



DATiX ThinServer Manual

for

DATiX Version 1.7.x

www.smartfletech.com

Copyright © SmartFLeX Technology, Inc. 2003 - 2007

Manual Index

- 3 DATiX Setup
 - 3 Server HW setup
 - 3 Startup
- 4 Select Server Type
 - 5 Dedicated File Server in a NT-Domain
 - 5 Member in a NIS-Domain
 - 5 Authentication Server
 - 5 Replication Server
- 5 Fileserver
 - 6 Creating a new Share
 - 6 Edit existing shares
 - 6 Delete a Share
 - 6 File Server for UNIX
 - 6 Expose shares via NFS
- 7 Terminal Server
- 7 Security Settings
- 8 Additional Server Services
 - 8 SSH -Server
 - 8 NFS-Server
 - 8 HTTP-Server
 - 9 FTP-Server
 - 9 MySQL-Server
 - 9 Printer-Server
- 9 Backup
 - 9 Backup erstellen
 - 9 Restore the Backup
- 10 Updating the ThinServer-Software
- 10 Special Users
 - 10 User: archiv
 - 10 User: htmladmin
 - 11 User: ftpadmin
 - 11 User: ttfadmin
 - 11 Access via Windows
- 11 Printing
- 11 Demonstration Network
 - 13 Configuration of the ThinServer
 - 13 Configuring the DHCP-Server
 - 13 Configuring the user accounts
 - 14 Enable shared data pools (Shares)
 - 15 Domain "THIN"
 - 15 Starting the Network

This Section describes the setup of the DATiX ThinServer.

First identify an appropriate location and setup the server HW. The server should be at location that guarantees enough cooling and safety so the sever may be operated continuously uninterrupted and unsupervised.

For the installation of the DATiX OS and initial basic configuration you will need to connect a keyboard and monitor.

Server HW setup

1. Install and secure HW base at selected location.
2. Connect the Power Cable.
3. Connect the Monitor.
4. Connect the Keyboard.
5. Connect the Network Cable.
6. Plug AC Cable into Power Outlet.

Startup

1. Turn on the monitor.
2. Insert the DATiX CD into the CD-ROM drive.
3. Power on the server (eventually you need to adjust your BIOS settings to allow the server to boot from the CD-ROM drive).
4. Wait for the server to boot all the way up until the DATiX OS asks you to press the enter key to continue installation. The DATiX OS will test the integrity of the CD content and then install the OS to the internal hard drive.
5. Once the installation is completed (installs in about 30 minutes and unattended) the DATiX OS will ask you to reboot the server. To do so remove the CD from the CD-ROM drive and press the reset button to reboot. The server should now reboot off the internal hard drive.
6. Wait until the OS is completely up and running and presents the login prompt. Type the user name **root** and press the enter key.
7. Type the password **smartflex** and press the enter key after which a very simple menu will be presented.
8. Select Option **s** by typing the letter s on the keyboard followed by the enter key.

9. Enter a valid IP-Address for the server. This IP address must be reachable from another computer in your network. For example, type 192.168.10.1, if your ThinServer is part of network 192.168.10.0 and the address 192.168.10.1 is still available. Press the enter key to conclude the entry.
10. Enter a valid netmask, 255.255.255.0 for example and finish with the enter key.
11. On a computer within the network start a browser and enter the following address:
http://<THINSERVER_IP_ADRESSE>:8081 an.
For above example in step 9, enter <http://192.168.10.1:8081> .
12. Enter the user name **root** the password **smartflex** to log into the remote administration desktop..
13. Follow these quick instructions to continue the server configuration:
 14. First create a server certificate so you can use an encrypted channel to administer the server. The entered certificate data, can be displayed with the browser by clicking on the lock sign on the bottom of the browser window. Create the certificate, after entering all relevant data, by clicking the **Create** button.
 15. After you have finished the certificate reconnect to the server via the following address: **https://<THINSERVER_IP_ADDRESS>:8082**. For above example in step 9, enter <http://192.168.10.1:8082> .
 16. Next you should change the root password. the new password should consist of letters and numbers and it should not be a word in a dictionary.
 17. First and most important you will need to permanently assign a valid network address to the server. The address we set during the first boot is only valid until the next reboot and must now be made permanent. The same is true for the netmask.
 18. Next, define the settings for the DHCP-Server or, if not needed, disable it.
 19. Now reboot the DATiX ThinServer by clicking the **[shutdown]** entry and then **restart** from the menu. Define the time it takes before the shutdown should begin in the **[minutes]** field. Set a value of 0 if the reboot should occur immediately.

Select Server Type

This section describes how the DATiX ThinServer can be integrated into a network and what tasks it can perform.

From a PC within the network connect to the ThinServer via a browser as described above. Login with user name **root** and your new password and select **[Server type]** from the menu.

You are presented with four (4) selections, each one relating to a specific server function:

Dedicated File Server in a NT-Domain

Select the **Authenticate against a NT Server** entry, if this ThinServer is to become a member in a NT-Domain. Provide the names of the NT-Domain and the Domain Server (NetBIOS-Name, NOT the IP-Adresse).

With this setting, any valid user of an NT Domain can use this ThinServer as a File Server. You can create shares that all users for example can access.

Member in a NIS-Domain

Choose the selection **Authenticate against a NIS Server** if this ThinServer is scheduled to be a member of a NIS-Domain. This selection does not have any real significance for the DATiX ThinServer, unless the server is expanded to become an application server.

Authentication Server

Choose the selection **This server is authentication server** if this ThinServer is used to manage a NT-Domain and a NIS-Domain. In this case you will need to supply the names of the NT-Domain and the name of the NIS-Domain, where both names can be, but do not have to be, identical. The NIS-Server is responsible for the network defined by its own IP-Address and netmask. For example, if the server owns the address 192.168.10.1 and the netmask 255.255.255.0, the server is responsible for the 192.168.10.0 network.

If this ThinServer Authentication Server is active, all user and group management is performed by this server. New users setups should be defined on this server, which allows each defined user to log into any Windows or Unix type system within the same network.

Note: The user root is the network administrator in a NT-Domain.

Replication Server

This ThinServer can also act as a Replication Server. In this operation mode a second ThinServer will copy its data to this ThinServer. In case the of a defect on the MasterServer the Replication ThinServer (SlaveServer) will become the MasterServer. Provide the IP Address of the MasterServer to the Replication Server. This is necessary to make sure that only the assigned MasterServer can copy data to the Replication Server. In the [Server typ] setup page of the MasterServer you will need to provide the IP-Address of the Replication Server.

Fileserver

This section describes the 'Fileserver' option of a DATiX ThinServer. A File Server provides storage space over the network to other computers. The storage space is called a share. Permission rights can be assigned for each individual share.

Creating a new Share

Select the [**fileserver**] option from the menu. Select "**create new share**". Assign a name to the new share, with which it is to be accessed by a user or a group. Add a short description, reflecting the content of the share.

If this share is to be made accesible to a group of users select the group form the selection box. If the share should be read only for all users, select the option "**Read only**" and define one user that can access the share with write permission to fill it with data.

Note: The share needs to be owned by the group the user belongs to that will be assigned write permissions. If more than one user should have write permissions, than all users need to belong to the same group.

Next, create the share by clicking "**create share**".

Edit existing shares

Select [**fileserver**] from the menu. You will see a graphical representation of all existing shares on the screen. Click the yellow folder of a share to change the setting of a share. You can change the permission settings and you can change the description of a share.

Delete a Share

Select [**fileserver**] from the menu. You will see a graphical representation of all existing shares on the screen. Click [**delete**] underneath a share to delete the share. Confirm the delete action. All data of the share will be collected into a zip-archive and stored into the users' archive directory.

File Server for UNIX

This DATiX ThinServer can expose the entire content of its data area (all shares and user directories on the hard drive) via NFS to all other computers. Therefore the NFS service needs to be running.

Expose shares via NFS

Select [**fileserver**] from the menu. Select "**Settings for UNIX clients**". Activate "**Export user directories**". Decide to assign full root rights to the NFS directory, or not (Allow full root access). It is safer not to allow root access.

Assign at least one network or client computer (IP address) that can access the NFS directory. NFS directories are not enabled for users, but for computers.

All established shares can be accessed and mounted by UNIX-Clients via **/home/shares/SHARENAME** on the ThinServer. The group owning the share has read/write permissions, even if the share is read only" for Windows.

Terminal Server

The Terminal Server allows special PXE boot clients to use this DATiX ThinServer as a LTSP Boot Server. These clients do not require any storage media and are therefore very robust. Functionality wise, a LTSP solution cannot reach the level of a flash based Thin Client solution, such as our NETiON SmartClient series. It is also not very well suited to support very large Thin Client network deployments.

Select [**Terminal server**] from the menu. Activate or Deactivate the Terminal Server bei setting either the Start or the Stop Terminal Server option.

The option “**New and unconfigured workstations [list of MAC addresses]**” shows the MAC Addresses of all unconfigured workstations. The [configure] option allows to configure each of these workstations individually.

The option

LTSP Workstations:

Client hardware address : Default **Default** [edit] [delete]

allows to change the LTSP workstation configuration or entirely delete the workstation.

We strongly recommend to study the LTSP manual to learn about the many configuration options available to the LTSP workstations.

Note: The ThinServer will automatically become a Fontserver as soon as the Terminal Server will be activated.

As a precondition to use this ThinServer as a Bootserver (Terminal Server) the integrated DHCP service needs to be activated.

There is a list of client hardware addresses on the Terminal Server Administrationpage of all workstations registered by the local DHCP server.

Security Settings

This ThinServer offers some useful security features. You can access the security setup page via the administration start page. Select “**Please Check Security Settings**”.

One decision to be made is to define if all newly created files should only be read by the owner and its group. The most secure setting is always to limit permission to the owner, but have in mind that this restriction may prevent you from exchanging files with other group members.

Furthermore you can decide to delete all user directory files that are dangerous to the system (superuser programs for example) during a restart or commit procedure. If this function is activated the system start will take much longer.

In addition, you can decide to delete the temp directory during a boot sequence.

Next to the “**Fingerprint of the security check file**” entry you will find a combination of numbers and letters, which you should make a record off. As long as no system upgrade is performed, this sequence should never change. Any change in the sequence in this number is a clear sign that important system files have been modified or replaced, which could be an indication that a non-authorized person broke into the system.

You can check which important system files have been changed by clicking “**Check important system files**”.

As a system administrator it is a good practice to regularly check the system log files, leave messages for other system administrators in “system chat”, and to read messages left by the system for you.

Additional Server Services

This section explains additional services the DATiX ThinServer provides. These additional services are accessible via the [**Services**] entry from the adminn interface menu.

SSH -Server

Activate this server (default: deactivated), to work on the console from a remote workstation or Thin Client. The connection is encrypted to provide maximum network security.

WARNING: This access method should only be used with extreme caution, even with ssh the connection can be snooped out. Only use it if you have total control over the workstation or Thin Client that initiates the ssh connection!

NFS-Server

Activate the NFS-Server if you like to use the ThinServer's user directories mounted to other computers as “their” local directory. This is most useful if the ThinServer is also a NIS-Server and remote Linux or UNIX Workstations need to access its data pool.

HTTP-Server

Activate the HTTP-Server if this DATiX ThinServer is to become a WEB server for the Intranet. This HTTP-Server is PHP4 enabled and can access the local MySQL database. Please refer to the section “**Special User**” for additional information.

WARNING: It is not recommended to use this DATiX ThinServer as a public HTTP-Server if it is also used as a file-, print-, or terminal server. The HTTP-Server is only intended to be used as “behind the firewall” Intranet Server.

FTP-Server

Activate the FTP-Server function, if you and other users of this ThinServer intend to use FTP Services to access the user directories and/or a public space of the data area. This FTP-Server is mandatory for all users described in the section "**Special User**".

MySQL-Server

Activate the MySQL-Server, if you or the HTTP-Server need a database system. Please refer to the section "**Special User**" for additional information.

Printer-Server

Activate this Server, if a local printer is to be connected to this ThinServer setup. Any configured printer will be exposed and become available for the entire network and can be used for printing via the "IPP" protocol (print server functionality).

Backup

The purpose of this section to familiarize you with the simple backup system, embedded into this server. The backup system saves user data to a CD-R compressed into zip archives. Of course, this function is only usable if your server includes a CD-Writer.

Backup erstellen

Please click the menu item [**backup**] and select "**Start backup now!**", if you like to create a backup of your user data. The drawer of your CD-Writer will open to receive a writable CD. After inserting a CD close the drawer and the ThinServer will check the CD-R. The backup will start immediately. After the backup is completed the CD-Writer drawer will open. Retrieve the CD, close the drawer, label the CD, and store it on a safe location. If the drawer opens again automatically again, insert a new empty CD as the backup process is not yet completed and requires additional CDs to continue. This procedure will continue as long and as often as it takes to save the entire user data content to a series of CDs.

Restore the Backup

Please select [**backup**] from the menu. Select "**Restore files from Backup**". Insert a Backup Data CD into to CD-ROM or CD-Writer drawer and select "**start restore**". The ThinServer will create a index of all the files on the CD and present it on the screen. By clicking on a directory or a file the directory of file will be restored.

WARNING: Existing Directories and files with similar names on the ThinServer will be

overwritten without further warning!

Updating the ThinServer-Software

The ThinServer software can be updated via CDs provided by your vendor, when new versions or bug fixes are released. To perform an update click the [**Update**] link in the menu. Insert the Update-CD into the tray of the CD-ROM device, close the CD-ROM tray and click “**Start Update**”.

Special Users

The subjects of this section are the special system users on the DATiX ThinServer, that are responsible for specific tasks.

User: archiv

Default status: inactive

The home directory of this user is a storage area where all zip-archives of deleted users and their data (Windows) are saved. This directory is accessible via ftp or nfs services if the user **archive** has been activated with a valid password. To assign a password please use the “[**Usermanagement**]” tool.

The purpose of this function is to prevent the system home directory space being maxed out by no longer active users and shares. The **archiv** users responsibility is, from time to time, to access the archive home directory and delete no longer needed archives.

To access the **archive** directory the FTP-Server or the NFS-Server needs to be activated.

User: htmladmin

Default status: inactive

This ThinServer incorporates an Apache-Webserver, with PHP4 and a MySQL-Database Server. Both, the Web-Server and the SQL-Server are started or stopped via the [**Services**] menu entry.

If Apache is being started the user **htmladmin**, if not already established earlier, will be created. The purpose of this user is to establish a ftp connection to the document tree of the Apache web server. To activate this user assign a password to the user **htmladmin** via the menu entry [**Usermanagement**].

Now you can use this user account to upload html content to the document tree of the local Apache web server. By default, the MySQL-admintool “phpMyAdmin” is installed and can be accessed via <http://SERVERNAME/phpMyAdmin/index.php> .

User: ftpadmin

Default status: inaktive

DATiX ThinServer includes a FTP-Server that can be activated in the [**Services**] section. During the first start a user **ftpadmin** is automatically created, but deactivated. By applying a password to this account ([**Usermanagement**]) the user will become active. This user is the ftp administration account for the public area (accessible by anonymous users) of the ftp server. After applying the password the user **ftpadmin** can gain access to the DATiX ftp server to transfer public data.

User: ttfadmin

Default status: inactive

User **ttfadmin** allows to install new TrueType®-Fonts on the DATiX ThinServer via ftp. This feature is only needed if the ThinServer is used as a font server (TCP port 7100) or if the LTSP server is activated.

The user **ttfadmin** is automatically created, but deactivated. By applying a password to this account ([**Usermanagement**]) the user will become active. By means of ftp copy the desired TrueType-Fonts to the ThinServer (TrueType-Fonts have the file extension .ttf). "Commit" the changes made to activate the new TrueType-Fonts.

Access via Windows

If this DATiX ThinServer is being used as the Primary Domain Controller you can use the "special user" accounts directly. In this case you can simply login to the ThinServer Domain as ftpadmin, htmladmin, or archiv.

Printing

This ThinServer can be used as a Print Server. For this the ThinServer exposes the IPP (Internet Printing Protocol) Interface on TCP port 631, which you can use to set up a local printer.

All printers created as local printer are automatically accessible from within the network and are therefor visible to other IPP-clients with the network.

Demonstration Network

The following is an example to demonstrate a possible network with a DATiX ThinServer.

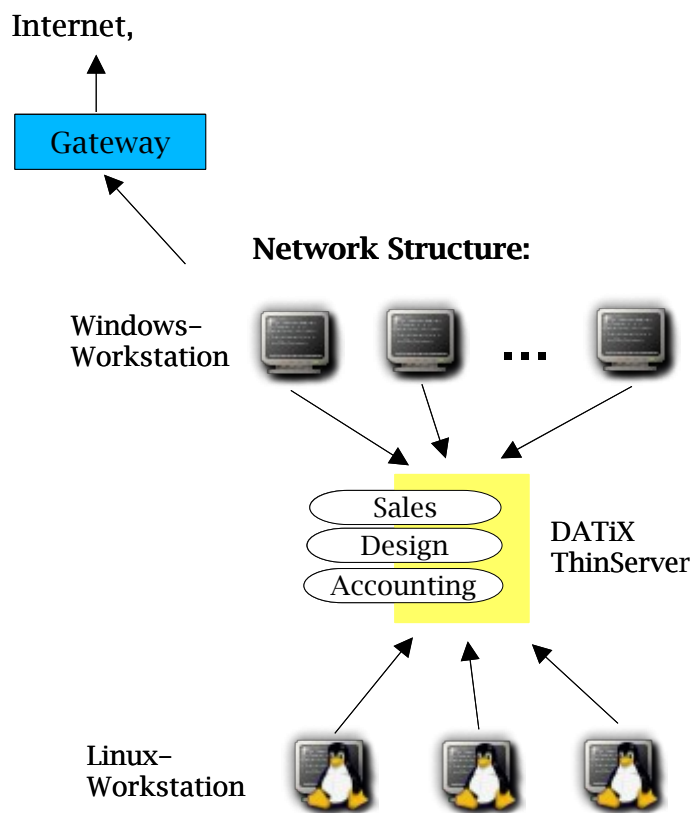
Scenario:

There are multiple Windows Workstations. Each user can login on any of these workstations to access his or her data located on the hard drive of the DATiX ThinServer. In addition there are 3 Linux Workstations. The users of these stations need to create and store data on the ThinServer that can be accessed and manipulated by any of the Windows users.

A Intranet is also needed, to provide WEB based information and work-rules for the users. A connection is made to the internet via an ADSL-Line.

There are three user groups: Sales, Accounting and Product Design. Each group has access to an individual directory, in which they save workdocuments that are exchangeable between the group members.

Furthermore there is a directory, that provides templates for documents. This directory is read only for all users and can be written to only by the owner.



Groups and Users:



Hardware

All Windows and Linux Computer will be installed as usual or already in use workstations will be used. The computers will be connected to a hub or switch via a twisted pair cable. The same is true for the DATiX ThinServer and the Gateway to the Internet.

Configuration of the ThinServer

Configure the server HW and install the DATiX OS with the recovery CD. After the CD is tested and installed, remove the CD and reboot the server.

Make sure to connect a keyboard and monitor for the first start procedure setup. Once the DATiX ThinServer is completely booted, login as **root** with password **smartflex**.

Select menu option "s" by typing the letter s on the keyboard, followed by the enter key. Now enter the IP address

192.168.100.1

and press the enter key.

Enter the netmask

255.255.255.0

and conclude with the enter key.

Now login on one of the PCs or workstations, for example on the PC with the IP address 192.168.100.5 and start a Firefox or IE or any other standard browser. Point the browser to URL address

<http://192.168.100.1:8081>

A login screen will be presented where you need to login as user **root** with password **smartflex**. Follow the instructions described in section "Startup". Select "Server1" as the system name and set the server IP address to 192.168.100.1.

From now on, when we refer to configuration Server1, we are in fact referring to the browser connection to Server1.

Configuring the DHCP-Server

Select the menu option [**dhcp**] and enter 192.168.100.50 as the start address and 192.168.100.100 as the end address. This setup allows up to 50 client computers to receive their IP addresses from this DHCP server.

Enter "test.net" as a domain name and use the DNS Server address provided by your ADSL provider as the DNS Server IP address. The IP address of your (ADSL) router is provided as the gateway address.

To finish the setup click "start dhcp service" and save the settings by clicking "set dhcp".

Configuring the user accounts

On Server1 select the menu option [**group management**] . Create three (3) user groups:

- Sales
- Design
- Accounting

On Server1 select the menu option [**user management**].

Create the user "thomas":

1. Select "add new user"
2. Type the login name "thomas"
3. Type "Thomas Smith" as the full name
4. Type "thomas" as a Password and Password retry (the password can be changed later by user thomas)
5. As a group assign "Sales"

Create the new user by clicking the "create user" menu option.

Repeat this procedure for the following user accounts:

- claudia, group Sales,
- steffi, group Sales,
- rolf, group Design,
- heiko, group Design,
- manuela, group Design,
- jutta, group Accounting,
- angela, group Accounting

Enable shared data pools (Shares)

Select menu option [**fileserver**] on Server1. Click "**Create new share**".

Enter the share name "Sales" and provide a short share description in the field "Comment".

As a group assign "Sales" as this directory is used also by the users thomas, claudia, and steffi, for data exchange.

Now create the share.

Create the shares "Design" and "Accounting" the same way by following the above procedure.

Finally, create an additional share with the name "Templates". Set this share "read only", but assign "write allowed for" rights to user "thomas", who creates these templates. This share should be owned by the group "Sales" which user "thomas" belongs to. Create the share.

Domain "THIN"

Select menu option [**server typ**] on Server1. Since Server1 is responsible for managing all user accounts, select the "**This server is authentication server**" option. Enter "THIN" as the name for the NIS-Domain and the NT-Domain. Save the settings with "**change settings**".

Starting the Network

After all above setup steps are completed select the menu option [**Commit Changes**] and commit all changes made. Select the menu option [**shutdown**] and then the option "restart". Enter 0 in the "**Shutdown in [minute]**" field, to force the ThinServer to immediately perform a restart, instead waiting for another minute (1 minute is the default setting).

After the ThinServer is restarted, use the manufacturers instructions to add the Windows PCs to the "Thin" Domain. This method requires the intervention of the the root user. The root user name and its password is required to perform this task.

After all Windows PCs have joined the Domain "Thin", all users can now use these PCs by logging in with their user names and passwords. Via network -> Server1 each user will find a directory with his or her name on Server1. This directory is the data directory for each individual user. The content of the "My data" -folder will be saved on the storage media of the ThinServer. User can create files and new subdirectories within their "My data" -folder. Once the user logs off the Windows PC all data will be automatically written to the ThinServer. If a user logs in on another PC he will have access to his or her data pool.

Connect the Linux Comouters via the Linux distributions standard tools to the NIS-Domain "Thin" (NIS-Server IP address in this example is 192.168.100.1) and mount the home directories of Server1 (192.168.100.1:/home) by adding the following line to /etc/fstab:

```
192.168.100.1:/home /home nfs defaults 0 0
```

Restart the Linux PC. All above established users can now login on all Linux PCs. The documents they create will be saved to the home directories of each user and are therefore also accessible to the Windows PCs and vise-versa.

Hardware Compatibility

DATiX has only three critical components in terms of HW compatibility: Network Adapter, Disk Subsystem, Processor.

Processors:

DATiX is designed to work with the following processors: Pentium - Pentium 4, Celeron, 32 Bit AMD, VIA C3 and EDEN

Disk Subsystem:

DATiX only supports IDE/ATA and SATA based Interfaces. SCSI or Firewire Interfaces are not

supported.

To (re-)install the DATiX OS you will need a bootable CD-ROM drive (IDE/ATA or USB). For CD-ROM based backup you will need an IDE CD-Writer installed.

A SCSI Interface for DAT is supported.

Memory:

A minimum of 128 MB RAM is required to install the DATiX OS.

Video:

DATiX does not run a graphical console, therefore any VGA type Video Adapter should work.

Network Adapter:

DATiX supports most auto-detect and all kernel supported network adapters.