OPPORTUNISTIC LOCKING

Opportunistic Locking is a feature within Windows NT-based computers such as Windows NT 4, Windows 2000, and Windows XP Professional. Windows XP home edition, which is based on the Windows NT kernel, will more then likely have opportunistic locking as well. Other file server products, such as Netware and Samba under Linux also have opportunistic locking which must be disabled.

On any machine that is housing the files opportunistic locking must be disabled. By default Opportunistic Locking is enabled under all Windows Operating Systems. Samba under Linux and most Netware Versions are also enabled by default and must be addressed to ensure data integrity.

It is recommended that the client keys be modified on all machines; however this is not required as long as the machine that is housing the files has the server service keys set to disable opportunistic locking.

Note: The registry key does not have to exist in order for the default value to be used.

Client Service Keys

The location of the client registry entry for opportunistic locking has changed in Windows 2000 from the earlier location in Microsoft Windows NT. In Windows 2000, the registry entry that disables opportunistic locking is:

Windows 2000
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MRXSmb\Parameters\
OplocksDisabled REG_DWORD 0 or 1
Default: 0 (False) Meaning that Oplocks are not disabled.

Windows NT
\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters
UseOpportunisticLocking   REG_DWORD   0 or 1
Default: 1 (true)

Server Service Keys

You can also set the Windows server service to deny the granting of opportunistic locks by setting the following registry entry on the machine functioning as the server. Even if the client has opportunistic locking enabled the server will not grant the lock on the files.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters
EnableOplocks REG_DWORD 0 or 1
Default: 1 (true)

With opportunistic locking, if a file is opened, the redirector requests an opportunistic lock of the entire file. As long as no other process has the file open, the server will grant this oplock, giving exclusive access to the specified file. This allows read-ahead, write-behind, and lock-caching, as long as no other process tries to open the file.

When a second process attempts to open the file, the original owner will be asked to Break Oplock or Break to Level II Oplock. At that point, the redirector must invalidate cached data, flush writes and locks, and release the oplock, or close the file.

Opportunistic locking level II, provides a method for granting read access to a file by more than one workstation, and these workstations can cache read data locally (read-ahead). As long as no station writes to the file, multiple stations can have the file open with level II oplock. ACT! uses multiple files and locks the information on a record level. The reading and writing of data to these files is controlled by the ACT! program. This is why opportunistic locking can destroy an ACT! database.

MORE INFORMATION - An illustration of how level II oplock work in Windows with an ACT! database:

- User 1 opens the database, requesting oplock from the machine that houses the files. Since no other station has the database open, the server grants station 1 exclusive oplock. (read and write access to the files)

- User 2 opens the database, windows has opportunistic locking enabled so the machine requests oplock on the database. Since station 1 has not yet written to the file, the server asks station 1 to Break to Level II Oplock.

- User 1 complies by flushing locally buffered lock information to the server and informs the server that it has Broken to Level II Oplock (read only access)

- The server responds to User 2's open request, granting it level II oplock. Other users can likewise open the file and obtain level II oplock.

- User 2 (or any user that has the file open) sends a write request and the server returns the write response to the files.

We believe the problem with opportunistic locking and ACT! is the incorrect write order to the files which first destroys the index files and then generally the information in the .BLB file.

Another way to explain the problems would be to compare opportunistic locking to pcAnywhere where the data is written at the file level and not the record level.

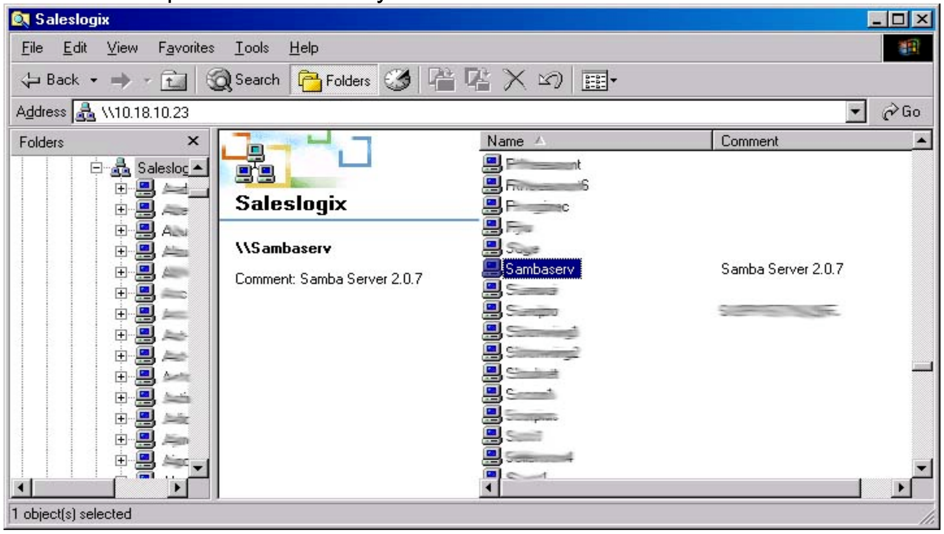
SAMBA RUNNING UNDER LINUX

Samba also has Level I and Level II opportunistic locking. An easy way to disable this is through the Browser Configuration Tool called SWAT. SWAT is included with most releases of Samba and updates to Samba can be downloaded from www.samba.org if they are running an older version. While we do not officially support Samba as a method of serving an ACT! database tests show that with opportunistic locking disabled Samba functions in the same way as an Windows NT machine serving the files.

To disable opportunistic locking under Samba, run the SWAT utility (a web-based Samba configuration utility) by going to *http://localhost:901* on the Linux machine.

- When prompted for login to the system login as the “root” user.
- Click on the shares button at the top of the page.
- To the right of where it says “Choose Share,” select the share that you are using for the ACT! database files from the drop-down and click on “Choose Share”.
- Click on Advanced View.
- Set the following under the advanced options for the share.
- **fake oplocks NO**
- **oplocks NO**
- **level 2 oplocks NO**

When Samba is correctly configured the machine will show up under Network Neighborhood. Below is the test server I setup called “Sambaserv”. You can access this share and map the drive like any other Windows shared drive.



Address: \\10.18.10.23

\\Sambaserv

Comment: Samba Server 2.0.7

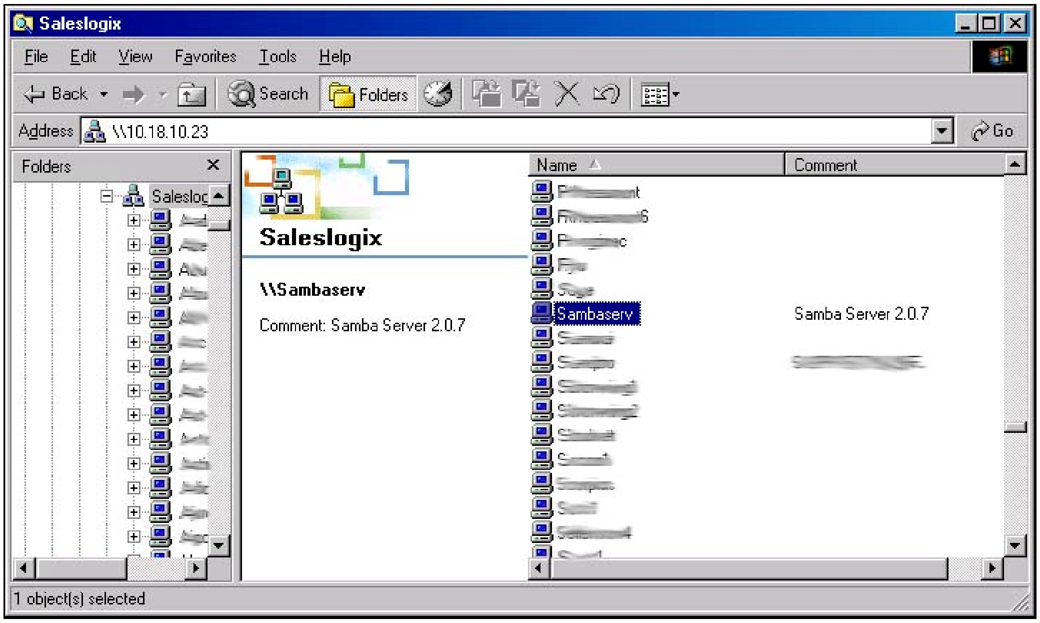
Name	Comment
Sambaserv	Samba Server 2.0.7

1 object(s) selected

NOVELL NETWARE AND OPPORTUNISTIC LOCKING / TRUE COMMIT

Your computer must run a NetWare redirector to see a Novell NetWare network. In computers running Windows this redirector is called Client Service for NetWare or Gateway Service for NetWare. This service allows access to NetWare servers and there resources.

The Opportunistic Locking option is Off by default. However you will need to set True Commit to on. This setting specifies whether file writes should be written to the server's disk immediately. Setting the value of this parameter to On guarantees data integrity when processing critical data. The default for True Commit is Off.



Address \\10.18.10.23

\\Sambaserv

Comment: Samba Server 2.0.7

Name	Comment
Sambaserv	Samba Server 2.0.7

1 object(s) selected

Modify the Clients Advanced setting by doing the following:
1. Exit all programs.
2. Right-click the Network Neighborhood icon and choose Properties from the shortcut menu.
3. Double-click on the Client 32 NetWare Client (or select it and click Properties).
4. Click the Advanced tab and ensure the following settings are in effect:

cache writes=off
file cache level=0
true commit=on

CITRIX METAFRAME RUNNING UNDER WINDOWS TERMINAL SERVER

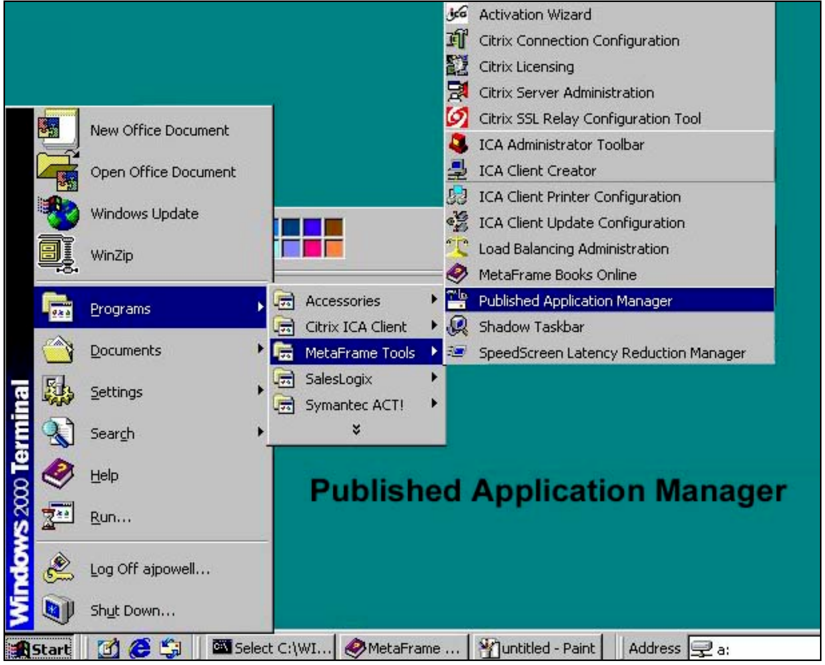
Officially, we do not support running ACT! on a Citrix server. Some problems that we have encountered include linking to Outlook as the email client and printing from a local printer while connected through Citrix.

To run ACT! on a Citrix server you will need to log into the Citrix server as a user with Administrator access and you will need to change to install mode.

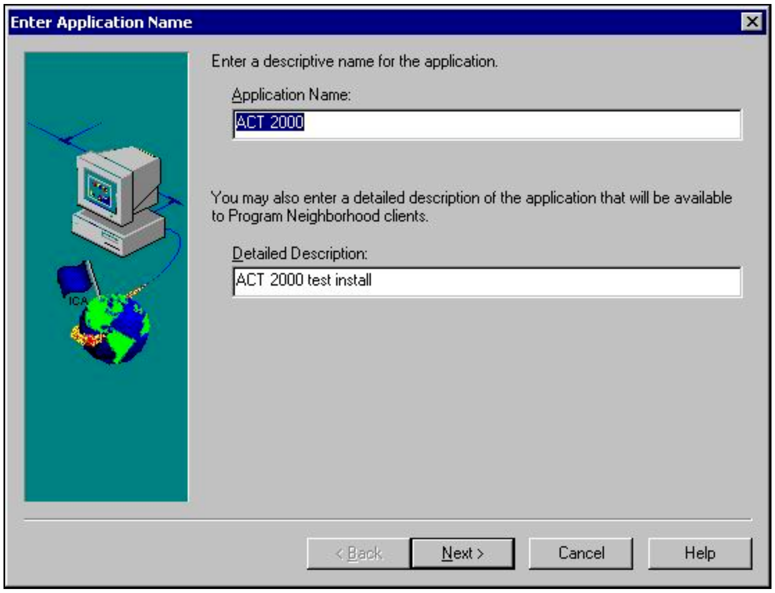
1. This is done by running the following from the command prompt: **change user /install.** You will then receive the message, "**User session is ready to install applications".**
2. Next you will install ACT! 2000 on the system in the same manner as a standard install. When installing ACT!, you will want to make sure you select the option "For all users" when prompted.

3. After installing ACT!, you will want to change back to "execute mode" by running the following at the command prompt: **change user /execute.**

4. The next step will be setting up the Application for use over Citrix. To start the setup process you will need to run the "Published Application Manager"



5. Here we enter the Application Name and Detailed Description that will be used within Citrix forACT!



Enter Application Name

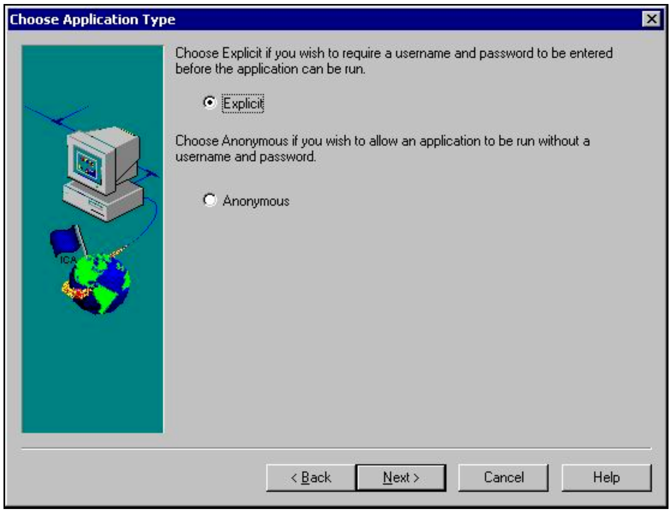
Enter a descriptive name for the application.

Application Name: ACT 2000

You may also enter a detailed description of the application that will be available to Program Neighborhood clients.

Detailed Description: ACT 2000 test install

6. You have the option of using Explicit or Anonymous access to the application. If set to Anonymous no login will be required to start ACT! This is not recommended



Choose Application Type

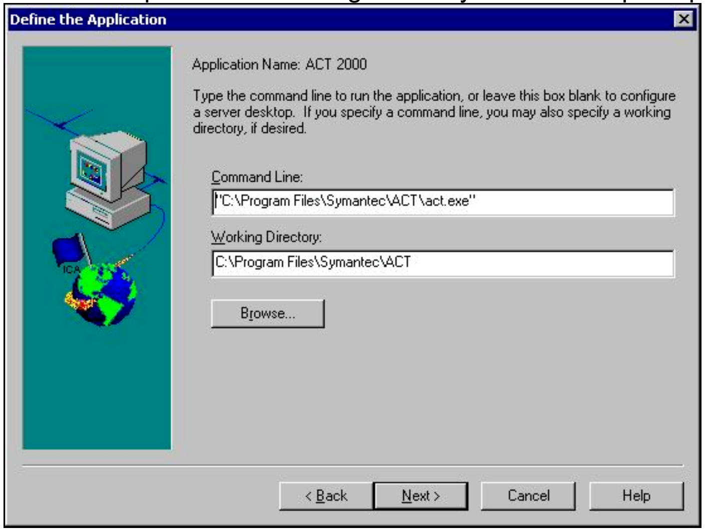
Choose Explicit if you wish to require a username and password to be entered before the application can be run.

● Explicit

Choose Anonymous if you wish to allow an application to be run without a username and password.

○ Anonymous

7. Here we enter the Command Line to start the application and the Working Directory. Note that you must use quotes for the command line if the path includes a space. The working directory does not require quotes.



Define the Application

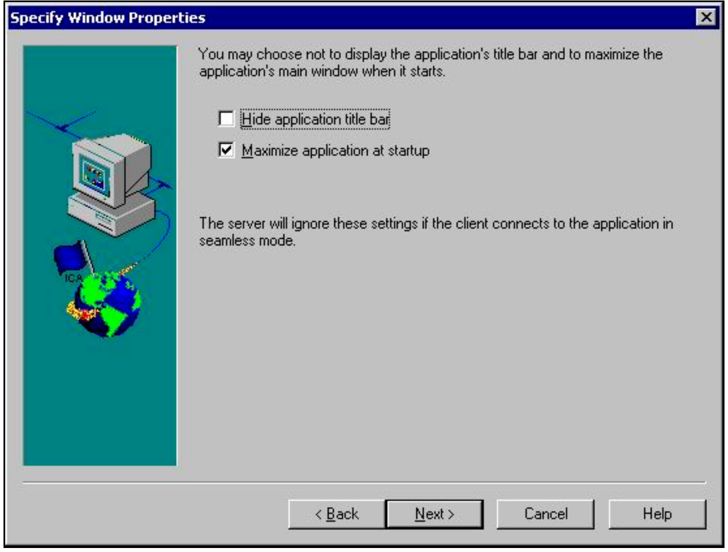
Application Name: ACT 2000

Type the command line to run the application, or leave this box blank to configure a server desktop. If you specify a command line, you may also specify a working directory, if desired.

Command Line: "C:\Program Files\Symantec\ACT\act.exe"

Working Directory: C:\Program Files\Symantec\ACT

8. Next we choose how to display the application title bar or to maximize the application at startup. We recommend setting this option to “Maximize application at startup”.



Specify Window Properties

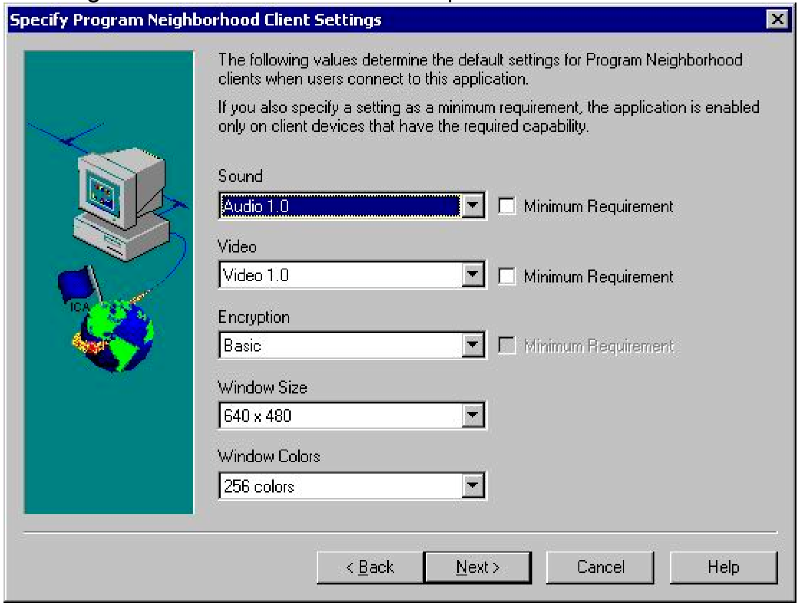
You may choose not to display the application's title bar and to maximize the application's main window when it starts.

□ Hide application title bar

☑ Maximize application at startup

The server will ignore these settings if the client connects to the application in seamless mode.

9. These settings determine Sound, Video, Encryption, Window Size and Resolution. We recommend that you use the default settings as shown above. The larger the resolution and color depth the more bandwidth that citrix will need.



The following values determine the default settings for Program Neighborhood clients when users connect to this application.

If you also specify a setting as a minimum requirement, the application is enabled only on client devices that have the required capability.

Sound: Audio 1.0 □ Minimum Requirement

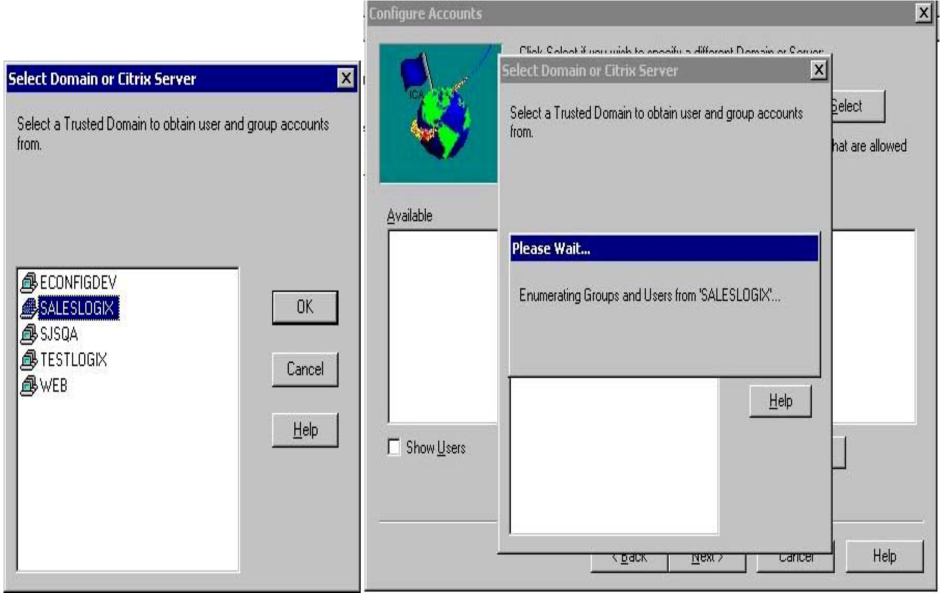
Video: Video 1.0 □ Minimum Requirement

Encryption: Basic □ Minimum Requirement

Window Size: 640 x 480

Window Colors: 256 colors

10. You will then choose a Domain to user and group accounts.



Select Domain or Citrix Server

Select a Trusted Domain to obtain user and group accounts from.

- ECONFIGDEV
- SALESLOGIX
- SJSQA
- TESTLOGIX
- WEB

Configure Accounts

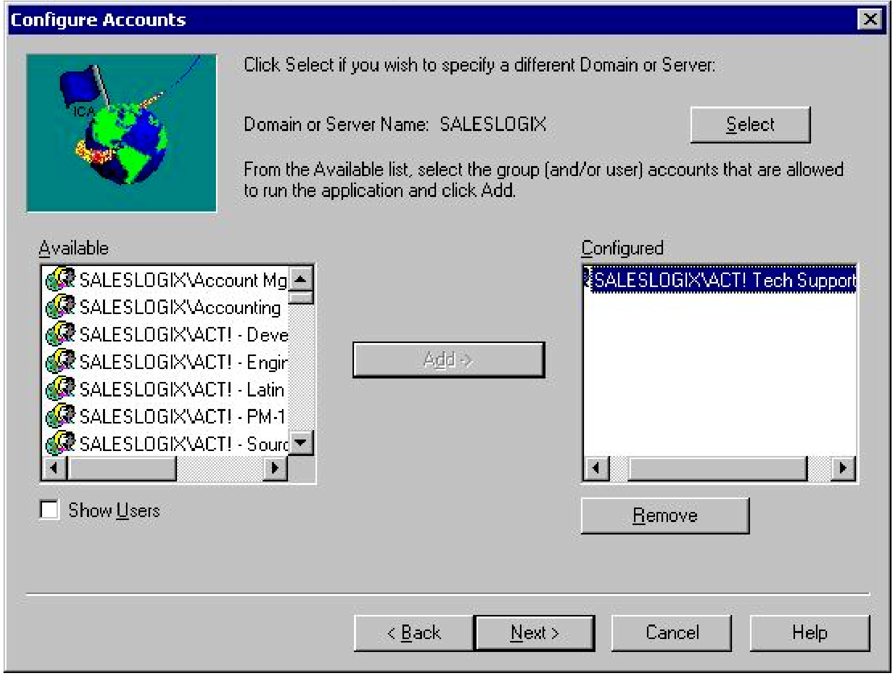
Select Domain or Citrix Server

Select a Trusted Domain to obtain user and group accounts from.

Please Wait...

Enumerating Groups and Users from 'SALESLOGIX'...

11. Then you choose the group or users from the available list on the left side for those that are going to be running this application.



Configure Accounts

Click Select if you wish to specify a different Domain or Server:

Domain or Server Name: SALESLOGIX

From the Available list, select the group (and/or user) accounts that are allowed to run the application and click Add.

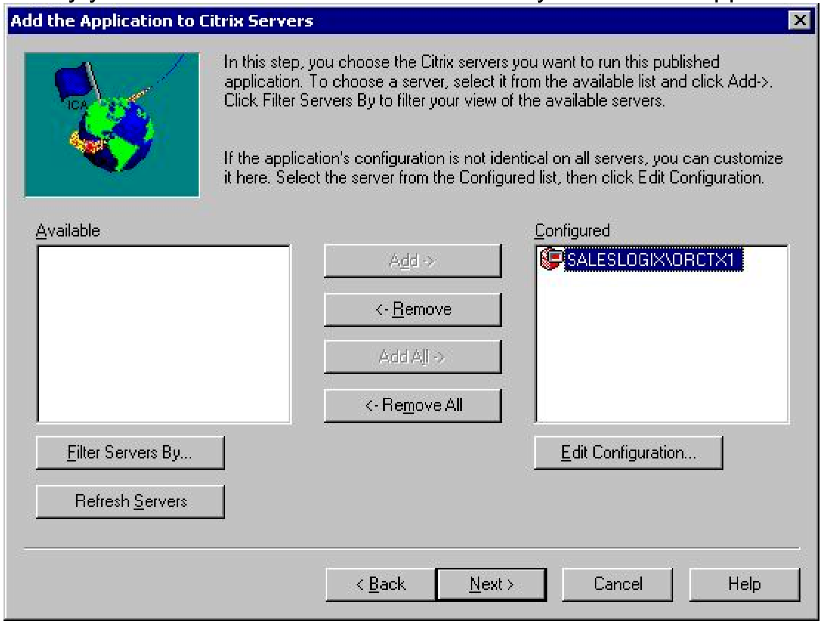
Available

- SALESLOGIX\Account Mg
- SALESLOGIX\Accounting
- SALESLOGIX\ACT! - Deve
- SALESLOGIX\ACT! - Engir
- SALESLOGIX\ACT! - Latin
- SALESLOGIX\ACT! - PM-1
- SALESLOGIX\ACT! - Sourc

Configured

- SALESLOGIX\ACT! Tech Support

12. Finally you choose the server or servers that you want this application to run on.



Add the Application to Citrix Servers

In this step, you choose the Citrix servers you want to run this published application. To choose a server, select it from the available list and click Add->. Click Filter Servers By to filter your view of the available servers.

If the application's configuration is not identical on all servers, you can customize it here. Select the server from the Configured list, then click Edit Configuration.

Available

Configured

SALESLOGIX\ORCTX1

13. After you have configured citrix for running the application you will need to modify the user interface page (generally a web page) if the client doesn't have a link to the console.

Note: Please consult the Citrix documentation for further instructions on Citrix usage.