Copyright and Disclaimer

RegAdmin™ Pro distribution version 1.0 copyright (C) 1996-1997 Midwestern Commerce, Inc. All Rights Reserved.

This program uses intricate security features of Windows NT. Improper use of this program may result in damage to your system.

This program is supplied on as-is basis. Midwestern Commerce, Inc. shall not be held responsible for any misuse or damage it may cause to your or other systems.

For updates please visit
http://www.NTsecurity.com/

Please send your questions and suggestions to
RegAdmin@box.omna.com

Program Description

RegAdmin Pro is a part of Administrator Assistant Tool Kit (A2NT) - a set of tools that substantially facilitates security administration of NT based networks. It gives an administrator functionality that native NT tools lack. Administrator Assistant currently consists of FileAdmin, RegAdmin and ScanNT.

RegAdmin Pro is a must-have tool to properly handle Registry Permissions. Unlike built-in NT security manager, RegAdmin allows a user to **add**, **clone**, **remove** or **modify** account permissions to a key or a group of keys and **propagate the changes through registry key tree without affecting other accounts' permissions**. Other key features:

- gives an administrator a center point for viewing and modifying registry permissions
- allows an administrator to set a similar to the existing set of permissions for a new group or
- user through **Clone** function
- provides comprehensive log information of changes, easy to audit permissions changes
- provides easy handling of deleted or unknown accounts through Security ID
- replaces Everyone in seconds

System Requirements

RegAdmin™ Pro is a powerful Administrator tool for MS Windows NT ™ 3.51 and 4.0.

The Windows NT Intel version requires Windows NT 3.51 or 4.0 server or Workstation on Intel platform. Only Intel Version is available at the moment.

DEMO Version

The DEMO version of *RegAdmin* has the following specific features:

- will not propagate changes through entire kee tree.

How to Change Permissions on a Registry Key

Introduction

Permissions on a registry key specify the type of access a *Group* or a *User* has to the key. New subkeys inherit their permissions from the key. When changing permissions for a key without propagating through entire tree, permissions on existing subkeys are not changed. Select **Propagate through entire tree** if you want to change permissions on all existing subkeys.

Permissions are cumulative except that the No Access (Special access - None) permission overrides all other permissions. For example, if a *User* is a member of a *Group* with *Read* permission and a member of a *Group* with *Full Control* permission, the *User* will have *Full Control* permission and if a User is a member of a Group with Read permission and a member of a Group with No Access permission, the user will have No Access permission.

Notes

To change permissions on a key, you must be the owner of the key or have been granted permission to do so by the owner.

To Change or View Permissions on a Key:

- Select the Key in the **Registry Key** window. You can browse keys by pressing **…** button in the **Registry Key** window. All groups and users that have some **Type of Access** to the selected key and their type of access will be listed in the main window.
- Select a group or user in the **Account** window. You can double click a group or user in the main window or press **…** button in the **Account** window to browse accounts not listed in the main window.
- Choose a permission from the **Type of Access** box.
- If you want the permission that you are setting on the selected key to override permissions previously set on its subkeys, select the **Propagate through entire tree**.
- Press **Change** button.
- Confirm changes by pressing **OK** in the **Warning** menu.

Important

If **Propagate through entire tree** selected:

- permission changes will affect ONLY the account selected in the Account window. Other permissions will be intact.
- permissions will be changed for all subkeys of the selected key.

To remove key permissions

To remove registry key permission select the name of the group or user in the Account window whose permission you want to remove. Choose the **Remove** button.

The default *Log File* options are *Error Log Only* and *Append to Log*. Open **Options** menu to change default settings

For help with any dialog box, choose the Help button while using the dialog box. For additional help use Registry Editor Help.

See Also
Registry Key Access Permissions
Example #1: Changing permissions

How to Remove Permission on a Registry Key

To remove permission on a key

- Select the Key in the **Registry Key** window. You can browse registry keys by pressing **…** button in the **Registry Key** window. All groups and users that have some **Type of Access** to the selected Key and their type of access will be listed in the main window.
- Select a group or user in the **Account** window whose permission you want to remove by double clicking a group or user in the main window.
- To remove permissions on all subkeys of the selected key, select **Propagate through entire tree**.
- Press **Remove** button.
- Confirm changes by pressing **OK** in the **Warning** menu.

Important

If **Propagate through entire tree** selected:

- permission changes will affect ONLY the account selected in the Account window. Other permissions will be intact.
- permissions will be changed for all subkeys of the selected key.

Check *Modify Auditing for Remove or Clone* in **Options** menu if you want to remove auditing

For help with any dialog box, choose the Help button while using the dialog box.

See Also
Example #3: Removing permissions

How to Clone Permissions

In some cases when you create a new group or user you need to assign a set of permissions for this group or user (**Target account**) similar to a set of permissions you already have for some group or a user (**Source account**). The easiest way to do that is to use **Clone** function to copy a set of permissions of **Source account** to **Target account**.

To clone permissions:

- Select the Key in the **Registry Key** window. You can browse keys by pressing **…** button in the **Registry Key** window. All groups and users that have some **Type of Access** to the selected Key and their type of access will be listed in the main window.
- Select the name of a group or user in the *Account* window whose permissions you want to clone (Source account). You can double click a group or user in the *main* window to select it.
- Press **Clone** button.
- *Select a Target Account* menu appears. Use … button to select a Target account.
- Confirm changes by pressing **OK** in the **Warning** menu.

After *Clone* is performed the **Target account** will have identical set of permissions as **Source account** for the registry key selected.

Check **Propagate through entire tree** option of *main* menu if you want the **Target account** to have identical set of permissions as **Source account** for all subkeys of the key selected.

Check *Modify Auditing for Remove or Clone* in **Options** menu if you want to *clone auditing*.

For help with any dialog box, choose the Help button while using the dialog box.

See Also
Example #2: Cloning permissions

How to Replace Account with a different Account

In some cases you need to replace a group or user with a different group or user with the same set of permissions. The best example is Everyone group.

To replace ALICE with BOB

- Use **Clone** function to copy ALICE (**Source account**) permissions to BOB (**Target account**) propagating through entire tree.
- Use **Remove** function to remove ALICE account propagating through entire tree.

Check *Modify Auditing for Remove or Clone* in **Options** menu when you *Clone* and *Remove.*

See Also
Example #4: Replacing permissions

Registry Key Access Permissions

When you set a registry key permission, abbreviations for individual permissions are displayed next to Account in the main window:

You can set the following permissions in **Type of Access** box:

1. To enable the user to read the key contents but not to save any changes made to the file, select **Read**.
2. To enable the user to access, edit, and take ownership of the selected key, select **Full Control**.
3. To give the user Special Access (for example, to enable a user to access and edit registry data in the selected key but not take ownership) select **Special Access**.

See Also
Special Access Permissions on a Registry Key
How to Change Permissions on a Registry Key

Special Access Permissions on a Registry Key

When you choose *Special Access* in **Type of Access** window, **Type of Access** menu appears. Check the appropriate boxes for *Individual Permissions* when creating Special Access permission:
If all *Individual Permissions* are unchecked than user will have “No Access” permission to the key. Note that permissions are cumulative except that the No Access (Special access - None) permission overrides all other permissions.

Query Value	To read a value entry from a registry
Set Value	To set value entries in a registry key
Create Subkey	To create subkeys on a selected registry key
Enumerate Subkeys	To identify the subkeys of a registry key
Notify	To audit notification events from a key in the registry
Create Link	To create a symbolic link in a particular key
Delete	To delete the selected key
Write DAC	To write to the key a discretionary ACL
Write Owner	To take ownership of the key
Read Control	To gain access to the security information on the selected key

See Also
Registry Key Access Permissions
How to Change Permissions on a Registry Key

Select Account Menu

To select account whose permissions you want to **Change**, **Clone** or **Remove** press **…** button in **Account** window. In **Select Account** menu:

- select domain in **List Names From** window
- select account and press **Add** button. Selected account will appear in **Add Name** window
- press **OK**. Selected account will appear in **Account** window of the main menu

For help with Select Account, Global Group Membership and Find Account dialog boxes use Registry Editor Help.

Select Registry Key Menu

Permissions will be changed, cloned or removed on the key selected in **Registry Key** window for account selected in **Account** window.
To select registry key whose permissions you want to **Change**, **Clone** or **Remove** press **…** button in **Registry Key** window. In **Select Registry Key** menu:

- select registry key and press **OK** button. Selected registry key will appear in **Registry Key** window
- to select registry key of a remote computer press **Connect** button, select computer and registry key

For help with Select Computer dialog boxes use Registry Editor Help.

Changing Permissions

Permissions will be changed on the key selected in **Registry Key** window for account selected in **Account** window. New permissions will be the permissions you select in **Type of Access** window. You can set the following permissions:

1. To enable the user to read the key contents but not to save any changes made to the file, select **Read**.
2. To enable the user to access, edit, and take ownership of the selected key, select **Full Control**.
3. To give the user Special Access (for example, to enable a user to access and edit registry data in the selected key but not take ownership) select **Special Access**.

Important

If **Propagate through entire tree** option is selected:

- permission changes will affect ONLY the account selected in the Account window. Other permissions will be intact.
- permissions will be changed for all subkeys of the selected key.

See Also
How to Change Permissions on a Registry Key

Cloning Permissions

In some cases when you create a new group or user you need to assign a set of permissions for this group or user (**Target account**) similar to a set of permission you already have for some group or a user (**Source account**). The easiest way to do that is to use **Clone** function to copy a set of permissions of **Source account** to **Target account**.

Check **Propagate through entire tree** if you want the **Target account** to have identical set of permissions as **Source account** for all subkeys of the selected key.

After *Clone* is performed the **Target account** will have identical set of permissions as **Source account** for the directory or file(s) selected.

Check *Modify Auditing for Remove or Clone* in **Options** menu if you want to clone auditing.

See Also
How to Clone Permissions

Removing Permissions

Permissions will be removed on the key selected in **Registry Key** window for account selected in **Account** window.

Important

If **Propagate through entire tree** option is selected:

- permission will be removed ONLY for the account selected in the Account window. Other accounts' permissions will be intact.
- permissions will be removed for subkeys of the selected key.

Check *Modify Auditing for Remove or Clone* in **Options** menu if you want to *Remove Auditing*.

See Also
How to Remove Permissions

Log File

To choose a *Log File* use **…** button in **Log File** window to browse files.

The following *Log File* options are available:

- Full Log - to log all changes.
- Error Log Only - to log only changes that could not be made.
- No Log

You can also select *Append to Log* if you want new changes to be appended to the old log file or *Overwrite Log* to overwrite the old log file.

Log file settings stay the same even if you exit the program.

To view the log file press **View Log** button.

For help with any dialog box, choose the Help button while using the dialog box.

Modifying Auditing

Check *Modify Auditing for Remove or Clone* in **Options** menu if you want to clone or remove auditing.

Special Handling of Deleted or Unknown Accounts

In some cases a user name cannot be resolved. Normally, it happens in the following situations:

- Account has been deleted.
- Domain controller for this Account is not accessible.
- Account belongs to a different NT installation on the same machine.

RegAdmin resolves *Unknown Account* in a textual *SID* (Security ID) and deals with textual SID the same way as with a normal User Name.

To transfer all permissions of a *deleted account* to a *new account* replace deleted account the same way you would replace a normal account.

Example #1: Changing permissions

In some cases an administrator needs to change permissions on a registry key and propagate changes through key tree (replace permissions on existing subkeys of the selected key). Unlike native NT Registry Editor this program will affect ONLY selected account permissions. Other accounts' permissions will be intact.

Example

Say you have some <root key> containing two subkeys: KEY1 and KEY2 and permissions for three users: Administrator, ALICE and BOB.
Say you want to change ALICE permissions on <root key> and all its subkeys to Read.

Initial permissions:

KEY1: Administrator (Full Control), ALICE (Read), BOB (Full Control)
KEY2: Administrator (Full Control), ALICE (Full Control), BOB (Read)

Use RegAdmin:

- Select <root key> as a key
- Check **Propagate through entire tree** radio button
- Select account **ALICE** and permissions **Read**
- Press **Change** button

After program execution:

KEY1: Administrator (Full Control), ALICE (Read), BOB (Full Control)
KEY2: Administrator (Full Control), ALICE (Read), BOB (Read)

NOTE: BOB's permissions are left intact.

See Also
How to Change Permissions on a Registry Key

Example #2: Cloning Permissions

In some cases an administrator needs to create a new group or user with a set of permissions similar but slightly different to a set of permissions that already exists for some group or user. The easiest way to do that is to use **Clone** function to copy a set of permissions of the existing account (**Source Account**) to a new account (**Target Account**) and then modify permissions according to the requirements for the new account.

Example

Say you have some <root key> containing two subkeys: KEY1 and KEY2 and permissions for three users: Administrator, ALICE and BOB.
Say you want BOB to have similar permissions on <root key> and all its subkeys as ALICE.

Initial permissions:

KEY1: Administrator (Full Control), ALICE (Read), BOB (Full Control)
KEY2: Administrator (Full Control), ALICE (Full Control), BOB (Read)

Use RegAdmin:

- Select <root key> as a key
- Check **Propagate through entire tree** radio button
- Select account **ALICE** as a Source account
- Press **Clone** button
- Select **BOB** as a Target account

After program execution:

KEY1: Administrator (Full Control), ALICE (Read), BOB (Read)
KEY2: Administrator (Full Control), ALICE (Full Control), BOB (Full Control)

See Also
How to Clone Permissions

Example #3: Removing Permissions

In some cases an administrator needs to remove permissions on a registry key and propagate changes through key tree (remove permission on existing subkeys of the selected key). Unlike native NT Registry Editor this program will affect ONLY selected account permissions. Other accounts' permissions will be intact.

Example

Say you have some <root key> containing two subkeys: KEY1 and KEY2 and permissions for three users: Administrator, ALICE and BOB.
Say you want to remove ALICE's permissions on <root key> and all its subkeys.

Initial permissions:

KEY1: Administrator (Full Control), ALICE (Read), BOB (Full Control)
KEY2: Administrator (Full Control), ALICE (Full Control), BOB (Read)

Use RegAdmin:

- Select <root key> as a key
- Check **Propagate through entire tree** radio button
- Select account **ALICE**
- Press **Remove** button

After program execution:

KEY1: Administrator (Full Control), BOB (Full Control)
KEY2: Administrator (Full Control), BOB (Read)

See Also
How to Remove Permissions

Example #4: Replacing Account

The “Everyone’s” case

Unfortunately some problems in the SMB implementation allow group “Everyone” (who always exists) access to a part of your system. To reduce the accessible part of your system it is important to deny NT’s “Everyone” group access to shares, file system and registry:

1. Create a new NT user group, for example “Every User”;
2. Include all your existing users into this group;
3. Use User Manager to grant all "Everyone" rights to “Every User”.
1. Use **RegAdmin** to replace "Everyone" with “Every User” on all your drives (read only access). Propagate the permissions through the entire key tree.

To replace ALICE to BOB

1. Use **Clone** function to copy ALICE (*Source Account*) permissions to BOB (*Target Account*) propagating through entire tree.
1. Use **Remove** function to remove ALICE account propagating through entire tree.

Example

Say you have some <root key> containing two subkeys: KEY1 and KEY2 and permissions for three users: Administrator, ALICE and BOB.
Say you want to replace ALICE with BOB and remove ALICE.

Initial permissions:

KEY1: Administrator (Full Control), ALICE (Read), BOB (Full Control)
KEY2: Administrator (Full Control), ALICE (Full Control), BOB (Read)

First Step: Use RegAdmin:

1) Select <root key> as a key
1) Check **Propagate through entire tree** radio button
2) Select account **ALICE**
3) Press **Clone** button
4) Select **BOB** as a *Target* account

After program execution:

KEY1: Administrator (Full Control), ALICE (Read), BOB (Read)
KEY2: Administrator (Full Control), ALICE (Full Control), BOB (Full Control)

Second Step: Use RegAdmin:

1. Select <root key> as a key
1. Check **Propagate through entire tree** radio button
2. Select account **ALICE**
3. Press **Remove** button

After program execution:

KEY1: Administrator (Full Control), BOB (Read)
KEY2: Administrator (Full Control), BOB (Full Control)

See Also
How to Replace Account with a different Account
How to Clone Permissions
How to Remove Permissions

Security Tips

Deny Everyone's Rights

Unfortunately some problems in the SMB implementation allow group **Everyone** (who always exists) access to a part of your system. To reduce the accessible part of your system it is important to deny **Everyone** group access to shares, file system and registry:

To replace Everyone:

- Create a new NT user group, for example **Every User**;
- Include all your existing users into this group;
- Use User Manager to substitute **Everyone** with **Every User** in all rights.
- Use RegAdmin to replace **Everyone** with **Every User** propagating the permissions through the entire key tree on the following keys.:
    1. HKEY_LOCAL_MACHINE
    2. HKEY_USERS

NOTE1:
Two warning messages saying that you are tampering with product settings may appear on NT 4.0. These messages appear because permissions to NT's product information keys have been changed - this has nothing to do with the product tampering, so just ignore the messages.
NOTE2:
NT will restore everyone's read access to root keys and some subkeys after reboot. Most of the keys will remain protected.

Deny Network registry access

You can effectively "Unshare" your registry by denying access to the NETWORK group. These settings are recommended for a stand-alone Internet server or for NT server used for file sharing only.

- Use RegAdmin to give NETWORK group "Special Access (None)" rights propagating the changes through entire key tree to the following keys:
    1. HKEY_LOCAL_MACHINE
    2. HKEY_USERS

NOTE1:
Two warning messages saying that you are tampering with product settings may appear on NT 4.0. These messages appear because permissions to NT's product information keys have been changed - this has nothing to do with the product tampering, so just ignore the messages.
NOTE2:
Nobody will be able to access your registry from the network. This means that you will not be able to administer this computer from a network: User Manager, Server Manager and other built-in NT tools will not connect to the computer because of the Access Denied error. The file shares will be available to network users with sufficient permissions.

See Also
For Security Tips updates *http://www.NTsecurity.com/A2NT*

Reporting Bugs

If you experience something you think might be a bug in RegAdmin, please report it by sending a message to **RegAdmin@box.omna.com**

Thank you.

Suggestions

Please send any suggestions or requests for new features to **RegAdmin@box.omna.com** Your input is always welcome and appreciated.

Thank you