



USB Admin Pro

Contents

SYSTEM REQUIREMENTS	2
CLIENT	2
SERVER	2
INTRODUCTION	3
PRE-INSTALLATION STEPS	3
INSTALLATION	4
INSTALLING USB ADMIN PRO ON A SERVER.....	4
USING THE USB ADMIN PRO GRAPHICAL USER INTERFACE	4
SETTINGS	4
<i>To setup a Default configuration file:</i>	4
<i>To setup an Individual Configuration:</i>	5
RESTRICT REMOVABLE MEDIA	5
LOCKOUT WARNING SCREEN	5
SCANNED DRIVE LETTERS	5
EMAIL NOTIFICATION	6
OTHER SETTINGS	6
<i>Location of Files: (UNC Path)</i>	6
<i>Custom Image for Client LockOut Screen (473 x 284)</i>	6
ENABLE A USB DISK	6
INSTALLING THE CLIENT	7
INSTALLATION ON A SINGLE COMPUTER	8
SECURING THE CLIENT	8
<i>Group Policy</i>	8
<i>Services</i>	8
<i>Local Folder</i>	8
UPDATING THE CLIENT	9
UNINSTALLING THE CLIENT	9
LOG FILES	9

System Requirements

Client

Operating System	Windows 98 or 98 SE Windows ME Windows 2000 Windows XP Windows 2003
Minimum Recommended Processor	Pentium 200 MHz
Minimum Recommended RAM	64 MB
Recommended Video Adapter (Not Required)	24-bit or higher color

Server

Operating System	Windows 98 or 98 SE Windows ME Windows NT 4.0 Windows 2000 Windows XP Windows 2003
Minimum Recommended Processor	Pentium 200 MHz
Minimum Recommended RAM	64 MB
Recommended Video Adapter (Not Required)	24-bit or higher color

Introduction

USB Admin Pro is an application that effectively restricts Removable Media. It not only restricts the media, but will also record log files locally and centrally. It will also send out critical email alerts, notifying you of someone trying to use one.

Another advantage is that you can give specific removable drives full access to any computer. For example, if you have a systems support staff, and they have thumb drives with drivers or software on them, you can enable their drives to work in any restricted computer. They won't even have to logoff or enter any passwords to use them on any computer. They would simply insert their disk, and start working. Anyone else trying to use their own disk will be greeted with an alert informing them that their removable media is not allowed, restricting use of their drive instantly. (See Figure 1.2)

This application consists of two parts: The server software, and the client software. (All included in the downloadable executable.) The server can be any file-sharing enabled computer. The client can be most any Microsoft Windows based machine.

The server share is only used when its time to install, upgrade, make changes to the configuration, or record log files from the client machine. It is used for no other purpose. It will not take up resources on the computer you install it on.

Installation on the client machines is very easy. All you have to do to install it from the client computer is to execute one file located on the Server Share. You can do this either by the login script, running it from the local machine, or remotely executing the file.

Pre-Installation Steps

- If you are going to host multiple clients, you will need to create a share on at least one centralized server. (If you are installing on only one computer, then there is no need to create a share, and installation to the default location will work.)
- In this example, we have 1 Windows Domain to host multiple clients. We will use \\server1\share for Domain1.
- Your client machines will need read rights to these shares.
- You will need only one server per Domain. (Note: a Domain is not a requirement, USB Admin Pro will work just as effective without Domains.)
- If you have multiple domains, it is best to choose one server per domain.

Installation

Installing USB Admin Pro on a Server

There are two parts to the installation of USB Admin Pro. You will install the first portion on a centralized server. Then you will install the client software from this centralized server. Use the following steps for your installation:

- Run SetupUSB.exe from your computer, or the server in which you are installing the host files on.
- When prompted for a location, type in the UNC path of the server. (Or you can use the default location “C:\Program Files\” if you are testing, or installing on a single computer.) We will type in [\\server1\share](#) for our example. Click Next.
- The following executable files will be copied to [\\server1\share](#):
- **InstallRSRV.exe** (Run from a client computer to Install the service.)
- **Rsrv.exe** (The main process that constantly runs on the client computers. This must be running to restrict Removable Media)
- **SendEmail.exe** (Used by the Client Software)
- **USBAdminGUI.exe** (Used to configure the clients. See Figure 1.1)
- Setup will automatically run USBAdminGUI.exe, which is used to setup the configuration of the clients.

Using the USB Admin Pro Graphical User Interface

Before you install the software on your client computers, it will be a good idea to setup a default configuration file, and any individual configuration files you may want.

Settings

To setup a Default configuration file:

- Make sure that the “Settings for all Computers” option is selected.
- Make the changes that you want applied to all computers as a default setting.
- Click the Save button.
- The default configuration will be used for all computers that do not have an individual configuration.



(Figure 1.1)

To setup an Individual Configuration:

- The individual configuration is used when you want specific computers to use a different configuration than the default configuration.
- Make sure that the “Individual Settings” option is selected.
- You can either load computers from a domain, or add them yourself.
- Select one or more computers from the list.
- Make your changes, and then click save.

Restrict Removable Media

- **Yes** – Enables the application on the client.
- **No** – Disables the application on the client machine. (Any user will have full access to any removable media on the computer you specify.)

LockOut Warning Screen

- **On** – Will lock the screen so the user cannot use the computer until they remove the removable drive from the computer.
- **Off** – Will not show any notifications of any kind. This option will still deny the user from accessing the removable media. (This option is still secure, but choosing “On” is recommended)



(Figure 1.2)

Scanned Drive Letters

The client software will scan drives B: through Z: by default. It is recommended that you leave it at the default setting. If you select drive A: as the Start Scan Drive Letter, all computers that have a floppy drive installed as Drive A: will be locked out if you have the LockOut Warning Screen enabled. Since the Removable Media is installed as drive D: through Z: by default, it will be safe to scan drives B: through Z:.

Email Notification

- **On** – Will send an email to the specified email account using an email server that you specify. When a user inserts an unauthorized removable drive, the client software will immediately send an email to the specified email account. This also works great to send text pages to cell phones and pagers.
- **Off** – Will not send an email notification. However, the client will still write to a local log file, and a central log file when a user inserts an unauthorized removable drive.

Other Settings

Location of Files: (UNC Path)

Type in the UNC Path ([\\server1\share](#)) of the location of the USB Admin Pro Graphical User Interface. You can click the “Use Current Directory” button if you opened the GUI using a UNC path. If the path includes drive [C:\](#) in the path, your clients will not be updated properly. Make sure the path points to a location that all clients will be able to see. ([\\server1\share](#))

Custom Image for Client LockOut Screen (473 x 284)

You can type in the path, or browse for a customized image to use for the LockOut Warning Screen. Use an image that is 473 x 284 or less in size. You can use a UNC path or a Local path.

Enable a USB Disk

This button is located at the top of the application. This will allow you to enable any Removable Drive to use on any computer that has been restricted. This is a valuable feature for an administrative support staff, since they can use Removable Media on any computer without the need of logging off or entering passwords.

****Note:** If you do not use the Administrative Graphical User Interface (Figure 1.1) to configure the settings before client installation, the clients will have the factory default settings enabled.



(Figure 1.3)

Installing the Client

USB Admin Pro runs as a system service on Windows 2000 or higher computers. It can also be used to secure Windows Systems older than 2000, but must be run via the login script or startup folder.

To install on Windows 2000 or higher:

- Make sure your logged into the client machine as a member of the local administrators group. (If installing with InstallRSRV.exe)
- Browse to the Server Share ([\\Server1\Share](#))
- Find and execute InstallRSRV.exe. (Use “InstallRSRV.exe /silent”, for silent mode)
- If you are installing with a login script, local Administrative rights is necessary. However, not all clients have administrative rights to the local computer. We have included an installer you can use instead of InstallRSRV.exe. The installer is called InstallAsAdmin.exe, and is in the same directory as InstallRSRV.exe. Do the following to install with local administrative privileges:
 - Edit csetup.ini to include the username, password, and computername or domain name of an account that will have local administrative rights to all of your client computers. The first 3 lines should read as follows:
 1. UserName
 2. Password
 3. DomainName or ComputerName (You can use a period [.] as a wildcard if installing on multiple computers.)
 - Then execute InstallAsAdmin.exe.
 - This will do the same thing as InstallRSRV.exe, but with the rights of the user that you specify in csetup.ini. This way, you can install very easily via a login script, and wont have to worry about the user having rights to the machine.
 - ****After your finished installing, it is recommended to erase the contents of csetup.ini for security purposes.**
- That’s it! It will install itself as a system service, and will always run, even if the computer is logged out.
- It is now ready to test. Insert a Removable Disk and watch what happens.

To run on a computer older than Windows 2000:

- Use InstallRSRV.exe, which will automatically run rsrv.exe at system startup.
Or:
 - Execute the following file from a login script or system startup:
 - Rsrv.exe ([\\Server1\Share\Rsrv.exe](#))

Installation on a Single Computer

You can use this software on a single computer if desired. The Server side and Client side will exist on the same machine. Do the following to install on a single computer:

- Run SetupUSB.exe from your computer.
- When prompted for a location, accept the default location, or choose your own.
- Setup will automatically run USBAdminGUI.exe, which is used to setup the configuration. *(Optional)*
- *(Optional Step)* After the Administrative Console is open (See Figure 1.1), make sure the “Settings for All Computers” option is selected, make the desired changes, and click “Save.”
- Run InstallRSRV.exe on the computer you installed it on. (Windows NT based computers only.)
- It is now ready to test. Insert a Removable Disk and watch what happens.

Securing the Client

Securing the client is an optional step. It is only used to provide added security.

USB Admin Pro is more secure on computers running Windows 2000 or higher. If the user does not have local administrative privileges, then it is already secure.

If the user has local administrative rights, you can do all of the following to completely secure the system:

Group Policy

- Enable “**User Config/Administrative Templates/System/Ctrl+Alt+Del Options/Remove Task Manager**”

Services

- Change access for the user or group to have no Read rights, or Deny on the following file: “C:\Windows\System32\services.msc”

Local Folder

- Change permissions on the following folder to give **Administrators** and the Local **SYSTEM** account Read and Write rights only. Remove everyone else: “C:\Programs Files\NTRDS\”

Updating the Client

You will need to Update the client anytime you make a change using the GUI. You will also need to Update the client whenever you download a newer version. Updating the client is very easy. Do the following to update the client:

- Run `C:\Program Files\NTRDS\Update.exe` from the Client machine (Can be either manually, through a login script, or remotely executed.)
- You can also run `Update.exe` with the ***/silent*** command to run an update undetected. (*C:\Program Files\NTRDS\Update.exe /silent*)

If your client requires Administrative Rights to the local machine, or if you are installing with a login script, do the following to update the client:

- Make sure `csetup.ini` on the server ([\\server1\share\csetup.ini](#)) is present, and has the username/password of the user who has administrative rights to your client machines. (See *Installing the Client* on page 7 for details on how to setup `csetup.ini`)
- Run `C:\Program Files\NTRDS\UpdateAsAdmin.exe` from the Client machine (Can be either manually, through a login script, or remotely executed.)
- You can also run `UpdateAsAdmin.exe` with the ***/silent*** command to run an update undetected. (*C:\Program Files\NTRDS\UpdateAsAdmin.exe /silent*)

**** (Security Note:** Be sure to remove the contents of `csetup.ini`, or at least deny read rights to `csetup.ini` after you are done with updating or installing.)

Uninstalling the Client

You uninstall the client by running the following command from the client:

- `C:\Program Files\NTRDS\rsrv.exe /u`

This will uninstall the service. It is now safe to remove the NTRDS directory.

Log Files

Log files are stored both on the client, and on the server directory.

- On the client, it is located in the `C:\Program Files\NTRDS\log.txt` file by default.
- On the Server, it is located in the server share directory as `log.txt`. If you want all of your clients to record log files to this central log file, then you will need to give the computer account the appropriate write rights to the `log.txt` file, or the share itself.