The Ataman™ Rlogind Service User's Manual

IMPORTANT:
Read the *Security Considerations* section before you install rlogind.

Overview

The Ataman Rlogind Service provides an implementation of the rlogin protocol defined in the Internet document, RFC 1282. The Ataman Rlogind Service allows users with a client rlogin program to logon to Windows NT systems. Users logon using the same password used in normal Windows NT user authentication. User processes started via this remote logon session run in the security context of that user. Additionally, if their rlogin client provides support for ANSI terminal escape sequences, users may run full-screen console apps, such as text editors. Rlogin clients that use ANSI escape sequences include, but are not limited to, those that emulate the following terminal types: VT100, VT220, xterms, xterm.

The Ataman Rlogind Service is distributed as shareware. It is not free! However, it is provided in a form that lets you try it out before you pay for it. If you are not familiar with the concept of shareware, see the **Shareware** section below.

Registered users of the Ataman Rlogind Service also receive the Ataman Rexecd Service. This service implements the "rexec" protocol found on many Unix systems. Also provided to registered users is the C programming language source code of an rexec client program suitable for porting to any Unix system you might have that does not provide an rexec client. Due to the many possible places and conditions this rexec client program might be used, it is provided without technical support. If you have experience in porting code between Unix systems, you may find it a convenience.
With an eye towards enhancing the software's compatibility with future versions of Windows NT, Ataman Software programmed these services using **no** undocumented Windows NT calls!

Shareware

The Ataman Rlogind Service is distributed and marketed via a method known as

shareware. The main characteristic of shareware is that the vendor of software allows a user to try a product before they actually buy it. The amount of time a user is allowed to try the software is known as the evaluation period. At the end of the evaluation period the user of the software is required either to buy the software or to stop using the software.

A side effect of the shareware method is that shareware vendors actually encourage you to copy and share the software with your friends and associates. In this manner, they too can decide whether or not the software fulfills their needs in a way that justifies its price. The important points here are that you can evaluate the product for free and you can give a free copy to your friends. However, payment must be sent to Ataman Software if they or you decide to continue to use the software after the evaluation period.

Users that have paid are called "registered" users and receive the latest version of the software and a "registration code" that allows them to use the software free of payment reminder screens and other forms of reminders. Ataman Software has designed its registration code with an additional feature. Later, if you acquire a new update of the product through shareware distribution channels (and if the new update is not a major revision of the product) then you will be able to use the same registration code with the new version.

If after trying the Ataman Rlogind Server you decide it meets your needs, the file `order.txt` provides the information necessary to purchase the product. If the copy of the Ataman Rlogind Service you have is missing that file, please contact Ataman Software. (See the **`Contacting Ataman Software's Technical Support`** section near the end of this document for contact information.)

Security Considerations

Microsoft Windows NT is not currently implemented with full support for remotely logged in users. While the Ataman Rlogind Service does allow users to remotely logon within their own security context, several security issues remain.

The discussion below also applies to the Ataman Rexecd Service.

Potential problems of interaction with the "local" user logged onto the main console.

Shared drive maps.

The remote user and the local user share the same "drive map". In other words the letters assigned to the various local and remote drives are shared between the local and remote users. If one user changes the map with "net use", "subst", etc., the other user is immediately (and without warning) affected by that change.

While the users do access the files through this map using their own security context, security issues still exist. For example, if the local user runs programs from a remote drive, the remote user may be able to redirect that drive to another location. Possibly

causing the local user to execute functions they did not intend. This is a potentially serious security hole often referred to as a "Trojan horse" attack.

Random message boxes appearing on the main console.
Windows NT does prevent remote users from starting up windowed apps. However, the startup of such apps may cause initialization failure messages boxes. These message boxes pop up on the main console... potentially confusing the locally logged on user.

Along the same lines, a remote user should not use the "start" command as this command will cause a new console window to be created. Worse, under Windows NT 3.1, this console window will be visible... providing the user logged in locally with a command prompt that is running under the security context of another user.

Random sounding of the system bell.
Remote users running programs may cause an action that requests a bell to ring. Because Windows NT provides no mechanism to redirect this function, the bell sounded will be the system bell normally associated with the main monitor. To locally logged users, this bell will seem to ring at random... possibly leading them to believe they have made a mistake.

The dangers of clear text passwords.

Many users of rlogin and rexec on Unix systems do not realize it, but the rlogin and rexec protocols send your account and password over the network wires unencrypted. The Ataman Rlogind Service and the Ataman Rexecd Service suffer from this same limitation. Before using this service you should assess the security risk that someone might monitor your network wires and thereby obtain the accounts and passwords sent by both protocols in "clear" (unencrypted) text.

No cleanup of child process.

Windows NT provides no way for a parent process to know about the children of its child processes. Further, no method of cleanly killing another process is provided. (There is a kill provided, but that kill does not notify DLL's that are attached to the killed process of the exit. This potentially leaves dead data inside those DLLs.) The net effect is that it is not possible for the rlogind and rexecd services to do cleanup. It is important that remote users be aware that they should always logout by exiting any applications they are running and typing the "exit" command to the command prompt.

Over a period of time, "orphaned" processes from remote users will likely take up an unacceptable amount of system resources. At this time the only known solution to the problem is to reboot the system. For systems that are used heavily by remote users, it may be advisable to schedule reboots on a regular basis.

Other issues.

The issues above are only the ones thus far discovered. As the current Windows NT implementation does not fully support remotely logged on users, it is quite likely that

new security holes will be found. In short, users allowed to remotely logon using the Ataman rlogind or rexecd services should be limited to those that are trusted enough that it can be assumed that they can potentially gain privileged access to the system. The installation section below covers the mechanism used to restrict the users allowed to logon.

Installation

Installation must be performed from an account that has Adminstrators or Doman Admins privilege levels.

On the system that you wish to install the Ataman Rlogind Service create a directory that is local to that system. For example:

```
mkdir c:\ataman
```

The directory you create must have its permissions set such that the executable (*.exe) files can be read and executed by the SYSTEM account and all user accounts that will be allowed to remotely logon. All directories in the path to the executables must be searchable by those accounts.

Change your working directory to this new directory and unzip the archive into this directory.

To install the rlogind service type:

```
rlogind install start
```

If you have registered your copy, then you will have also received a copy of the Ataman Rexecd Service. It is installed in the same manner:

```
rexecd install start
```

You now need to give those users that you want to allow to remote logon permission to "Log on as a Service". **IMPORTANT:** You must have previously read the **Security Considerations** section before taking the next step!

If you are not running on a Windows NT Advanced Server machine, you can do this by:

- Run the "User Manager" program located in the "Administrative Tools" program group.
- Select the "User Rights" item in the "Policies" Menu.
- Click the "Show Advanced User Rights" check box, then scroll the "Right:" drop-down list until you get to "Log on as a service" entry.
- From here you can then add those users or groups you wish to allow to logon remotely.

If you are running on a Windows NT Advanced Server machine, you can do this by:

- Run the "User Manager for Domains" program located in the "Administrative

Tools" program group.

- If you want to allow users to logon remotely to the system on which you are running Advanced Server, make sure the title bar on the "User Manager for Domains" window read: "User Manager - _Your_Domain_Name_". If it does not, select the domain for which your system is the domain controller by selecting the "Select Domain" item in the "User" menu.
- If instead you want to allow users to logon remotely to another system that is not running Advanced Server, select the "Select Domain" item in the "User" menu. In the dialog box where it says "Domain:", type "\\MachineName" where "MachineName" is the host name of the system for which you wish to edit privileges. Once you push the "OK" button, you will then be able to edit the privileges for that system.
- To clarify the last two points: user rights are assigned on a per system basis. Thus on every system to which you wish to allow remote logons, you must edit the user rights for that system. Editing the user rights for the domain affects only the user rights on the domain controllers for that domain.
- Select the "User Rights" item in the "Policies" Menu.
- Click the "Show Advanced User Rights" check box, then scroll the "Right:" drop-down list until you get to "Log on as a service" entry.
- From here you can then add those users or groups you wish to allow to logon remotely.

Removal

Ataman Software is committed to making the use of its software as easy as possible for the end user. Most users prefer software that removes as easily as it installed, thus we provide a procedure to uninstall the software. The uninstall procedure removes the service and all associated registry entries. It does not remove the disk files as you may simply be moving the software to a different machine.

If you need to remove the Ataman Rlogind Service from your system, type:

```
rlogind stop remove
```

If you need to remove the Ataman Rexecd Service from your system, type:

```
rexecd stop remove
```

You may also wish to remove the user rights to "Log on as a service" you added when you installed the services. To do this follow the instructions in the Installation section; selecting remove instead of add.

Registration

What is registration.

If after evaluating the Ataman Rlogind Service you find it meets your needs, you need to purchase a license to use the product. Ordering information can be found in the file

`order.txt`. If this file is missing, please contact Ataman Software using the information found in the **`Contacting Ataman Software's Technical Support`** section near the end of this document.

Once Ataman Software has processed your order, you will receive a diskette containing the latest version of the software and a **registration code**. This registration code acts as a key to the software. It instructs the software that you are now a registered user and that it should disable payment reminders and other reminder features designed to insure that evaluating users not use the software beyond the evaluation period.

One nice feature of the registration code is that if you later acquire a newer version of the product through shareware channels (and the newer version of the product is not a major revision), then you will be able to use your registration code with this newer version. (Major revisions to a product add significant new features to the product and thus normally require an upgrade price. Ataman Software will notify all registered users when a new major upgrade is available. Minor upgrades generally contain fixes and minor enhancements.)

Registration codes are tied to the name of the registered user and cause the product to list that user as the proper licensee of a product. You should never share your registration code with another user as it will be your name that must appear as the licensee of that copy for that registration code to work.

How to register your copy.

Registering the Ataman Rlogind Service is simple. In filling your order, Ataman Software will send you a diskette containing the latest version of the product. Remove the old version using the information found in the **Removal** section above. Then install the new version using the **Installation** section above. In the directory where you installed the new version, you will find a program called "`register.exe`". This program allows you to install the registration information so that the Ataman Rlogind Service will know that you are a registered user.

To use "`register.exe`", start a command prompt and use the information provided in the letter of registration that arrived with your diskette to issue the following command:

```
register rlogind "Name of Registered User" registration_code
```

The two quotes (") above must be used if the name of the registered user is more than one word. You should replace *`Name of Registered User`* with the name listed beside the "Registered User:" entry in the registration letter and replace *`registration_code`* with the code listed beside the "Registration Code:" entry. (Typically the *`Name of Registered User`* will be either your name or your company's name.) Be sure to list the name spelled as shown in the letter, even if there is a mistake in spelling because the registration code is time to that spelling of the name.. (If a mistake in spelling has occurred, contact Ataman Software's Technical Support and a new code will be issued.)

The Ataman Rlogind Service needs to be restarted before the registration become

effective, you can either reboot your system or issue the following command:

```
rlogind stop start
```

Be sure to save your registration information. You will need it any time you reinstall the software.

Using the Ataman Rlogind Service

Logging On: Simple vs. Advanced.

After connecting to the rlogind service and giving your password you will see the following prompt:

```
Use advanced features (requires ANSI terminal emulation)? (y/n) [x]?
```

This prompt lets you select between the simple and advanced modes of the Ataman Rlogind Service. If you want to use the advanced mode type y'; to use simple mode use n'. The default value shown as "[x]" will be y' if your client program reports a terminal type of "vt100", "vt220", "ansi", "xterm", or "xterms". It will be n' otherwise. The default value is selected by typing the <return> key.

Advanced Mode.

This mode allows you to run full-screen console programs such as text editors. In order to use this feature your client program must support ANSI terminal escape sequences. ANSI escape sequences are used by most terminal emulation programs. In general if you are running a program emulating a VT100 or VT220 terminal or the "`rlogin`" program when running from inside the "`xterm`" program that comes with most Unix systems, you will be able to use the advanced mode.

The full range of DOSKEY-style command line editing is available in advanced mode. See the **Sending Special Keys** section below for information about how to send keys such as "Home".

Due to the manner in which Advanced Mode works (and the fact that the Win32 API does not provide good facilities for remote logon) the ^S and Pause keys do not suspend output as they do in a local command prompt window. If you are issuing a command that will have more than one screen of output... piping its output to the Windows NT "`more`" command is advisable.

Example:

```
type longfile.txt | more
```

If you are logging in remotely and are coming in over a slow link, such as a modem, you may want to choose simple mode, even if your client program can support advanced mode. Simple mode is much less data intensive and if you are not going to make use of full-screen console programs, it will work much faster over slow links.

Simple Mode.

Simple mode allows you to use most console-mode programs that read from standard input and write to standard output.

Limited command line editing is available in simple mode:

<ESC>, ^U	Erase the current line.
^H, ^?	Erase the last character typed.
^C	Interrupt Process (as in CMD.EXE).
^S	Suspend Output (as in CMD.EXE).
^Z	Send End Of File (as in CMD.EXE).

Account Naming Issues

Windows NT account names can exist in several name spaces. For example a Windows NT station in an Advanced Server domain has a local "Administrator" account and also has a corresponding "Administrator" account in its default domain. The Ataman Rlogind Service and the Ataman Rexecd Service use the following rules to disambiguate account names:

- If the account name is qualified (contains a backslash), the name preceding the backslash is first treated as a domain name, if there is no corresponding domain, then it is treated as a machine name. (Example: "MainDomain\Adminstrator").
- If the account name is not qualified (does not contain a backslash), the name is first looked up on the local machine. If the account name is not found, it is then looked up in the default domain of the machine.

The rlogind protocol was defined in a Unix environment where its limitation of 16 characters in an account name was generally not a problem. Unfortunately, this is too weak to accommodate Windows NT account naming. In attempting to overcome this problem, the Ataman Rlogind Service and the Ataman Rexecd Service do not enforce the 16 character limit. And fortunately most rlogin / rexec clients do not enforce this limit either. If you are trying to use an account name that is longer than 16 characters and are getting unexpected failures, try using an account with a shorter account name. This will help you to determine if the problem is cause by your client program truncating the account name to 16 characters.

User Environment.

When users logon, their environment will contain all system-wide environment variables that are set on the local system. They will not receive their normal user environment settings (the Win32 API does not provide this ability). To circumvent this omission in the Win32 API, the Ataman Rlogind Service and the Ataman Rexecd Service automatically set the following environment variables:

USERDOMAIN	The domain name in which the user account is defined.
USERNAME	The account name of the user.
HOMEPATH	The path name of the home directory of the user. If the user's home directory is a remote path, then this will contain the Universal Naming Convention (UNC) name of the user's home

directory.

HOMESHARE — Always set to NULL. See the comments on remote directories below.

HOMEDRIVE — If the user's home directory is local, this contains the drive letter followed by a colon. If the home directory is remote, this is set to NULL.

Because the remote user shares the drive map with all other users, it is not possible to automatically mount a remote user's remotely named directory on its normal drive letter. However many sites may wish to establish conventions whereby remote users are allowed to use certain drive letters remotely. Further, other environment variables may need to be set at logon. Thus both the Ataman Rlogind Server and the Ataman Rexecd Server execute the file "`remote.cmd`" if present in the user's home directory. Because the usage of rexec normally needs uncorrupted output, it is advisable to have the first line of "`remote.cmd`" be "`@echo off`".

If a remote user's home directory is specified as a remote directory, the user's initial directory will be "C:\". If desired, this can be overridden in "`remote.cmd`".

The TERM variable.

When in simple mode, the value passed in by your client program is put into the **TERM** environment variable. Under advanced mode programs work best if they do not use terminal escape sequences, but instead use the native Win32 Console API. For this reason the **TERM** variable is not set in advanced mode.

Sending Special Keys – (Advanced Mode Only).

The rlogin protocol is defined only over the ASCII character set. However, many DOS, OS/2 and Windows NT applications expect the availability of keys defined outside the ASCII set. Unfortunately, there is no ANSI specification for special keys. In place of such a standard, the sequences below were adopted in the hope that they were reasonably easy to generate manually and as easy as possible to remember.

Check the documentation that came with your client rlogin program. Many such programs contain the ability to create keymaps.

Character Sequence Typed	Special Character Generated
`^A^A`	^A
`^A^R`	Causes the screen to be redrawn.

For applications that work in line input mode (for example the Command Prompt itself) ^R alone works too.

`^Au`	Up Arrow
`^Ad`	Down Arrow
`^Al`	Left Arrow
`^Ar`	Right Arrow
`^Ai`	Insert

^Ax	Delete
^Ah	Home
^Ae	End
^Ap	PageUp (Previous)
^An	PageDown (Next)
^A1	F1
^A2	F2
^A3	F3
^A4	F4
^A5	F5
^A6	F6
^A7	F7
^A8	F8
^A9	F9
^A0	F10
^A-	F11
^A=	F12

Screen buffer size limits.

Due to both the method used to copy the console screen buffer to the remote screen and an internal limit in a Win32 API call used to perform the copy, screen buffer sizes are limited to a maximum of 60 lines and 132 columns. If the Ataman Rlogind Service is used via slower links (for example over a 14.4K modem), performance will be best when using smaller screen buffer sizes.

Manual resize necessary when screen buffer size is changed on the server end.

The rlogin protocol provides no means for a server to communicate a size change to a client. Thus if you run a DOS or OS/2 character mode application (which can automatically cause screen buffer size changes) or use an application that explicitly changes the size of the screen buffer (for example the “mode con” command), you must manually resize the client to match the change in the screen buffer size.

Provided that your client rlogin program implements feature, size changes initiated via resizing the client window, will be passed to the rlogind server. This will cause the remote screen buffer to be resized to match the client.

To check the size of your remote screen buffer use the “mode con” command with no additional arguments.

Using the Ataman Rexecd Service

The Ataman Rexecd Service is used by invoking an rexec client program of your choosing. The discussion of Account Naming Issues and User Environment for Ataman

Rlogind Service above applies here as well.

Troubleshooting / Technical Support

List of known problems.

Input to DOS/OS/2 1.X programs reading directly from the keyboard fails.
Under Windows NT 3.1, DOS and OS/2 1.X programs that read directly from the keyboard, rather than from standard input, are unable to receive input via the mechanism used by the Ataman Rlogind Service. This is a problem with Windows NT, and as of this writing has been fixed in the current beta of Windows NT 3.5. It is therefore expected that the problem will not exist under the upcoming Windows NT 3.5 release.

Remote users use CPU time even when they are idle.
This occurs only when using rlogind in Advanced Mode and is not a problem, but rather an artifact of the method used to provide full-screen support. Windows NT does not have inherent remote full-screen support but does provide a means to read the screen's current contents. In order to provide a remote snapshot of the current screen's content, the screen has to be examined periodically to see what changes (if any) have occurred. If the CPU usage by remote users proves too much of a load, consider having some of your remote users use Simple Mode.

WinQVT keeps reporting that remote logon has failed.
WinQVT version 3.94 does not work properly with the rlogind services of most systems. WinQVT version 3.97 fixes that problem and works fine with the Ataman Rlogind Service. Thus we recommend contacting the makers of WinQVT for an upgrade.

Contacting Ataman Software's Technical Support.

Free technical support is provided exclusively via electronic mail. From CompuServe the address is: 70363,1373. From the Internet use: 70363.1373@compuserve.com.
Technical support can be made available via other mechanisms on a fee basis,. However, the electronic mail support will have equal priority to the fee-based support and should be used if at all possible.
To arrange alternate fee-based technical support contact:

Ataman Software, L.C.
1338 Foothill Drive, #303
Salt Lake City, UT 84108
(801) 583-9132

Bug fixes are worked into minor releases that are distributed on the Internet and CompuServe via standard shareware distribution channels. You may also obtain the latest version from Ataman Software for a distribution fee. You only need to obtain one copy to upgrade all the copies for which you have a license. You may share the upgrade with other registered users. Your registration code will work with all minor version releases.

Only the latest major release version is eligible for full technical support. When a new

major version is released, support for the old version will be phased out over a 3 month period.
