

IBM NetVista Thin Client with Turbolinux 7

This document describes common elements of IBM NetVista Thin Client with Turbolinux 7 for Linux servers and Windows servers.

Thin Client Models Supported

The N70 model is supported with NetVista Thin Client with Turbolinux 7. Following is the complete list of supported thin clients with this release:

- N70 (also known as 8366)
- N2200 (also known as 8363)
- N2800 (also known as 8364)

Hints and Tips on the Web

The IBM Support web site for IBM NetVista Thin Clients is occasionally updated to include hints and tips. Please take a look at this web site for additional information:

1. <http://www.pc.ibm.com/support>
2. Click **NetVista and NetVista thin client**
3. Click **NetVista thin client**
4. Click **Hints and tips**
5. Select **All** for the **Hints and tips by category** (and click **Go** if the page is not refreshed automatically)
6. Scroll down to see all the hints and tips available by publication date

Important Information

Model 2200 and Model 2800 - IMPORTANT NS Boot version Information

The IBM NetVista Thin Client models N2200 and N2800 ship from manufacturing with firmware (also called NS Boot version or boot prom). Depending on the manufacturing date of the thin client you have, the firmware level may be 07/17/00, 01/12/01, 07/16/01 or 12/06/01.

Significant changes have been made in IBM NetVista Thin Client with Turbolinux 7. To use the NetVista Thin Client with Turbolinux 7 on model N2200 and N2800 thin clients, the firmware level (**12/06/01 or later**) must be installed on these clients. An automatic upgrade of the firmware has been implemented in for clients with the 07/16/01 level firmware).

Will the firmware be updated automatically?

- Yes, for those clients with firmware level 07/16/01, the firmware will automatically be upgraded when the client boots to a server or flash card with NetVista Thin Client with Turbolinux 7.
- No, for those clients with firmware level of 01/12/01, 07/17/00 or 12/06/01 . Therefore, the following manual steps should be followed to upgrade the firmware on clients with those levels of firmware:

How do you manually upgrade the firmware for clients with the 01/12/01, 07/17/00 or 12/06/01 level?

For manual upgrading of the firmware, special "bootable" firmware images are provided in the installation on your server with the following files:

- For Model 2200 - /nstation/linux/bflash.2200
- For Model 2800 - /nstation/linux/bflash.2800

To upgrade to the new firmware level, use the NSBoot Setup Utility. When the client is starting to boot, after the message "Hardware testing in progress" is removed, press the ESC key to start the NSBoot Setup Utility and then follow these steps:

1. If the screen presented has an option to press F5 for Advanced Configuration, press F5
2. From the Advanced Configuration screen, select the menu option to "Configure Network Settings." and set all appropriate network environment options for this thin client.
3. Press ENTER to continue to the "Change boot file server settings" screen.
4. Set the first Boot file server IP address to your server IP.
5. Change the boot file server directory and file name by using the PAGE DOWN key to display a blank field and entering **/nstation/linux/bflash.2200** for N2200 models, **nstation/linux/bflash.2800** for N2800 models, and **NFS** as the protocol.
6. Press ENTER as often as needed until you are back at the Advanced Configuration screen and then press F10 to reboot the thin client.

Rebooting will cause your firmware level to be updated. Follow the instructions during this process. **Do not power off your thin client while the firmware is being updated.**

The firmware has been updated...now what?

If the firmware was updated automatically, the settings you had previously will be preserved. Because the updated firmware has some new menus, you may choose to take a look at it.

If the firmware was updated manually, you may need to reset the boot protocol and other settings within the NSBoot Setup Utility. As the thin client starts, press the ESC key just after the message "Hardware testing in progress" has been removed.

7. Select the keyboard type and display settings when prompted.
8. Move the cursor to highlight "Configure network settings" and press ENTER. If you are not using DHCP for both the client IP address information and network configuration:
 1. Disable this first option and enable the appropriate network priority and fill in the values as needed
 2. Select the boot file source (flash for flash booting and network for server or peer booted clients)
 3. Set your Profile Server location (default is boot source). Press ENTER to exit this screen
 4. If you selected boot file source as network, you will be prompted to specify the IP address of the boot server along with the boot path (the default is /nstation/linux/kernel.2x00 and is correct for peer boot clients and is correct for server booted clients if the product was installed without changing the default installation path. Press ENTER to exit this screen.
 5. If you selected a Profile Server other than boot location, you will be prompted to specify profile server information. The default port for TCM Operations Utility servers should be correct unless you have modified your installation. Press ENTER to exit this screen.
9. Press F10 to reboot the thin client.

Once the client is up and running, you can use the Setup Utility or the TCM Operations Utility to change the client's profile server or boot source (to switch the client to boot to/from flash/server).

Updating Flash Images from NetVista Thin Client with Turbolinux for Model 2200 and Model 2800 Thin Clients

It is necessary to perform a flash recovery to update your flash card image from the old release. There are several suggested methods for performing this update and they depend on the firmware level on the client. However, before you use any method, be sure to boot a client to the server with NetVista Thin Client with Turbolinux 7 and setup the server settings and desktop settings required profile components (see NetVista Thin Client with Turbolinux 7 Release in this document for more information on profile components).

- For clients with firmware older than 7/16/01,, use the TCM Operations Utility to first upgrade the firmware to the current Linux firmware level and then reboot the flash booted client and perform the flash recovery.
- For clients with the 07/16/01 firmware, use the TCM Operations Utility. Using the GUI interface you can identify the clients with flash cards and have them all perform a recovery (and you can schedule this task to run at a convenient time).

- For clients with the firmware dated before 07/16/01 manually upgrade the firmware (steps provided previously in this document) and then server boot to the server with the IBM NetVista Thin Client with Turbolinux 7 and perform flash recovery:
 - Start the Setup Utility (press Ctrl+Alt+Shift)
 - Click **Management**, Click **Flash Recovery**
 - Enter the server IP containing the new release and click **Continue**
 - Click the mount point (**/instation/linux**) and click **Continue**
 - Click on the desired flash image (be sure to specify a flash image with name starting as NetVista_2x00 as this identifies images for the model 2200 and model 2800) and click **Continue**
 - Click **Continue** on the confirmation screen
 - The client will be restarted and the flash card will be updated. Following the flash card update, the client will be set to boot to the flash card.

- For clients with the 07/16/01 firmware, use the Setup Utility from the flash booted client. This method is not difficult but is required to be performed on each client. This method can be used if you have the NetVista Thin Client with Turbolinux release and the 07/16/01 firmware. The flash card will be upgraded and the firmware will automatically be updated if needed. On the flash booted client, start the Setup Utility (press Ctrl+Alt+Shift) and do the following:
 - Click **Management**, Click **Flash Recovery**
 - Enter the server IP containing the new release and click **Continue**
 - Click the mount point (**/instation/linux**) and click **Continue**
 - Click on the desired flash image (be sure to specify a flash image with name starting as NetVista_2x00 as this identifies images for the model 2200 and model 2800) and click **Continue**
 - Click **Continue** on the confirmation screen
 - The client will be restarted
 - If the client is using the DHCP protocol, the client will not boot to the server without the following manual steps:
 - Press the ESC key after an error is displayed and then press any key when prompted to do so to continue
 - Use the down cursor key to highlight **Configure network settings** and press **ENTER**
 - Highlight the field for "Local (NVRAM)" and press the PageDown key several times until the value is changed to **Disabled**
 - Highlight the field for "DHCP" and press PageDown to switch the value to **First**
 - Again, highlight the field for "Local (NVRAM)" and press the PageDown key several times until the value is changed to **Override**
 - Press **F3** to save and return
 - Press **F10** to reboot
 - You may notice the client booting twice. This is because the first boot to the server will cause the firmware to be updated. The second boot to the server will cause the flash card to be updated.
 - Following the flash card update, the client will be reset to boot to the flash card.

How to Specify Boot Path Information

Protocol: IP Address from DHCP or Static IP

Thin Client	Boot Path Settings for Server or Peer Boot
--------------------	---

Model	(note: flash boot path is automatic -- no prompting)
N2200 and N2800	Boot path /nstation/linux/kernel.2x00 Profile server default path for boot or remote NFS server /nstation/profiles Profile server default port for TCM Operations Utility server 8561
N70	Boot Path /nstation/linux Profile Server in URL format nfs://x.x.x.x/nstation/profiles for boot or remote NFS server http://x.x.x.x:8561 for TCM Operations Utility server (be sure to specify the port)

Protocol: IP Address and Network Configuration from DHCP

Thin Client Model	DHCP Settings
N2200 and N2800	Option 66 - server IP 0.0.0.0 for flash boot x.x.x.x for server or peer boot Option 67 - path /kernel.2x00 for flash boot /nstation/linux/kernel.2x00 for server or peer boot Option 211 for boot protocol nfs
N70	Option 17 - server and path in URL format nfs://127.0.0.1/nstation/linux for flash boot (or not specified) nfs://x.x.x.x/nstation/linux for server or peer boot
All Models	Option 214 - profile server in URL format nfs://x.x.x.x/nstation/profiles for boot or remote NFS server http://x.x.x.x:8561 for TCM Operations Utility server

Notes Specific to Thin Clients using DHCP

- There is no DHCP class identifier support for any of the NetVista Thin Clients with Turbolinux 7.
- Trap server settings (DHCP option 212) can also be set within a trap profile component. In the event a client has received values for trap server settings from both DHCP and a trap profile component, the values within the profile component will be honored. And, for this reason, it is suggested you use a trap server settings profile component rather than the DHCP option.
- DNS settings (DHCP option 6) can also be set within the server settings profile component. In the event a client has received values for DNS from both DHCP and a server settings profile component, the values within the profile component will be honored.

Flash Images, Flash Boot, and Peer Boot Support

Provided Flash Images

IDF Builder and SDF Creator are two applications that help in flash management. We ship four default IDFs that can be used to create a flash card -- a 32 MB and 64 MB image for the N2200 and N2800 models, and a 32 MB and 64 MB image for the N70 model thin client:

NetVista_2x00_Communicator4.x_ICA6.x_IBM3270_IBM5250_64MB.idf

- A 64 MB image for the N2200 and N2800 models containing Netscape Communicator 4.x, ICA 6.x, both the IBM 3270 and 5250 emulators, and peer boot support for N2200 and N2800 clients.

NetVista_2x00_ICA6.x_IBM3270_IBM5250_32MB.idf

- A 32 MB image for the N2200 and N2800 models containing ICA 6.x, both the IBM 3270 and 5250 emulators, and peer boot support for N2200 and N2800 clients.

NetVista_N70_Communicator4.x_ICA6.x_IBM3270_IBM5250_64MB.idf

- A 64 MB image for the N70 model containing Netscape Communicator 4.x, ICA 6.x, both the IBM 3270 and 5250 emulators, and peer boot support for N70 clients.

NetVista_N70_ICA6.x_IBM3270_IBM5250_32MB.idf

- A 32 MB image for the N70 model containing ICA 6.x, both the IBM 3270 and 5250 emulators, and peer boot support for N70 clients.

SDF Creator is used to create software packages such as Netscape that you would like to install on a flash card. IDF Builder is a tool that is used to create an IDF that includes a SDF that defines what will be placed on the flash card. These tools only run on server booted clients. There is online help for these tools where you can learn more about the tools and how to use them.

NOTE: A flash recovery is required to upgrade flash cards from releases prior to IBM NetVista Thin Client with Turbolinux.

Custom Flash Images

You can create custom flash images using the IDF/SDF Builder. Note, if you created custom flash images in the previous release, you will need to recreate them in the new release. The previous release IDF and SDF files are located in the directory /nstation/linux/IBM/update/.old and can be used as reference (but they cannot be used with the IDF/SDF Builder tools in this release).

N70 Flash Support

You can add a flash card to the N70 and use one of the standard IDF files provided or create a custom flash image. This N70 can also provide peer boot support to other N70 clients.

Peer Boot Support

The default IDF flash card images contain peer boot support. This means, a thin client model N2200 or N2800 with a flash card can be used as a Master server providing boot support to N2200 and N2800 clients without flash cards. Similarly, an N70 with a flash card can be a Master server providing boot support to N70 clients without flashcards.

In order to use peer boot support, the Master must **enable** peer boot support. This setting is found in the Services Profile Component used by the Master.

Note, the boot path for peer booted clients has changed from the NetVista Thin Client with Turbolinux release. It is now the same as server booted clients:

- N2200 and N2800 peer booted clients specify boot path and filename:
/nstation/linux/kernel.2x00
- N70 clients only need to specify the boot path: **/nstation/linux**

NetVista Thin Client with Turbolinux 7 Release

Profile Components

Profile Components is a concept that allows NetVista Thin Clients to save and retrieve their configuration information for NetVista thin clients in a variety of places and then to manage those configurations. In some previous releases, NetVista thin clients could only save their configuration information to their boot location (flash card for flash booted clients and the boot server for server booted clients)..

The term **profile component** means a "logical set" of configuration information. For example, desktop settings is a set of information that defines the desktop -- it contains configuration information about the applications and desktop.

There are many profile components you can configure and use on the thin clients. However, only two of them are required and if they are not found, the Setup Utility is automatically started and the user is prompted to setup these profile components via a wizard like interface. The two **required** profile components are:

- **Server settings** - contains the DNS and Time Server information
- **Desktop settings** - contains the information regarding the desktop mode and the configuration of the applications available on the desktop.

Following is the complete list of user and workstation profile components:

User Profile Components

- Desktop settings
- Window manager Settings
- Netscape Settings
- Audio Settings
- Mouse Settings
- Printer - User Settings
- Language/Environment Variables

Workstation Profile Components

- Server Settings - DNS and Time
- Printer - Machine Settings
- Seriald Settings
- Trap Server Settings
- Mount Point Settings
- Services - Telnetd, Peer Boot

The profile server identifies the server storing the profile components to be used. And, the profile server types allow for different naming conventions to identify the profile components to be sent to the client. Specifically,

- When the profile server is the **Boot Server or a Remote NFS Server**, the profile components sent to the client must be named DEFAULT (to obtain system default profile components), <CLIENT> for workstation profile components, and <USERID> for user profile components.
 - When the client requests **workstation** profile components, the profile server will send all the <CLIENT> profile components found and send the remaining profile components defined as DEFAULT.
 - When the client requests user profile components, the profile server will send all the <USERID> profile components found and send the remaining profile components defined as DEFAULT.
- When the profile server is **TCM Operations Utility**, the profile components sent to the client can be named anything...however, in TCM Operations Utility, you must identify the client in a workstation group and the user in a user group, and have profile components assigned to these groups.
 - When the client requests **workstation** profile components, the TCM Operations Utility profile server will send the profile components associated with the profile group the client is a member. If the client is not defined in a profile group, the workstation profile components configured as the defaults (not named DEFAULT but rather configured within TCM Operations Utility as the default profile components) are sent.
 - When the client requests **user** profile components, the TCM Operations Utility profile server will send the profile components associated with the profile group the user is a member. If the user is not defined in a profile group, the user profile components configured as the defaults (not named DEFAULT but rather configured within TCM Operations Utility as the default profile components) are sent.

As you can see there are many profile components available to configure and using profile components can be a very powerful and easy way to manage your clients and users. It is essential the Administrator understands profile components, the profile server types, and the naming conventions for profile components based on the profile server location. For additional details, please see the document on profile component available on the Hints and Tips web site (follow the steps at the top of this document to locate this web site).

Summary of Updated Support

The most current NS Boot firmware version is 07/29/02. The 07/29/02 firmware better handles network noise during the initial kernel load. If your hardware has the 07/16/01 level of firmware, the firmware will automatically be upgraded when booting to NetVista Thin Client with Turbolinux 7 SU 2. To update from other versions of the firmware please reference the "How do you manually upgrade the firmware section of this README.

The operating system uses the Linux **2.4 kernel** In addition, the following applications are part of IBM NetVista with Turbolinux 7:

- **GDM Login and the ICE Window Manager**
- **IBM JVM (version 1.3)**
- **ICA Client (version 6.x)**
- **Netscape Communicator (version 4.x)**

The following support is in NetVista Thin Client with Turbolinux 7:

- **Authentication methods** - Additional authentication methods along with the ability to set the user's HOME directory on a remote server is provided (see the details included later in this document).
- **Language selection** - this setting is included in the Language / Environment Variables profile component and includes Euro support.
- **Screen lock** - the settings in the Window Manager profile component allow you to add the screen lock icon to the launch bar or enable the key sequence to activate the screen lock program.
- **Seriald** - this is configured within the Seriald profile component.
- **RDATE** time server protocol support - the time server configuration is set in the Server Settings profile component. Both NTP and RDATE time server protocols are supported (note that in this release, you can use an RDATE time server without any manual configuration).
- **Flash Recovery while server booted** - the Flash Recovery option within the Setup Utility is enabled for Flash and Server booted clients.
- **Wireless enablement** - this is supported for **N70 flash booted clients** only and requires manual configuration (see the details included later in this document).
- **Mount points** - the ability to configure additional user mount points is included in the Mount Points profile component.

Migration of Configuration Settings From NetVista Thin Client with Turbolinux Release

When you install NetVista Thin Client with Turbolinux 7, system defaults from a NetVista Thin Client with Turbolinux 6.07 install will automatically be migrated to the new profile component

format. In addition, you can elect to have the 6.07 release machine and user configurations migrated to the new profile component format.

The migration of system defaults, client, and user configuration information takes place when the first client boots to the upgraded server. The upgrade process takes a few minutes and messages are displayed on the client in order to keep you informed of the progress.

Specific details regarding the naming of profile components once migrated and the manual steps you may need to perform in order to make use of the migrated profile components is provided further in this document.

NOTE: A flash recovery is required to upgrade flash cards from the NetVista Thin Client with Turbolinux 6.07 release.

Included APAR Changes

SA93569	Corrected a problem so that the host name defined with the IBM NetVista Setup Utility will be used as the client's host name.
SA94034	Corrected a problem so the host name is correctly defined when flash booting.
SA94035	Corrected a problem following a change to the client IP address when the client was not immediately restarted. The Setup Utility will now automatically reboot after the IP Address is changed so the user does not need to remember to do so.
SA94204	Resolved the problem which resulted in a lock file error when using Netscape on peer booted clients.
SA94237	Resolved the NFuse errors that happen when HOME on the flash card is full.
SA94278	Corrected a problem whereby the client was not properly failing over to the backup DNS server defined in the Setup Utility.
SA94303	Corrected a problem so that an Xterm that is started from the setup utility can be closed with a click on the term window decoration 'x'.
SA94335	Added the Swedish language to the keyboards listed in the Setup Utility.
SA94370	Resolved a print problem for flash booted clients by adding Ghostview to the provided flash images.
SA94372	Corrected a problem for Finnish customers so they no longer need to manually set the LANG environment variable -- the Setup Utility now allows for a language profile component and Finnish is one of the selectable languages.
SA94544	Resolved a problem whereby flash booted clients with non-English keyboards defined were sometimes getting English as the language setting.
SA94575	Corrected the definition for the German keyboard such that the degree, "*", and "/" keys will behave as they are expected with a German configuration.
SA94587	Resolved a problem in the emulator SDF so that now the emulator SDF no longer requires the Netscape SDF in order to use the 5250 Setup Utility or 3270 Setup Utility on a flash card.

SA94588	Removed the need for the strip command to be available on the Linux server. To physically fit the 32 MB flash images onto a 32 MB compact flash card, the Thin Client binaries need to be stripped. The strip binary used during install was expected to be part of the Linux server code. And, if the Linux distribution on the server did not contain strip, the Thin Client binaries would then be larger than they needed to be causing the 32 MB flash images to not fit onto 32 MB compact flash cards.
---------	---

Authentication Support

Additional authentication methods are provided with this release along with enhancements to the existing authentication and non authentication modes. This means you can configure an authentication profile components to use any of the following methods:

Non Authentication

With non authentication mode, you can now specify whether or not the client's home directory persists between sessions. In addition, you can specify different profile user names for the non authenticated users in order to obtain different profile components for these non authenticated users.

Local Authentication

With local authentication mode, you can now specify the location of the user's home directory -- it is no longer restricted to reside on the authentication server. Local authentication is not available on flash or peer booted clients.

NIS Authentication (Linux server authentication)

This new authentication method allows users to authenticate to Linux servers (not restrictive to boot server).

Windows Authentication (CIFS/SMB)

This new authentication methods allows users to authenticate to Windows servers. There are several key elements to understand the support and setup for this authentication method so be sure to read the information provided further in this document regarding Windows Authentication.

Windows Authentication Feature - Details...

The Windows Authentication feature allows Linux thin client users to login using an account defined on a Windows server. This feature is enabled using the client Setup Utility under Workstation -> Authentication Profile.

Windows accounts do not have a Linux user ID (UID) or group id (GID) association. There are two methods for assigning UID/GID values to a Windows authenticated users.

1. Create a local account using kuser with the special word "cifsuser" included anywhere in the Full Name field. This tag indicates the user should be authenticated using the specified Windows authentication server but will use the UID, GID, and home directory specified in the local passwd file. The local password is not used and should not be set.
 - **Advantage:** Administrator can assign a unique UID and GID.

- **Disadvantage:** A parallel user account must be created on the client's boot server. The password in the local account is not used and does not need to be synchronized.
- 2. Use the common UID/GID. If there is no local user account, but the username and password are valid on the Windows authentication server, the user will be logged in using the common UID/GID. The user's home directory will be /home/<username> and will be created if it does not exist.
 - **Advantage:** Local account does not need to be created in /etc/passwd.
 - **Disadvantage:** Although users authenticated this way will have their own unique home directory, they will share the same UID/GID with other users authenticated using this method. This will allow them to read and write in each others home directories that share the same UID/GID. This may be a security risk depending on the customer's implementation.

Note: Local user accounts are still supported and have priority when Windows authentication is enabled.

Supported Windows Servers

- Windows NT 4 Server (PDC, BDC, or member server)
- Windows 2000 Server (Domain Controller or member server)

Configuration Parameters

Parameter	Description
Authentication Server	Primary Windows authentication server. You must enter the server's host name, not IP address.
Authentication Server Alternate	Alternate authentication server to use if the primary server is not available. You must enter the server's host name, not IP address.
Domain	Windows domain name.
Common UID	UID that is used for all Windows authenticated users that do not have a special entry in the local /etc/passwd file.
Common GID	GID that is used for all Windows authenticated users that do not have a special entry in the local /etc/passwd file.

Limitations

- Users in the local /etc/passwd have precedence over users on the Windows authentication server.
- Windows usernames are not case sensitive. For consistency in the Linux file system, Windows authenticated user names must be entered in lowercase letters.
- Password length and complexity requirements are determined by the policies on the Windows server.
- Password change is not supported from the Linux client if the authentication server is a Windows NT 4 Backup Domain Controller (BDC) or a member server.

You must change the user's password with User Manager on the authentication server.

- When logged into the Linux client as root, the password for a Windows user cannot be changed using the "passwd" command or similar utility. The password must be changed with User Manager on the authentication server.
- Use caution when changing the common UID or GID in the Windows authentication profile in the setup utility. Changing these values after a user has already logged in at least once can remove access to their home directory. It is best to select a common UID/GID before any Windows authenticated users login in. If the common UID/GID values are changed, an administrator will need to update the owner and group values for all files and directories in any user's home directory that were created with a different common UID/GID.
- If a common GID other than the default of 65001 is used, the system administrator must add this GID to the file <install location>/etc/group where <install location> is the directory where the client files are installed.

NetVista Thin Client with Turbolinux 6.07 Migration Considerations

The migration of system defaults, client, and user configuration information takes place when the first client boots to the upgraded server. The upgrade process takes a few minutes and messages are displayed on the client in order to keep you informed of the progress.

- For servers installed with NetVista Thin Client with Turbolinux 6.07 setup for user authentication, the configurations for userid root will be saved as profile component **DEFAULT** and if user configurations were selected to be migrated, they will be created as profile components name <**USERID**>.
- For servers installed with NetVista Thin Client with Turbolinux 6.07 setup for non authentication, the configurations for the systemdefault be saved as profile component **DEFAULT** and if machine configurations were selected to be migrated, they will be created as profile components name <**CLIENT**> (where <CLIENT> is the MAC Address or IP Address of the client).
- A single Authentication profile component will be created (named DEFAULT) with settings equivalent to the installation mode of NetVista Thin Client with Turbolinux 6.07 Similarly, a single Server Settings profile component will be created (named DEFAULT) with settings including the time server information as defined by the system defaults in NetVista Thin Client with Turbolinux 6.07

User Profile Components Created During Migration:

- **Desktop Settings** - This is a required profile component and a DEFAULT is created during migration based on the root user settings for authentication installations and the system default settings for non authentication installations. <USERID> and <CLIENT> profile components are created as appropriate. NOTE: ICA Client sessions will not be migrated to the desktop so you will need to recreate them as needed.
- **Window Manager Settings** - <USERID>, and <CLIENT> profile components are created as appropriate. The DEFAULT profile component is created during migration if the root user had ICE Window Manager settings in NetVista Thin Client with Turbolinux 6.07

- **Netscape Settings** - <USERID>, and <CLIENT> profile components are created as appropriate. The DEFAULT profile component is created during migration if the root user had Netscape preferences in NetVista Thin Client with Turbolinux 6.07
- **Audio Settings** - <USERID>, and <CLIENT> profile components are created as appropriate. The DEFAULT profile component is created during migration if the root user had audio settings in NetVista Thin Client with Turbolinux 6.07
- **Mouse Settings** - <USERID>, and <CLIENT> profile components are created as appropriate. The DEFAULT profile component is created during migration if the root user had mouse settings in NetVista Thin Client with Turbolinux 6.07
- **Printer - User Settings** - The DEFAULT profile component is created during migration if the root user had printer settings in NetVista Thin Client with Turbolinux 6.07
- **Language/Environment Variables** - <USERID> and <CLIENT> profile components will be created during migration. The DEFAULT profile component is created based on the root user settings for authentication installations and the system default settings for non authentication installations. Note however, these profile component will contain environment variables only as language settings are new this release. Also note, the default language for the thin client is based on the keyboard language if the language setting is not found in this profile component.

Workstation Profile Components Created During Migration:

- **Server Settings - DNS and Time** - No profile component is created during migration. As this is a required profile component, the Setup Utility will automatically start on the next client boot and will prompt you via the wizard like interface to create this profile component.
- **Printer - Machine Settings** - The DEFAULT profile component is created during migration if the root user or system default for non authenticated installations had printer settings in NetVista Thin Client with Turbolinux 6.07
- **Serial Settings** - No profile component is created during migration as this support is new.
- **Authentication Server Settings** - Only the system DEFAULT is created during migration and it contains settings based on the NetVista Thin Client with Turbolinux 6.07 installation (authentication or non authentication).
- **Trap Server Settings** - No trap server profile components are created during migration.
- **Mount Point Settings** - No profile component is created during migration as this support is new.
- **Services - Telnetd, Peer Boot** - DEFAULT, <USERID>, and <CLIENT> profile components will be created during migration, however, they will contain the setting for Peer Boot only as the ability to set Telnetd services is new this release.

After the migration process completes, the profile components created are stored at /nstation/profiles/user and /nstation/profiles/machine on the server. **Further action is needed by the Administrator in order to fully deploy these profile components.**

- The profile components created during the migration process can be moved to a TCM Operations Utility server so they can be managed and assigned to user and client groups. Specifically, the directories on the TCM Operations Utility server where the profiles should be copied to are
 - /NetVista/TCM/profiles/user/
 - /NetVista/TCM/profiles/machine/
- ICA Client sessions will not be migrated to the desktop settings profile component so you will need to recreate them as needed.

- Workstation or user specific settings will be created as <CLIENT> and <USERID> profile components. In order to use these profile components, you may need to rename them accordingly.
 - In general, installations with NetVista Thin Client with Turbolinux 6.07 configured for Authentication migrate without the need for manual renaming of profile components by the Administrator.
 - If your installation with NetVista Thin Client with Turbolinux 6.07 was setup for IP Addressing (rather than MAC Addressing for workstation configurations), you will need to rename these profile components as the NetVista Thin Client with Turbolinux 7 does not support IP Addressing for workstation profile components.
 - Installations with NetVista Thin Client with Turbolinux 6.07 configured for Non Authentication require more action by the Administrator. Specifically, notice that during migration, some user profile components named <CLIENT> will be created because all of the settings were saved to client specific directories in NetVista Thin Client with Turbolinux 6.07. However, because these profile components are **user** profile components, they must be renamed to a USER name (such as KIOSK) if they are going to be used by clients/users with an NFS profile server (boot location or remote NFS server).
 - Regardless of the installation, the type of profile server you use may also dictate renaming of profile components. The profile server identifies the server storing the profile components to be used. And, because the profile server types allow for different naming conventions to identify the profile components to be sent to the client, you may need to rename some profile components. Specifically,
 - When using the boot server or a Remote NFS server as the profile server, the profile components sent to the client must be named DEFAULT (to obtain system default profile components), <CLIENT> for workstation profile components, and <USERID> for user profile components.
 - When using a TCM Operations Utility server as the profile server, the profile components sent to the client can be named anything...however, in TCM Operations Utility, you must identify the client in a workstation group and the user in a user group, and have profile components assigned to these groups.

N70 Wireless Support for Flash Booted Clients

IBM High Rate Wireless LAN PCI Adapter support is available for the N70 flash booted clients. This 802.3b PCI Wireless Adapter offers a solution for NetVista Customers who require wireless LAN capability in a Thin Client environment.

This section contains a general description of the steps required to setup the wireless environment. More details on the wireless parameters can be found at <http://www.linux-wlan.com>

To enable wireless on the flash booted N70 client, two options are described. The second option requires more commands to run but allows the user a little more flexibility.

When using a wireless LAN connection, please note the following:

1. The flash recovery and update options are not supported and should not be used.
2. The profile server must be the local flash (boot location) -- profile components must be stored and retrieved from the flash card.

Setup Steps for Both Installation Methods:

1. Install the IBM High Rate Wireless LAN PCI Adapter in your N70. Use the standard bracket and standard length antenna.
2. Power on the N70 and it should boot and present the "IBM NetVista Thin Client Configuration Program" screen. Set the following parameters to the values outlined below:

- Configuration --> Static IP Address
- Network Adapter --> Ethernet
- Boot Mode --> Local
- Client IP --> 0.0.0.0

Move the cursor to highlight the **Save** option and press ENTER to save the changes and continue the boot sequence.

3. The system should continue to boot to the "IBM NetVista Setup Utility". In the Setup Utility, configure the application as appropriate, keep in mind that:

- Profile Server must be the boot location (local flash) -- profile components must reside on the flash card.
- You will need root access to an Xterm to complete configuration of the wireless adapter.
- Set the appropriate DNS for the wireless network in the Server Settings profile component (you can change this profile component by using the Setup Utility menus Profiles->Workstation Profile Components->Server Settings - DNS and Time.

Installation method 1 (recommended): Running as user root, execute the following steps:

1. Copy the sample wlan configuration file (`/etc/wlan.conf.sample`) to file `/configs/wlan.conf`
2. Edit `/configs/wlan.conf` file. Outlined below are the sections of this file that need modification and the symbol --> indicates the particular settings that will most likely need changing. Note, there are two settings that are needed for the initial run: First set the SSID to your AP's SSID. Then set the WEP settings accordingly.

Subset of `/configs/wlan.conf` -- first section to edit:

```

=====
--> USER_MIBS="p2CnfRoamingMode=1 \
-->     p2CnfOwnChannel=6 \
-->     dot11DesiredBSSType=infrastructure"
#=====WEP=====
# [Dis/En]able WEP. Settings only matter if PrivacyInvoked
# is true
--> dot11PrivacyInvoked=true # true|false
dot11WEPDefaultKeyID=0 # 0|1|2|3
dot11ExcludeUnencrypted=true # true|false, in AP this means WEP
# is required for all STAs
# If PRIV_GENSTR is not empty, use PRIV_GENTSTR to generate
# keys (just a convenience)
PRIV_GENERATOR=/sbin/nwepgen # nwepgen, Neesus compatible

```

```
PRIV_KEY128=false # keylength to generate
--> PRIV_GENSTR="snoopy"
```

Subset of /configs/wlan.conf -- second section to edit:

```
#=====STA START=====
# SSID and authtype are all we have for now
AuthType="opensystem" # opensystem | sharedkey
--> DesiredSSID="linux-wlan"
=====
```

3. If static IP address are used in the configuration of the wireless lan, edit the **/configs/rc.local** file and add the following commands:

```
/etc/rc.d/init.d/wlan start wlan0
ifconfig wlan0 <IP> netmask <netmask> broadcast <broadcast>
route add default gw <gateway>
```

4. If DHCP is to be used for IP address, edit the **/configs/rc.local** file and add the following commands:

```
/etc/rc.d/init.d/wlan start wlan0
dhclient wlan0
/etc/rc.d/rc.IBM_NS.env
/etc/rc.d/rc.IBM_NS.netconfig
```

5. Verify the **/configs/rc.local** and **/configs/wlan.conf** files have execute permission, and then restart the N70.

Installation method 2: Running as user root, execute the following steps. Note the **wlanctl-ng** command may require additional parameters.

1. If static IP address are used in the configuration of the wireless lan, edit the **/configs/rc.local** file and add the following commands:

```
insmod -f /lib/modules/2.4.5-IBM/kernel/net/wlan/p80211.o
insmod -f /lib/modules/2.4.5-IBM/kernel/net/wlan/prism2_pci.o
wlanctl-ng wlan0 Inxreq_autojoin ssid=<AP's SSID> authtype=opensystem
ifconfig wlan0 <IP> netmask <netmask> broadcast <broadcast>
route add default gw <gateway>
```

2. If DHCP is to be used for IP address, edit the **/configs/rc.local** file and add the following commands:

```
insmod -f /lib/modules/2.4.5-IBM/kernel/net/wlan/p80211.o
insmod -f /lib/modules/2.4.5-IBM/kernel/net/wlan/prism2_pci.o
wlanctl-ng wlan0 Inxreq_autojoin ssid=<AP's SSID> authtype=opensystem
dhclient wlan0
/etc/rc.d/rc.IBM_NS.env
/etc/rc.d/rc.IBM_NS.netconfig
```

3. Verify the **/configs/rc.local** and **/configs/wlan.conf** files have execute permission, and restart the N70.

Other Noteworthy Items

Case sensitivity

Be aware that Windows NTFS file naming is case insensitive whereas Linux file naming is case sensitive. Therefore from a thin client point of view, the creation of the files ProjectExpansion and Projectexpansion are two different files if they reside on a Linux server, whereas they are the same file if they reside on a Windows server.

Model N70 and Screen Saver

The screen saver setting is ignored when using the model N70. However, the model N70 has advanced power management and therefore after ten minutes of inactivity, the power saver mode is engaged and the monitor screen goes blank (any keyboard or mouse activity automatically restores the previous screen contents).

Printing

The following web site has helpful print support information: <http://www.linuxprinting.org/>

Behaviors to be aware of:

Root user id and screensaver configured to lock

Even when properly configured, the screensaver will not lock the screen for the root user id. The workstation should be locked using the lock ICON or hotkey sequence.

The root password will not unlock the screensaver lock running under another users ID. If the signed in user cannot enter their password, the Network Station should be rebooted.

Local Authentication with Windows Servers - Passwd and adduser commands

If you are using local authentication or have user information stored locally in the password file, using the passwd and adduser commands does not work consistently when booted from a Windows Server. If you receive a "Critical error - immediate abort" error after attempting to use the passwd command or "adduser: unable to lock password file" message when attempting to use the adduser command, you may be seeing this problem. Use the KDE User Manager (User Config from the ICE menu or type 'kuser' from an Xterm window), where you can configure users and change user passwords for local authentication setups.

If you do receive either of those error messages after using either passwd or adduser, there will be lock files created in your /etc directory. As root, you may delete those files.

There are five different potential lock files:

- passwd.lock
- shadow.lock
- pwd.lock
- spwd.*
- pwd.%d.*

- Note: Both the spwd.* and pwd.%d.* files are created with the process id (*) as part of the file name, so you would see names like spwd.317 and pwd.%d.317.

Model N2800 Flash Booted Clients -- Reboot/Logout

When logging out from a flash booted N2800 (the logout menu item is available on the launch bar when set in the Window Manager profile component), the client will actually perform a reboot. The reason for this is to avoid a hang condition which would require a reboot to correct the problem.

Model N70 and Installing RPMs

Installing an RPM from an N70 thin client will not work without first removing a symbolic link and creating a directory. From the N70 thin client, open an Xterm session and issue the following commands (when running as root user):

```
rm /var/lib/rpm
mkdir /var/lib/rpm
```

Following these two commands, you can successfully install an RPM from the N70 thin client.

Model N70 and ICA Audio Support

When using a model N70, the ICA audio support is currently limited to high quality audio. IBM has informed Citrix of this situation.

To set the audio quality for ICA, start the ICA Remote Application Manager (we recommend making the change to the Desktop Settings Profile Component).

- Start the Setup Utility
- Click Profiles and then click User Profile Components
- Click Desktop Settings and click on the currently highlighted desktop setting (or load the profile you want to change)
- Click on 'Start ICA Remote Application Manager' button (this will be on the screen presented if you have a single desktop mode otherwise you will first need to click on the ICA or ICA Remote Application Manager item for the launch bar selections and click Modify to get to the screen with this button).
- Click Continue on the panel explaining the ICA Remote Application Manager will be started in preview mode
- Select the connection you want to modify
- Click Entry and then click Properties
- Click on the top-most button which current says Network and select Connection
- On the screen presented, look at the values set for "Enable Sound" and "Quality" and make the desired changes.

ICA Client Sessions Started from ICA Remote Application Manager

ICA sessions with descriptions that include blank spaces will not start from the ICA Remote Application Manager.

Readme Files, Tutorials and CD Contents

IBM NetVista Thin Client with Turbolinux - for Linux installs

- This install readme includes prerequisites and information about installing on Linux servers.
- Linux location on CD - /Linux/products/nvTCLinux/readme.txt

IBM NetVista Thin Client with Turbolinux - for Windows installs

- This install readme includes prerequisites and information about installing on Windows servers.
- Windows location on the CD - [drive:]\Windows\products\nvTCLinux\readme.txt
- Windows install location - [drive:]\{float}\NetVista_Linux\readme.txt

IBM Turbolinux Thin Client Readme

- (This readme file) Information and tips that are common between the Linux servers and the Windows servers.
- Linux location - /nstation/linux/IBM/ReadmeClient.html
- Windows location - [drive:]\{float}\NetVista_Linux\Linux\IBM\ReadmeClient.html

Contents of IBM NetVista Thin Client with Turbolinux CDs

- IBM NetVista Thin Client with Turbolinux installation CD -- Includes installation programs for both Windows servers and Linux servers on the same CD.
- Turbolinux Workstation 7 CD -- This CD is requested while installing on a Linux server.
- Turbolinux Workstation 7 Source RPM CD -- This CD contains source code for some of the Turbolinux 7 RPM's.

**** End of Document ****