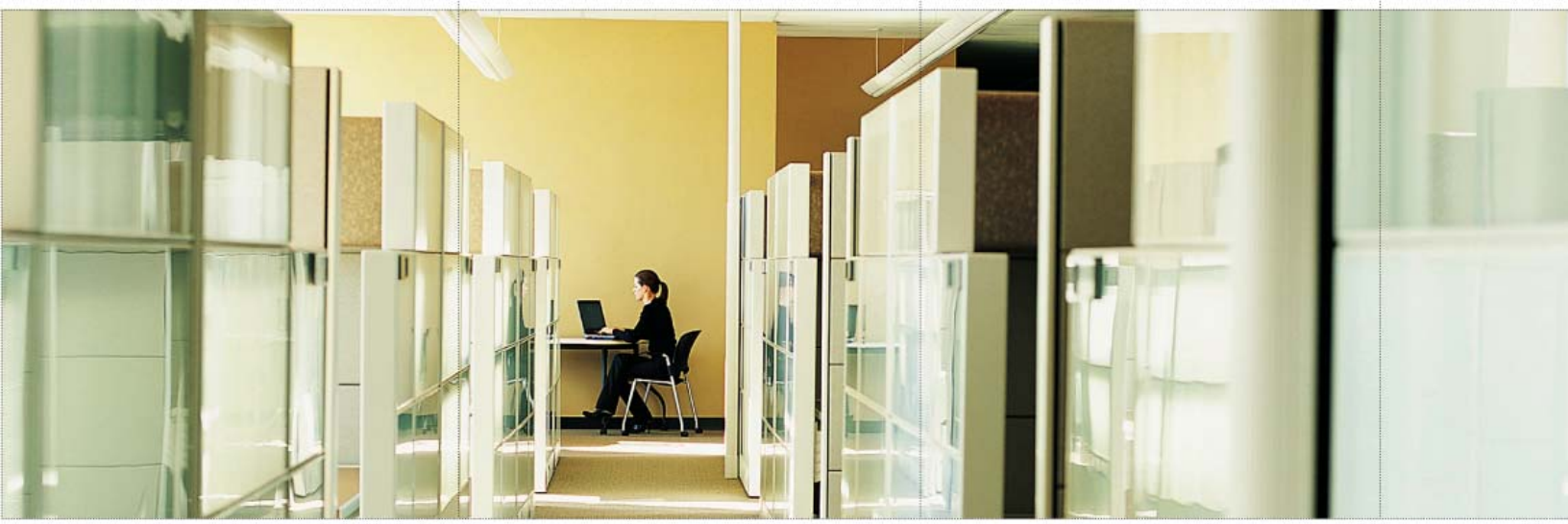


altiris®

Altiris Products Ports and Protocols

White Paper

November 7, 2006

ABOUT ALTIRIS

Altiris, Inc. is a pioneer of IT lifecycle management software that allows IT organizations to easily manage desktops, notebooks, thin clients, handhelds, industry-standard servers, and heterogeneous software including Windows, Linux and UNIX. Altiris automates and simplifies IT projects throughout the life of an asset to reduce the cost and complexity of management. Altiris client and mobile, server, and asset management solutions natively integrate via a common Web-based console and repository. For more information, visit www.altiris.com.

CONTENTS

Introduction **1**

Altiris Deployment Server 6.x **2**

Client Communication 2

Deployment Agent for Windows and DOS 2

Remote control via Console to Deployment Agent for Windows (AClient) 2

Wake-On LAN 2

Set up PCs to use Wake-On LAN 3

Deployment Solution for Clients/Servers and PXE 4

Understanding PXE 4

PXE client boot sequence 5

The PXE Client Boot Sequence 5

Additional Considerations 8

Network Ports 9

PXE MTFTP 11

PXE Manager and PXECfg Service 11

Deployment Web Console (Web Console) 12

DB Management (Middle Man) 13

Deployment Server 13

Deployment Console (Win32 Console) 14

Deployment Agent on Windows (AClient) 15

Deployment Agent on Linux 15

Client/Server File Transfer Port 16

RapiDeploy Ports 16

Imaging 17

RapiDeploy: Imaging engine 17

UDP 401 for multicasting 18

RapidInstall (RIPS) 18

User Profile Migration 19

PCTransplant 19

Real-time Migration 19

PC Transplant Real-time Destination Agent 20

PCTWeb 20

Changing Default settings 20

Multicast settings 22

Direct IP connection or TCP connection 23

Deployment Server Web Console 23

Notification Server 25
Notification Server 25
Power Management 25
Package multicast 26
Task Server 26
Altiris Agent Installation 26
Ports used by Win32 Altiris Agent after installation 27
Accessing the Altiris Console using a Remote Computer 27
AD Connector 27
SMS Connector 28
Additional Solutions for Notification Server 28
Application Management Solution 28
Application Metering Solution 28
Barcode Solution 28
Carbon Copy Solution 28
Deployment Solution for Network Devices 29
Deployment Solution for Network Discovery Connector 29
Helpdesk Solution 29
HP Client Manager Software 30
Inventory Solution for Macintosh 30
Inventory Solution for Palm 30
Inventory Solution for Windows 30
Monitor Solution 30
Patch Management Solution 30
Protect 30
Recovery Solution 30
Site Monitor Solution 32
Software Delivery Solution 32
Web Administrator for Windows Solution 32
Web Admin for SMS 32
UNIX and Mac Solutions 32
More Information 36

INTRODUCTION

The primary purpose of this document is to provide consolidated information regarding the ports and protocols used by Altiris version 6.x Products. In an effort to make the data useful, it will be separated by Deployment Solution for Client/Servers (Windows) and Notification Server and its additional solutions.

ALTIRIS DEPLOYMENT SERVER 6.X

Client Communication

Deployment Agent for Windows and DOS

Deployment Agent for Windows and DOS use a static port (402) to locate the server.

Deployment Agent for Windows and DOS are capable of either using multicast or a direct IP connection to find the Altiris Server Service (axengine.exe).

Routers should be enabled for multicast using these IP ranges:

Deployment Agent for Windows (AClient) uses 225.1.2.3.

RapiDeploy (image engine rdeploy.exe) uses 224.2.0.2 to 224.2.0.20 by default.

After communications have been established, the server and the clients use a dynamic port to do the file transfers (similar to FTP). Routers need to be configured much like they would for FTP -- allow TCP connections through as the primary port number 402 and then allow secondary connections on all other dynamic ports (above 1024). Sometimes with routers and switches, both **401 AND 402 ports should be enabled as bi-directional**.

The Altiris Server Service (axengine.exe) uses directed broadcasts. Routers need to allow directed broadcasts through, but not general (255.255.255.255) broadcasts.

Ports 1 – 1024 are statically assigned ports for known protocols. Deployment Server uses 401 and

402 for no other reason than they are unassigned. Ports above 1024 are assigned dynamically and the TCP/IP stack chooses any available port.

Port 401: Is used to tickle the AClient.

Remote control via Console to Deployment Agent for Windows (AClient)

This process uses IP and doesn't use a specific port. The Windows operating system picks a free port number to use. That port number is sent to the client and the client makes another connection back to the console on that port. Remote control uses dynamic ports much the same as file copy. Consequently, if file copy works, remote control should also work.

Wake-On LAN

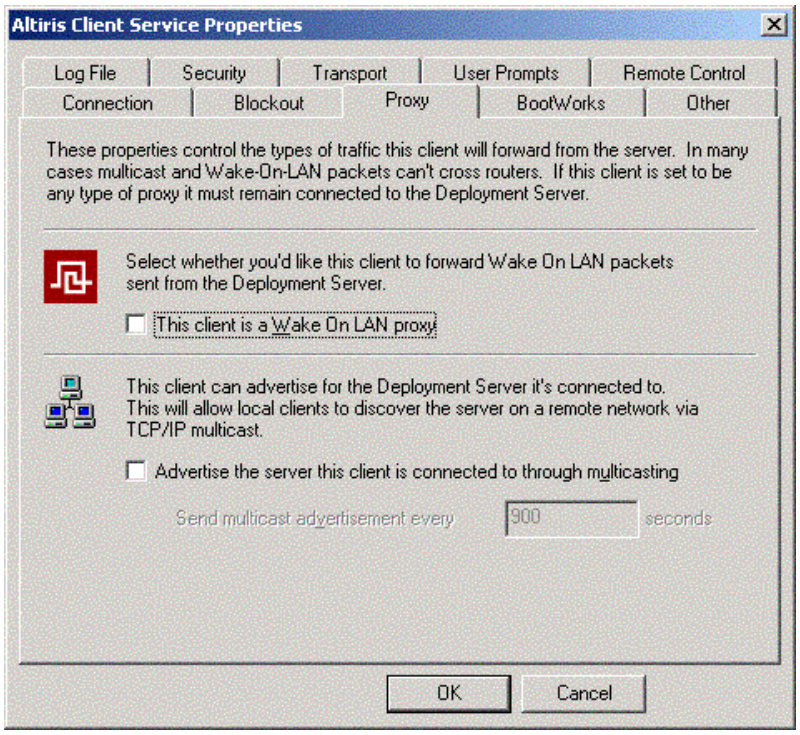
Wake-On LAN allows client PCs to be started that have been turned off. This includes clients powered down from Windows, from the console, or with the power switch. Clients enabled for Wake-On LAN have a cable attaching the network card to the motherboard. The network card

maintains power even when the system is shut down or powered off. When the card receives a Wake-On LAN packet from the network, it sends a signal to the motherboard to turn on the power supply and power up the client.

Wake-On LAN packets are sent via UDP on the same port that the Deployment Agent for Windows uses to connect to the Altiris Server Service (default 402).

“Magic Packet” is just another name used for a Wake-On LAN packet.

If the router will not forward magic packets, Deployment Solution for Clients/Severs has the ability to use Wake-On LAN proxies. Deployment Agent for Windows can be set to be proxies, which allows it to work.



Set up PCs to use Wake-On LAN

Note: The motherboard and network card must support Intel's Wired for Management specification.

1. Enable the available wake-up features in the client computer's BIOS (each BIOS is different and may not list all of these features).

Feature	Available State
Power Management	ON/ENABLED

Suspend/Wake-up Features	ON/ENABLED
Wake-On LAN	ON/ENABLED
Remote Power Up	ON/ENABLED
Power Switch	Suspend/Wake Up

2. Some network cards have their own setup utilities. If there is a Wake-On LAN option, enable it.

Deployment Solution for Clients/Servers and PXE

Deployment Solution for Clients/Servers includes the ability to install a PXE Server to load boot files and the Altiris Deployment Agent for DOS (bootwork.exe) executable into a client computer's RAM without the need to manually insert a floppy disk at boot up.

Altiris Deployment Solutions for Clients/Server PXE uses the following ports:

- Non-configurable (fixed) ports:
  - UDP 67 and 68 to grab and reply to DHCP (and PXE request) packets
  - UDP 4011 for PXE requests when PXE is installed on a computer with a DHCP server
- Configurable ports:
  - TCP 402 to communicate with the Altiris Server Service
  - UDP 1758 & 1759, for TFPT and MTFTP transfer of PXE image
  - TCP 1010 for PXEConfig to communicate with the PXE Configuration service

Understanding PXE

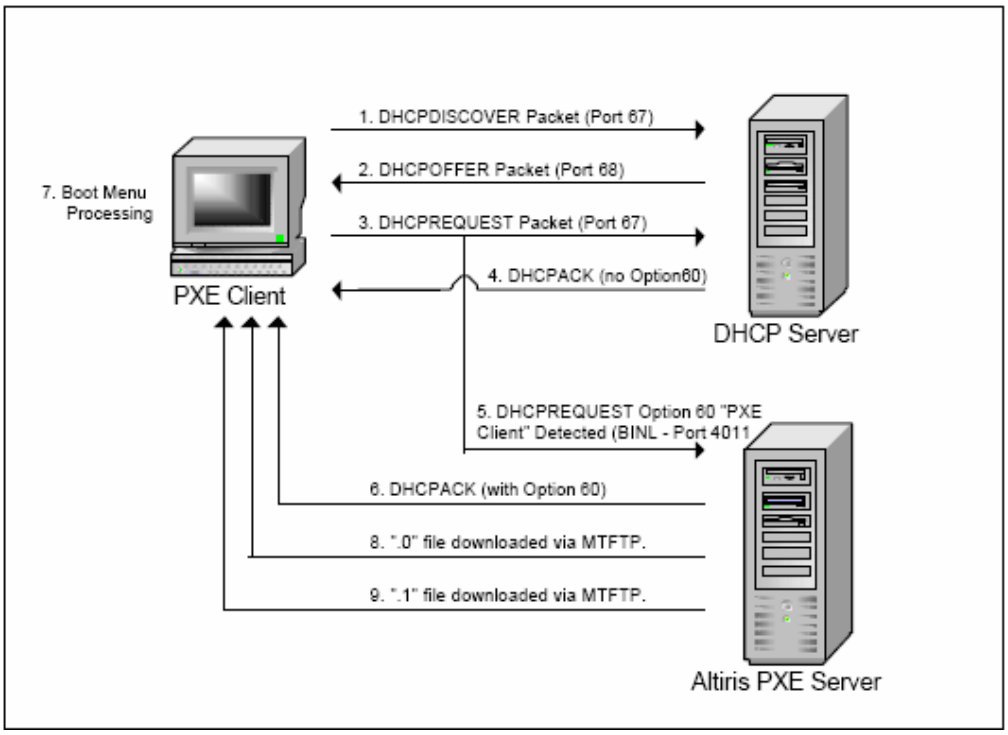
With PXE, client computers can load and execute a boot image from a server on the network (instead of a local hard disk or boot diskette) prior to booting the operating system on the local hard drive. This boot process is "hands off," meaning nothing needs to be done at the computer.

When a PXE-enabled client boots, it obtains an IP address from a DHCP server. It then finds the ProxyDHCP server in the Altiris console which provides the client with a list of boot servers. Boot servers are servers containing client boot image files. The client computer communicates with the appropriate boot server to get the name of the boot image, downloads the image (using TFTP), and boots.

Intel documentation states that the following ports are required for PXE:

- DHCP - Ports 67 & 68
- MTFTP - Port 69
- Extended DHCP PXE request - Port 4011

PXE client boot sequence



The PXE Client Boot Sequence

This section details the PXE Client boot sequence used in standard Altiris PXE Server operations. These steps can be organized into two phases.

1. The first phase enables the PXE Client to obtain two critical pieces of information:
    a. An IP address
    b. The location of a PXE Server
2. The second phase provides the client with all necessary boot files to create a virtual boot disk in RAM. Altiris BootWorks executes in this environment and checks with Altiris Deployment Server for pending job assignments.

    The bootstrap process common to all computers is a sequence of one program starting another, each more intelligent than the last. Immediately after a system is powered on, system voltage stabilizes and the Power-On-Self-Test (POST) executes. The BIOS then begins an examination for extension ROMS (example:

video, disk controllers, and NIC) and ultimately determines an extension ROM that has an initialization point for a boot device. In PXE enabled computers, this initialization point is realized in the special software residing in the NIC flash ROM. This software is called the “boot agent.” After the boot agent begins execution, the following sequence of events occurs.

a. The PXE boot agent directs the execution of normal DHCP operations by broadcasting a DHCPDISCOVER packet (255.255.255.255) to port 67 on its local physical subnet to discover any available DHCP Servers. (Issues related to routing broadcast and multicast traffic are discussed in the “Configuring PXE” section later in this document.) Any available DHCP servers respond with a broadcast DHCPOFFER packet indicating the server’s IP address. When the client has chosen a target DHCP server, it broadcasts a DHCPREQUEST packet that includes its MAC address as well as the IP of the chosen DHCP server in the packet’s Server IP field. This DHCPREQUEST packet’s option 60 identifies the client as a “PXE Client.” Dynamic Host Configuration protocol allows clients to receive “options” from the DHCP server indicating various services that may be available on the network. Numerous standard and customizable options are available that can convey a vast amount of information to DHCP clients. Option 60 deals specifically with PXE related services. Both PXE Clients and PXE Servers use option 60 to convey specific information about both the PXE services needed and the PXE services being provided. All DHCP servers examine the DHCPREQUEST packet and if the IP address differs from the value in the Server IP field, the server reclaims the IP address supplied in the respective DHCPOFFER packets. The target DHCP Server recognizes its IP in the DHCPREQUEST packet and supplies a DHCPACK packet to the client to acknowledge the client’s receipt of its IP. If the DHCP Server and PXE Server are installed on the same computer, option 60 in the DHCP Server’s DHCPACK packet will indicate to the PXE Client that a PXE Server is installed at the same address as the DHCP Server. If the DHCP Server and PXE Server are NOT installed on the same computer, the DHCP Server’s DHCPACK packet will not contain an option 60.

b. During this DHCP activity, the Altiris PXE Server has been monitoring the wire for DHCPREQUEST packets with an option 60 value indicating that the packet originated from a “PXE Client” (see step a above).

c. Upon recognizing a PXE Client DHCPREQUEST packet, the PXE Server uses the PXE client’s MAC address to look up any pending job assignments in the express database

via the Altiris Server Service. If no jobs are present, the PXE boot is skipped and the boot order proceeds in the manner directed in the BIOS. If a job assignment is found, the PXE boot continues with the PXE Server broadcasting a DHCPACK packet (much like the DHCP Server's DHCPACK packet). This packet contains no IP information, but it does contain an option 60 value indicating the packet originated from a "PXE Server."

The PXE client receives an IP address via standard DHCP services and the location of a boot server via option 60 in a DHCPACK packet from the PXE Server. If the PXE Server and DHCP Server are on the same computer, the client computer only receives one DHCPACK packet. If the PXE Server and DHCP Server are on separate computers, the PXE Client receives two DHCPACK packets: one from a DHCP Server providing an IP assignment and the other from a PXE Server identifying its location. In this case, the PXE client then sends a second request directly to the PXE Server, at port 4011 on that computer.

d. If the PXE client receives an option 60 packet directly from a PXE Server, it then examines option 43 in the packet for a PXE boot menu to display. If the PXE client receives an option 60 identifier from a DHCP Server, the boot agent connects back to the IP address of the DHCP server on port 4011 and requests the boot menu from the PXE Server.

   PXE Clients are provided with both a menu and a set of options for how the menu is to be displayed. The first menu option in the list is considered the default option. A timeout value between 0 and 255 is also provided. A value of 0 to 254 displays the menu for the number of seconds indicated and then automatically executes the default option if no other option is selected first. A value of 255 instructs the boot agent to display the menu indefinitely until user input is received.

   Each option in the PXE boot menu defines the location of a boot server and any other information necessary to execute the menu selection. In the Altiris implementation, every menu selection points back to the same PXE Server.

   Note: PXE versions have minor operational differences. In .9x and 1.0 PXE versions, a separate program, "bstrap.0," was requested by the client in order to facilitate boot menu display. In 2.0 PXE, which is the most common version in use today, the required display code is included in the boot agent. A separate download is not required ("bstrap.0" is no longer used).

After determining whether a menu option has been selected, the boot agent requests a set of boot files to be downloaded from the PXE Server via MTFTP.

e. The Altiris PXE Server maintains a database of MAC addresses for computers that have run the “Initial Deployment” event in Deployment Solution. PXE clients with an unrecognized MAC address execute the “Initial Deployment” and receive the “newcomp” set of boot files. PXE clients registered with the database that have job assignments receive the “managed” set of boot files.

   Note: If no job assignment is present, no boot files are received. Both file sets are identical except for a command line switch added on a single command in the “managed” file set autoexec.bat file.

   Both file sets contain “.0” and “.1” files (“managed.0” and “managed.1” are the managed boot files; “newcomp.0” and “newcomp.1” are the newcomp boot files). In either file set, the “.0” file functions as another bootstrap loader.

   This file creates a RAM disk and manipulates the BIOS interrupt vectors, interrupt structures, and hardware information tables to make the RAM disk function exactly like a typical floppy disk. After the “.0” file has executed successfully, the PXE client will not respond to a physical floppy disk for the duration the PXE boot is active. The “.0” file copies the “.1” file byte by byte and sector by sector into the newly created RAM disk.

   The “.1” file is an image of a boot disk floppy with modifications to autoexec.bat and the files that will ultimately provide for the execution of the Altiris BootWorks program from a network share. After the “.1” file copy is complete, the “.0” file transfers control to the RAM drive and the files there begin execution. This signifies the end of PXE operations.

   The entire PXE process is employed simply to create a virtual boot floppy in the client that loads the Altiris BootWorks program. The BootWorks program functions as a DOS client for Altiris Deployment Server. This program checks for and executes any pending work assigned to the client computer by the Deployment Server management console.

Additional Considerations

- PXE won't work with a DHCP relay or DHCP gateway, like Cisco's DHCP relay. The reason for this is that the RELAY makes the request for the IP address which means it provides the wrong MAC address. The computers will PXE boot but will not be able to

automatically detect if there is work for that computer, instead it will default to the Initial Deployment event boot.

- When using Cisco switches there can be problems with PXE timing out while going through its spanning tree states. When using a Cisco switch with spanning tree configured, the computer request might time out because the switch will not let any traffic go through the port until the spanning tree negotiation is finished. The Cisco Spanning Tree time out is 45-55 Seconds. The work around for this is to use the PortFast command on the Cisco switches which allows traffic to go through the port before negotiation is finished.
- It may be prudent to configure the routers with statements to forward DHCP discovers to both the DHCP and the Altiris PXE servers.

Network Ports

This section lists the details of the ports used by Deployment Solution. It also includes the steps to configure the ports that are configurable.

Component	Service	Port	Protocol	Where is this port connected?	Is this port configurable?
PXE MTFTP	Altiris PXE MTFTP Server	69	UDP	PXE Client	No (Industry standard port)
	Altiris PXE MTFTP Server	1758 1759	UDP (Multicast)	PXE Client	Yes
PXE Server	Altiris PXE Server	67	UDP	PXE Client	No
	Altiris PXE Server	68	UDP	PXE Client	No
	Altiris PXE Server	4011	UDP	PXE Client	No
PXE Manager	Altiris PXE Manager	405	TCP	PXEConfig	Yes
	Altiris PXE	406	TCP	PXECfg	Yes

Component	Service	Port	Protocol	Where is this port connected?	Is this port configurable?
	Manager			Service	
PXECfg Service	Altiris PXE Config Helper	407	TCP	PXE Server and PXE MTFTP	Yes
Deployment Web Console (Web Console)	Altiris Deployment Server Console Manager	8081	HTTP	DSWeb	Yes
	Altiris Deployment Server Data Manager	8080	HTTP	DSWeb, Console Manager	Yes
DB Management (Middle Man)	Altiris Deployment Server DB Management	505	TCP	Win32 console, Axengine, PXEManager	Yes
Deployment Server	Altiris eXpress Server	402	TCP/UDP (multicast)	Agents, PXE Server, DataManager, PXEManager	Yes
Deployment Console (Win32 Console)		5001	TCP	AClient	Yes

Component	Service	Port	Protocol	Where is this port connected?	Is this port configurable?
		5002	TCP	AClient	Yes
Deployment Agent on Linux (ADLAgent)	Altiris Network Management Client for Linux	415	TCP	Remote Client	Yes
Deployment Agent on Windows (AClient)	Altiris Client Service	402	UDP	Deployment Server	Yes
	Altiris Client Service	401	UDP	AClient (Wake-on-LAN Proxy)	No

PXE MTFTP

The Altiris PXE MTFTP Server service is used to transfer file data between the PXE Server and the PXE Booting client. This service supports both MTFTP and TFTP standard interfaces.

To configure the 1758 and 1759 ports

1. Go to the datastore path.

   Note: By default, the path is: C:\Program Files\Altiris\eXpress\Deployment Server.

2. Open the **PXE** folder.
3. Open the pxe.INI file in a text editor.
4. In the **[MTFTPD]** section, set the **MCAST_CLNT_PORT** value to 1758 and the MCAST_SRVR_PORT value to 1759.
5. Save the pxe.INI file.
6. Restart PXE services.

PXE Manager and PXECfg Service

The Altiris PXE Manager Service controls the data associated with the PXE components that are included in the PXE package. The PXE Configuration Utility and PXE Servers use the PXE Manager to route,

store, and retrieve information about the status, image availability, user input, and so on.

To configure the 405, 406, and 407 ports

1. Go to the datastore path.

   Note: By default, the path is: C:\Program Files\Altiris\eXpress\Deployment Server.

2. Open the **PXE** folder.
3. Open the RPC.INI file in a text editor.
4. In the **PMData class for PXEConfig and PXE Manager** section, set the **ServerIPPort** value to 405.
5. In the **PCSData class for PxeCfgservice and PXE Manager** section, set the **ServerIPPort** value to 406.
6. In the **PHData class for PxeServer/PxeMtftp and PreCfgService** section, set the **ServerIPPort** value to 407.
7. Save the RPC.INI file.
8. Restart PXE services.

Deployment Web Console (Web Console)

The Deployment Web Console allows you to remotely administer a Deployment Server installation using a Web browser. The Web Console provides the options to deploy and manage Windows and Linux computers (both client and server editions) in real-time with many features present in the Deployment Console.

The Deployment Web Console can be installed on any computer running Microsoft IIS Server, a computer running a Deployment Server or a Notification Server, or a remote computer running only Microsoft IIS.

To configure the 8080 and 8081 ports

1. From the Windows Explorer, select **My Computer > Local Disk (C drive)**.
2. Run the **axInstall.EXE** file in the **DSSetup** folder. The **Deployment Server Install Configuration** wizard appears.

   Note: The DSSetup folder is created on extracting a build.

3. Select the **Custom Install** option and click **Install**.
4. The Software License Agreement dialog appears. Click **Yes**. The **Deployment Share Information** dialog appears.
5. Select the **License file** option and click **Browse** to enter the path of the License file. Click **Next**. The **Deployment Server Information** dialog appears.
6. Select the **On this computer** option.

Note: You can choose whether you want to install the Deployment Server on a local computer or a remote computer.

7. By default, the **Port** is 8080. This port is used by the DataManager service.
8. Enter the **Service** password and click **Next**. The **Deployment Database** dialog appears.
9. Click **Next**. The **Gathering Information** dialog appears.
10. Select the appropriate option, provide the authentication information and click **Next**. The **Pre-boot Operating System** dialog appears.
11. Enter the required information and click **Next**. The **PXE Server Information** dialog appears.
12. Enter the required information and click **Next**. The **Deployment Agent Connection to Deployment Server** dialog appears.
13. Enter the required information and click **Next**. The **Deployment Console Information** dialog appears.
14. Select the required option and click **Next**. The **Deployment Web Console Information** dialog appears.
15. The **Console Port** is 8081 by default. Click **Next**. The Installation Information dialog appears.

    Note: This port is used by the Console Manager service. You can change this port if required.
16. Click **Install**.

DB Management (Middle Man)

This component is used for secure communication between the Console and the Database and the Console and the Server.

To configure the 505 port

1. Open the Registry Editor.
1. In the left pane, select **HKEY_LOCAL_MACHINE > SOFTWARE > Altiris > Altiris eXpress > MMProc > Port 505**. The **Edit DWORD Value** dialog appears.
2. Set the required value and click **OK**.
3. Restart the **Altiris® Deployment Server DB Management** and the **Altiris® eXpress Server** services after this change.

Deployment Server

The Altiris® Deployment Server controls the workflow and information exchange between the managed computers and the other Deployment Server components, such as Deployment Console, Deployment Database, and Deployment Share. Managed computers connect and communicate with the Deployment Server to register inventory and

configuration information and to run deployment and management tasks. Computer and deployment data for each managed computer is then stored in the Deployment Database.

There are two methods to configure the 402 port.

To configure the 402 port

Option 1:

1. From the Start Menu, click **Settings > Control Panel > Altiris Deployment Server Configuration Utility**.
2. Click the **Transport** tab.
3. Enter **402** in the **TCP Port** field and in the **Multicast Port** field. Click **OK**.

Option 2:

1. Open the Registry Editor.
2. In the left pane, select **HKEY_LOCAL_MACHINE > SOFTWARE > Altiris > Altiris eXpress > Options > TCP Port 402** or **Multicast Port 402**.

   Note: This is the port where the server accepts all client connections, such as AClient (Windows Agent), ADLagent (Linux Agent), and DataManager.
3. The **Edit DWORD value** dialog appears for each port. Set the required values for both **TCP Port 402** and **Multicast Port 402** and click **OK**.
4. Restart the **Altiris® eXpress Server** service.

About the Multicast Port:

On the client computers there is an option in the **Altiris Client Service Properties** dialog called **Discover Deployment Server using TCP I/P Multicast**. On selecting this option the client locates the deployment server by multicasting. You have to enter the **Multicast Address** for using the multicasting option. On finding a Deployment Server, the client computer connects to the port that is received from the server.

Deployment Console (Win32 Console)

The Deployment Console is the Win32 user interface for Deployment Solution. You can install this Win32 console on computers across the network to view and manage resources from different locations. In addition, from this console, you can access the Deployment Database on other Deployment Server systems to manage sites across the enterprise.

Note: You can remotely control an active client computer from the Win32 console. Right-click the name of a connected client and select **Remote Control**.

To configure the 5001 and 5002 ports

1. Open the **Deployment Console** and click **Tools > Options**. The **Program Options** dialog box appears.
2. Click the **Global** tab.
3. Select the **Remote control ports** checkbox.
4. Enter port number **5001** in the **Primary** field.
5. Enter port number **5002** in the **Secondary (Optional)** field.

   Note: Port 5002 is the backup port in case Port 5001 is not available.
6. Click **OK**.

   Note: By default, Port 5001 is used for controlling the clients remotely.

Deployment Agent on Windows (AClient)

The Deployment Agent is installed on each client computer in the Deployment Server system to remotely manage the computers from a Deployment Console. The Deployment Agent on Windows runs on Windows computers, including desktops, notebooks, and servers.

To configure the 402 port

1. Click the **AClient** icon on your desktop. The **Altiris Client Service** dialog appears.
2. Click **Properties**. The **Altiris Client Service Properties** dialog appears. By default, the **Server Connection** tab is selected.
3. Select the **Connect directly to this Deployment Server** option or select the **Discover Deployment Server using TCP/IP multicast** option.
4. Enter the port number.

   Note: By default, this port number is 402.

   Note: When the AClient is connected to the Deployment Server on port 402, it internally creates a listening UDP socket on port 402 to accept Wake-up packets from the server.

Deployment Agent on Linux

The Deployment Agent is installed on Linux workstations and server to establish communication between Linux computers and the Deployment Server. This agent collects and sends data from the client computer to the Deployment Server, executes deployment tasks sent from the server, installs packages, and runs management processes as directed from a Deployment Console.

To configure the 402 port

1. To edit the configure file directly, open the adlagent.conf file at the following path: **/opt/altiris/deployment/adlagent/conf**.
2. Change the value corresponding to the **TCPport=** if necessary. The default value is 402.
3. Restart the ADLAgent service.

To configure the 415 port

1. To edit the configure file directly, open the trace.conf file at the following path: **/ opt/altiris/deployment/adlagent/conf**.
2. Change the value corresponding to the **TcpTracePort=** if necessary. The default value is 415.
3. Restart the ADLAgent service.

   Note: Port 415 is used to remotely view debug messages from the ADLAgent. These messages include the debug information and communication details between the ADLAgent and the Deployment Server. This port connects to the Remote Client.

Client/Server File Transfer Port

Open the **Copy File To** dialog of the Copy File task and click the **Advanced** button. Select the **Copy files using Deployment Server** option. The files will be copied using this port.

To configure the Client/server file transfer port

1. From the main menu, open the **Deployment Console** and click **Tools > Options**. The **Program Options** dialog appears.
2. Click the **Global** tab.
3. Select the **Client/server file transfer port** checkbox.
4. Enter the port number in the **Client/server file transfer port** field.
5. Click **OK**.

RapiDeploy Ports

This feature optimizes the multicasting ability of the RapiDeploy application in Deployment Server. This allows you to deploy images to a group of computers simultaneously, download an image from a file server, or access a local hard drive, and manage the imaging of several client computers.

Because RapiDeploy is more efficient when writing directly to the IP address of the network adapter driver, you can enter a range of IP addresses when using the multicasting feature to speed computer deployment and management. Deployment Server accesses the range of computers using the defined IP pairs and avoids retrieving the computers through the port and OS layers.

However, some network adapter cards do not handle multiple multicast addresses. In such instances, you can define a range of ports to identify these computers. On the first pass Deployment Server accesses the selected computers using the list of IP numbers. On the second pass, Deployment Server accesses the selected computers using the port numbers.

To configure the RapiDeploy ports

1. From the main menu, open the **Deployment Console** and click **Tools > Options**. The **Program Option** dialog appears.
2. Click the **RapiDeploy** tab.
3. Enter the range of ports in the **Port > Range** fields.

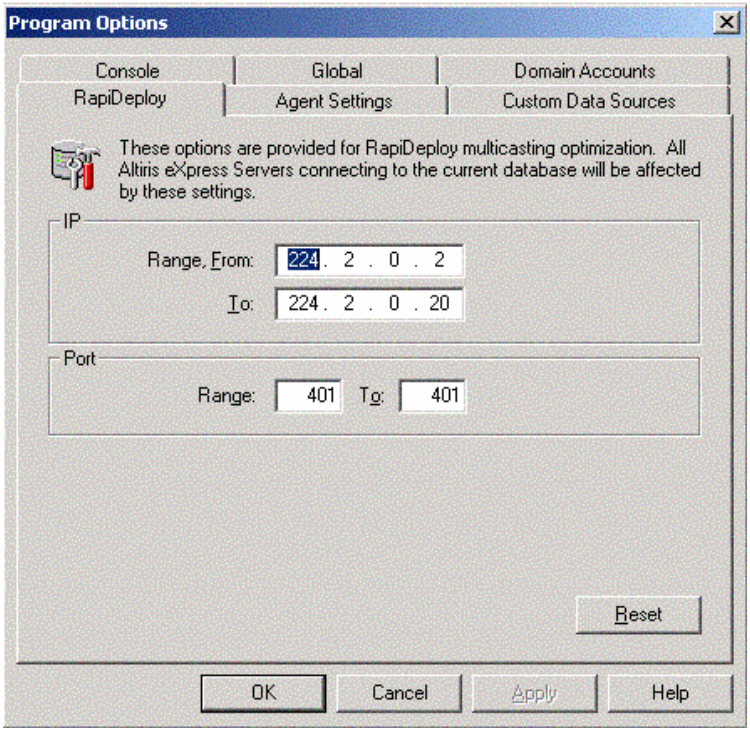
   Note: The port values are 401 by default.
4. Click **OK**.

Imaging

RapiDeploy: Imaging engine

The ports and IP address/multicast ranges used by **RapiDeploy** can all be configured.

Multicast is configured for RapiDeploy from within the Deployment Server Console. Go to **View>Options** and select the RapiDeploy Tab.



The Default IP Range is 224.2.0.2 – 224.2.0 and can be extended to 224.2.0.2 to 224.2.0.20

The default Port Range is UDP 401 – 401.

UDP 401 for multicasting

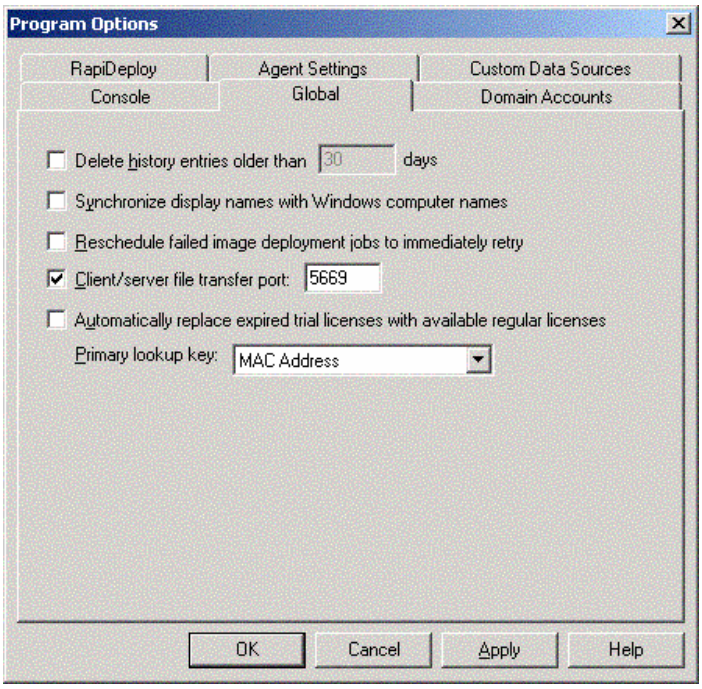
This feature optimizes the multicasting ability of the RapiDeploy application in Deployment Solution for Clients/Servers.

Multicasting allows images to be deployed to a group of computers simultaneously, downloading an image from a file server, or accessing a local hard drive, and managing the imaging of several client computers concurrently. Because RapiDeploy is more efficient when writing directly to the IP address of the NIC driver, entering a range of IP addresses when using the multicasting feature speeds computer deployment and management. Deployment Solution accesses the range of computers using the defined IP pairs and avoids retrieving the computers through the port and operating system layers. However, because some NIC cards do not handle multiple multicast addresses, a range of ports is used to identify these computers. On the first pass, Deployment Solution accesses the selected computers using the list of IP numbers. On the second pass, Deployment Solution accesses the selected computers using the port numbers or higher level operating system ID's.

Note: If using Gigabit 1000Mb NICs, including the 10/100/1000 series, on the Deployment Solution computer, "Offload Transmit TCP Checksum" needs to be configured to "Off". The TCP Checksum offloads are part of the NDIS 5 specification. If the Deployment Server NIC is not using the NDIS 5 drivers then this option will not be available. There are known issues with the NDIS 5 driver when connecting to a client running in DOS. Connections in this instance fail when the card is installed on the Deployment Server due to a difference in packet size and will not work correctly with DOS Clients. In the reverse direction, this is not an issue when the NICs are used with the client because the DOS driver is loaded when booting to PXE or BootWorks.

RapidInstall (RIPS)

RapidInstall is used for the deployment of RIP's (RapidInstall packages) and MSI's. RapidInstall doesn't use any multicast IP ranges. The packages are copied down with the normal file copy method. RIPS are deployed to clients using a file transfer protocol (this is not FTP), which are dynamic by default. The port used by file transfer can be configured to a static port within the Deployment Solution Console. Go to **View < Options** and select the General Tab.



User Profile Migration

PCTransplant

PCTransplant allows creation of a Personality package to migrate user profiles and setting.

A Personality Package is a self-extracting executable file created by the PC Transplant Wizard.

Because a Personality Package is a self-contained executable file, it can be distributed in many ways: floppy disk, e-mail, network share, CD, Web download, or removable media such as Iomega JazTM, ZipTM, or PeerlessTM drives. Personality Packages can also be deployed using services, such as Windows Task Manager, Microsoft SMS, and Altiris Deployment Server, a total computer management and deployment solution. Personality Packages are deployed to clients using File Transfer protocols which are dynamic by default.

Real-time Migration

Through a network connection, it is possible to transplant a computer's settings and files directly in real time to another computer, eliminating the need of creating Personality Packages. Real-time migration includes the following features: user mapping, user properties, user account creation, application installation, and destination computer application information.

PC Transplant Real-time Destination Agent

The PC Transplant Real-Time Destination Agent provides the option for real-time migrations. This agent is run on the computer to which you want to transplant a personality. The PC Transplant Wizard is loaded on the source computer and can communicate with the agent on the destination computer through a network connection. Real Time migration allows selection and transfer of the same elements of a Personality Package without the need of creating Personality Package files.

PCT has five of its own internal ports that are used during Real Time migration. Two are used to communicate between the source and destination, two are used to broadcast a datagram out to find a real time destination agent, and the other was added to manage connection drops. The ports include 4949, 3829, 4950, 4951, and 4952.

Port 4949 and 3829 are used to communicate between PCTWiz and the RTDestAgent.

Ports 4950 and 4951 are used to search for the RTDestAgent.

Port 4952 is for managing the connection drops.

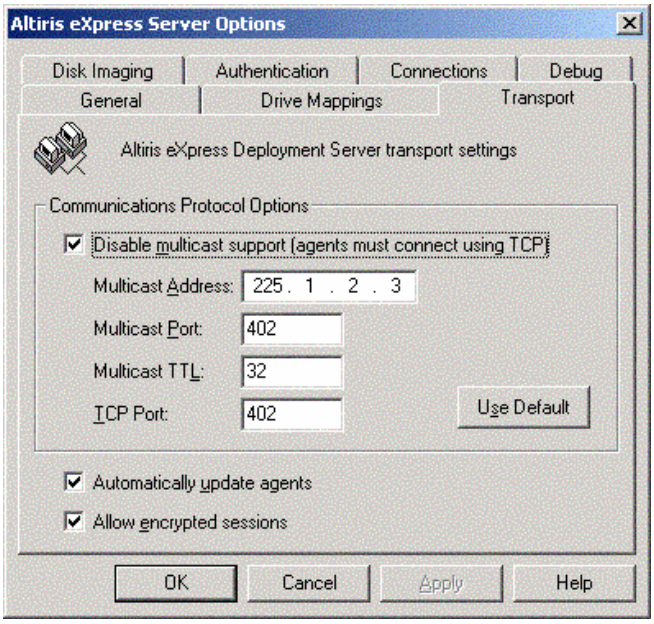
PCTWeb

PCTWeb uses the HTTP port for storing a package on the Web, and the FTP port for updating setting files from the Altiris site.

Changing Default settings

Included in Deployment Solution is the ability to change the default setting which Deployment Solution uses to communicate with client computers. This includes the ability to set specific multicast ports and IP address ranges for multicasting as well as client communication port.

Accessing the Deployment Server Configuration Settings is done from the **Control Panel** and then selecting the **Altiris eXpress Server** icon. The Transport settings Tab allows changes to a number of settings for Client Communication including whether the server service will allow connections from multicast clients or not.



Multicast settings can be modified, such as:

1. Multicast Address (default 225.1.2.3)

   Managed computers can use the multicast address **if** they are on the same segment as the Deployment Server **and** they are not using default PXE boot files.

2. Multicast Port (default 402)

   Use the default multicast IP address and port number if possible to avoid client connection problems.

3. Multicast TTL **(default 32)**

   The TTL field specifies the number of “hops” or hubs that the client can go through to multicast.

4. TCP Port (default 402)

   Port used by the Altiris Client Service and Altiris Server Service to communicate.

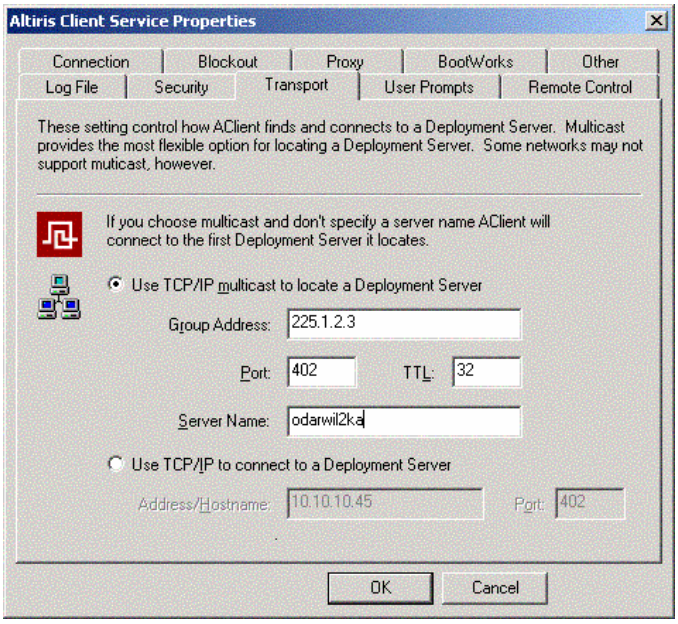
Disable Multicasting and the Altiris Client Service must then connect to the Altiris Server Service using Direct IP connection.

Note: When using TCP to connect the Altiris Client Service to the Altiris Server Service, it must be set to use the same IP address as the Deployment Solution server computer NIC IP address for the VLAN segment where the Deployment Server is connected. For instance, if NIC card (1) is using the address 192.168.0.1 and NIC card (2) is using 11.11.11.1 and the Altiris Client Service is configured for workstations installed to the network on the second VLAN, then the IP address under **Transport Settings** in the Altiris Client Service properties must be set to

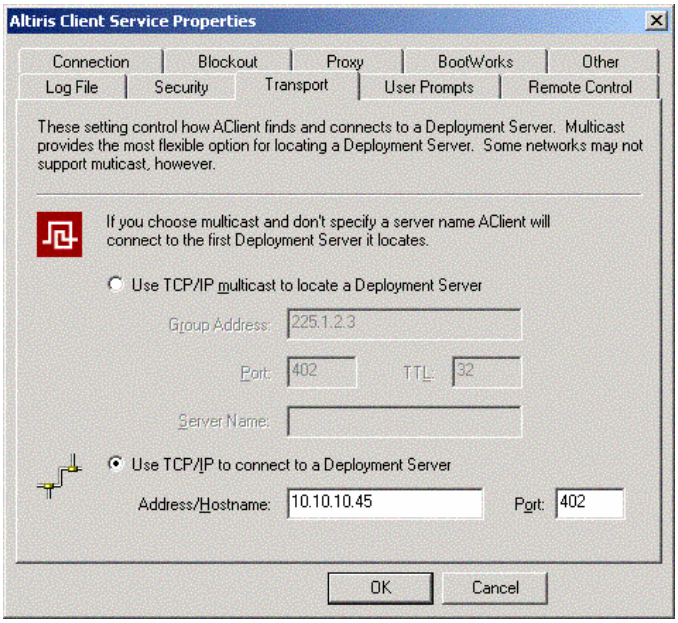
11.11.11.1. If the Altiris Client Service for the workstations is installed to the first VLAN, then the IP address must be set to 192.168.0.1.

Note: If the above settings are changed, then the Altiris Client Service **MUST** be configured accordingly. The Altiris Client Service properties can be configured via the **Altiris Client Services Properties**. These settings can be changed at the local computer by double-clicking the Altiris Client Service icon in the systray. Alternatively, it is possible to **right-click** on the computer icon within the **Deployment Solution Console** and select **Change agent settings < Windows/Linux** to manage the Altiris Client Service remotely. For new computers, go to **Tools < Remote Agent Installer** and select the **add** button to add the computers to install the Deployment Agent for Windows. All these settings can be defined at installation.

Multicast settings



Direct IP connection or TCP connection



Deployment Server Web Console

Deployment Server Web Console 6.1 lets the Altiris Administrator control multiple Deployment Servers from a single Web Console.

The new web console in Deployment Solution 6.1 offers improved integration with the Altiris 6 Console. Administrators can install local or remote Deployment Servers and manage multiple Deployment Servers from a single location. Administrators can also schedule jobs across Deployment Server boundaries. Other enhancements include:

- Improved image and event replication
- Support for adding, modifying and deleting computers, jobs, and tasks
- Schedule jobs to computers and vice versa
- Support for managing virtual computers
- Support for error handling and return codes
- ADS Integration (including managing multiple ADS controllers from a single location).

Web Console introduces the use of two new services:

- **Console Manager** uses TCP port 8081.

  This is only used on the local IIS server to the Console Manager Service so it is not traveling across the network; however, it can cause conflicts if other applications are using this port on the same server.

- **DataManager** uses TCP/HTTP port 8080 by default and can be changed in the install.

  Any communication going from the IIS Server to multiple DataManager's across the network need to have this port open in order to communicate through HTTP to the remote servers.

NOTIFICATION SERVER 6.X

The Notification System is the heart of the entire Altiris Infrastructure. The Notification System provides the core components needed by each Altiris solution.

The key Notification System components are:

- Altiris Agent (including versions for Windows, DOS, Linux, Macintosh, and UNIX)
- Notification Server (the standard Altiris Server)
- Notification Database
- Web-based management consoles
- Package Server
- Task Server
- Reports (automated reporting with drill-down hyperlinks)
- Inventory data forwarding
- Software delivery
- Notification Policies

Notification Server

Notification Server uses port 80 http by default, but this is configurable.

Altiris Agent is connected to Notification Server.

Services created by Notification Server:

- Altiris Service
- Altiris Client Message Dispatcher
- Altiris NS Receiver

Component	Port	Protocol	Is this port configurable?
NS	1024-65536 Default = 52028	TCP/IP	yes
NS	1024-65536 Default = 52029	TCP/IP Multicast	yes
Agent	80	HTTP	yes

Power Management

This does not have its own service.

It is not connected to anything. It works through the Altiris agent.

Ports used:

- TCP/IP port 52028, configurable
- TCP/IP multicast port 52029, configurable

Package multicast

This does not have its own service.

It is not connected to anything. It works through the Altiris agent.

Port used:

- TCP/IP port 52030 by default, port configurable.

Task Server

Component	Protocol	Direction	Port	Connections	Configurable
Tickle Server (Altiris Object Host Service (atrshost.exe))	TCP	Inbound	50123	From task servers	Yes, Altiris.ClientTask.TickleService.config
Task Server (Altiris Object Host Service (atrshost.exe))	TCP	Inbound	50124	From client task agents	Yes, Altiris.ClientTask.Server.config
Task Server (IIS or Altiris HTTP Server)	TCP	Inbound	80 (HTTP) 443 (HTTPS)	From client task agents	Yes, either through IIS, or with Altiris HTTP; use the Altiris.Http.config file
Task Server (Altiris Object Host Service (atrshost.exe))	TCP	Local Only	50121, 50122	Task server web talking to task server process	Yes, Altiris.ClientTask.Remoting.config

Altiris Agent Installation

Notification Server uses standard MS ports to connect to the workstation from the Notification Server to copy over the bootstrap and then HTTP from the workstation to the Notification Server to download the agent.

Initial connection Notification Server to client

- UDP 138 (NETLOGON)
- TCP 445 (MS DS/CIFS/SMB)

Initial connection Client to Notification Server (after Service Starts)

- TCP 80 (HTTP) client download
- ICMP Type 8 (PING) package server speed check

Ports used by Win32 Altiris Agent after installation

HTTP Client / Server communications, such as policy updates and posting events:

The Agent establishes a connection to server port TCP 80 for HTTP and server port TCP 443 for SSL. This port is configurable by the user, however, and can be set to any free port.

Downloading packages from the Notification Server or Package Servers:

Clients can download via HTTP (see above for port assignment) or via SMB connection. SMB uses MS standard NETBIOS ports UDB (135, 137, 139), TCP (135, 139). For SMB over TCP (CIFS), port UDP & TCP 445 is required.

Wake on LAN and Power Management:

Use the port configured in the 'Advanced' section of the Agent communications policy. By default, this is port 52028, or 52029 for multicast.

Accessing the Altiris Console using a Remote Computer

Communication between Notification Server and the Altiris Console uses RPC, DCOM, and HTTP, so make sure RPC services are running on the Notification Server and the appropriate ports are open. The following is a list of ports associated with services in use:

- HTTP - port 80
- DCOM - port 135
- RPC - ports 135, 1500, 2500, (Dynamic)
- SQL - ports 53, 135, 137, 139, 1433

When using a remote console, Notification Server uses HTTP to connect to the server and download the client application / admin console content. After the HTTP connection is made, RPC and DCOM connections are made to the server side processes for DB queries to be executed on the server side.

AD Connector

Initiates an outbound TCP connection from the Notification Server on a random port above 1024 to port 389 on the target DC.

SMS Connector

- Initiates an outbound connection from the Notification Server on a random port above 1024 to SMS's SQL Server on whatever port it is listening on, usually TCP 1433 but it may also be NetBIOS(TCP/UDP135, UDP 138 and TCP 139) or CIFS(TCP 445).
- Initiates an outbound TCP connection to the XXX_CAP share (where XXX is the site name) on the SMS Server to both read and write files. This uses NetBIOS (ports as above).

Additional Solutions for Notification Server

When adding Altiris solutions to the Notification System, the role changes from that of doing tasks to the role of defining policies that automate tasks. Altiris solutions allow a way to deploy programs from Notification Servers to Altiris Agent computers and run the programs on a scheduled basis. Inventory information can be gathered about the Altiris-enabled computer including hardware, software, and much more.

Application Management Solution

Application Management uses the Altiris Agent for all communication. Application Management has no networking code in it at all.

Application Metering Solution

Application Metering uses the Altiris Agent for all communication.

Barcode Solution

Barcode Solution uses standard HTTP ports or windows networking for the (80 and 138,139).

Carbon Copy Solution

Carbon Copy utilizes both TCP and UDP ports when making connections. To configure use on a firewall, the following ports must open: 1680 for TCP and 1680 through 1701 for UDP.

The TCP port is controlled by the CCW32.INI setting TCP_PORT as described below.

Parameter: TCP_PORT	**Section:** [Carbon Copy]
Default: 1680	Valid Value(s): 1024-65535
Description: Specifies the TCP port. The parameter must be set on both the sides of the connection. If the parameter is used without an argument, the default is 1680. If an argument is used that is too low or too high, the default of 1680 is used.	

UDP ports are controlled by the CCW32.INI setting MAX_PORTS as described below.

Parameter: MAX_PORTS	**Section:** [Carbon Copy]
Default: 20	Valid Value(s): 10 or higher
Description: Specifies the maximum number of UDP ports. When negotiating a connection, Carbon Copy starts with UDP port 1680 and then tries subsequent ports until it finds an unused port. If an argument is used that is too low, then 10 will be used. **Note**: If a Client is installed on a computer with Routing and Remote Access Service (RRAS) enabled, the maximum ports may require adjustment based on the number of installed devices.	

The following table gives you information needed for configuring a firewall.

Component	Service	Port	Protocol	What is connected?	Is this port configurable?
CC Agent	shellker.exe	1680	TCP	CC Console	Yes
CC Console/Full Viewer	shellker.exe	1680	TCP	CC Agent	Yes
CC Console/Light Viewer	iexplore.exe (ActiveX control embedded in IE)	1680	TCP	CC Agent	Yes

Deployment Solution for Network Devices

This solution uses SNMP (161) to perform network discovery and management. This solution also exposes functionality through a web service (HTTPS:443). This solution has a “PORT SCANNING” capability that lets the user configure what ports to scan on remote systems. The network discovery engine does have the capability to use ALL ports based on user configuration.

Deployment Solution for Network Discovery Connector

This solution uses SNMP (161) to perform network discovery and management. This solution also exposes functionality through a web service (HTTPS:443). This component utilizes the same network discovery engine that Deployment Solution for Network Devises uses; therefore using SNMP (161).

Helpdesk Solution

Helpdesk is a pure HTTP application and doesn’t explicitly use any ports. Helpdesk Solution only uses standard ports as configured by IIS.

HP Client Manager Software

This solution does not use any TCP ports

Inventory Solution for Macintosh

This solution uses only the standard HTTP ports

Inventory Solution for Palm

This solution uses only the standard HTTP ports

Inventory Solution for Windows

Inventory Solution's Win32 inventory agent uses the Altiris Agent for all communication with the Notification Server and its database with regards to the scheduled inventory scans and the data output.

However this solution is capable of posting via FTP as well as through the use of Floppy disks and Logon Scripts as well as other means of gathering its data.

Monitor Solution

Monitor Solution uses port 1011. This port is used by the Performance Monitor for real-time data on the monitored aspects of a computer. This port can be configured by the user through the Agent Configuration settings.

Patch Management Solution

Patch Management works through the Altiris Agent. There is no difference from that of the Win32 Altiris Agent ports.

Protect

Protect does not use any ports. The only time it might is if network storage is being archived. In this case, it uses whatever ports the particular network access method uses.

Recovery Solution

Port used on RS Client:

- **TCP/IP Port 43189** - Server connects to this RS client port to start/stop client jobs: scheduled snapshot, manual snapshot, and rollback.

Ports used on RS Server:

- **UDP Port 43190** - RS Client pings RS Server by this port to determine the RS Server online status before DCOM call.
- **DCOM Ports (TCP/IP Port 135 plus random ports from DCOM pool)**

Component	Service	Port	Protocol	What is connected?	Is this port configurable?
RS Server	rsserver.exe	43190	UDP	RS Client	yes
	rcp.exe	135	TCP	RS Client	no
RS Agent	rsagent.exe	43189	TCP	RS Server	yes

Table of Ports used when using DCOM (RPC) over http.

Protocol	Ports	Direction
TCP	43189	Inbound to client
UDP	43190	Inbound to Server(Repository)
TCP	1024 and above (unassigned)	Inbound/outbound

To use Recovery Solution via firewalls, several ports must be enabled to allow communication between the client and server. Recovery Solution utilizes RPC TCP port 135, TCP Port 43189 and UDP Port 43190. To allow communication, Port 135 must be enabled for inbound/outbound (RPC endpoint mapper and COM Service), TCP Port 43189 inbound to the client, and UDP Port 43190 inbound on the Server (repository). DCOM uses Remote Procedure Call (RPC) dynamic port allocation. By default, RPC dynamic port allocation randomly selects port numbers above 1024. Consequently, unassigned ports need to be provided, which is utilized as RPC dynamically assigns ports randomly above port 1024.

Protocol	Ports	Direction
TCP and UDP	135	Inbound/outbound
TCP	43189	Inbound to client
UDP	43190	Inbound to Server(Repository)
TCP	1024 and above unassigned	Inbound/outbound

RPC ports are dynamically allocated for incoming communication and the firewall can be configured to confine incoming external communication to only those ports: port 135 (the RPC Endpoint Mapper port) and ports 43189 - 43190.

For more information related to Recovery Solution and configuration settings, see KB articles: **# AKB1623 and # AKB1624**

Site Monitor Solution

Site Monitor Solution uses specific ports based on the configured monitoring policies. This product is designed to monitor specified ports associated with common applications, (example: Exchange and SQL). What makes this different is that the solution is verifying a return because the administrators is monitoring something that should be open as opposed to worrying about configuring the specific ports for the product to function.

Software Delivery Solution

Software Delivery Solution works through the Altiris Agent. There is no difference from that of the Win32 Altiris Agent ports.

Web Administrator for Windows Solution

Ports used by Web Administrator for Windows Solution:

Server Side:

Port	Direction	Used By
7	IN/OUT	ping, traceroute utilities
80	IN	HTTP to view the pages
135	IN/OUT	DCOM/RPC for WMI communication with the client
389	OUT	LDAP for security/authentication checks
1026	OUT	ASP.NET for some internal system processes
1433	OUT	MS SQL for connection to SQL server

Web Admin for SMS

Web Admin for SMS is a pure HTTP application and does not explicitly use any ports. Web Admin for SMS Solution only uses standard ports as configured by IIS.

UNIX and Mac Solutions

Agent for UNIX, Linux, and Mac

Notification Server uses SSH or Telnet to connect to the client computer to copy over the bootstrap and then HTTP or HTTPS from the client computer to the Notification Server to download the agent.

Initial connection Notification Server to UNIX, Linux or Mac client

- TCP 22 (SSH, configurable)

- TCP 23 (Telnet, in case if SSH is unreachable, configurable)

Initial connection Client to Notification Server (after Service Starts)

- TCP 80 (HTTP), 443 (HTTPS) or other custom port depending on Notification Server configuration for Agent download

Connection Client to Package Server

- ICMP Type 8 (PING) package server speed check
- TCP 80 (HTTP), 443 (HTTPS) or other custom port depending on Package Server configuration for package download

Further communication with Notification Server uses configurable ports specified in the policies (defaults are standard HTTP, HTTPS, or FTP ports).

The 5.6 Unix Agent Tickle daemon uses UDP port 6868.

The 6.x Unix Agent uses the same multicast and TCP settings as the Win32 Altiris Agent which can be configured from the Notification Server User Interface. The defaults are:

- TCP/IP Port 52028
- Multicast Address: 224.0.255.135
- Multicast Port: 52029

Ports used by Altiris Agent for UNIX, Linux, and Mac:

Component	Protocol	Direction	Port	Connections	Is configurable
Notification Server	TCP	Inbound	80 (HTTP) or 443 (HTTPS)	From client computers	Yes, depends on the port used by the website the Notification Server is residing on
UNIX, Linux or Mac client computer	TCP	Outbound	Destination port 80 (HTTP) or 443 (HTTPS)	To the Notification Server	Yes, depends on the port used by the website the Notification Server is residing on
	TCP	Outbound	Destination port 80 (HTTP) or 443 (HTTPS)	To Package Servers	Yes, depends on the ports used by the website the Package Server Agent is integrated with
	TCP	Outbound	Source ports 1024 and	To the Notification	No, the ports randomly selected

			above	Server and Package Servers	when connection is established.
	TCP	Inbound	22 (SSH) or 23 (Telnet)	Push install from the Notification Server	Yes, depends on the port used by SSHD or Telnetd
	TCP	Inbound	52028	Tickle / Power Management messages	Yes, configurable in the Altiris Console
	UDP	Inbound	52029	Tickle / Power Management messages	Yes, configurable in the Altiris Console
UNIX or Linux client computer used as Package Server	TCP	Inbound	80 (HTTP) or 443 (HTTPS)	From client computers	Yes, depends on the port used by the website the Package Server Agent is integrated with

UNIX Agent

Communication with Notification Server uses configurable ports specified in the policies (defaults are standard HTTP, HTTPS or FTP ports).

The 5.6 Unix Agent Tickle daemon uses UDP port 6868.

The 6.0 Unix Agent uses the same multicast and TCP settings as the Win32 Altiris Agent which can be configured from the Notification Server User Interface. The defaults are:

- TCP/IP Port 52028
- Multicast Address: 224.0.255.135
- Multicast Port: 52029

Software Delivery Solution for UNIX, Linux, and Mac

Does not use any specific ports, all communication is done via the UNIX Agent.

Inventory Solution for UNIX and Linux, Inventory Solution for Mac

Does not use any specific ports, all communication is done via the UNIX Agent.

UNIX Server Monitor Agent

Uses port 1011 for the socket server (communication with Altiris Console). This is the default, but it is configurable.

MORE INFORMATION

For more information on Altiris visit the following link:

Altiris website: www.altiris.com