Reboot
  · Schedule shutdown
  · Schedule reboot
  · Cancel scheduled shutdown / reboot

· Services Update
  · Control Service
    · Query service status
    · Start service
    · Stop service
    · Continue service
    · Pause service
    · Restart service
  · Configure Service
    · Disable service
    · Change startup mode
  · Remove Service
  · Change logon

· Registry Update
  · Add value
  · Delete value
  · Change value
  · Read value
 · Add key
  · Delete key
  · Copy key

· File Management
  · Copy files

- Delete files

- File Information

- Logged on Users

- Execute Processes

- WMI

Other Features
- Support for user-defined custom groups
- All actions can be logged to a text file
- Intuitive interface
  - Context-menus
  - Custom groups can be manipulated via drag-and-drop
- Application settings and custom groups are automatically saved upon exit and restored when re-launched
- User-defined presets allow the user to save/load GUI states

5.1   Ping

Ping remote hosts.
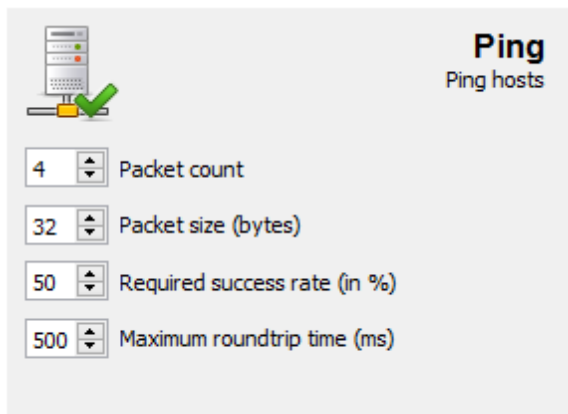
Packet Count
The number of ICMP packets to send to the remote system.

Packet Size (bytes)
The size of each packet sent to the remote system.

Required success rate (in %)
Specifies a lower-bound on the number percent of packets that must be received correctly. Violation of this threshold will result in the offending computer flagged as an error. Specifying zero effectively disables this check. Note: this only affects how results are displayed in AutoAdministrator, it does not affect how they are gathered.

Maximum roundtrip time (ms)
Similar to *Required success rate,* this specifies a threshold that, if violated, will result in the offending computer flagged as an error.

5.2 ODBC

Update ODBC DSN configurations and driver files on remote hosts.
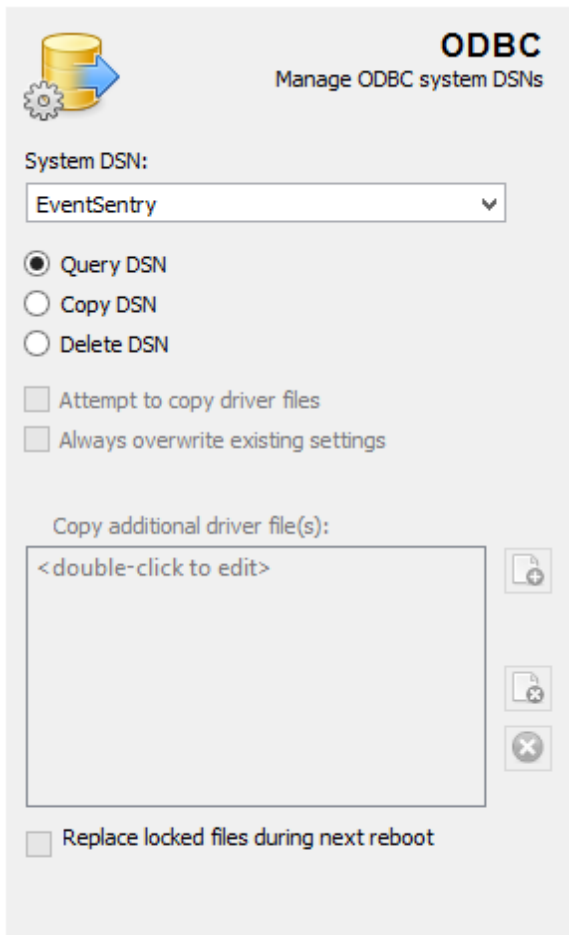
> ❌ All ODBC actions, with the exception of Query DSN, cannot be undone and are permanent. Use these features with care.

System DSN
The System DSN (Data Source Name) that for the action. The drop-down list is initialized from the local system.

Copy DSN
The selected System DSN will be copied to the remote system.

Delete DSN
The selected System DSN will be removed from the remote system. The options to copy additional files are unavailable.

Query DSN
The selected DSN will be will be queried and information about the driver and database will be displayed. The options to copy additional files are unavailable. **This is action is non-destructive**.

Attempt to Copy Driver Files
Check this box if AutoAdministrator should attempt to copy the driver file that is associated with the ODBC driver as well.

Why "*attempt*"? Many ODBC drivers (e.g. MS SQL Server) consist of dozens of files that make up the ODBC driver, all of which may depend on other ODBC DLLs. Copying drivers like these using AutoAdministrator will not produce the desired result since AutoAdministrator doesn't know which files to copy. *Copy additional driver file(s)* can be used to specify additional extra files (see below).

> This option should be used with extreme care, as overwriting system files can destabilize parts (e.g. ODBC) of or the entire Operating System. NETIKUS.NET ltd cannot be held responsible for any damage caused by incorrect use of this option.

Some ODBC drivers (e.g. MySQL) only consist of one file (the file referenced in the ODBC configuration) and can therefore easily be copied and rolled out with AutoAdministrator.

> The file that will be copied when using this option is the one specified by the Driver value in the HKLM\Software\ODBC\ODBCINST.INI\<Driver> registry key, where <Driver> is the name of the referenced ODBC driver.

Always Overwrite Existing Settings
By default, AutoAdministrator does not overwrite existing settings and files. If the specified DSN name does already exist on the remote machine then the configuration will not be copied. This also applies to files that already exist on the remote machine.

Activate this option to force AutoAdministrator to always copy the ODBC settings (and files), regardless to whether they exist on the remote machine or not.

Copy Additional Driver Files
This option provides a mechanism to copy extra files in cases where the ODBC driver consists of more than a single file. Files specified here will be copied to *%systemroot%\system32*, regardless of their original location. See File Copy for a description of file dialog controls.

> This option should be used with extreme care, as overwriting system files can destabilize parts (e.g. ODBC) of or the entire Operating System. NETIKUS.NET ltd cannot be held responsible for any damage caused by incorrect use of this option.

Replace locked files during next reboot
This option can be used to schedule the replacement of files that are locked by the operating system (e.g. the file is currently in use). The files will be copied to *%systemroot%* and moved to *%systemroot%\system32* when the machine is rebooted. AutoAdministrator can be used to schedule a subsequent reboot on remote machines, see Shutdown / Reboot.

5.3 Password

Reset, change or verify passwords of a user on remote hosts.

Password
Manage user passwords

Update type:	Verify Password ▾
Username:	JohnDoe
Current password:	●●●●●●●●●●●
New password:	
Verify:	

☐ Show passwords

Update Type

Change password	Changes a single user's password on selected computers. The current password must be supplied for this operation. This is the default option.
Reset password	Resets the user's password without the knowledge of the current password.
Verify password	Checks if a supplied password is the valid password for the user account on selected computers. It is recommended to use this option on Windows XP, Windows Server 2003 and higher for performance reasons. **This is action is read-only**.

Username
The username on the remote machine.

Current Password
The current password of the account. Only available for *Change password* or *Verify password.*
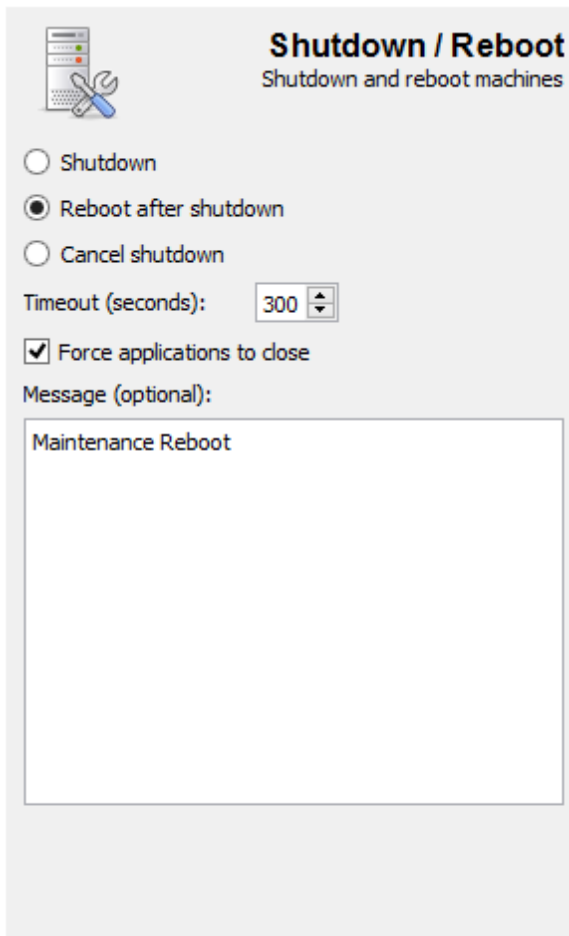
New Password / Verify
Specify the new password to be assigned to the username. Only available for *Change password* or *Reset password.*

Show passwords
Displays typed passwords (checked) or not (cleared).

5.4 Shutdown / Reboot

Shutdown, reboot, or cancel pending shutdown of remote hosts.

Shutdown / Reboot after shutdown

This option causes the selected computers to shut down or reboot after the timeout period has elapsed. The optional messages is displayed to users of the remote systems.

> The number of computers to be shutdown/rebooted will be displayed in a pop-up before the shutdown is sent to the remote hosts. Please take care to make sure that this number matches the number of computers that are intended to be shutdown/rebooted.
> **Once the timeout period has elapsed, a shutdown or reboot cannot be aborted.**

Cancel shutdown

This option aborts a previously scheduled shutdown. This option will cancel any pending shutdown requests on the remote system (even if the request did not originate with AutoAdministrator). When this option is selected the *Timeout*, *Force applications to close*, and *Message* fields are disabled.

Timeout

The timeout field specifies a delay in seconds before the remote systems are shutdown or rebooted. This gives affected users some time to save their data or abort the shutdown, if necessary.

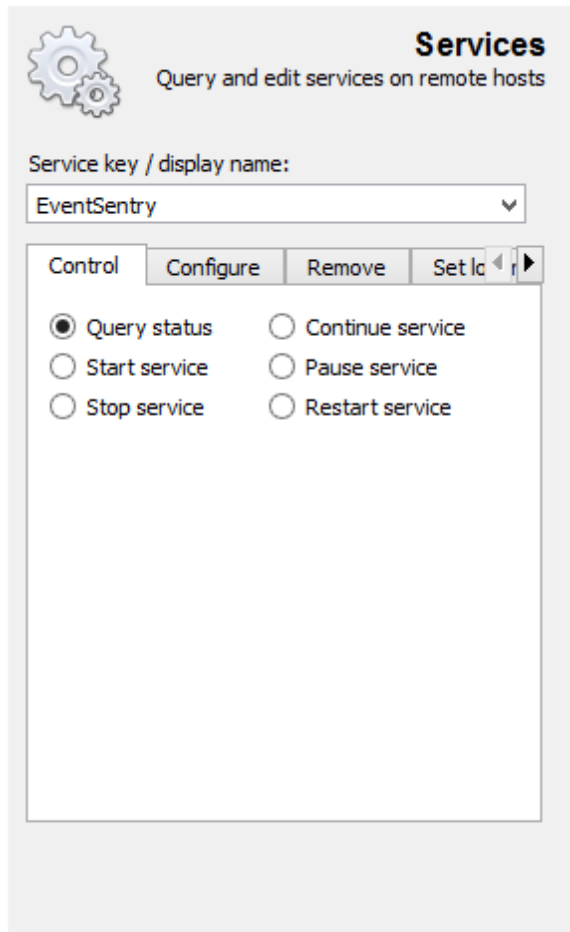## Force applications to close

Selecting this option will cause remote computers to be shutdown/rebooted even when applications with unsaved data are open. Use this option with care.

Message (optional)
If specified, this message will be displayed on the remote computers before the computer is shutdown or rebooted. A timeout value (see above) long enough to give the read a chance to read and respond to the message should also be set.

5.5   Services

Configure services on remote hosts.

Services
Query and edit services on remote hosts

Service key / display name:
EventSentry

| Control | Configure | Remove | Set lc ◀ ▶ |

- ◉ Query status   ○ Continue service
- ○ Start service   ○ Pause service
- ○ Stop service   ○ Restart service

Service Display Name
The display name of the service to manage. The drop-down list is initialized from the local machine. If known, the service key name (can be found either in the registry or in the service details on Windows 2000 and higher) can be entered instead, after a colon (':'). This informs AutoAdministrator that the value is using a service key name. For example, the Workstation service has the key name **lanmanworkstation**. To use this name enter

:lanmanworkstation

into the **Service display name** field.

Control Service

Query status	Outputs information about the service. This is a non-destructive operation. Example query output: *Service "Alerter" is STOPPED (Manual), using account LocalSystem* This is a non-destructive operation.
Start service	Attempts to start the specified service
Stop service	Attempts to stop the specified service
Continue service	Attempts to continue a paused service
Pause service	Attempts to pause a running service
Restart service	Attempts to restart a running or stopped service

Configure Service

Set startup type to manual	Sets the startup mode of the service to manual so that the service is not automatically started when the Operating System boots. The service can still be started if other services start it.
Set startup type to automatic	Sets the startup mode of the service to automatic so that the service is automatically started when the Operating System boots.
Set startup type to disabled	Disables the service so that it cannot be started, unless reconfigured to manual or automatic startup mode.

Remove Service

Remove service	Stops the service (if running) and deletes the service configuration. Service specific data (such as files, configuration) is not removed.
Remove service and file	Stops the service (if running), deletes the service and removes the associated file. Some service specific data may still be left, if the service used multiple files and/or saved configuration data in the registry.

Set Logon

Changes the logon settings for the service. These changes will not go into effect until the service is restarted (e.g. via "restart service" check-box, manual restart or system reboot).

5.6 Registry

Manipulate or query the registry on remote hosts.

❌ All registry actions, with the exception of **Read**, cannot be undone and are permanent. Use this feature with care.

Actions:
- Add a value
- Delete a value
- Change a value
- Read a value
- Add a key
- Delete a key

The following data types are supported:
- REG_DWORD
- REG_SZ
- REG_EXPAND_SZ

· Copy a key

Main key
Specifies the root key that will be affected by the update. The following choices are available:

HKEY_LOCAL_MACHINE (default)
HKEY_CLASSES_ROOT
HKEY_CURRENT_USER
HKEY_USERS

Key
The target key under the main key. e.g. to update HKLM\SOFTWARE\SomeProduct\SomeValue First set *Main key* to *HKEY_LOCAL_MACHINE*. Then enter *software\SomeProduct* in the *Key* field.

Value/Subkey name
The target key/value for the update. The field accepts a value name when a value action is selected (e.g. *Add value*) and a subkey name when a key action is selected (e.g. A*dd key)*. This field is not available when *Copy key* is selected.

Value Data
Data to be written to the value specified in the *value name* field. Only available when *Add value* or *Change value* is selected.

Value Type
The data type for the value provided in the *Value data* field. Only available when *Add value* or *Change* value is selected May be one of:

REG_EXPAND_SZ
REG_SZ
REG_DWORD

Action Type
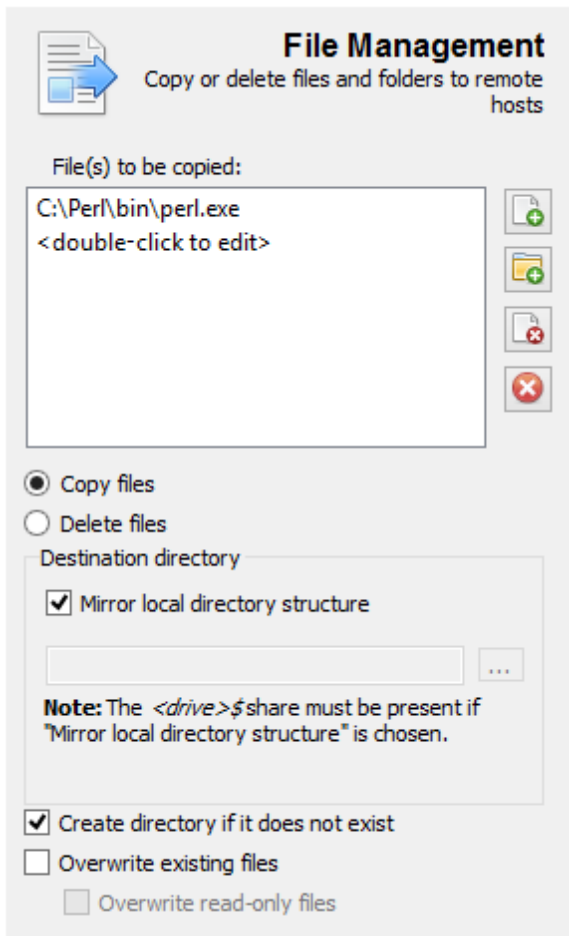Specifies the type of registry update to perform. The following choices are available:

Add value	Adds a new value to an existing registry key
Delete value	Deletes an existing value from an existing registry key
Change value	Changes an existing value of an existing key to a new value
Read value	Reads an existing value of an existing key. This operation is non-destructive.
Add key	Adds a new registry (sub)key
Delete key	Delete and existing registry key
Copy key	Copies an existing registry key to a new registry key

> All registry actions, with the exception of **Read**, cannot be undone and are permanent. Use this feature with care.

5.7   File Management

Manage files on remote hosts.

File Management
Copy or delete files and folders to remote hosts

File(s) to be copied:

| C:\Perl\bin\perl.exe |
| <double-click to edit> |

- ⦿ Copy files
- ○ Delete files

Destination directory

☑ Mirror local directory structure

[   ] [...]

Note: The *<drive>$* share must be present if "Mirror local directory structure" is chosen.

☑ Create directory if it does not exist
☐ Overwrite existing files
☐ Overwrite read-only files

File(s) to Be Copied/Deleted
A list of some number of Files and/or directories to be copied or deleted on the remote host.

	Add file...	Displays the add file dialog. Multiple files can be selected by holding down *Ctrl* or *Shift* keys.
	Add folder...	Displays the add folder dialog. The contents will be recursively copied to the target system.
	Remove	Removes selected item from the list.
	Remove all	Removes all items from the list.

Copy Files

Copies files to remote hosts.

Destination Directory

The target path for the copying operation. If *Mirror local directory structure* is checked, all files will be copied to the same paths as the local machine. If unchecked, then a remote path must be specified and all files will be copied using this path as the root. In this case the user is responsible for making sure that file names do not conflict. **Results are undefined in the case of a naming conflict**. In particular AutoAdministrator makes no guarantees as to which copy of the file, if either, will be written to the destination,

For example, suppose the following three items are in the list:
```
c:\mydir
c:\folder1\textfile.txt
c:\folder2\textfile2.txt
```

If *Mirror local directory structure* **is** checked, then after copying the remote machine will have the following items:
```
c:\mydir\<contents of mydir>
c:\folder1\textfile.txt
c:\folder2\textfile2.txt
```

If *Mirror local directory structure* **is not** checked, and the target directory is set to *c:\targetFldr*, then after copying the remote machine will have the following items:
```
c:\targetFldr\mydir\<contents of mydir>
c:\targetFldr\textfile.txt
c:\targetFldr\textfile2.txt
```

Finally, suppose the file list also contained `c:\folder3\textfile.txt` and that *Mirror local directory structure* **is not** checked. In this case there is name clash between `c:\folder1\textfile.txt` and `c:\folder3\textfile.txt`. The state of the target machine is undefined in this case.

Create Directory if it Does not Exist

If checked this option cause the target directory structure to be created on the remote machine, if needed. If unchecked the target directories must exist, or the copy operation will fail.

Overwrite Existing Files

If checked, this forces existing remote files to be replaced by the local files.

Care must be used when selecting this option. This could result in replacing newer file versions with older ones, which could destabilize the target system. This option should only be used when it is certain that local file versions are correct. **This operation cannot be undone.**

Delete Files
Deletes files on remote hosts.

- ○ Copy files
- ● Delete files

- ☐ Delete read-only files
- ☐ Recursively remove directories

Care must be used when selecting this option. This operation cannot be undone.

Delete Read-Only Files
Deletes files on the remote host even when the files are marked as "read-only".

Recursively Remove Directories
For every folder specified in the "Files to be deleted" list, selecting this option will delete all files and folders that are contained within that folder. The folder itself will then be deleted. If this option is not selected, then only empty folders will be successfully deleted.

5.8 File Information

Queries information on files located on remote hosts.

File Information
View file details on remote hosts

File:

C:\Windows\system32\kernel32.dll ...

☑ Checksum
   Algorithm:
   SHA-1 ▼
   Value (optional):

☑ Size   ☑ Version
☐ Attributes   ☐ Company
☐ Modification time   ☐ Description

ⓘ   This action is read-only

File
The name of the file to check. Only one file may be checked at a time.

Hash
If selected, computes the hash of the file using the specified algorithm. AutoAdministrator supports the following hash algorithms:

CRC-32
MD5
SHA-1
SHA-256

The hash output is color coded, with files sharing the same checksum using the same color. This makes it easy to group files which share the same checksum.

Value
If a hash value is specified, files are checked to see if they have the same hash value. Files that do not match the provided value are treated as errors.
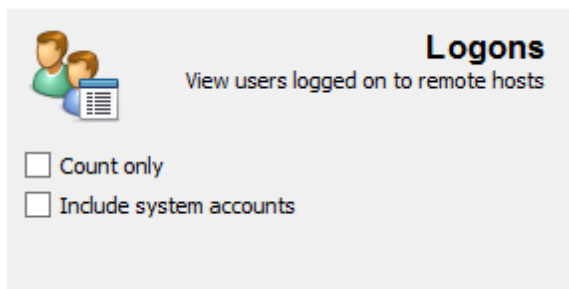
Other properties
Any combination of the following properties can be displayed:

File Size	*Version* (executable files only)
Attributes	*Company* (executable files only)
Modification Time	*Description* (executable files only)

5.9   Logons

Queries information about users logged on to remote hosts.
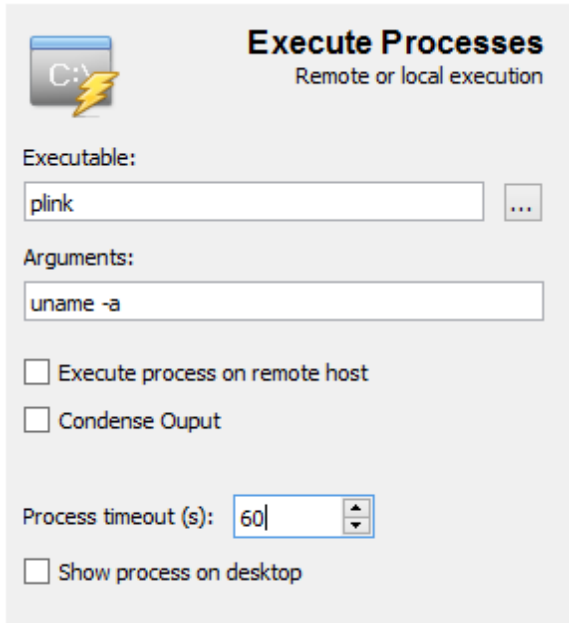

ⓘ   This action is read-only

Count only
Displays only the number of logon to the remote host.

Include System Accounts
Includes system accounts in the result.

5.10   Execute Processes

Executes processes on remote hosts or the local system and displays their output inside AutoAdministrator.

Executable
File to execute. File must exist on remote host(s) when executing processes remotely.

Arguments
Arguments passed to the process. *$HOSTNAME* will be replaced with the name of the host being processed.

Execute process on remote host

Remote Execution
When executing process remotely, AutoAdministrator temporarily creates the "AutoAdministrator Remote Execution Service" (AARemoteExecSvc) which then executes the command remotely and transmits the output back to AutoAdministrator.

Local Execution
When executing processes locally the $HOSTNAME variable will be resolved to the host name which is currently being processed. For example, specifying **ping** as the executable and **$HOSTNAME** as the argument will ping every selected host.

When working with Unix networks, AutoAdministrator can utilize a tool like plink.exe to execute commands on a remote Unix host and display the output inside AutoAdministrator.

Condense Output
When checked, removes all new line characters of the process output and replaces it with the space character. Hovering over the output will show the full output in a tooltip.

Process Timeout (Local Execution Only)
The maximum number of seconds the process will be allowed to run. Set to 0 to indicate no timeout.

Show Process on Desktop (Local Execution Only)
If checked, shows the process' window on the desktop.

5.11 WMI

Executes WMI queries on remote systems and displays the output inside AutoAdministrator.

WMI
Execute WMI queries

WMI Namespace:

root\CIMV2

WMI Class:

Win32_Share

Object:

Name

Object List:

Path
Name

+

-

☑ Add labels to output

25 ⏶⏷ Output record limit

ℹ This action is read-only

WMI Namespace
The WMI namespace.

WMI Class
The WMI class. Values are retrieved based upon the selection of the WMI Namespace field.

Objects
List of WMI objects corresponding to the selected WMI Class field.

Object List
List of objects to be operated upon. All objects must be members of the same namespace / class.

Add Labels to Output
Prepends the object name to the displayed output message. Labels will also be present in log files.

Output Record limit

Limits the number of records displayed to the user. Maximum value is 100.

6 Questions or Problems?

Questions

If you have any questions or problems please visit the support forums: http://forums.netikus.net/categories/autoadministrator.

Please include the following information:
- The Operating System (incl. Service Pack Version) on which AutoAdministrator is running
- Version of AutoAdministrator
- Your question or
- An exact description of the problem. Include information such as:
    - Does this problem occur on one or more installations?
    - Did it happen once or does it happen repeatedly?
    - What can we do to reproduce the problem?

7 Suggestions?

At NETIKUS.NET ltd, we rely on feedback from our customers.

If there is a feature you would like to see implemented in a future release we would love to hear about it. We have implemented many features from customer suggestions in the past! Please sent an e-mail to suggestions@netikus.net.

And include the following information:

- A description of the feature
- Why and how this feature would benefit you
- An example

After reviewing your request we will let you know if and when we will add your feature to AutoAdministrator.