Copyright and Disclaimer

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
FileAdmin@box.omna.com

Program Description

***FileAdmin** Pro* is a part of Administrator Assistant Tool Kit (A2NT) that is 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.

***FileAdmin** Pro* is a must-have tool to properly handle File System Permissions. Unlike built-in NT security manager, **FileAdmin** allows a user to **add**, **clone**, **remove** or **modify account permissions** to a file, directory or a group of files and **propagate the changes through directory tree without affecting other accounts' permissions**.

Other key features:

- gives an administrator a center point for viewing and modifying files and directory permissions
- allows an administrator to set a similar to the existing set of permissions for a new group or
- user through **Clone** function
- allows an administrator to set permissions on *specific group of files* (e.g. executables and DLLs)
- 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

FileAdmin™ 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 ***FileAdmin*** has the following specific features:

- will not propagate changes through entire directory tree.
- the DEMO version is available for download from http://www.NTsecurity.com

How to Change Directory Permissions

Introduction

Permissions on a directory specify the type of access a *Group* or a *User* has to the directory. New files and subdirectories in the directory inherit their permissions from the directory. When changing permissions for a directory without propagating through entire tree, permissions on existing files and subdirectories are not changed. You can select **Asterisks** (*.*) to change permissions on existing subdirectories and files within selected directory. Select **Propagate Through Entire Tree** to change permissions on all existing subdirectories and their files.

Permissions are cumulative except that the *No Access* 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 *Change* permission, the *User* will have *Change* 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 the directory, you must be the *owner* of the directory or have been granted permission to do so by the owner.
- *Groups* or *Users* granted *Full Control* permission for a directory can delete files in that directory no matter what permissions protect the files.
- You can set directory permissions only on drives formatted to use NTFS.

To Change or View Directory Permissions:

- Select the directory in the *Directory* window. You can browse directories by pressing **…** button in the *Directory* window. All groups and users that have some **Type of Access** (including **No Access**) to the selected Directory and their type of access will be listed in the main window.
- Select the name of a group or user in the *Account* window. You can double click a group or user in the main window to select it or press **…** button to browse accounts not listed in the main window.
- Choose a permission from the **Type of Access** box.
- Press **Change** button.
- Confirm changes by pressing **OK** in the *Warning* prompt.

Important

If **Propagate Through Entire Tree** 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 files and subdirectories down the directory tree
- if you select **Special Access** you have to specify type of Special Access for subdirectories and files.

To remove directory permissions

To remove directory permissions select the name of the group or user in the *Account* window. 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.

See Also

Directory Access Permissions
Example #1: Changing permissions

How to Change File(s) Permissions

Introduction

Permissions on a file specify the type of access a group or user has to the file. New files and subdirectories in the directory inherit their permissions from the directory.

Permissions are cumulative except that the *No Access* 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 *Change* permission, the user will have *Change* 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 file, you must be the *owner* of the file or have been granted permission to do so by the owner.
- Groups or users with *Full Control* permission for a directory can delete files in that directory no matter what permissions protect the files.
- You can set file permissions only on drives formatted to use the Windows NT file system (NTFS).

To Change or View File(s) Permissions:

- Select the file(s) or group of files using wildcards (e.g. *.exe, *.*, etc.) in the Directory window. You can browse directories and files by pressing … button in the Directory window. All groups and users that have some Type of Access (including No Access) to the selected File(s) and their type of access will be listed in the main window.
- Select the name of a group or user in the Account window. You can double click a group or user in the main window to select it or press … button to browse accounts not listed in the main window.
- Choose a permission from the Type of Access box.
- Press Change button.
- Confirm changes by pressing OK in the Warning menu.

To remove file(s) permissions

To remove file(s) permissions select the name of the group or user in the Account window. Choose the **Remove** button.

Important

When **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 files and subdirectories down the directory tree with the same name as the file(s). For example, if you select ***C:\*.exe***, permissions will be changed for all files and subdirectories of *C:\* with the name ***.exe***. If you select **Special Access** you have to specify type of *Special Access* for subdirectories and files.

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.

See Also

File Access Permissions
Example #1: Changing permissions

How to Set Special Access Permissions

Use Standard Permissions Whenever Possible

To keep things simple use standard directory and file permissions whenever it is possible
To create a custom set of permissions use *Special Access* permissions. Remember that new files and subdirectories in the directory inherit their permissions from the directory.

You can set special access permissions on directory, all files in directory, or selected files.

To Set Special Access Permissions:

- You can set **Special Access** permissions on directory, all files in directory, or selected files.
- To set permissions on directory, select the directory in the *Directory* window.
- To set permissions on selected file(s), select the file or group of files (e.g. ***.exe**) in the *Directory* window.
- You can browse directories and files by pressing **…** button in the **Directory** window. All groups and users that have some **Type of Access** (including **No Access**) to the selected Directory or file(s) and their type of access will be listed in the *Main* window.
- Select the name of a group or user in the **Account** window. You can double click a group or user in the main window to select it or press **…** button to browse accounts not listed in the *Main* window.
- Choose **Special Access** from the **Type of Access** box.
- Select permissions in **Type of Access** menu and press **OK**.
- Press **Change** button.
- Confirm changes by pressing **OK** in the **Warning** menu.

Important

When **Propagate Through Entire Tree** option is selected, permissions will be changed for all files and subdirectories down the directory tree with the same name as the selected directory or file(s). For example, if you select ***C:\*.exe***, permissions will be changed for all files and subdirectories of ***C:\*** with the name ****.exe***. You have to specify type of *Special Access* for subdirectories and files.
For help with any dialog box, choose the Help button while using the dialog box.

See Also
Special Access Directory and File Permissions

How to Remove Directory or File(s) Permission

To remove directory or file(s) permission

- Select the directory or file(s) in the *Directory* window. You can browse directories by pressing **…** button in the *Directory* window. All *Groups* and *Users* that have some Type of Access (including *No Access*) to the selected *File*, *Directory* or *base Directory* (if asterisks are used) 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 remove. You can double click a group or user in the *Main* window to select the name of the group or user whose permission you want to remove.
- Press **Remove** button.
- Confirm changes by pressing **OK** in the *Warning* prompt.

Check **Propagate Through Entire Tree** if you want to remove permissions in all subdirectories and files of the selected directory.

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 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**.

To clone permissions:

- Select the directory or file(s) in the *Directory* window. You can browse directories by pressing **…** button in the *Directory* window. All groups and users that have some Type of Access (including *No Access*) to the selected Directory or file(s) 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* prompt.

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

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 group **Everyone**.

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* to clone *Auditing*.

See Also
Example #4: Replacing permissions

Directory Access Permissions

When you set a directory permission, two sets of abbreviations for individual permissions are displayed next to it: The permissions set on the directory and the permissions set on files in the directory. For example, when you set *Add & Read* permission on a directory, you see **(RWX)** signifying *Read*, *Write*, and *Execute* permissions on the directory, and **(RX)** signifying Read and Execute permission on files in the directory.

When access to files is shown as **(Not Specified)**, that group or user cannot use files in the directory unless access is granted by another means; for example, by setting permissions that grant access on individual files.

Note

Groups or users granted **Full Control** permission on a *Directory* can delete files in that directory no matter what permissions protect the files.

You can set the following *Standard Permissions* on directories:

No Access (None)(None)

Prevents any access to the directory and its files. No Access permission overrides all other permissions. Specifying No Access for a User prevents access even if that user belongs to a group that has access to the directory.

List (RX)(Not Specified)

Allows:

- Viewing filenames and subdirectory name
- Changing to the directory's subdirectories.

Does not allow:

- Access to files, unless granted by other directory or file permissions.

Read (RX)(RX)

Allows:

- Viewing filenames and subdirectory names.
- Changing to the directory's subdirectories.
- Viewing data in files and running applications.

Add (WX)(Not Specified)

Allows:

- Adding files and subdirectories to the directory.

Does not allow:

- Access to files, unless granted by other directory or file permissions.

Add & Read (RWX)(RX)

Allows:

- Viewing filenames and subdirectory names.
- Changing to the directory's subdirectories.
- Viewing data in files and running application files.
- Adding files and subdirectories to the directory

Change (RWXD)(RWXD)

Allows:

- Viewing filenames and subdirectory names.
- Changing to the directory's subdirectories.
- Viewing data in files and running application files.
- Adding files and subdirectories to the directory
- Changing data in files.
- Deleting the directory and its files.

Full Control (All)(All)

Allows:

- Viewing filenames and subdirectory names.
- Changing to the directory's subdirectories.
- Viewing data in files and running application files.
- Adding files and subdirectories to the directory.
- Changing data in files.
- Deleting the directory and its files.
- Changing permissions on the directory and its files.
- Taking ownership of the directory and its files.

See Also

File Access Permissions
Special Access Directory and File Permissions
How to Change Directory Permissions

File Access Permissions

When you set a file permission, a set of abbreviations for individual permissions is displayed next to it. For example, when you set *Read* permission on a file, you see *(RX)* signifying *Read* and *Execute* permission.

Note

Groups or users granted **Full Control** permission on the directory containing a file can delete the file no matter what permissions protect it.

You can set the following *Standard Permissions* on files:

No Access (None)

Prevents any access to the file. Specifying **No Access** for a user prevents access even if a User belongs to a group that has access to the file.

Read (RX)

Allows:

- Viewing the file's data.
- Running the file if it is a program file.

Change (RWXD)

Allows:

- Viewing the file's data.
- Running the file if it is a program file.
- Changing data in the file.
- Deleting the file.

Full Control (All)

Allows:

- Viewing the file's data.
- Running the file if it is a program file.
- Changing data in the file.
- Deleting the file.
- Changing permissions on the file
- Taking ownership of the file.

See Also
Directory Access Permissions
Special Access Directory and File Permissions
How to Change File(s) Permissions

Special Access to Directory, File

When you choose *Special Access* in **Type of Access** window, **Type of Access** menu appears. Check the appropriate boxes for *Special Directory Access* or *Special File Access*.

You can set the following *Individual Permissions* when creating special access permission for

Special Directory Access:	**Special File Access:**
Read (R) Allows viewing the names of files and subdirectories.	**Read (R)** Allows viewing the file's data.
Write (W) Allows adding files and subdirectories.	**Write (W)** Allows changing the file's data.
Execute (X) Allows changing to subdirectories in the directory.	**Execute (X)** Allows running the file if it is a program file.
Delete (D) Allows deleting the directory.	**Delete (D)** Allows deleting the file.
Change Permissions (P) Allows changing the directory's permissions.	**Change Permissions (P)** Allows changing the file's permissions.
Take Ownership (O) Allows taking ownership of the directory.	**Take Ownership (O)** Allows taking ownership of the file.

See Also
Directory Access Permissions
File Access Permissions
How to Set Special Access Permissions

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

Changing Permissions

Permissions will be changed on the directory or file(s) selected in **Directory** 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 on

Directories:	**Files:**
No Access (None)(None)	**No Access (None)**
List (RX)(Not Specified)	
Read (RX)(RX)	**Read (RX)**
Add (WX)(Not Specified)	
Add & Read (RWX)(RX)	
Change (RWXD)(RWXD)	**Change (RWXD)**
Full Control (All)(All)	**Full Control (All)**
Special Access	**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 files and subdirectories down the directory tree

See Also
How to Change Directory Permissions
How to Change File(s) Permissions

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 subdirectories and files of the selected directory.

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 directory or file(s) selected in **Directory** 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 all files and subdirectories down the directory tree

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.

FileAdmin 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 directory and propagate changes through entire directory tree. Unlike native NT File Manager this program will affect ONLY selected account permissions. Other accounts' permissions will be intact.

Example

Say you have some <root directory> containing two subdirectories: DIR1 and DIR2,   three files: File1, File2 File3 and permissions for three users: Administrator, ALICE and BOB.

Initial permissions:

DIR1: Administrator (Full Control), ALICE (Read), BOB (Change)

- File1: Administrator (Full Control), ALICE (Read), BOB (Change)
- File2: Administrator (Full Control), ALICE (Read)

DIR2: Administrator (Full Control), ALICE (Change), BOB (Full Control)

- File3: Administrator (Full Control), ALICE (Change), BOB (Full Control)

Use FileAdmin:

- Select <root directory> as a directory
- Check **Propagate Through Entire Tree** radio button
- Select account **ALICE** and permissions **Read**
- Press **Change** button

After program execution:

DIR1: Administrator (Full Control), ALICE (Read), BOB (Change)

- File1: Administrator (Full Control), ALICE (Read), BOB (Change)
- File2: Administrator (Full Control), ALICE (Read)

DIR2: Administrator (Full Control), ALICE (Read), BOB (Full Control)

- File3: Administrator (Full Control), ALICE (Read), BOB (Full Control)

See Also

How to Change Directory Permissions

How to Change File(s) Permissions

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 permission 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 to a new account and then modify permissions according to requirements for the new account.

Example

Say you have some <root directory> containing two subdirectories: DIR1 and DIR2,   three files: File1, File2 File3 and permissions for three users: Administrator, ALICE and BOB.

Initial permissions:

DIR1: Administrator (Full Control), ALICE (Read), BOB (Change)

- File1: Administrator (Full Control), ALICE (Read), BOB (Change)
- File2: Administrator (Full Control), ALICE (Read)

DIR2: Administrator (Full Control), ALICE (Change), BOB (Full Control)

- File3: Administrator (Full Control), ALICE (Change), BOB (Full Control)

Use FileAdmin:

- Select <root directory> as a directory
- Check **Propagate Through Entire Tree** radio button
- Select account **ALICE**
- Press **Clone** button
- Select **BOB** as a Target account

After program execution:

DIR1: Administrator (Full Control), ALICE (Read), BOB (Read)

- File1: Administrator (Full Control), ALICE (Read), BOB (Read)
- File2: Administrator (Full Control), ALICE (Read) , BOB (Read)

DIR2: Administrator (Full Control), ALICE (Change), BOB (Change)

- File3: Administrator (Full Control), ALICE (Change), BOB (Change)

See also
How to Clone Permissions

Example #3: Removing Permissions

In some cases an administrator needs to **Remove** permissions on a directory or file(s) and propagate changes through entire directory tree. Unlike native NT File Manager this program will affect ONLY selected account permissions. Other accounts' permissions will be intact.

NOTE:

If a group or user is not on a *permissions list* it is not equivalent to *No Access* permission for that group or user. *No Access* permission overrides all other permissions and if, for example, 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.

Example

Say you have some <root directory> containing two subdirectories: DIR1 and DIR2, three files: File1, File2 File3 and permissions for three users: Administrator, ALICE and BOB.

Initial permissions:

DIR1: Administrator (Full Control), ALICE (Read), BOB (Change)

- File1: Administrator (Full Control), ALICE (Read), BOB (Change)
- File2: Administrator (Full Control), ALICE (Read)

DIR2: Administrator (Full Control), ALICE (Change), BOB (Full Control)

- File3: Administrator (Full Control), ALICE (Change), BOB (Full Control)

Use FileAdmin:

- Select <root directory> as a directory
- Check **Propagate Through Entire Tree** radio button
- Select account **ALICE**
- Press **Remove** button

After program execution:

DIR1: Administrator (Full Control), BOB (Change)

- File1: Administrator (Full Control), BOB (Change)
- File2: Administrator (Full Control), BOB (Change)

DIR2: Administrator (Full Control), BOB (Full Control)

- File3: Administrator (Full Control), BOB (Full Control)

See Also
How to Remove Permissions

Example #4: Replacing Permissions

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**.
4. Use **FileAdmin** to replace **Everyone** with **Every User** on all your drives. Propagate the permissions through the entire directory trees

NOTE:

There are some special NT shares with **Everyone's** access that cannot be revoked. The best known example is NT registry itself. Use ***NTsecurity.com*** utility **RegAdmin** to replace **Everyone** with **Every User** (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.
2. Use **Remove** function to remove ALICE account propagating through entire tree.

Example

Say you have some <root directory> containing two subdirectories: DIR1 and DIR2, three files: File1, File2 File3 and permissions for three users: Administrator, ALICE and BOB.

Initial permissions:

DIR1: Administrator (Full Control), ALICE (Read), BOB (Change)

- File1: Administrator (Full Control), ALICE (Read), BOB (Change)
- File2: Administrator (Full Control), ALICE (Read)

DIR2: Administrator (Full Control), ALICE (Change), BOB (Full Control)

- File3: Administrator (Full Control), ALICE (Change), BOB (Full Control)

Step 1: Use FileAdmin:

1. Select <root directory> as a directory
2. Check **Propagate Through Entire Tree** radio button
3. Select account **ALICE**
4. Press **Clone** button
5. Select **BOB** as a *Target* account

Results 1: After program execution:

DIR1: Administrator (Full Control), ALICE (Read), BOB (Read)

- File1: Administrator (Full Control), ALICE (Read), BOB (Read)
- File2: Administrator (Full Control), ALICE (Read) , BOB (Read)

DIR2: Administrator (Full Control), ALICE (Change), BOB (Change)

- File3: Administrator (Full Control), ALICE (Change), BOB (Change)

Step 2: Use FileAdmin:

1. Select <root directory> as a directory
2. Check Propagate Through Entire Tree radio button
3. Select account ALICE
4. Press Remove button

Results 2: After program execution:

DIR1: Administrator (Full Control), BOB (Read)

- File1: Administrator (Full Control), BOB (Read)
- File2: Administrator (Full Control), BOB (Read)

DIR2: Administrator (Full Control), BOB (Change)

- File3: Administrator (Full Control), BOB (Change)

See Also

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*:

A. For a NEW installation:

1. Go to *File Manager* and give the following permissions to the **C:\** drive (propagate permissions through entire tree):

Full Control	Administrators
Full Control	SYSTEM

2. Go to ***FileAdmin*** and add **Users** group with the following permissions:

List Only	C:\ (propagate)
Add	C:\TEMP
Read	%SYSTEMROOT% (Propagate)
No Access	%SYSTEMROOT%\Config
No Access	%SYSTEMROOT%\Repair
Change	%SYSTEMROOT%\system32\Spool\Printers
Add	%SYSTEMROOT%\system32\Spool\Profiles

3. Go to ***FileAdmin*** and add **CREATOR OWNER** group with the following permissions:

Full Control	C:\TEMP
Full Control	C:\Users (Propagate)

4. Clone **Users** permissions for other than **Users** group if necessary

NOTE: This is probably the minimum permissions required for users to logon on NT and run software installed by an Administrator.

B. In an EXISTING installation:

- 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 ***FileAdmin*** to replace **Everyone** with **Every User** on all your drives. **Important**: Propagate the permissions through the entire directory tree

NOTE: There are some special NT shares with Everyone's access that can not be revoked. The best known example is NT registry itself. Use ***NTsecurity.com*** utility **RegAdmin** to replace *Everyone* with *Every User* (read only access). Propagate the permissions through entire KEY tree.

Reporting Bugs

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

Thank you.

Suggestions

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