ThinkVantage

Access Connections Deployment Guide

Date: April 15, 2008

ThinkVantage

Access Connections Deployment Guide

Date: April 15, 2008

Third Edition (April 2008)

Preface

This guide is intended for IT administrators, or those who are responsible for deploying the Access Connections™ program on computers in their organizations. The purpose of this guide is to provide the information required for installing Access Connections on one or many computers, provided that licenses for the software are available for each target computer. The Access Connections application provides application help, which administrators and users can consult for information about using the application itself.

ThinkVantage® Technologies is developed for IT professionals and the unique challenges they may encounter. This deployment guide will provide instructions and solutions for working with Access Connections. If you have suggestions or comments, communicate with your Lenovo™ authorized representative. To learn more about the technologies that can help you lower the total cost of ownership and to check for periodic updates to this guide, visit the following Web site:

`www.lenovo.com`

Contents

Chapter 1. Overview

Access Connections is a connectivity assistant program which helps to configure various network connections including wireless LANs. Users can create and manage location profiles that stores the network and Internet configuration settings needed to connect a client computer to a network from a specific location, such as home or at work. The network connection can be made using a modem, a wired network adapter, a broadband device (DSL, cable modem, or ISDN), or a wireless network adapter. Virtual private network (VPN) connections are also supported. By switching between location profiles as you move your computer from place to place, Access Connections can quickly and easily help users connect to a network without having to reconfigure network settings manually. A location profile supports advanced security settings, default printer, and automatic application launch.

Access Connections has the ability to support automatic location switching between Ethernet and wireless LAN connections.

Features

Access Connections has features that enable you to find wireless and network connections quickly and effortlessly. These features increase the portability of your wireless activity. Access Connections includes the following functions:

- **Create new location profiles**

  Access Connections provides a wizard that helps you create location profiles that define the settings required to connect to various types of networks. The Connection Status window is opened by default when Access Connections is started.

- **View location profile and connection status**

  The Connection Status window allows you to view the status of the network connection associated with each location profile defined in Access Connections allowing you to switch between location profiles. When you open the window, status is shown for the network connection and for the components used by the currently applied location profile.

- **Switch between location profiles**

  Access Connections allows you to change location profiles. You can simply choose another location profile from the list and connect to it. A progress indicator window shows the state of the connection. If the connection fails, a button appears to help you fix the connection.

- **Wireless Connectivity**

  Access Connections software accommodates wireless wide area networking (WAN) and Bluetooth Technology. With the introduction of 3G cellular technologies, wireless WAN services are emerging as effective alternatives for high-speed wireless access to networks. Access Connections provides portability when users are away from the office and not near a public WLAN hot spot.

- **Find wireless networks.**

  Access Connections can search for wireless networks that are in range of your wireless adapter. This feature is useful when you are traveling or in a public place, and you are not sure about what, if any, wireless networks are available to you. You can attempt to connect to any wireless networks that are found. If the

connection attempt is successful, a new wireless location profile will be created using the detected wireless network name and default settings. You can also manually create a location profile for a detected wireless network if you know the appropriate settings.

- **Automatic switching of location profiles**

  If a network associated with your currently applied location profile becomes unavailable, Access Connection can search for available networks and automatically switch to a matching location profile. You can automatically switch between wireless location profiles, and Ethernet location profiles. You can establish a wireless priority list that allows you to define which wireless location profile will be made active when your computer is in range of multiple wireless networks, or when more than one location profile uses the same wireless network name.

- **Create location profiles for remote deployment administrator only**

  An Access Connections administrator can define location profiles for export to the client computers.

  Access Connections provides an icon in the system tray which allows you to launch the application, view the status of the current location profile, and switch between profiles.

Considerations for deploying Access Connections

Collecting information about the various places where users might attempt to connect and the kinds of connections available in those locations will help you develop pre-configured profiles that users can import and use right away. By capturing working configurations in profiles which can be deployed with the initial image, support calls can be reduced and users can immediately take advantage of their network connections without intervention.

The Administrator Feature Enabler tool available with version 4.0 or later simplifies the task of deploying location profiles, global settings, and control policies to individuals or groups of individuals running Access Connections in a corporate environment. The deployment of profiles and settings can be accomplished during the initial system deployment as part of the preload image or after systems are in the field using standard remote deployment methods.

Requirements and specifications for deployment

To view the current list of supported ThinkPad® systems and wireless WLAN and WAN drivers, see the following Web site:

`http://www.lenovo.com/pc/support/site.wss/document.do?sitestyle=lenovo&lndocid=MIGR-4ZLNJB`

Access Connections deployment features

The Access Connections Administrator Profile Deployment feature is required to deploy location profiles that you create for client users. The Administrator Profile Deployment feature is available to IT professionals only at:

`http://www.lenovo.com/pc/support/site.wss/document.do?sitestyle=lenovo&lndocid=ACON-DEPLOY`

For more information about the Administrator Profile Deployment feature, see: Chapter 3, “Working with the Administrator Feature,” on page 7.

The following list of features help IT administrators deploy and manage Access Connections:

- Administrators can create location profiles and distribute them as part of a preload image or install them after the client systems have been deployed.
- Control policies can be set for each profile.
- Distribution control lists can be created to limit who can import various deployment packages.
- A client configuration policy can be set to configure the operation of Access Connections on the client computer.
- Deployment packages are encrypted and password protected to be sure that only authorized individuals can import the location profiles that may contain wireless security information such as WEP or static password, for example.

Chapter 2. Installing Access Connections

The following instructions provide installation procedures for the standalone version of Access Connections. For instructions on installation of the integrated Access Connections package, see Appendix B, “Integrated Packaging,” on page 31.

Installing Access Connections without user interaction

To install Access Connections without user interaction, complete the following steps:

1. Start Microsoft® Windows® 2000, Windows XP, or Windows Vista® and then log on with administrative privileges.
2. Extract the Access Connections software package to the hard disk drive. For example: C:\Drivers\W2k\Accon.
3. Click **Start**, and then click **Run**.
4. The following command can be used to install Access Connections.
   a. To install interactively, type:
      ```
      <path>\setup.exe
      ```
   b. To install silently with default path for install log, type:
      ```
      <path>\setup.exe -S-SMS-f2x
      ```
   c. To install silently with customized setup script with log path specified, type:
      ```
      <path>\setup.exe -S-SMS-f1<fullpath>\setup.iss-f2<path>\setup.log.
      ```
   d. To install silently from a CD, type:
      ```
      <path>\silent.bat
      ```

Note: If you are installing Access Connections onto Windows Vista, install the Access Connections designed specifically for Windows Vista. Other versions of Access Connections may not function properly with the Vista operating system.

Uninstalling Access Connections

To uninstall Access Connections, complete the following steps:

1. Start Windows 2000, Windows XP or Windows Vista, and then log on with administrative privileges.
2. Click **Start**, then click **Run**.
3. The following commands will uninstall Access Connections:
   a. To uninstall interactively type,
      ```
      <path>\setup.exe -0x9 anything
      ```
   b. To uninstall silently with a customized script,
      1) Create a uninst.iss file by completing the following steps:
         a) Go to the Access Connections install directory and Run setup.exe -r -remove.
         b) Click **Uninstall** when prompted.
         c) Click **No** to restart the system later. This will prevent automatic restart.
         d) Copy the script file generated at C:\Windows\setup.iss to your local directory.

e) Rename the script file to uninst.iss.

2) Enter the following command:

```
<path>\setup.exe -S-f1<fullpath>\uninst.iss anything -f2x
```

Chapter 3. Working with the Administrator Feature

This chapter provides you with the information you need to enable and use the administrator features of Access Connections.

Enabling the Administrator feature

Access Connections must be installed on your system prior to enabling the Administrator feature. To enable the Administrator feature, complete the following steps:

1. To deploy Access Connections on to client systems, download and install the Administrator Profile Deployment feature from the following Lenovo Web site:

   `http://www.lenovo.com/pc/support/site.wss/document.do?sitestyle=lenovo&lndocid=ACON-DEPLOY`

   Note: The Import/Export feature of Access Connections is used for migrating profiles only. Do not use the Import/Export feature for deploying Access Connections.
2. Run AdmEnblr.exe that is installed in the following path:

   `C:\Program Files\ThinkPad\ConnectUtilities`
3. Click **Enable**, and then click **Exit**. This will create the deployment feature menu on Access Connection main application panel.

Figure 1. Enabler for Administrator Profile Deployment Feature for Windows 2000 and XP

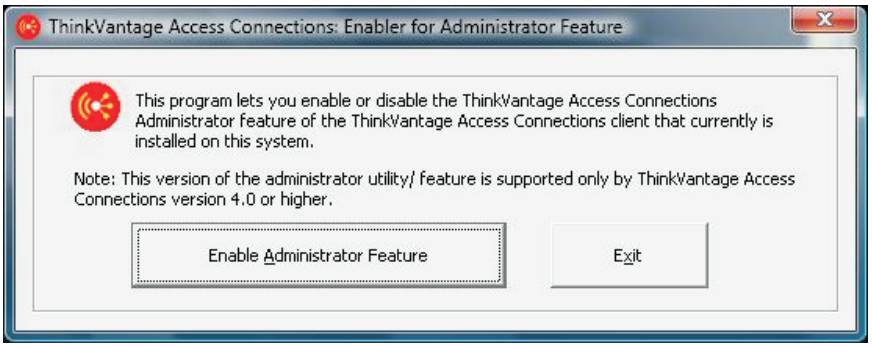

Figure 2. Enabler for Administrator Profile Deployment Feature for Windows Vista

4. Click **Enable Administrator Feature**.
5. Click **Exit** to close the Enabler.
6. Start Access Connections.

Using the Administrator feature

After you have enabled the administrator feature, you can manage location profiles for users by creating or editing distribution packages. Distribution packages have the file extension of .loa and contains the metadata for location profiles used by Access Connections. The following steps provide the ideal scenario for using the administrator feature of Access Connections:

1. Using Access Connections, create location profiles. Consider the following scenarios as you create the location profiles:
   - Office and building connections
   - Home connections
   - Branch-office connections
   - Connections while traveling and hot-spot connections

   For instructions on how to create location profiles, or how to use Access Connections, see the Access Connections User's Guide located at the following Lenovo Web site:

   `http://www.lenovo.com/pc/support/site.wss/document.do?sitestyle=lenovo&lndocid=MIGR-63042`
2. Create or edit a distribution package with the Administrator Profile Deployment feature.
3. Deploy the distribution package to client systems.

Creating a distribution package

Complete the following steps to create a distribution package:

1. Click **Profile Distribution** and then click **Create Distribution Package**.

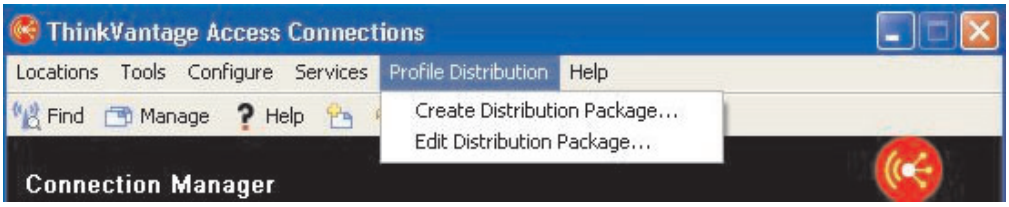

Figure 3. Create Distribution Package

2. Select the location profiles that you want to deploy. If a profile that is selected contains a wireless profile with encryption enabled, you will be prompted to re-enter the wireless settings data to ensure sensitive data is not exposed. When deploying location profiles that provide a wireless network connection, the donor and recipient must contain wireless adapters which support the capabilities defined in the location profile. If the location profile being deployed is configured for LEAP authentication, the adapters on the recipient systems must support LEAP authentication.

The following screen captures provide examples for Windows 2000 or XP, and Windows Vista:

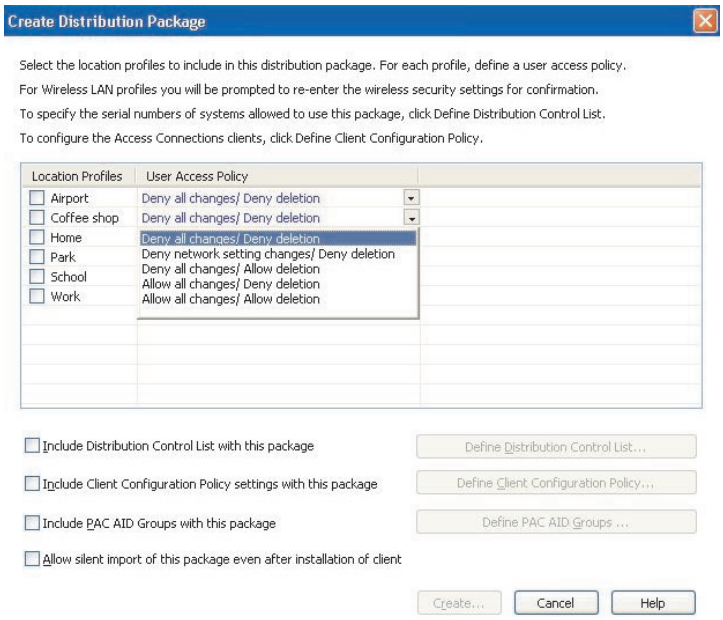

Figure 4. Create Distribution Package panel for Windows 2000 and XP

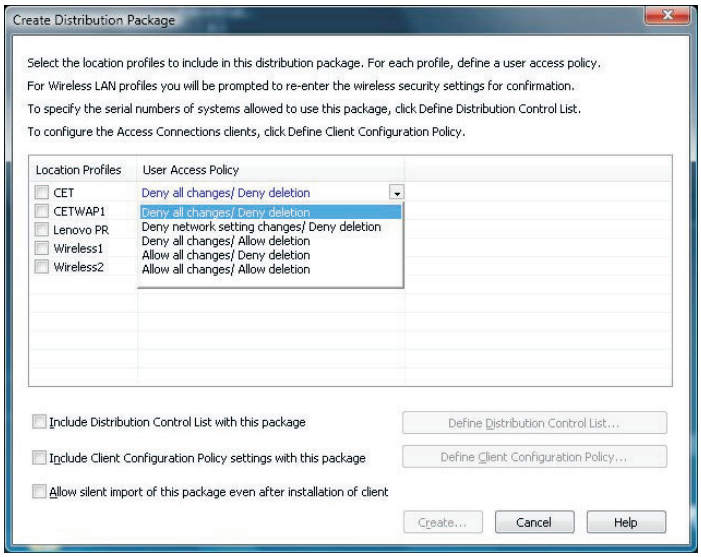

Figure 5. Create Distribution Package panel for Windows Vista

3. Select the **User Access Policy** from the drop down menu. The user access policy defines the restrictions that are in place for a particular profile. User access policies can be defined per profile and can have the following values:
   - **Deny all changes / Deny Deletion**: Users cannot perform operations such as modify, copy, or delete on the profile.
   - **Deny network setting changes / Deny deletion**: The network settings in the profile cannot be modified, deleted or copied. The non-modifiable parameters are TCP/IP settings, Advanced TCP/IP settings, and wireless settings. The profile cannot be deleted.

- **Deny all changes / Allow deletion**: Users can not modify or copy the profile; however, users can delete the profile.
- **Allow all changes / Deny deletion**: Users can modify the profile; however, users cannot delete the profile.
- **Allow all changes / Allow deletion**: Users can modify, copy and delete the profile.

4. Define the Access Connections policy settings for the following options:
   - "Distribution Control List with this package"
   - "Client Configuration Policy" on page 11
   - "PAC AID Groups with this package (Windows 2000 and XP only)" on page 18
   - "Allow silent import of this package after client installation" on page 20
5. Click the **Create** button located at the bottom of the **Create Distribution Package** panel.
6. When prompted, enter a passphrase to encrypt the *.loa file. This same passphrase will be required to import the deployment package (*.loa) on client systems. The passphrase is also encrypted in a *.sig file which is needed to import the deployment package silently.
7. On the Export Location Profiles dialog box, navigate to your applicable directory path. and type the name for your .loa file. By default, the .loa and .sig files which are required for deployment are saved in C:\Program Files\Thinkpad\ConnectionUtilities\Loa directory.

   Attention: For image deployment, the *.loa file must reside in the Access Connections install directory - (C:\PROGRAM FILES\THINKPAD\CONNECTUTILITIES).
8. Click **Save**.

Defining policies for Access Connections

The following settings control the Access Connections policies for the user. If you do not set a policy, the applicable function will be greyed out for the user.

Distribution Control List with this package

This setting is used to define the Distribution Control List based on computer serial numbers.

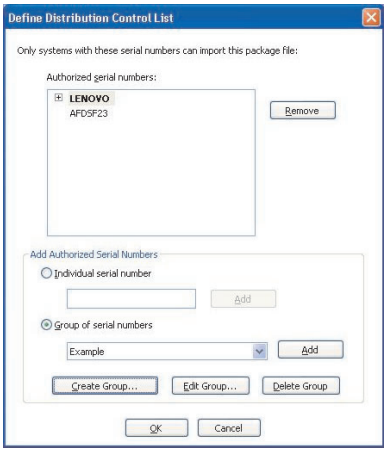

Figure 6. Define Distribution Control list

This method of distribution enables you to type individual serial numbers or to create different groups of serial numbers that represent different organizations of users who need different location profiles. This optional step is designed primarily for securing the distribution of the profile location file (*.loa), when it is being sent to remote users for manual importing. Distribution control lists ensure that individuals install appropriate network connection profiles only. The Distribution Control List helps reduce unauthorized network access.

Creating Groups: When creating groups of serial numbers, flat text files can be imported which contain the group of serial numbers.

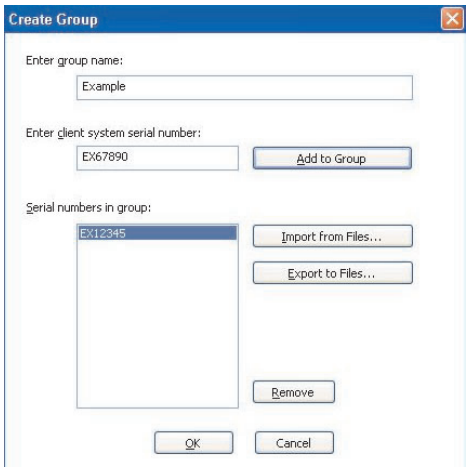

Figure 7. Create Group

The file must be formatted such that each line contains a single serial number. These text files can be created by exporting a list that has been created with the Administrator Feature or by an asset management system if it has such capabilities. This simplifies the process of controlling distribution to a large number of computers based on their serial number.

Client Configuration Policy

This setting defines the Client Configuration Policy, which controls the capabilities that will be available to the user after the *.loa file is imported. Marking the box beside **Do not allow clients to become an administrator:** will prevent users from enabling the Administrator Feature on their installation of Access Connections. This setting is useful in large enterprise environments when you want to prevent others from creating and distributing network access profiles. You can also control a users ability to complete the following tasks:

- Create, import and export location profiles.
- Change global settings, see “Global settings” on page 12.
- Create and apply WLAN location profiles using the Find Wireless Network function for Windows users without administrator privileges.
- Automatic location profile switching.
- Checking for updates.

The following screen capture displays the settings you can configure for the Client tab of the Client Configuration Policy:

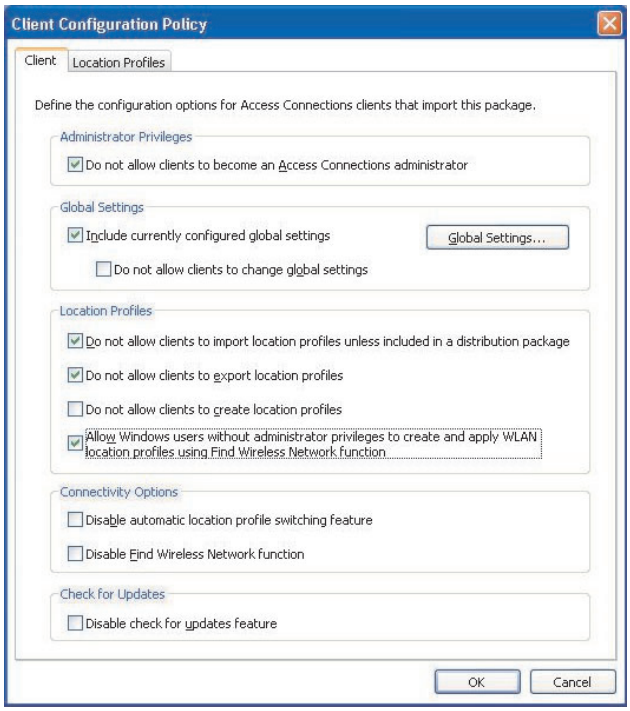

Figure 8. Client Configuration Policy

Marking the box beside **Do not allow clients to become an administrator:** will prevent users from enabling the Administrator Feature on their installation of Access Connections. This setting is useful in large enterprise environments when you want to prevent others from creating and distributing network access profiles. You can also control a users ability to complete the following tasks:

- Create, import and export location profiles.
- Change global settings, see "Global settings."
- Create and apply WLAN location profiles using the Find Wireless Network function for Windows users without administrator privileges.
- Automatic location profile switching.
- Checking for updates.

Global settings: On the **Network** panel of Global Settings, you can set the following policies:

- **Allow Windows users without administrator privileges to create and apply location profiles**
- **Allow wireless connection at Windows logon**
- **Close all wireless network connections when a user logs off**
- **Disable Adhoc connection type option in wireless LAN profiles**
- **Enable automatic wireless LAN radio control**
- **Allow selection of location profiles with Fn+F5 On Screen Display menu**
- **Disable Ethernet adapter when Ethernet cable is unplugged**

  Note: If this setting is enabled, the Ethernet port will be disabled when the Ethernet cable is unplugged from the system. The Ethernet port will remain

disabled even when the Ethernet cable is plugged in again. To re-enable the Ethernet port, manually apply the profile for the Ethernet connection.

- **Enable auto deletion of unused profiles**
- **Disable the Peer to Peer community feature**

The following screen captures provide examples for the Global Settings panel for Access Connections when installed on the Windows 2000 or XP operating system, and for Access Connections when installed on the Windows Vista operating system:

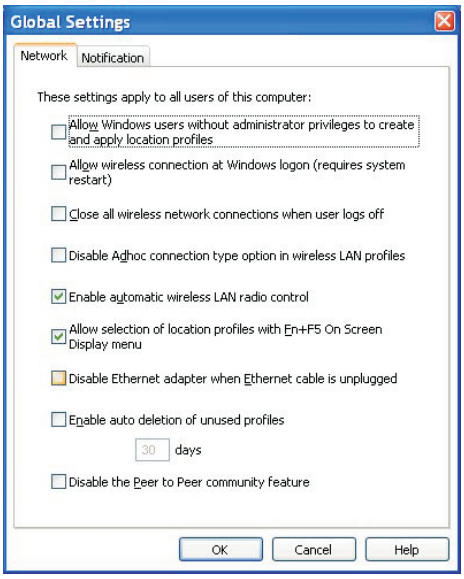

Figure 9. Network Global Settings for Windows 2000 and XP

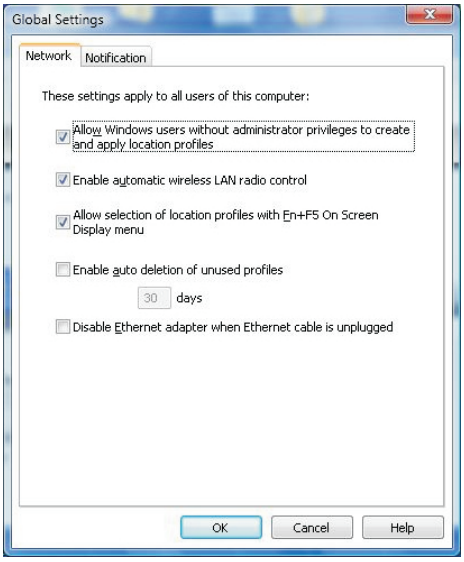

Figure 10. Network Global Settings panel for Windows Vista

On the **Notification** panel of Global settings, you can set the following policies:

- **Show ThinkVantage Access Connections status icon in task tray**
- **Show the wireless status icon in the task tray**
- **Display the progress indicator window when a profile is being applied**

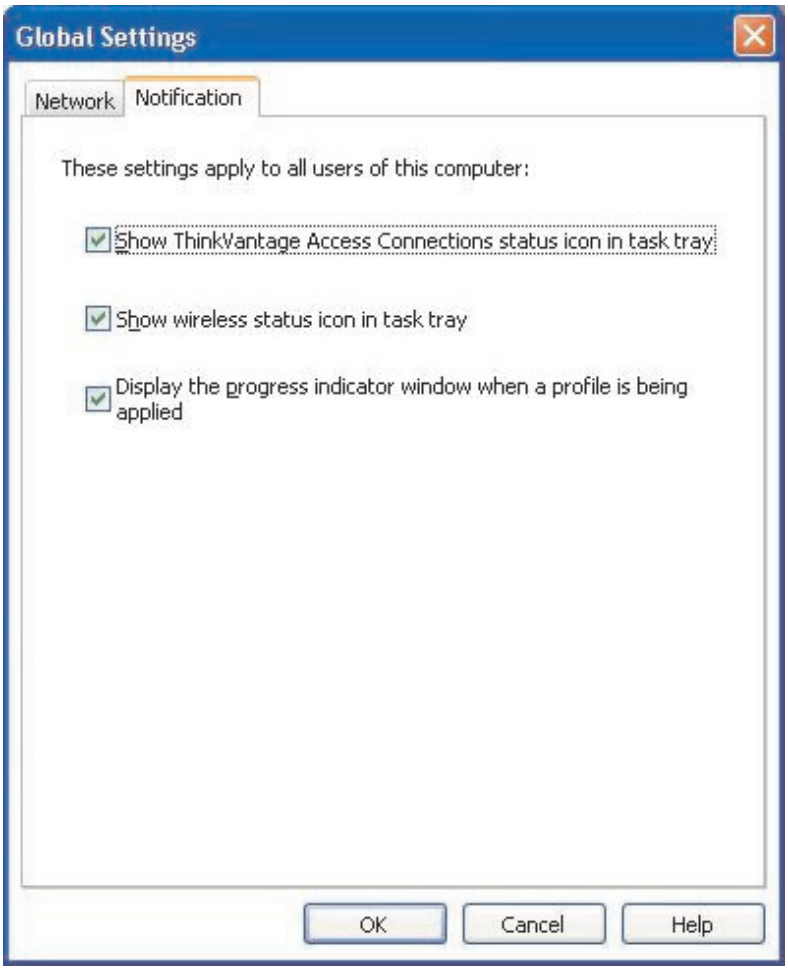

Figure 11. Notification for Global Settings

Location Profiles: Set the following Internet Explorer policies:

- **Set browser home page**
- **Set proxy settings**

For the Optional Settings, you can set the following policies:

- **Security settings**
- **Start applications automatically**
- **Set default printer**
- **Use VPN connection**
- **Override TCP/IP and DNS defaults**

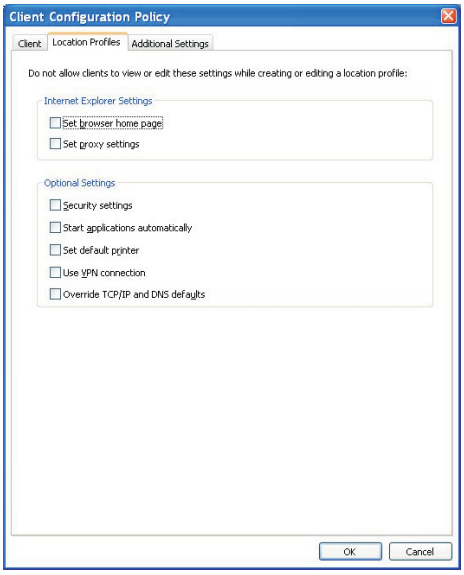

Figure 12. Define Location Profiles

Additional Settings for Windows XP: Using the Windows XP operating system, you can set the following policies on the Additional Settings tab for Access Connections:

General Options

- Do not show warning message when connecting to an unencrypted network
- Do not show the Services menu

Roaming Options

- Do not automatically include the new Wired/Wireless profile in the new roaming list

  Note: If this option is selected, all the new Wired/Wireless profiles will not be added to automatic locations switching.
- Do not allow clients to change automatic location switching settings

  Note: If this option is selected, the automatic location switching settings for the end users is greyed out.
- Do not automatically include wireless profiles without security in the roaming list

Note: If this option is selected, none encryption profile will not be added to the automatic location switching.

Default Options for Additional Settings

- Network Security
  - Disable internet connection sharing
  - Enable Windows firewall
  - Disable file and printer sharing
- Start applications automatically
- Set default printer
- Override TCP/IP and DNS defaults
- Enable VPN connection
- Override Home page
- Override Proxy Configurations

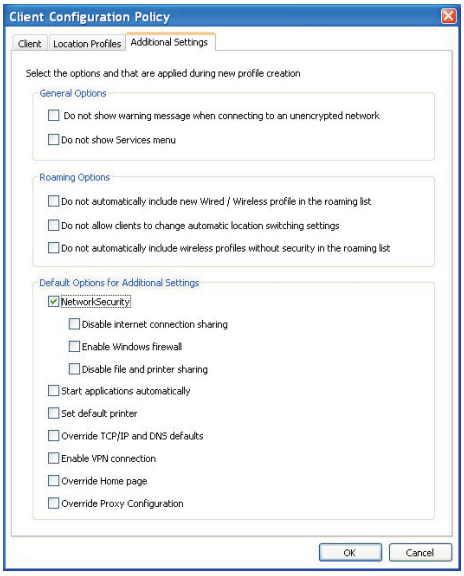

Figure 13. Additional Settings for Windows XP

Additional Settings for Vista: Using the Windows Vista operating system, you can set the following policies on the Additional Settings tab for Access Connections:

General Options

- Do not show warning message when connecting to an unencrypted network
- Automatically create location profiles using Active Directory deployed wireless settings

Roaming Options

- Include the new Wired/Wireless profile in the roaming list automatically
- Do not allow clients to change automatic location switching settings

Default Options for Additional Settings

- Network Security
  - Disable internet connection sharing

  - Enable Windows firewall
  - Disable file and printer sharing
- Start applications automatically
- Set default printer
- Override TCP/IP and DNS defaults
- Enable VPN connection
- Override Home page
- Override Proxy Configurations

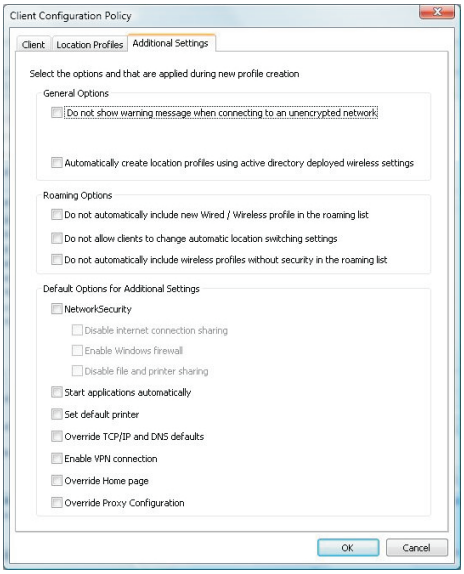

Figure 14. Additional Settings for Windows Vista

PAC AID Groups with this package (Windows 2000 and XP only)

Protected Access Credentials (PAC) protects user credentials that are exchanged with the Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) and a PAC key. All EAP-FAST authenticators are identified by an authority identity (AID).

The local authenticator sends its AID to an authenticating client, and the client checks the PAC AID group referenced in the location profile being applied, to see if the authenticating AID belongs to the group. If yes, then the client tries to use an existing PAC if available with out any confirmatory message. If not, then a confirmatory message is shown to the user to use the existing PAC. If a matching PAC does not exist for the user, then the client system requests a new PAC.

The .loa package imports and exports the PAC AID Groups to target systems. To include PAC AID Groups when you create the distribution package, mark the check box **Include PAC AID Groups with this package**:

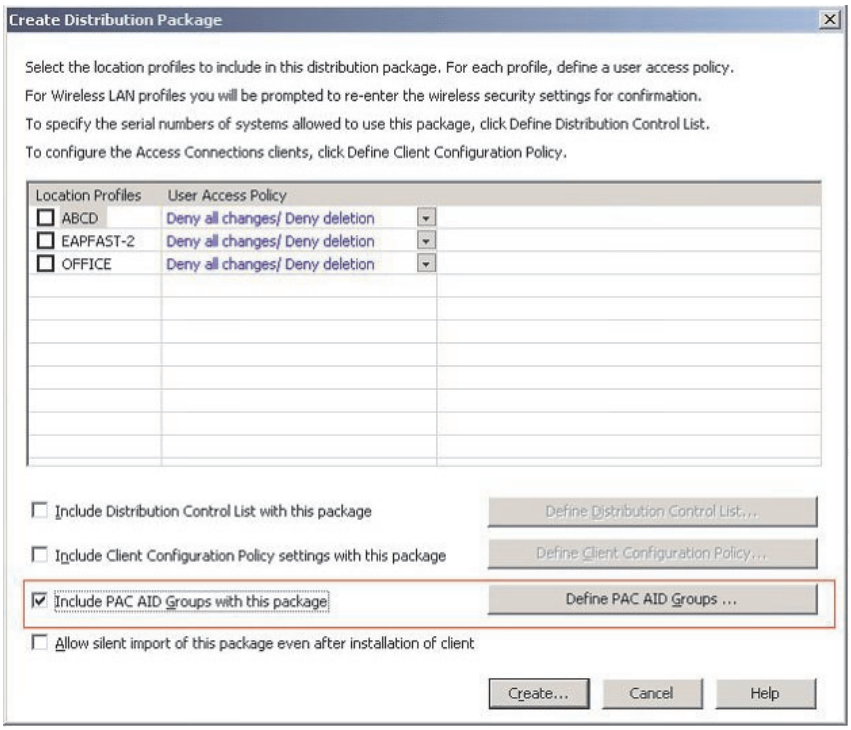

Figure 15. Create Distribution Package

Create a new PAC AID Group by completing the following steps:

1. On the Define PAC AID Groups panel, click **Groups**.
2. Right click on **Available Pacs**.

   Note: The PAC with the AID which is intended to included in the Group must be present on the machine where the AID group is being created.
3. From the drop down menu, click **Create Group**.

You can add or remove PAC AID Groups to a distribution package. To add a group, select it from the drop down menu and click **Add**. To remove a group, select the group from the available PAC AIDS list and then click **Remove**.

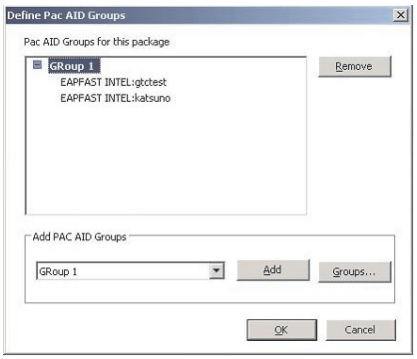

Figure 16. Creating PAC AID Groups

Allow silent import of this package after client installation

By default, profiles in a *.loa file cannot be imported silently by Access Connections once it has been installed. Deployment packages (consisting of *.loa and *.sig files) created with the check box on Figure 15 on page 19 can be copied to the installation folder of Access Connections and will be detected and imported silently on the next reboot.

Chapter 4. Deploying Access Connections

After creating the location profiles required for client users, you can also manage and deploy new, updated, or revised location profiles to client computers. The following examples describe deployment scenarios used in deploying Access Connections:

- Deploy Access Connections and Location Profiles on new client computers.
- Deploy Location Profiles and Client Policy on existing client computers running Access Connections.
- Upgrade existing Access Connections and migrate Location Profiles on existing client computers.

Deploy on new computers

To deploy Access Connections location profiles on new computers that do not have Access Connections installed, complete the following steps:

1. Create an Access Connections distribution package (*.loa and *.sig) with the Location Profiles that contain the desired user access policy and client configuration policy as described in Chapter 3, "Working with the Administrator Feature," on page 7. For unattended import, enable the setting **Allow silent import of this package even after installation of client** while creating the .loa file.
2. Create an integrated package as described inAppendix B, "Integrated Packaging," on page 31 with Access Connections, Wireless LAN driver/application, Hotkey Fn+F5 utility, and Power Management driver.
3. Include the distribution package .loa and .sig files in the CONWIZ folder of the integrated package. You can choose not to include the distribution package in the integrated package and instead after the installation of the integrated package or Access Connections, copy them into the Access Connections installed directory (default installed directory is C:\Program Files\ThinkPad\ConnectUtilities).
4. Install the integrated package as desired for attended or unattended mode, as described in Appendix B, "Integrated Packaging," on page 31.
5. After restarting the system, Access Connection is runs automatically, detect and import the distribution package silently. If the silent import option was not selected, a user can select import from the manage profiles window and manually import the package by providing the same passphrase at the prompt that was used to create the package by administrator.

Deploy on existing client computers

To deploy Access Connections location profiles on existing computers that have Access Connections already installed and running, complete the following steps:

1. Create an Access Connections distribution package (*.loa and *.sig) with the location profiles that contain the desired user access policy and client configuration policy as described in Chapter 3, "Working with the Administrator Feature," on page 7 earlier. If only the client configuration policy needs to be modified, you can create a distribution package without exporting any profiles but only include the modified client configuration policy. For

unattended import, enable the setting **Allow silent import of this package even after installation of client** while creating the .loa file.

2. Copy the distribution package (*.loa and *.sig) into the Access Connections installed directory (default installed directory is C:\Program Files\ThinkPad\ConnectUtilities) of the existing client computer.
3. After restarting the system, Access Connection runs automatically and detects the distribution package and import the package. The import can be forced by using the following commands:

```
<path> \qctray.exe /importsilently
<path> \qctray.exe /killac
<path> \qctray.exe /startac
```

Deleting locked profiles

There are two ways to delete a locked Access Connections profile.

1. Uninstall Access Connections with profiles from Add/Remove programs on the client system.
2. To delete locked profiles remotely complete the following steps:
   - Create another unlocked .loa profile which has the same name and passphrase as the originally deployed in the .loa file.
   - Deploy the.loa file that you created to client systems.
   - Use following command to delete the profile:

     ```
     <path>\qctray.exe/del<location profile name>
     ```

Updating deployed Profiles

To update your currently deployed profiles to new encryption and security settings, you will have to create another .loa profile with the same name and passphrase of the originally deployed .loa profile. Deploy this newly created .loa to client systems.

Upgrade Access Connections on existing computers

To upgrade Access Connections to newer version and migrate the existing location profiles on existing client computers, complete the following steps:

1. Create an integrated package as described in Appendix B, “Integrated Packaging,” on page 31 with the new version of Access Connections, recommended version of wireless LAN driver/application, Hotkey Fn+F5 utility, and Power Management driver.
2. Install the integrated package as desired in attended or unattended mode and described in Appendix B, “Integrated Packaging,” on page 31. This will overinstall the older version without removing the location profiles and keeps all other existing settings.
3. After restarting the system, Access Connection runs automatically and will detect the existing location profiles and automatically migrate to the newer version.

Chapter 5. Working with Active Directory and ADM files

Active Directory provides a mechanism that gives administrators the ability to manage computers, groups, end users, domains, security policies, and any type of user-defined objects. The mechanisms used by Active Directory to accomplish this are known as Group Policy and Administrative Template files (ADM). With Group Policy and ADM files, administrators define settings that can be applied to computers or users in the domain.

For more information about Active Directory or Group Policy, see the following Microsoft Web site:

`http://www.microsoft.com`

Adding Administrative Templates

Designed to save your time and effort, Lenovo provides an Administrative Template file, "tvtacad.adm", which can be used with Group Policy to set the configuration policies for Access Connections. The tvtacad.adm file can be downloaded from Lenovo Web site.

Complete the following steps for adding the Access Connections Administrative Template (ADM file) to the Group Policy editor:

1. On the machine running the Active Directory server, click **Start Menu** > **Control Panel** > **Administrative Tools** > **Group Policy Management**. The Group Management console is opened.
2. Right click on **Default Domain Policy** node, and select **Edit**. The Group Policy Object Editor is displayed.
3. Under **Computer Configuration**, right click on **Administrative Templates**.
4. Click **Add** , and then select the tvtacad.adm file.
5. Click **Close** on the Add/Remove Templates dialog box.
6. Under the **Computer Configuration**, click the **Administrative Templates**. A new tab named **ThinkVantage** is present. Under the **ThinkVantage** tab there will be a **Access Connections** tab. All the available settings can be configured now for this machine.

Installing the client configuration plugin for Access Connections

Designed to save you time and effort, Lenovo has provided supplemental plug-in files to set client configuration policies for Access Connections. The following supplemental file is compressed in the acplgin45.exe:

- **tvtacad.adm** - This administrative template is used with Group Policy to set the configuration policies for Access Connections.

This file supports Access Connections 4.2 and above.

Group Policy settings

This table provides policies settings for Access Connections that can be modified using the ADM file template.

Table 1. Computer Configuration > Administrative Templates > ThinkVantage > Access Connections

Policy setting	Description
Block admin feature	Do not allow clients to use Access Connections administrator feature so that they can not deploy profiles or policies.
Block create profile	Do not allow clients to create location profiles.
Block export	Do not allow clients to export location profiles.
Block global setting changes	Do not allow clients to modify the global settings set by this policy.
Block import	Do not allow clients to import location profiles unless the location profiles are included in a distribution package.
Close connection at logoff	To enhance security, wireless connection would be disconnected when user logs off. This setting is not available in Windows Vista.
Default enable VPN	**Enable VPN connection** button is enabled by default.
Default ICF	**Enable Windows firewall** button is enabled by default.
Default ICS	**Disable internet connection** button is enabled by default.
Default network security	**Network security** button is enabled by default.
Default override homepage	**Override home page** button is enabled by default.
Default override proxy config	**Override proxy configuration** button is enabled by default.
Default override TCPIP	**Override TCP/IP and DNS defaults** button is enabled by default.
Default printer share	**Disable File and printer sharing** button is enabled by default.
Default set printer	**Set default printer** button is enabled by default.
Default start applications	**Start applications automatically** button is enabled by default.
Default roaming selection for no sec WLAN profile	Newly created wireless profile with no security will not be automatically included in the roaming list.
Default roaming selection for profile	Newly created wired or wireless profile will not be automatically included in the roaming list.
Disable adhoc	Adhoc connection type will not be available when creating wireless LAN profiles. This setting is not available in Windows Vista.
Disable auto switching	Disable the automatic location profile switching feature.
Disable check update	Disable the check for updates feature.
Disable ethernet adapter	Ethernet adapter will be disabled when the Ethernet cable is plugged out.
Disable find wireless network	Disable the Find Wireless Network function.

Table 1. Computer Configuration > Administrative Templates > ThinkVantage > Access Connections (continued)

Policy setting	Description
Disable location switching feature changes	Automatic location switching can not be changed by clients.
Disable peer to peer community	The Peer to Peer community feature will not be available. This setting is not available in Windows Vista.
Enable auto WLAN radio control	When automatic wireless LAN radio control is enabled, wireless radio would be turned off automatically whenever it is not associated with any access points to save power and enhance security.
Enable create profile with FWN	Allow Windows users without administrator privileges to create and apply WLAN location profiles using Find Wireless Network function.
Enable FnF5 menu	Location profiles can be switched from Fn+F5 On Screen Display menu.
Enable single sign on	The wireless connection would be established at Windows logon. The wireless authentication can be configured to use the Windows logon credentials. After enabling this option, system restart is required. Not available Windows Vista.
Enable user mode	Users with limited privileges are allowed to create new location profiles with Ethernet or wireless connections and switch between any existing location profiles provided Access Connections administrator enables this option.
Hide browser homepage setting	Do not allow clients to view or edit browser home page setting in location profile.
Hide browser proxy setting	Do not allow clients to view or edit browser proxy setting in location profile.
Hide printer	Do not allow clients to view or edit default printer setting in location profile.
Hide security setting	Do not allow clients to view or edit security setting in location profile.
Hide services menu	Do not show services menu. This setting is not available in Windows Vista.
Hide start application	Do not allow clients to view or edit start applications automatically setting in location profile.
Hide TCPIP	Do not allow clients to view or edit Override TCP/IP and DNS settings.
Hide VPN	Do not allow clients to view or edit VPN connection setting in location profile.
Hide warning msg for unencrypted NW	Warning message will not be displayed when connecting to an unencrypted network.
Show ACTray icon	**Access Connection status** icon would be added in task tray notification area.
Show wireless tray icon	**Wireless LAN and WAN status** icon would be added in task tray notification area.
Show progress indicator	The progress indicator windows showing the status while connecting would be displayed.

Deploying .LOA and .SIG files through Active Directory with logon scripts

The .loa file and .sig file will be stored in c:\programfiles\thinkpad\connectutilities\LOA. When deploying the .loa and .sig files through Active Directory with logon scripts, mark the check box **Allow silent import of this package even after installation of client** on the Create Distribution Package panel of Access Connections.

For additional information about .loa and .sig files, see Chapter 3, "Working with the Administrator Feature," on page 7.

Adding logon scripts into Group policy

The following steps provide instruction on how to setup logon scripts for the user or computer in Group policy:

1. Launch the Group policy Management editor.
2. Right click on the domain name and click **Create and Link GPO**.
3. Type the name of your Group Policy Object (GPO).
4. Right click on your GPO name, and then click **Edit**.
5. From the Group Policy Object Editor panel, navigate to the following:
   `User Configuration->Windows Settings->Scripts (Logon/Logoff)->Logon`
6. From the Logon Properties panel, select the Acloa.bat file and then click **Add**.
7. On the Add a Script dialog box, click **Browse** and select your script.
8. Click **OK**.
9. Copy the Acloa.bat file your Logon scripts location.
10. Click **Open**, and the Logon bat file will be added.
11. On the ADS Test panel under the Security Filtering section, click **Add** to give rights to a user, group or computer.

Creating the Acloa.bat file

You can use the following example to create the Acloa.bat file:

```
:Begin

If exist "c:\program files\thinkpad\connectutilities4\
Silent.txt" goto SilentImportDoneBefore

copy \\conwiz.com\NETLOGON\user01\*.* "c:\program files\
thinkpad\connectutilities4"

cd c:\program files\thinkpad\connectutilities4

qctray /importsilently

Echo Silent Import was performed > "c:\program files\
thinkpad\connectutilities4\Silent.txt"
Echo Silent Import was performed
goto SilentImportDone

:SilentImportDoneBefore
Echo Silent Import was done before


:SilentImportDone
```

Acloa.bat

When a user logs onto a domain, the Acloa.bat executes and does the following:

- Checks for the file silent.txt at the following client location:

  ```
  c:\programfiles\thinkpad\connectutilities
  ```

- If the silent.txt file exists, it does not copy the .loa and .sig files but exits.
- If the silent.txt file does not exist, it copies the. loa and .sig files from the server to client:

  ```
  c:\programfiles\thinkpad\connectutilities
  ```

- To import the profile into Access Connections silently, execute the following command

  ```
  qctray /silentimport
  ```

- This creates a file called silent.txt at c:\programfiles\thinkpad\connectutilities and ends the operation.

Appendix A. Command line interface

Access Connections can accept command line input to switch between location profiles and to import or export locations profiles. You can input these commands interactively within a command prompt window, or you can create batch files for use by other users. Access Connections does not need to be running before these commands are executed.

- Apply Location Profile.

  <path>\qctray.exe/set <location profile name>
- Disconnect Location Profile.

  <path>\qctray.exe/reset <location profile name>
- Delete Location Profile.

  <path>\qctray.exe/del <location profile name>
- Import Location Profile (valid only for files with .LOC extension)

  <path>\qctray.exe/imp <location profile path>
- Perform silent imports of all profiles.

  <path>\qctray.exe/importsilently
- Export Location Profiles (valid only for files with .LOC extension.)

  <path>\qctray.exe/exp <location profile path>
- Apply a test SSID profile for wireless cards (regardless of which profile was most recently active) and return immediately. Do not turn off the Wireless Radio

  <path>\qctray.exe/disconnectwl
- Close AcMainFUI, Ac Tray, AcWIIcon modules.

  <path>\qctray.exe/exit
- Enter a special monitor mode in which all roaming is blocked, Ethernet as well as Wireless. Also when the third party application that has called this API is closed, reset the monitor mode

  <path>\qctray.exe/setmonitormode
- Reset the monitor mode

  <path>\qctray.exe/resetmonitormode
- Stop all Access Connections processes. Considering this requires administrative privileges, the command will be routed through AcPrfMgrSvc to close all other Access Connections processes except for profile manager service.

  <path>\qctray.exe/killac
- Restart all Access Connections processes. Considering this requires administrative privileges, the command will be routed through AcPrfMgrSvc.

  <path>\qctray.exe/startac
- Find Wireless networks.

  <path>\qctray.exe /findwInw
- Display QCTRAY help information.

  <path>\qctray.exe /help

Appendix B. Integrated Packaging

Designed for the challenging deadlines of IT professionals, Lenovo provides Integrated Packaging for Access Communications. Integrated Packaging is used to simplify the installation process by bundling installation files.

The integrated Access Connections package

This scenario provides information on how to complete an integrated package installation for Access Connections that requires no user interaction. For this integrated package installation, obtain Access Connections version 3.82. Access Connections version 3.82 can be obtained under the Previous version downloads section at the following Lenovo Web site:

`http://www.lenovo.com/pc/support/site.wss/document.do?sitestyle=lenovo&lndocid=MIGR-4ZLNJB`

1. Download the following package:

   `Access Connections version 3.82 with wireless drivers`

   This package includes an earlier version of Access Connections and relevant drivers and setup utility files needed to create the integrated package installation. Extract the package by running the download executable. The default directory where modules are extracted is C:\Drivers\W2K\ACCONWLD.
2. Download and extract each of the following:
   - **Access Connections** (latest version)

     The latest version of Access Connections can be downloaded from the Lenovo Web site at:

     `http://www.lenovo.com/pc/support/site.wss/document.do?sitestyle=lenovo&lndocid=MIGR-4ZLNJB`
   - **Hotkey utilities**

     The Hotkey utilities can be downloaded from:

     `http://www.lenovo.com/pc/support/site.wss/document.do?&lndocid=MIGR-38953`
   - **Power Management driver**

     The Power Management driver can be downloaded at:

     `http://www.lenovo.com/pc/support/site.wss/document.do?&lndocid=MIGR-4GXPEG`
   - **Wireless LAN drivers**

     Refer to the wireless driver table on the following Lenovo Web site for the Wireless LAN driver required for your system:

     `http://www.lenovo.com/pc/support/site.wss/document.do?sitestyle=lenovo&lndocid=MIGR-4ZLNJB`
   - **LSID**

     This driver is required for Access Connections to interface with the Lenovo ThinkPad /L3000 system BIOS. Using a lower layer system BIOS interface, Access Connections controls wireless devices and system dependent hardware features.
3. Delete the following folders from the C:\Drivers\W2k\ACCONWLD directory:
   - CONWIZ
   - IBMPM

- OSD sub-folder from the Hotkey Utilities package
- Wireless LAN drivers such as WLANCX2, WLLANATH, or WLLANINT.

4. Copy the following folders from the extracted location and place into the C:\Drivers\W2k\ACCONWLD directory.
   - **CONWIZ** for Access Connections.
   - **IBMPM** for Power Management.
   - **OSD** for the Hotkey utilities package and On screen display.
   - All **Wireless LAN drivers** that you extracted during Step 2. such as WLANCX2, WLLANATH, or WLLANINT. You do not need to replace all of the drivers in the directory, only the drivers required for your wireless system.

   Note: This package is ready for customization to prepare for installation and contains the Software Installer. The Software Installer searches your sub directories for up-to-date versions of wireless drivers, Access Connections, and Power Management.
5. The following commands will install the integrated Access Connections package:
   a. To install interactively, type:
      ```
      <path>\setup.exe
      ```
   b. To install silently, all the relevant packages with prompt for system restart at the end of installation type:
      ```
      <path>\setup.exe /S /H /R
      ```
   c. To install silently, all the relevant packages with no restart. A restart is required to complete the installation type:
      ```
      <path>\setup.exe /S /H /R:0
      ```
   d. To install silently, all the relevant packages with forced system restart at the end type:
      ```
      <path>\setup.exe /S /H /R:2
      ```

Directory structure

The following files are placed inside the folder where you extracted the downloaded package. When the integrated package is extracted, the following subdirectory under ACCONWLD containing each of the following packages is created:

- CONWIZ is the folder that contains the main Access Connections application files.
- IBMPM is the folder that contains the Power Management driver files.
- OSD is the folder that contains the On screen display utilities including the Fn+F5 Hotkey utilities setup.
- WLANCX2 is the folder that contains the Intel® Pro/Wireless Driver (11a/b/g and 11b/g).
- WLLANATH is the folder that contains the ThinkPad Wireless LAN Adapter Software (11a/b, 11b/g, and 11a/b/g) setup.
- WLLANINT is the folder that contains the Intel Pro/Wireless LAN 2100 3B Mini PCI Adapter Driver Setup (Intel 11b).
- LSID is the driver that is required for Access Connections to interface with Lenovo ThinkPad /L3000 system BIOS. Using a lower layer system BIOS interface, Access Connections controls wireless devices and system dependent hardware features.

Appendix C. Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area. Any reference to an Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the users responsibility to evaluate and verify the operation of any other product, program, or service.

Lenovo may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

Lenovo (United States), Inc.
500 Park Offices Drive
Research Triangle Park, NC 27709
USA
Attention: Lenovo Director of Licensing

LENOVO GROUP LTD. PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information contained in this document does not affect or change Lenovo product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary.

Lenovo may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any references in this publication to non-Lenovo Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this Lenovo product, and use of those Web sites is at your own risk

Any performance data contained herein was determined in a controlled environment. Therefore, the result in other operating environments may vary

significantly. Some measurements may have been made on development-level systems, and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Trademarks

The following terms are trademarks of Lenovo in the United States, other countries, or both:

Access Connections
Lenovo
ThinkVantage
ThinkPad

IBM is a trademark of International Business Machines Corporation in the United States, other countries, or both.

Microsoft and Windows 2000, Windows XP and Windows Vista are trademarks of Microsoft Corporation in the United States, other countries, or both.

Intel is a trademark of Intel Corporation in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

ThinkVantage™

Printed in USA