

# AXEL Thin Clients

## AX3000 Model G10 & G15

(FK70 and FK75)

*User Manual*

*Firmware 2232a*



Reproduction and translation of this manual, or part of this manual, is prohibited. For further information, please contact:

**AXEL**

14 Avenue du Québec  
Bât. Kentia - BP 628  
91962 Courtabœuf cedex - FRANCE  
Tel.: +33 1.69.28.27.27  
Email: [info@axel.fr](mailto:info@axel.fr)

The information contained in this document is given for information only (it corresponds to firmware revision 2232a. It is subject to change without notice. AXEL cannot, under any circumstances, be held responsible for errors that may have occurred there.

© - 2024 - AXEL - All rights reserved

# TABLE OF CONTENTS

<b>INTRODUCTION</b>	<b>1</b>
<b>- 1 - PRESENTATION</b>	<b>3</b>
1.1 - "ULTRA THIN CLIENT" TECHNOLOGY	4
<i>Dedicated hardware and No operating system</i>	4
<i>No embedded applications</i>	4
<i>No local administration</i>	4
1.2 - MAIN FUNCTIONS	4
1.2.1 - Network	4
1.2.2 - Multisession, protocols and emulations	5
1.2.3 - Print server and serial channel	5
1.2.4 - Management of other peripherals	5
1.2.5 – DUO mode (G100)	5
1.2.6 - Administration	5
1.4 - TABLE OF MAIN CHARACTERISTICS BY MODEL G1x	6
<b>- 2 - FIRST POWER ON</b>	<b>7</b>
2.1 - THE QUICK SETUP	8
2.1.1 – <i>Setting Up</i>	9
2.1.2 - <i>Selection of the network interface</i>	9
2.1.3 - <i>Network interface</i>	10
2.1.4 - <i>Screen session</i>	10
a) Microsoft TSE / RDS - Microsoft RemoteApp Desktop	10
b) Microsoft TSE / RDS – Direct, Broker access or Access by Gateway	11
c) Citrix Receiver - Citrix Receiver desktop	11
d) Citrix Receiver - XenApp / XenDesktop	12
e) Citrix Receiver - MetaFrame	12
f) Citrix Receiver - VDI-in-a-Box	12
g) Citrix Receiver - Direct Access	13
h) VMware View Client	13
i) VNC	14
j) Systancia AppliDis	14
k) 5250 or 3270	14
l) Text Emulation	15
2.1.5 - <i>Citrix Receiver - Choice of a resource</i>	16
2.1.6 - <i>Peripherals</i>	17
2.1.7 - <i>Summary of the setup</i>	17
2.2 - THE AUTO-CONFIGURATION FUNCTION	18
2.2.1 - <i>Step 1: network verification</i>	18
2.2.2 - <i>Step 2: sending of DHCP requests</i>	18
2.2.3 - <i>Step 3: sending requests to AxRM</i>	18
2.2.4 - <i>Step 4: receiving a firmware download</i>	20
2.2.5 - <i>Step 5: receiving a configuration</i>	20
<b>- 3 - INTERACTIVE SET-UP</b>	<b>21</b>
3.0 - GENERAL	22
3.0.1 - <i>Access protected by password</i>	22
3.0.2 - <i>The first dialog</i>	23
3.0.3 - <i>General product information</i>	24
a) The hardware	24
b) The "Firmware" and its "comp number".	24
c) Ethernet MAC address.	24
d) The 802.11 MAC address and the "Control domain".	24
e) Name of the terminal and its IP address	25

f) Memory	25
g) Kerberos Security	25
3.1 - ETHERNET OR 802.11 INTERFACE CONFIGURATION	25
3.1.1 - <i>General</i>	25
a) Terminal name	26
b) Active Interface	26
c) Emergency interface	26
d) DNS domain	26
e) Associated comment	27
3.1.2 - <i>Wired Ethernet interface</i>	27
a) The link	27
b) DHCP parameters	28
c) "DNS parameters"	29
d) Routing	30
e) 802.1X security	30
3.1.3 - <i>802.11 wireless interface</i>	31
a) Choice of SSID	32
b) Security parameters	32
b1) "Access control" set to "none"	33
b2) "Access control" set to "personnel (PSK)"	33
b3) "Access control" set to "company (EAP)"	34
b4) "Access control" set to "802.1X"	35
c) Advanced parameters	35
3.1.4 - <i>Server management</i>	38
3.1.5 - <i>SSH parameters</i>	39
3.1.6 - <i>Reverse SSH</i>	40
3.1.7 - <i>Active Directory</i>	41
3.2 - GENERAL PARAMETERS	42
3.2.1 - <i>Keyboard and mouse</i>	42
a) General keyboard parameters	42
b) Administration of keyboard shortcuts	43
c) Mouse settings	43
3.2.2 - <i>The screen</i>	44
a) Dual screen management	44
b) Resolution and orientation	45
c) Screen saver	45
d) Management of touch screens	46
<b>d') USB touch screens</b>	46
<b>d'') USB-Serial touch screens:</b>	47
3.2.3 - <i>The local desktop</i>	48
a) Theme	48
b) Taskbar	49
c) Session change keys	49
3.2.4 - <i>Audio</i>	50
a) Audio device	50
b) Sound Alerts	51
3.2.5 - <i>Global RDP / ICA</i>	51
a) RemoteFx or XenDesktop	51
b) Keyboard	52
3.2.6 - <i>Date and Time settings</i>	53
a) Local clock	53
b) Time zone	54
c) Automatic shutdown and restart	54
3.2.7 - <i>Remote control of the thin client</i>	55
a) Remote control	55
b) Telnet setup	55
3.2.8 - <i>Security</i>	56

a) Access to the local desktop	56
a.1 - Access by “Local Logon” authentication	56
a.2 - Access by “Active Directory” authentication	57
a.3 - Free access	57
b) Access to the setup with password	58
3.2.9 - <i>Miscellaneous</i>	59
a) Text emulation and local printing	59
b) Number format	59
3.2.10 - <i>Foot pedal (HID)</i>	60
3.2.11 - <i>Dictaphone (SMK)</i>	61
3.3 - SESSIONS	61
3.3.1 - <i>Applications desktop (RemoteApp or Citrix Receiver)</i>	61
3.3.2 - <i>Predefined</i>	62
a) Type of sessions	62
b) Duplicate the configuration of a session	62
3.3.3 - <i>TLS security</i>	63
a) Version of the TLS client	63
b) Personal certificate (optional)	64
c) Control and verifications	64
d) Authentication and encryption capabilities	64
3.4 - USB MANAGEMENT	65
3.4.1 - <i>Specifications</i>	65
3.4.2 - <i>Connecting a USB keyboard</i>	65
3.4.3 - <i>Connection of a USB barcode reader</i>	66
3.4.4 - <i>Connection of a USB mouse</i>	66
3.4.5 - <i>Connecting a HUB</i>	66
3.4.6 - <i>Connecting a printer</i>	66
3.4.7 - <i>Connection of a USB-COM adapter</i>	66
a) Presentation	66
b) Configuration	67
3.4.8 - <i>Connection of a USB touch screen</i>	68
3.4.9 - <i>Connecting a storage device</i>	68
3.4.10 - <i>Connection of a USB smart card reader</i>	69
3.4.11 - <i>Audio Devices</i>	70
3.4.12 - <i>The USB logical USB logical ports</i>	70
a) Attachment of a logical port	71
b) Configuration of the logical port	71
c) Freeing a logical port	72
3.4.13 - <i>List of connected USB devices</i>	72
3.5 - SETTING AUXILIARY AND LOGICAL PORTS	72
3.5.1 - <i>Port configuration</i>	73
a) Setting Serial Ports (G15)	73
b) USB logical ports	75
c) Network printers	76
3.5.2 - <i>Configuration of an LPD printer</i>	76
3.5.3 - <i>Configuration of a serial terminal</i>	77
3.5.4 - <i>Configuration of other devices (tty)</i>	78
3.5.5 - <i>Using a “USB-COM” adapter as the main port for a session</i>	78
3.5.6 - <i>Other uses (rtty or rsh)</i>	79
a) Use of rtty	79
b) Printing with the rsh or rcmd command	79
3.6 - ADVANCED PARAMETERS AND FUNCTIONS	80
3.6.1 - <i>Tuning</i>	80
3.6.2 - <i>Auto-Configuration at each power-up</i>	80
3.6.3 - <i>Remote administration</i>	81
a) RSH administration	82
b) XML administration	82

3.6.4 - <i>Factory setting</i>	82
3.6.5 - <i>Local Store</i>	82
3.6.6 - <i>Smart card readers</i>	83
<b>4 - USING THE THIN CLIENT</b>	<b>84</b>
4.1 - POWER ON	85
4.2 - LOGON ACTIVE DIRECTORY	86
4.3 - LOCAL DESKTOP	88
4.3.1 - <i>"Standard Task Bar"</i>	90
4.3.2 - <i>"Classic Task Bar"</i>	91
4.4 - SESSION CONNECTION	92
4.4.1 - <i>Activating a session</i>	92
4.4.2 - <i>Local authentication</i>	92
4.4.3 - <i>Verification of the TLS certificate</i>	93
4.4.4 - <i>Possible choice of the published resource</i>	94
4.4.5 - <i>Application desktop Connection</i>	94
4.4.6 - <i>USB port (RemoteFX or XenDesktop)</i>	95
4.5 - CHANGING SESSIONS	95
4.6 - RETURN TO LOCAL OFFICE	96
4.7 - SESSION DISCONNECTION	96
4.8 - SPECIAL FUNCTIONS	96
4.8.1 - <i>Information on the current session</i>	96
4.8.2 - <i>Screen Lock</i>	97
4.8.3 - <i>"Copy / Paste" function</i>	98
a) Copy	98
b) Paste	98
4.8.4 - <i>USB port redirection</i>	99
4.8.5 - <i>Reverse SSH</i>	99
4.8.6 - <i>Local calculator</i>	100
4.8.7 - <i>Local volume</i>	100
4.9 - SWITCHING OFF OR REBOOT	100
4.9.1 - <i>Operation carried out locally</i>	100
4.9.2 - <i>Operation carried out remotely</i>	101
4.10 - AVAILABLE KEY COMBINATIONS	102
<b>- 5 - INSTALLATION UNDER WINDOWS</b>	<b>103</b>
5.1 - MICROSOFT TSE / RDS SESSION	105
5.1.1 - <i>Access mode</i>	106
a) Load balancing	106
b) RDS or TS gateway	106
5.1.2 - <i>Connection properties</i>	106
5.1.3 - <i>Authentication</i>	107
5.1.4 - <i>Display parameters</i>	108
5.1.5 - <i>Additional parameters</i>	110
5.1.6 - <i>Resource Redirection</i>	112
a) Declaration of redirected printers	112
b) Declaration of redirected COM / LPT ports	113
c) Resource redirection	114
5.1.7 - <i>Performance</i>	115
5.2 - CITRIX RECEIVER SESSION	118
5.2.1 - <i>"Connection parameters and Browser Settings" section</i>	118
a) StoreFront protocol	118
b) WEB Interface and VDI-in-a-Box protocols	119
c) TCP / IP + HTTP protocol	120
d) Direct access	120
5.2.2 - <i>"Published Resource " section</i>	120
5.2.3 - <i>"Session Parameters" section</i>	122

5.2.4 - <i>Connection properties</i>	122
5.2.5 - <i>Authentication</i>	123
5.2.6 - <i>Display parameters</i>	124
5.2.7 - <i>Additional parameters</i>	124
5.2.8 - <i>Resource Redirection</i>	125
a) <i>redirected printers</i>	125
b) <i>Declaration of redirected COM / LPT ports</i>	125
c) <i>Redirecting resources</i>	125
d) <i>Reassignment of COM / LPT ports</i>	126
5.2.9 - <i>Bandwidth management</i>	127
5.3 - <b>REMOTEAPP AND CITRIX RECEIVER OFFICES</b>	128
5.3.1 - <i>Activation of the "Application desktop"</i>	128
5.3.2 - <i>"Connection parameters" section</i>	129
a) <i>Exploration protocol and server</i>	129
b) <i>Connection properties</i>	130
c) <i>Authentication</i>	130
d) <i>Desktop Parameters</i>	131
5.3.3 - <i>"Session parameters" section</i>	132
5.4 - <b>"VMWARE VIEW CLIENT" SESSION</b>	133
5.4.1 - <i>Configuration of the session</i>	133
a) <i>Authentication</i>	134
b) <i>Menu of available offices</i>	134
5.4.2 - <i>Configuration of the "View Manager"</i>	134
5.5 - <b>"SYSTANCIA APPLIDIS" SESSION</b>	136
5.6 - <b>PRINTER MANAGEMENT</b>	137
5.6.1 - <i>Configuring the thin client</i>	138
5.6.2 - <i>Configuration of a Windows 2016, 2022 server or Windows 11</i>	139
<b>- 6 - INSTALLATION UNDER OS / 400</b>	<b>141</b>
6.1 - <b>5250 SCREEN SESSION</b>	142
6.1.1 - <i>Configuration of the session</i>	142
6.1.2 - <i>Display parameters</i>	143
6.1.3 - <i>Parameters for 5250 emulation</i>	143
a) <i>Additional parameters</i>	144
b) <i>Programmable sequences</i>	146
c) <i>Palette</i>	148
6.1.4 - <i>Authentication (Auto-SignOn)</i>	148
6.1.5 - <i>Connection properties</i>	149
6.2 - <b>USE OF THE CLIENT</b>	149
6.2.1 - <i>ZIO: 5250 status line</i>	149
6.2.2 - <i>Equivalence of the 5250 keyboard with the PC / AT keyboard</i>	151
6.2.3 - <i>Programming of function keys (Record/Play)</i>	152
a) <i>Programming of a key</i>	152
b) <i>Execution of a key</i>	153
6.2.4 - <i>The mouse</i>	153
6.2.5 - <i>Transparent mode</i>	154
a) <i>Introduction sequence</i>	154
b) <i>Operating rules</i>	154
c) <i>Character or hexadecimal mode</i>	154
d) <i>Examples</i>	155
e) <i>Management of DTR and RTS signals</i>	155
6.3 - <b>PRINTER MANAGEMENT</b>	155
6.3.1 - <i>Configuration and use of a PRT5250 printer</i>	156
a) <i>General configuration</i>	156
b) <i>Enhanced parameters</i>	157
c) <i>Use</i>	157
d) <i>In the event of a problem ...</i>	158

6.3.2 - <i>Configuration and use of an LPD printer</i>	158
6.4 - <i>TO GO FURTHER ...</i>	159
<b>- 7 - INSTALLATION UNDER OS/390</b>	<b>160</b>
7.1 - 3270 SCREEN SESSION	161
7.1.1 - <i>Setting a Session</i>	161
7.1.2 - <i>Display Parameters</i>	162
7.1.3 - <i>Customizing the 3270 Emulation</i>	162
a) 3270 Emulation Additional Parameters	163
b) Remapping 3270 Functions to any PC Keyboard keys	165
c) Palette	166
7.1.4 - <i>Connection Properties</i>	167
7.2 - USING THE THIN CLIENT	168
7.2.1 - <i>The 3270 Status Line</i>	168
7.2.2 - <i>Using a PC/AT Keyboard (102/105 keys)</i>	169
7.2.3 - <i>Programming Function Keys (Macro Feature)</i>	170
a) Programming a Function Key	170
b) Processing a Key Sequence	170
7.3 - 3270 PRINTER	171
7.4 - REMOTE ADMINISTRATION	172
<b>- 8 - INSTALLING UNDER UNIX/LINUX</b>	<b>173</b>
8.1 - TEXT MODE SESSION (TCP/IP OR SERIAL MODE)	174
8.1.1 - <i>Setting a Session Profile</i>	174
8.1.2 - <i>Protocols: telnet, tty, ssh, ssh2 or serial</i>	175
a) The TELNET Protocol	175
b) The SSH Protocol	175
c) The TTY Protocol	176
d) Serial Ports and USB-COM adaptors	177
8.1.3 - <i>Selecting the Emulation</i>	177
8.1.4 - <i>Display Parameters</i>	178
8.1.5 - <i>Customizing the Emulation</i>	178
a) Emulation Additional Parameters	179
b) Editing Keyboard Table	181
c) Key Mapping	182
d) Palette	183
8.1.6 - <i>Coloring Mode</i>	183
8.1.7 - <i>Underline Attribute Management</i>	183
a) Using the Session as a Monochrome Session	183
b) Using the Coloring Mode	183
c) Using Underline Attribute in Color Mode	184
8.1.8 - <i>Connection Properties</i>	184
8.1.9 - <i>Login Script</i>	185
a) Enabling a Login Script	185
b) Example	185
8.2 - GRAPHICAL MODE SESSION (VNC)	186
8.2.1 - <i>Connection Properties</i>	187
8.2.2 - <i>Display Parameters</i>	187
8.2.3 - <i>Additional Parameters</i>	188
8.3 - CONTROLLING PRINTERS	190
8.3.1 - <i>The tty Protocol</i>	190
8.3.2 - <i>The LPD Protocol</i>	190
8.3.3 - <i>The rsh Command</i>	191
8.3.4 - <i>Using Transparent Mode</i>	191
8.4 - THE AXEL TTY SERVER	191
8.4.1 - <i>Overview</i>	191
8.4.2 - <i>Installing an AXEL tty server</i>	192



8.4.3 - Using an AXEL tty server	193
a) Overview	193
b) Running the Axel Tty Server	194
8.4.4 - The axttyd Mechanism	194
8.4.5 - Uninstalling	195
8.4.6 - In Event of Problems...	195
a) Message "Cannot bind TCP port"	195
b) Message "Waiting for connections from TCP/IP socket"	195
8.5 - REMOTE ADMINISTRATION	195
8.5.1 - AxRM Software	195
8.5.2 - Using Unix/Linux Commands	195
<b>- 9 - TOOLS AND STATISTICS</b>	<b>197</b>
9.1 - HANDLING A CONFIGURATION FILE WITH A MEMSTICK	198
9.1.1 - Obtaining and Storing the Configuration File	198
9.1.2 - Send a Configuration File to the Thin Client	199
9.2 - UPDATING THE FIRMWARE	199
9.2.1 - From a MemStick	199
9.2.2 - With bootp/tftp Protocols	200
9.3 - THE PING COMMAND	200
9.4 - CONNECTION MANAGEMENT	201
9.4.1 - Global Connection List.	201
9.4.2 - "TCP Server" and "TCP Client" Connection Information	203
9.5 - ETHERNET INTERFACE INFORMATION	203
9.5.1 - Ethernet Interface	203
a) State	204
b) DHCP/DNS	205
c) Statistic	206
9.5.2 - Wireless Interface	207
a) State	207
c) Statistic	208
9.6 - USB STATISTICS	208
<b>- 10 - REMOTE ADMINISTRATION</b>	<b>209</b>
10.1 - AXRM: THE AXEL MANAGEMENT SOFTWARE	210
10.2 - REMOTE CONTROL	211
10.3 - INTERACTIVE TELNET SET-UP	212
10.4 - BATCH REMOTE SET-UP	213
10.4.1 - AX3000 Remote Set-Up	213
10.4.2 - Configuration File Format	213
a) Header	213
b) Substitution Commands	214
c) End of File	214
<b>APPENDIX</b>	<b>215</b>
A.1 - USING THE INTERACTIVE SET-UP	216
A.1.1 - Entering the Set-Up	216
A.1.2 - Navigation	216
a) The Horizontal General Menu	217
b) Vertical Menus	217
c) Dialog Boxes	217
A.1.3 - Enter Data	217
A.1.4 - Special Notation	218
A.1.5 - Exiting the set-up	218
A.2 - NETWORK OVERVIEW	218
A.2.1 - Ethernet Addresses	218
A.2.2 - IP Address	219

A.2.3 - Router	219
A.3 - THE DHCP PROTOCOL	221
A.3.1 - Overview	221
A.3.2 - Setting-Up the AX3000	222
A.3.3 - Using the AX3000	222
A.3.4 - Errors	222
a) Boot Time Failure	222
b) Re-negotiation Failure	223
A.4 - THE DNS PROTOCOL	223
A.4.1 - Overview	223
A.4.2 - Resolving a Name	224
a) Resolution Strategy	224
b) Resolution Method	225
c) Messages Displayed on the AX3000 Screen	225
A.4.3 - Publishing the Thin Client Name	226
a) By the DHCP Server	226
b) By the Thin Client	226
A.5 - SETTING-UP AXEL DHCP OPTIONS	227
A.5.1 - 'axrmserv' Option: XML auto-configuration	228
A.5.2 - 'axrmservssl' Option: XML-SSL auto-configuration	228
A.6 - RSH ADMINISTRATION COMMAND LIST	229
A.7 – TO GO FURTHER ...	229
A.7.1 - Reload Factory Settings	229
A.7.2 - General Level: Advanced Parameters	229
a) Network Menu	230
b) Keyboard/Screen Menu	231
c) Mass Storage Device Menu	231
d) Miscellaneous Menu	232
A.7.3 - Session Level: Enhanced Parameters	233
a) 'Secondary Server' Parameter	233
b) 'TCP port' Parameter	233
c) 'mss' and 'Window' Parameters	233
d) 'Time to Live' Parameter	234
e) 'TCP port Assignment' Parameter	234
f) 'Nagle's Algorithm' Parameter	234
g) 'Keepalive' Parameter	235
h) 'Additional Time-Out for Reconnection (sec)' Parameter	235
i) 'Break Code' Parameter	235
j) 'Enabling NAWS' Parameter	235
k) 'Always add NULL after CR' Parameter	235
l) 'National Language Negotiation' Parameter	235
A.7.4 - Keyboard Codes and Time Zone Names for RDP/ICA Sessions	236
a) Keyboard Codes	236
b) Name of Time Zone	237
A.7.5 – Displaying Text Session in Graphics Mode	240
a) Full Screen Mode	240
b) Size and spacing of characters	241
c) Information about Current Session	242
A.7.6 - Setting the IP Address by a PING Command	242
A.8 - HARDWARE AND FIRMWARE INFORMATION	244
A.8.1 - Hardware Information	244
A.8.2 - Firmware Information	245
A.8.3 – Compilation Index	245

# INTRODUCTION

This manual provides the information necessary for installation and use of Axel thin clients.

This document consists of the following chapters and appendices:

- **Chapter 1:** presentation  
Description of the main functionalities of the thin client.
- **Chapter 2:** first power-up  
During the first power-up, the quick setup allows you to configure the thin client in a few seconds. In addition, the auto-configuration function is activated.
- **Chapter 3:** interactive setup.  
Description of the interactive setup which allows you to configure the accessible network environment, the application desktop, sessions and connected devices.
- **Chapter 4:** using the thin client  
Presentation of the local desktop, the concept of multisession and stopping the thin client
- **Chapter 5:** implementation under Windows  
Description of the application desktops (RemoteApp / Citrix) and TSE / RDS sessions, Citrix and VMware View Client.
- **Chapter 6:** Implementation under OS / 400  
Description of the 5250 emulation and implementation of the specific features of OS / 400.
- **Chapter 7:** Implementation in OS / 390  
Description of the 3270 emulation and implementation of specific features in OS / 390.
- **Chapter 8:** implementation on Unix / Linux  
Description of the implementation of specific features on Unix / Linux (tty server, multi-shell, VNC server ...).
- **Chapter 9:** Tools and Statistics  
Presentation of the administration and statistics tools integrated into the thin client.
- **Chapter 10:** remote administration
  - Presentation of the AXRM administration software.
  - Description of the remote control command, access to the interactive setup via a TELNET command and storage of the configuration of the thin client in a text file.
- **APPENDICES:**  
The appendices provide details on the following points:
  - A.1 - Use of the interactive setup
  - A.2 - Callback on networks (Ethernet addresses, IP addresses and routers)
  - A.3 - DHCP protocol
  - A.4 - DNS protocol
  - A .5 - Configure DHCP vendor options
  - A.6 - List of rsh administration commands
  - A.7 - To go further ...
  - A.8 - Information on hardware and firmware

**- 1 -  
PRESENTATION**

This chapter presents the main features of Axel thin clients.

## 1.1 - "ULTRA THIN CLIENT" TECHNOLOGY

The main benefits of "Ultra Thin Client" technology are:

### Dedicated hardware and No operating system

The innovative Axel "Ultra Thin Client" technology makes available all the power of Hardware:

- High Performance Graphics display
- high robustness and high availability
- No memory fragmentation after time of use
- full protection against computer viruses
- Quick Boot
- Reliability and stability maintained over time

### No embedded applications

Having installed applications on a thin client creates many issues:

- Management of security patches for critical applications
- Maintenance of updates
- Amount of memory and CPU sufficient after upgrades.
- Consistency of the fleet (Axel products have long lives – so you build a fleet of identical devices over time)

### No local administration

In terms of configuration, the Axel architecture does not have the complexity of an operating system:

- No "file system" or "registry",
- No user management,
- Except in special cases, ie after being re-configured there is never a need to reboot),

Despite its advanced technology and functionality, the Axel thin client is administered like a traditional terminal. That is to say through an interactive setup. In addition, this setup is designed to be accessible both locally and across the network.

## 1.2 - MAIN FUNCTIONS

### 1.2.1 - Network

The Axel thin client offers extensive network functionalities:

- DHCP management: obtaining an IP address and other parameters.
- DNS management: publication of the name of the thin client and name resolution.
- routing: connection through routers (WAN)

These Models offers a choice of network interfaces: **Ethernet** as standard or optional **802.11**.

Only one interface is active at a time, but each interface has its own IP parameters (DHCP, DNS, routers, etc.)

### **1.2.2 - Multisession, protocols and emulations**

The different protocols and emulations allow the thin client to connect to most multi-user environments.

An Axel thin client supports up to **six** simultaneous and independent **sessions**. These sessions can be used in three ways:

- **Predefined session:** the session is defined to connect to a given server with a protocol and a predefined configuration (resolution, number of colors ...)
- **Free session:** the session is defined to connect with a protocol and a predefined configuration (resolution, number of colors ...) but the destination server is selected just prior to connection.
- **Applications Desktop:** after authentication, the thin client displays the icons of the published applications. When the user clicks on one of these icons, a dynamic session (RDP / ICA) is created.

A task bar or a configurable key combination allows the user to open a new session or instantly hot-key to another session.

### **1.2.3 - Print server and serial channel**

In addition to USB printers, these models allow direct printer connections to aux1, aux2 ports of the G15 models and compatibility with USB/Com or USB/Parallel adapters on each of USB ports. Ports emulated in this way can be managed in different ways:

- by a network service: LPD or PRT5250 for printers, TTY for serial ports.
- through RDP / ICA protocols: device redirection or USB redirection.
- by escape sequences: compatibility with text terminals.

### **1.2.4 - Management of other peripherals**

The management of many peripherals is integrated as standard:

- Headphones or speaker (Jack or USB),
- Barcode reader,
- Touch screen,
- USB memory sticks,
- Chip card reader,
- Various other USB peripherals ...

### **1.2.5 – DUO mode (G10)**

DUO Mode for G10, allows two independent users to use the same thin client.

This operating mode, which only AXEL's "Ultra Thin Client" technology allows, can be activated on G10 thin clients by a simple firmware download.

All instructions for implementing DUO mode are included in a documentation addendum which is available on our website.

### **1.2.6 - Administration**

Axel thin clients can be administered remotely through a dedicated protocol. The administration software (AxRM) is free and can be downloaded from our WEB site.

More information on chapter [10](#)

## 1.4 - TABLE OF MAIN CHARACTERISTICS BY MODEL G1x

	<b>Model G10 (FK70)</b>	<b>Model G15 (FK75)</b>
<b>Connection</b>		
Ethernet (TCP / IP)	Gigabit	Gigabit
Wireless (optional)	802.11 a / b / g / n 2.4 and 5 GHz	802.11 a / b / g / n 2.4 and 5 GHz
Serial (RS232)	Via USB	2
<b>Video Ports</b>		
- Display Port ++	<b>2</b>	<b>2</b>
- VGA with adapter (not included)	YES	YES
- HDMI with adapter (not included)	YES	YES
- DVI with adapter (not included)	YES	YES
Maximum resolution	1920x1200 (x2)	1920x1200 (x2)
Number of colors	32 bpp (16 million)	32 bpp (16 million)
<b>Sessions</b>		
Microsoft Client <sup>(2)</sup>		
- RDS /TSE & RemoteApp	YES	YES
- RDS Gateway	YES	YES
Citrix Client		
- Metaframe	YES	YES
- XenAPP / XenDesktop	YES	YES
- Web Interface	YES	YES
- StoreFront and NetScaler	YES	YES
VMware Client (RDP)	YES	YES
VNC client	YES	YES
Text emulations	YES	YES
<b>Connectors</b>		
Parallel port	By USB	By USB
Serial port	By USB	2
USB (2.0) port	4	4
<b>Redirection RDP / ICA</b>		
Printer	YES	YES
COM port	YES	YES
USB storage	YES	YES
Chip card	YES	YES
Audio	YES	YES
USB RemoteFX / XenDesktop	YES	YES
<b>Other functions</b>		
Wake On LAN	YES	YES
Power Supply	External	Internal
Commercial reference	<b>G10</b>	<b>G15</b>

\*: Compatible with Windows 2003 to 2022 servers and Windows XP to Windows 11 virtual machines.



**- 2 -**  
**FIRST POWER ON**

*This chapter provides the information necessary for installing an Axel thin client via the 'quick setup' or auto-configuration functions.*

When powering up for the first time, the thin client offers two configuration options:

**Quick setup:** a series of dialog boxes allows you to configure the thin client in a few seconds for typical use.

**Auto-configuration:** this function allows the thin client to automatically report to the AxRM software in order to obtain a firmware and / or configuration. The auto-configuration function is stopped as soon as the keyboard is used.

**IMPORTANT:** this function only uses the Ethernet interface; the thin client must therefore be connected to a network compatible with AxRM.

## 2.1 - THE QUICK SETUP

The quick setup allows you to quickly and easily configure an AXEL thin client for a single environment.

It can also be used to create a basic configuration which will then be further modified to take into account the requirements of your environment.

It consists of a series of screens (wizard) which allows you to be guided during the configuration of the thin client.

Before the final validation of the quick setup, it is possible to modify the configuration in detail to take into account specific options.

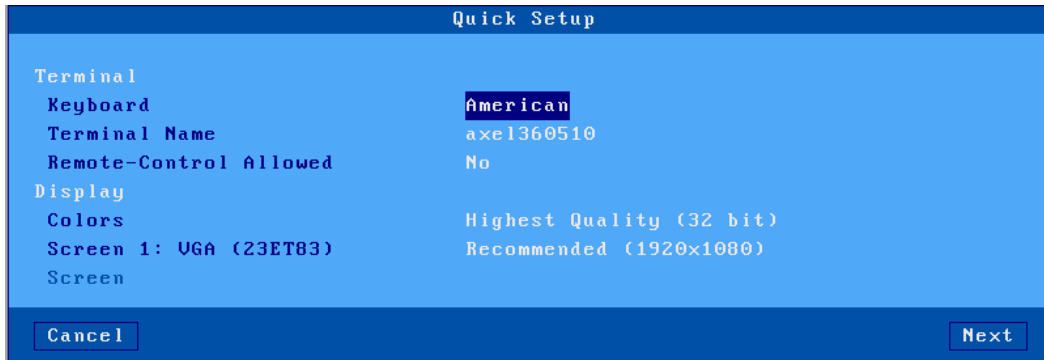
Navigation in the quick setup can be done either with the mouse or with the keyboard.

The main navigation keys in the quick setup are:

- **[Enter]:** execute the action of the current button or if no button is selected access to the default button (**[Validate]**, **[Next]** ...)
- **[Space]:** execute the action of the current button, change the value of the current field (for example yes / no) or open the list of current choice
- **[Esc]:** abort the current entry or select the **[Cancel]** button
- **[Tab]** or **[ ]**: access the next field
- **[Shift] + [Tab]** or **[ ]**: access the previous field
- **[F10]:** select the validation button for the current window.

**2.1.1 – Setting Up**

This first screen makes it possible to define the general parameters of the thin client, in particular the graphical environment and the keyboard type:



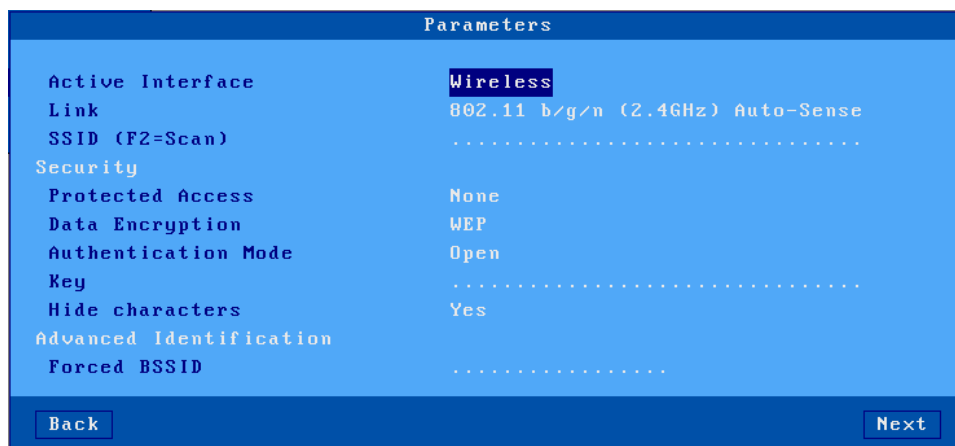
Description of the parameters:

- **Keyboard:** nationality of the keyboard used.
- **Terminal name:** see annex [A.4.3](#).
- **Remote control authorized:** allows you to take control of the thin client (see chapter [10.2](#)).
- **Colors:** 16, 24 or 32 bpp
- **Screen:** two screens can be managed. For each screen detected, the port (VGA or DisplayPort) and the model are displayed. A list provided by the monitors (EDID) allows you to choose the desired resolution. The "recommended" resolution allows whatever monitor connected to use the optimal resolution given by EDID function of the monitor.

**Note:** The cable used must comply with the "DDC2B" standard in order to be able to provide EDID information to the thin client, for VGA cable, this information is conveyed by pins 9, 12 and 15 of the connector.

**2.1.2 - Selection of the network interface**

For a thin client equipped with the 802.11 option, this screen for choosing the network interface is displayed:



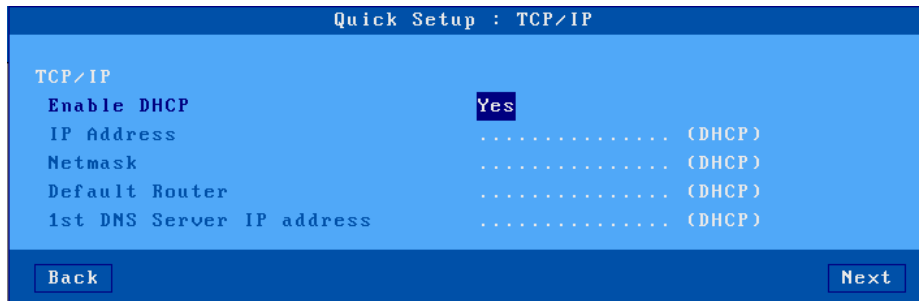
Description of the parameters:

- **Active interface:** two possibilities:
  - **Ethernet:** no other parameters are necessary.

- **Wireless:** connection and security parameters are requested.
- Other parameters: see chapter [3.1.3](#) for more information.

**2.1.3 - Network interface**

The screen for entering network parameters is as follows:



Parameter description:

- **DHCP activation:** two possible answers:
  - **yes:** DHCP server supplies to the terminal: IP address, network mask, default router, DNS server details).
  - **no:** manual entry of parameters.
- **IP address:** mandatory entry if DHCP is inactive
- **Default router:** optional
- **IP address 1st DNS server:** optional

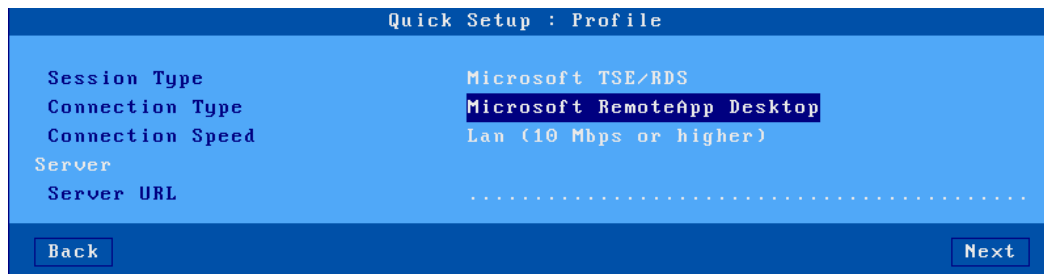
For more information on the DHCP and DNS protocols, see appendices [A.3](#) and [A.4](#).

**2.1.4 - Screen session**

This screen allows you to define the use of the thin client by selecting a "Session type" and depending on choice: "Connection type".

**a) Microsoft TSE / RDS - Microsoft RemoteApp Desktop**

After authentication the icons of published resources are displayed on the desktop. RDP sessions are created dynamically:

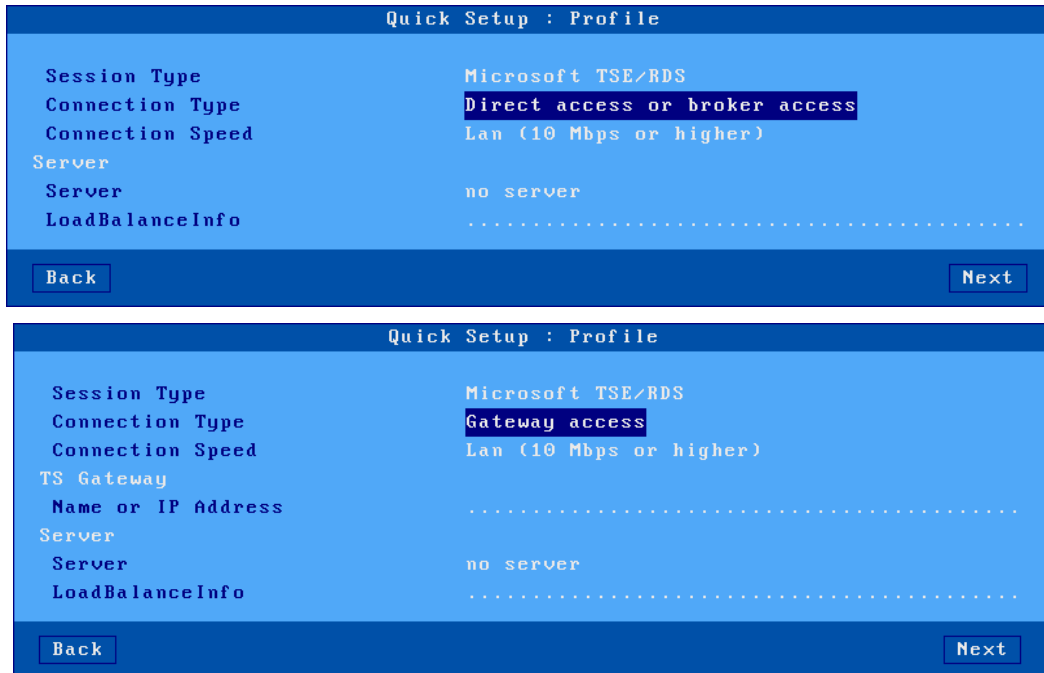


Description of parameters:

- **Connection speed:** choice of network type from a list.
- **Server URL:** the syntax is **[https://] server [: port] [/ config]**
  - "https": use is optional (by default http)
  - "server": DNS name or IP address of the RemoteApp server
  - " Port ": optional, by default 80 for http and 443 for https
  - "/ config": optional path to the configuration file ("/rdweb/feed/webfeed.aspx" by default)

**b) Microsoft TSE / RDS – Direct, Broker access or Access by Gateway**

Connection of an RDP session to a broker or directly to the TSE / RDS server (referenced by its IP address or DNS name):

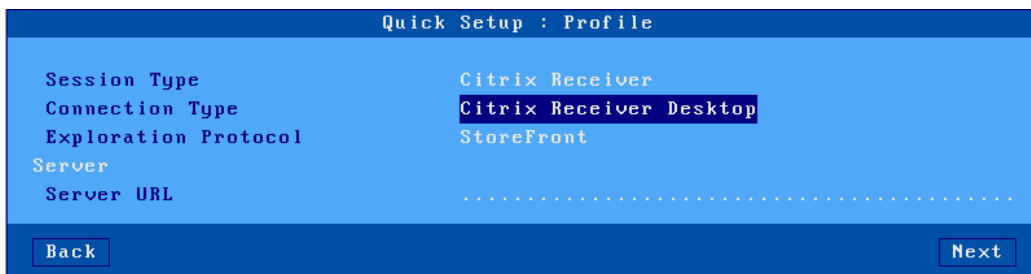


Description of parameters:

- **Connection speed:** choice of network type from a list.  
In the case of "Access via a gateway", the Gateway must be defined:
- **Name or IP address:** (only for access by gateway): DNS name or IP address of the gateway.
- **Server:** DNS name or IP address of the broker or RDS server.
- **LoadBalanceInfo:** "loadBalanceInfo" string for load balancing, see chapter 5.1.1 for more information

**c) Citrix Receiver - Citrix Receiver desktop**

After authentication through the selected exploration protocol (StoreFront, Web Interface or TCP / IP + HTTP), the published resource icons are displayed on the desktop. ICA sessions are created dynamically as established:



Parameter description:

- **Server URL:** the syntax is [https: //] server [: port]  
"https": use is optional (default http)  
"server": name DNS or IP address of the Citrix farm access server  
"port": optional, by default 80 for http and 443 for https

**d) Citrix Receiver - XenApp / XenDesktop**

Connection of an ICA session to a resource published by the selected exploration protocol (StoreFront, Web Interface or TCP / IP + HTTP):

Quick Setup : Profile	
Session Type	Citrix Receiver
Connection Type	XenApp/XenDesktop
Exploration Protocol	StoreFront
Server	
Server URL	.....
Store	Default
Choose a Published Resource	No
<input type="button" value="Back"/> <span style="float: right;"><input type="button" value="Next"/></span>	

Parameter description:

**Server URL:** the syntax is [https: //] server [: port]

"https": use is optional (by default http)

"server": DNS name or IP address of the access server the Citrix farm

"port": optional, by default 80 for http and 443 for https

**Store:** (Only for StoreFront) allows you to choose the "default store" or give the user the possibility of choosing one from the list of stores at time of connection.

**Choose a published resource:**

- **no:** the user will have at his disposal the list of his published resources at the time of connection.
- **yes:** A resource can be chosen in the following quick setup screen (but the thin client will have to rebooted). See chapter [2.1.5](#).

**e) Citrix Receiver - MetaFrame**

Connection of an ICA session to a resource published with "TCP/IP + HTTP" :

Quick Setup : Profile	
Session Type	Citrix Receiver
Connection Type	MetaFrame
Server	
Server and XML Port	.....
Choose a Published Resource	No
<input type="button" value="Back"/> <span style="float: right;"><input type="button" value="Next"/></span>	

Parameter description:

**Server and XML port:** the syntax is Server[:port]

"server": DNS name or IP address of the access server the Citrix farm

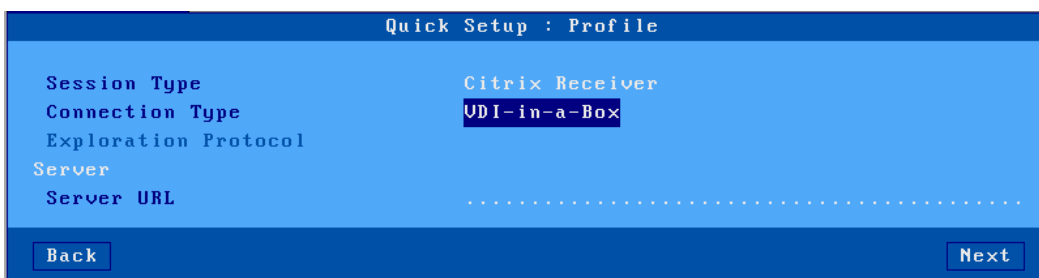
"port": optional, by default 80

**Choose a published resource:**

- **no:** the user will have at his disposal the list of his published resources at the time of connection.
- **yes:** A resource can be chosen in the following quick setup screen (but the thin client will have to rebooted). See chapter [2.1.5](#).

**f) Citrix Receiver - VDI-in-a-Box**

With VDI-in-a-Box, after authentication, the icons of the published desktop are displayed on the desktop of the thin client. ICA sessions are created dynamically as needed:



Parameter description:

**Server URL:** the syntax is [https: //] server [: port] [/ config]

"https": use is optional (by default http)

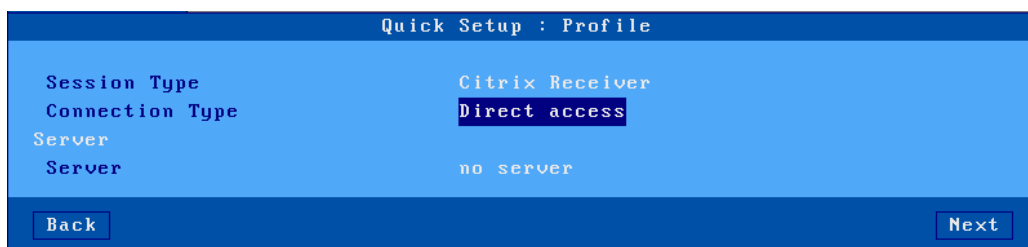
"server": DNS name or IP address of the server access to the Citrix farm.

" port": optional, by default 80 for http and 443 for https

"/ config": optional path to the configuration file "/dt/PNAgent/config.xml" by default)

### g) Citrix Receiver - Direct Access

Connection of a predefined session ICA to a Citrix server (referenced by its IP address or DNS name):

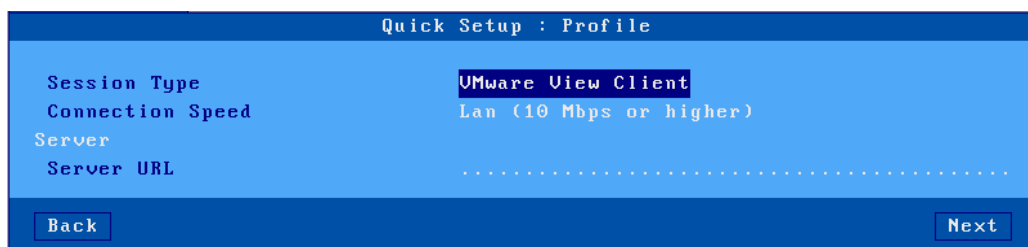


Description of the parameter:

**Server:** DNS name or IP address of the server.

### h) VMware View Client

With VMware View Client, after authentication, a predefined session displays the list of available desktops. An RDP connection is established after selecting the required desktop:



Description of the parameters:

**Connection speed:** choice of network type.

**Server URL:** the syntax is [https: //] server [: port]

"https": use is optional (by default http)

"server": DNS name or IP address of the VMware farm access server

" port": optional, by default 80 for http and 443 for https

**j) VNC**

Connection of a predefined VNC session to a Linux server (referenced by its IP address or DNS name):

Quick Setup : Profile	
Session Type	VNC
Server	no server
TCP Port	5901
<div style="display: flex; justify-content: space-between;"> <span>Back</span> <span>Next</span> </div>	

Description of parameters:

**Server:** DNS name or IP address of the server.

**TCP / IP port:** default 5901

**j) Systancia AppliDis**

Only thin clients with firmware with the APD option allow this type of session.

The "AppliDis" solution developed by the Systancia company allows a simplified administration of a farm of TSE / RDS servers:

Quick Setup : Profile	
Session Type	Systancia AppliDis
Connection Type	TSE/RDS Desktop
Connection Speed	Lan (10 Mbps or higher)
Server	.....
Server URL	.....
<div style="display: flex; justify-content: space-between;"> <span>Back</span> <span>Next</span> </div>	

Description of the parameters:

- **Connection type:** choice from a list:
  - **TSE / RDS desktop:** for connections on servers using only AppliDis as load balancing.
  - **Virtual Desktop:** a secure desktop with applications opened only by the icons and the Systancia menu.
  - **Session marker:** allows you to track an application (and not a desktop) and retrieve it regardless of the TS server where it is open.
- **Connection speed:** choice of network type from a list.
- **Server URL:** the syntax is **[https: //] server [: port]**
  - "https": use is optional (by default http).
  - "Server": DNS name or IP address of the Citrix farm access server.
  - " port": optional, by default 80 for http and 443 for https.

**k) 5250 or 3270**

Connection of a predefined 5250 (or 3270) session to an iSeries (or zSeries) server. This server is referenced by its IP address or DNS name:



Quick Setup : Profile	
Session Type	5250
Number of Sessions	1
Server	no server

Back Next

Description of the parameters:

**Number of sessions:** possibility to create from 1 to 6 sessions.

**Server:** DNS name or IP address of the iSeries or zSeries server.

### ***I) Text Emulation***

Connection of a predefined telnet or SSH session to a Unix / Linux server (referenced by its IP address or DNS name):

Quick Setup : Profile	
Session Type	Text Emulation
Emulation	ANSI
Protocol	telnet
Number of Sessions	1
Server	no server

Back Next

Description of parameters:

**Emulation:** choose from a list. See chapter [8.1.3](#).

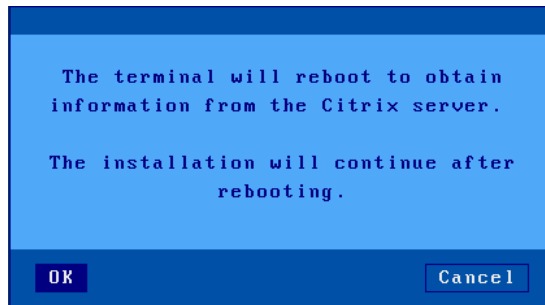
**Protocol:** telnet or ssh

**Number of sessions:** possibility to create from 1 to 6 sessions.

**Server:** DNS name or IP address of the server.

**2.1.5 - Citrix Receiver - Choice of a resource**

With the 'Citrix Receiver' connection types, a resource can be predefined (see previous chapter). In this case, the thin client displays the following dialog:



After the reboot, a dialog box like this one sent by the Citrix server is displayed:

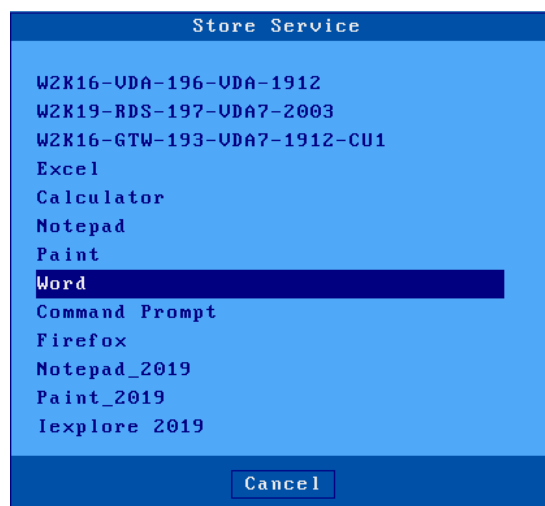


Description of the parameters:

**User name:** Name of the user for which the resource is published, the domain followed by a "\" must be entered before the name

**Password:** Password of this user

If the authentication is correct, a list of the published resources is displayed:



Then, select a resource from the list.

**2.1.6 - Peripherals**

This dialog box is displayed for all types of sessions:



Description of parameters:

**Printer connected:** printer auxiliary port (none, Aux1, Aux2, Parallel, Usb1).

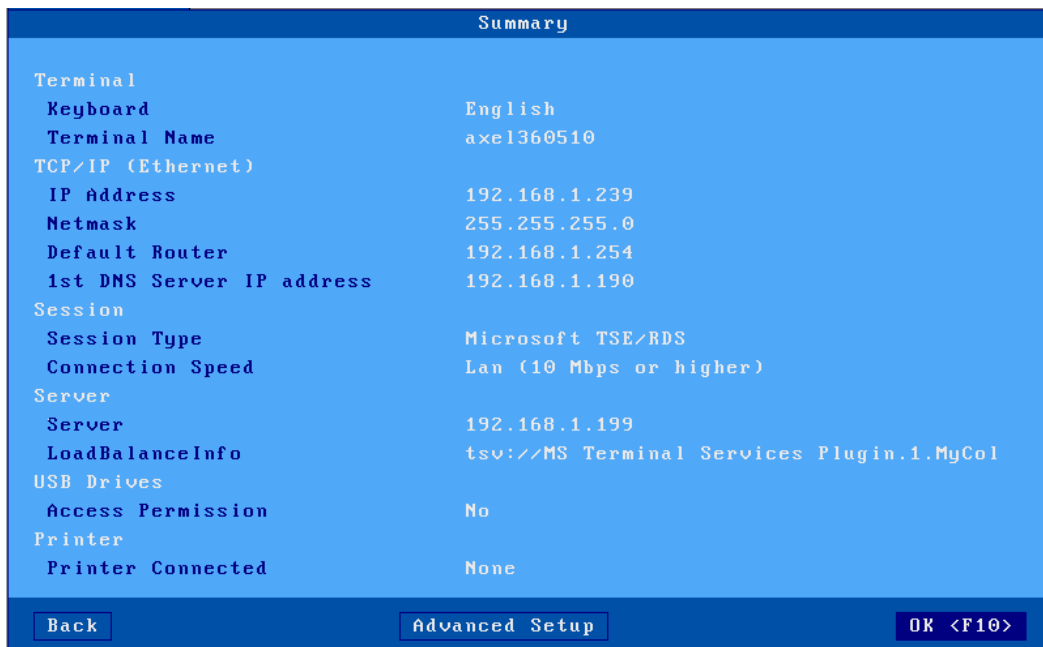
**Protocol:** LPD, TSE, Ptr5250 or Prt3270. The available parameters depend on the protocol chosen:

- o LPD: **Queue** (name assigned to the auxiliary port)
- o TSE and Citrix: **Printer Name** and **Native Windows Driver**
- o Prt5250: **Printer name** and **Driver** (type and model)
- o Prt3270: **Printer name**

**Access Permission:** management of storage devices. Only for Microsoft TSE / RDS and Citrix Receiver sessions.

**2.1.7 - Summary of the setup**

At the end of the Wizard, a screen summarizing the choices is displayed. For example:



The button **[OK <F10>]** confirms these choices. After an automatic restart, the thin client is ready to use.

You can also continue to modify the detailed setup parameters using the button **[Advanced Setup]**

The **[Back]** button allows you to return to the last validated screen.

## 2.2 - THE AUTO-CONFIGURATION FUNCTION

The auto-configuration function allows a “new” thin client to receive a firmware and / or a configuration file without any human intervention.

For more information on auto-configuration of the AxRM software, see the manual: *Axel Remote Management - Version 4*.

The auto-configuration function is started:

- automatically during the very first power-up (or when the terminal is set back to factory defaults - see appendix A.7.1). This mechanism can be interrupted by using the keyboard.
- through a setting, each time the thin client is booted. For more information, see chapter [3.6.2](#).

The auto-configuration steps are as follows:

- network good-link check
- sending of DHCP requests to retrieve an IP address and possibly other configuration parameters.
- transmission of auto-configuration data to the AxRM server
- possible reception of a download command (followed by a reboot)
- receipt of a configuration update (followed by a reboot)

### 2.2.1 - Step 1: network verification

On boot at bottom of screen a message detailing the use of the quick setup is shown. If the presence of a network cable is detected, the message “Auto-Conf” is displayed. The thin client goes to step 2.

```
Auto-conf.
```

### 2.2.2 - Step 2: sending of DHCP requests

To obtain an IP address (and possibly other parameters) DHCP requests are sent. If a DHCP server responds its IP address is displayed in the status line. Which gives:

```
Auto-conf. / DHCP : aaa.bbb.ccc.ddd /
```

The thin client goes to step 3.

### 2.2.3 - Step 3: sending requests to AxRM

When the DHCP search is successful, the thin client can start sending request auto-configuration frames to the AxRM server.

How does the terminal find the IP address and TCP port of the AxRM server?

The location of AxRM is determined by cycling through following methods. Method 1 is therefore the highest priority.

- Method 1:  
The DHCP server gives the IP address (or DNS name) of AxRM server, the TCP port and the protocol (XML or XML-SSL) can also be given by the DHCP server.  
For more information on using Axel DHCP options, see appendix A.5.
- Method 2:  
If no Axel DHCP option is given by the DHCP server, the terminal tries to resolve the DNS names "axrmservssl" and "axrmserv". If the resolution is successful, the IP address obtained is used as the assumed location of the AxRM server. The TCP port used is 443

(XML-SSL protocol) if the name "**axrmervssl**" is resolved and 80 (XML protocol) for the name "**axrmerv**".

- Method 3:  
If method 2 fails, the IP address of the DHCP server is used as the assumed location of the AxRM server. The TCP port used is 80 (XML protocol).
- Method 4:  
This method is only used when the location of the AxRM machine (IP address / name, TCP port and protocol) is specified in the setup. See chapter [3.6.2](#).

The assumed location of the AxRM server (with the method used in parentheses) is displayed in the status line. Which gives:

```
Auto-conf. / DHCP : aaa.bbb.ccc.ddd / AxRM (1) : www.xxx.yyy.zzz:nnnn.....
```

Frames for auto-configuration requests are sent by the thin client. These frames are sent every 5 seconds. If there are no responses after 10 frames sent, the thin client starts this mechanism again in step 1.

The transmission of these frames stops if the AxRM server responds or the keyboard is pressed.

### **2.2.4 - Step 4: receiving a firmware download**

From this step the mechanism can no longer be interrupted and the thin client displays an auto-configuration progress dialog box.

**Note:** this step is optional because a firmware may not be sent. In this case, the thin client goes directly to step 5.

Here is the progress box:

```

Auto-Configuration
Network Detection ..... 100BT FullDuplex
IP Address ..... 192.168.1.200
DHCP Server ..... 192.168.1.165
AxRM Server ..... 192.168.1.12:8080
Firmware Update ..... in progress
Config Update .....
Reboot .....

Auto-Conf. / DHCP : 192.168.1.165 / AxRM (1) : 192.168.1.12:8081...

```

After receiving the firmware, the thin client automatically restarts and repeats steps 1, 2 and 3 before going to step 5.

### **2.2.5 - Step 5: receiving a configuration**

Here is the progress box:

```

Auto-Configuration
Network Detection ..... 100BT FullDuplex
IP Address ..... 192.168.1.200
DHCP Server ..... 192.168.1.165
AxRM Server ..... 192.168.1.12:8080
Firmware Update ..... TCP.XX.1236b.3TD
Config Update ..... in progress
Reboot .....

Auto-Conf. / DHCP : 192.168.1.165 / AxRM (1) : 192.168.1.12:8081...

```

**Note:** if the firmware has been previously updated, the version of this new firmware is displayed.

After receiving the configuration, the thin client restarts:

```

Auto-Configuration
Network Detection ..... 100BT FullDuplex
IP Address ..... 192.168.1.200
DHCP Server ..... 192.168.1.165
AxRM Server ..... 192.168.1.12:8080
Firmware Update ..... TCP.XX.1236b.3TD
Config Update ..... OK
Reboot ..... in progress

Auto-Conf. / DHCP : 192.168.1.165 / AxRM (1) : 192.168.1.12:8081...

```

The thin client is now ready to be used.

**- 3 -  
INTERACTIVE SET-UP**

This chapter provides the information necessary to configure the thin client via the interactive setup.

### 3.0 - GENERAL

To enter the setup, several methods are available:

- Locally:
  - Using the key combination **[Ctr] [Alt] [Esc]**
- Remote:
  - Using “remote control” with AxRM (see chapters [10.1](#) and [10.2](#)).
  - Or a TELNET command with the IP address of the thin client and the TCP port associated with the setup as a parameter (see chapter [10.3](#)).

#### 3.0.1 - Access protected by password

If access to the setup is protected by password (see chapter [3.2.8](#)), entering this password is essential to modify the configuration parameters of the thin client:



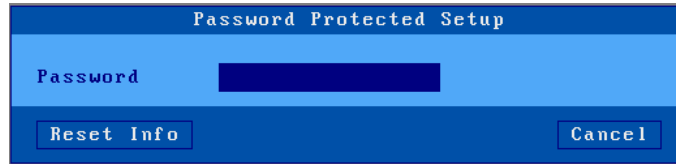
Three actions are then possible:

- Enter the password to access the setup
- Type **<Esc>** or select the button **[Cancel]** to exit this dialog box and exit the setup mode.
- Select the button **[Consultation]** to access the setup without knowing the password. In this situation, all actions are possible **except saving the modifications at the end of the setup**



(this mode can be used by the end client to communicate setup information to their administrator).

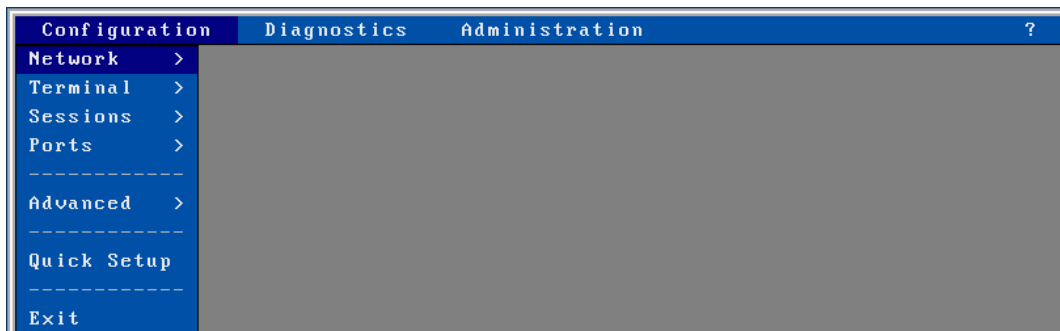
This "Consultation" mode is not available if the " parameter" **Authorize consultation without password** is set to "no". See chapter [3.2.8](#), in the following dialog box that appears:



**Note:** if you forget the password, a "factory password" allows you to enter the setup. This super password is "yaka". It can only be used from the local interactive setup provided the parameter **Authorize factory password** is set to "yes". See chapter [3.2.8](#)

### 3.0.2 - The first dialog

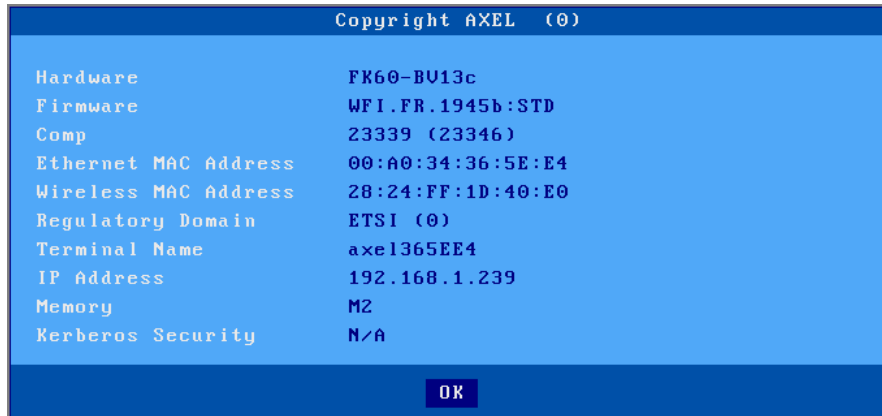
The first dialog of the setup is as follows:



The navigation in the setup can be done either with the mouse or with the keyboard. The use of the interactive setup is described in detail in chapter [A.1](#).

### 3.0.3 - General product information

To view information on the version and hardware of the thin client select the menu **[Configuration]** - **[? ]-[Information]**



Next to the *Copyright AXEL* is a number in parenthesis "**(x)**", it is used to reset the terminal in case of loss of the setup password, see appendix A.7.7.

#### a) The hardware

This information allows to know the type of hardware and version of bootcode. Here the hardware type is "**FK60**" and the bootcode version is "**BV13c**". For more information, see Appendix A.8.1.

#### b) The "Firmware" and its "comp number".

These two pieces of information define the version of the firmware of the thin client as well as its possible options. For more information, see Appendix A.8.2.

#### c) Ethernet MAC address.

Also called an Ethernet physical address, it is an identifier made up of 6 bytes in hexadecimal form separated by ":" which makes it possible to uniquely identify the thin client at the Ethernet level.

The following table gives the first 4 bytes corresponding to the different models:

G10 (FK70)	<b>00: A0: 34: 44</b>	or	<b>00: A0: 34: 45</b>
G15 (FK75)	<b>00: A0: 34: 46</b>	or	<b>00: A0: 34: 47</b>

#### d) The 802.11 MAC address and the "Control domain".

This is the equivalent of the physical Ethernet address (described above) for the additional wireless link card, this card is only present if the WIFI option was ordered when purchasing the thin client.

The regulatory domain corresponds to the countries in which the thin client can be used, in Europe the domain must be "ETSI".

### e) Name of the terminal and its IP address

The name of the terminal and the IP address are defined in the setup by the administrator of the thin client, for more information see chapter [3.1](#) which follows.

### f) Memory

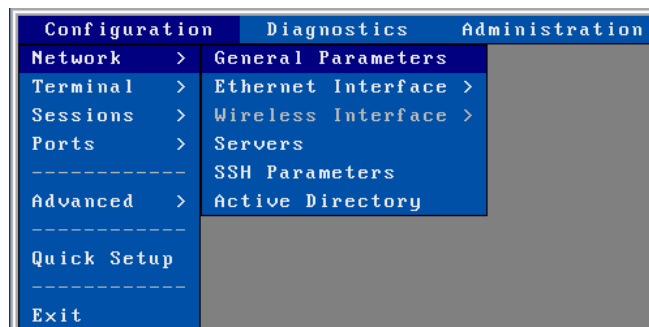
This information corresponds to the type of memory installed in the thin client.

### g) Kerberos Security

This information corresponds to the security type used by Kerberos for the connection via Active directory (all N/A, forced RC4\_HMAC\_MD5, forced AES\_HMAC\_SHA1).

## 3.1 - ETHERNET OR 802.11 INTERFACE CONFIGURATION

The network parameters can be accessed via the menu **[Configuration] - [Network]**:



This chapter describes the network configuration of the thin client. The points covered are:

- **General parameters:** Settings identification of thin client and activating the communication interface
- **Interface configuration (Ethernet or Wireless):** generic settings, IPv4, DNS protocol and routers,
- **Servers:** managing the local server table.
- **SSH Settings and reverse SSH:** SSH security setting and "Reverse SSH" parameters.
- **Active Directory:** configuration of the AD environment to restrict access to the thin client.

**Note:** if necessary, additional information is given in the following appendices:

- Appendix A.2: Ethernet addresses, IP addresses and routers
- Appendix A.3: DHCP protocol
- Appendix A.4: DNS protocol

### 3.1.1 - General

Parameters to configure the type of communication and the identification of the thin client, select the menu **[Configuration] - [Network] - [General parameters]**. The following dialog box appears:

Network General Parameters	
Terminal Name	axel360510
Active Interface	Ethernet
Backup Interface	None
DNS Domain	Default DNS Domain
Terminal Comment	.....
<input type="button" value="OK &lt;F10&gt;"/> <input type="button" value="Cancel"/>	

### a) Terminal name

It is mandatory to assign a name to an Axel thin client. This default name offered is "axel" suffixed by the last 3 digits of the Ethernet address of the thin client.

In this example the default name is "axel360510" because the Ethernet address of this thin client is "00: A0: 34:36:05:10"

**Note:** if the option "Terminal name" is selected in the DHCP options, this field is inaccessible (grayed out).

This name is used as the default connection name for RDP and ICA sessions as well as for publication with a DNS server.

The publication of the name of the thin client can be carried out by the DHCP server or the thin client itself. For more information see the following chapter and appendix [A.4.3](#).

### b) Active Interface

The AXEL thin client can only use one interface at a time, this parameter allows you to choose which interface to use.

The 802.11 interface is only available if the thin client has a firmware of type "FKxx.WFI ..." (verifiable in the general product information see chapter [3.0.3](#))

Two choices possible:

- **Ethernet:** Connection with an RJ45 Ethernet cable.
- **Wireless:** Connection without cable with WIFI option.

### c) Emergency interface

Automatically uses the "Wireless" interface if it is present at the hardware level, as a backup interface when the "good link" of the Ethernet link is not present at the terminal boot and only at that time (if the "good link" is lost in the running court the backup interface is not activated).

When this option is positioned at "Wireless" it allows you to set up the Ethernet interface and Wireless interface, otherwise only one or the other interface is configurable according to the "Active Interface" setting.

### d) DNS domain

If the name of the thin client is to be published (ie registered with a DNS server), the DNS domain is necessary. Registration with a DNS server requires a FQDN name (Fully Qualified Domain Name). If this "DNS Domain" is empty, the "Default DNS Domain" (possibly given by the DHCP server) will be used. If the "Default DNS domain" is empty, the name will not be published.

### e) Associated comment

This character string is used to enter a description of the thin client. This description will be retrieved by the AxRM administration software during a network discovery operation. And the thin client can be more easily identified within the AxRM database.

### 3.1.2 - Wired Ethernet interface

To configure the Ethernet interface, select the menu **[Configuration] - [Network] - [Ethernet Interface] - [Parameters]**. The following dialog box appears (the MAC address of the Ethernet interface is specified in the title bar):

Ethernet Interface 00:A0:34:36:05:10	
<b>Interface</b>	
Link	Auto-Sense
<b>IPv4</b>	
Enable DHCP	No
IP Address	192.168.1.239
Netmask	255.255.255.0
<b>DHCP Parameters</b>	
<b>DNS</b>	
1st DNS Server IP address	192.168.1.190
2nd DNS Server IP address	.....
DNS Parameters	[Edit]
<b>Routers</b>	
Default Router	192.168.1.254
Other Routers	[Edit]
<b>802.1X Security</b>	
Activation	No
<b>Settings</b>	

OK <F10>      Disconnect      Cancel

The following sub-chapters describe:

- Configuration of the Ethernet link,
- Configuration of IPv4 addressing,
- Configuration of the DNS protocol,
- Router management,
- 802.1X security.

#### a) The link

The "parameter **Link**" indicates the operating mode of the interface. The default mode is "**Auto-Sense**". The other modes are possible:

- 10BT HalfDuplex,
- 10BT FullDuplex,
- 100BT HalfDuplex,
- 100BT FullDuplex,
- 1000BT FullDuplex.

## b) DHCP parameters

The parameter **"DHCP activation"** enables the use of the DHCP protocol. This protocol allows the thin client to automatically obtain an IP address (and possibly other parameters) when it is powered up.

If **"DHCP activation"** is set to **"no"**, you must enter an IP address and a subnet mask corresponding to the type of network on which you want to connect the thin client. For more information see Annex [A.2.2.](#)

If **"DHCP activation"** is set to **"yes"**, the **"IP address"** field is inaccessible and the DHCP protocol is configured by selecting the **"DHCP parameters"** option. The following dialog box appears:



The list of DHCP options allows you to select the parameters requested from the DHCP server (in addition to the IP address of the thin client).

The other parameters are:

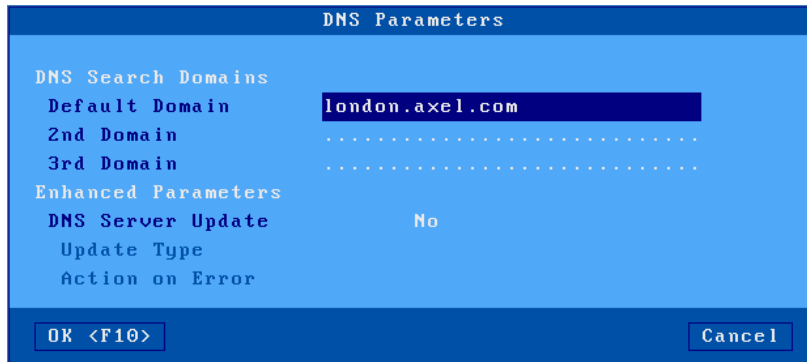
- **"Lease Time (minutes)":** the "lease time" is the period of validity of the IP address proposed to the DHCP server (The server decides after receiving the client's proposal of the value that will be used). At the end of the lease time the thin client automatically negotiates an extension. 720 minutes.
- **"Release IP addr when shutdown":** when this parameter is "no", the thin client will offer its previous IP address as an option to the DHCP server. The DHCP server can agree to re-use or issue new IP address. If set to "Yes" the terminal simply asks the DHCP server for an IP address
- **"Client identifier":** identifies the client by a criterion other than the Ethernet address (useful for checking the IP address of a thin client).
- **"User class Identifier":** allows the DHCP server to communicate information specific to a class of devices.
- **"Check IP address":** after an IP address has been proposed by the DHCP server, the thin client can verify whether this address is actually available on the network. This verification takes a few seconds. Default "yes"

### c) "DNS parameters"

To resolve a name, the thin client contacts a DNS server for which it must know the IP address. Two DNS servers can be entered.

**Note:** if the option 'DNS servers' is selected in the list of DHCP options, these two parameters are inaccessible.

Other DNS parameters are available by selecting the "DNS parameters" option. The following dialog box is displayed:



The parameters are:

- **DNS search domains:** for the resolution of a name or for the publication of the name of the thin client, search domains are possibly concatenated with the name to be resolved (see appendix A.4).
- **Note:** if the "Default DNS domain" option is selected in the list of DHCP options, the "Default domain" parameter is inaccessible (grayed out).
- **DNS server update:** allows to indicate the method used to publish the name of the thin client:
  - **no:** the name of the thin client is not published.
  - **by the DHCP server** (only if DHCP is enabled): the publication of the name of the thin client is carried out by the DHCP server. This assumes that the "DDNS" (Dynamic DNS) function is activated on the DHCP server. See annex [A.4.3](#).
  - **by the terminal:** it is the thin client itself which updates the DNS server. In this case, the "In case of error" parameter indicates the behavior of the thin client if the DNS server indicates reports an error during the update (see appendix A.4.3)

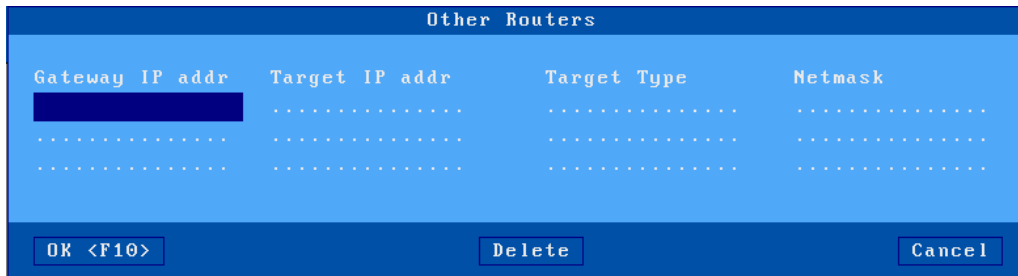
**d) Routing**

A router is a gateway between two networks.

The "**default router**" is a router that is able to route frames to any destination outside the network.

**Note:** if DHCP is active and "default router" is selected in the list of DHCP options, this parameter is inaccessible (grayed).

It is also possible to define other routers to address specific destinations. Select "**Other routers**". The following dialog box is displayed:



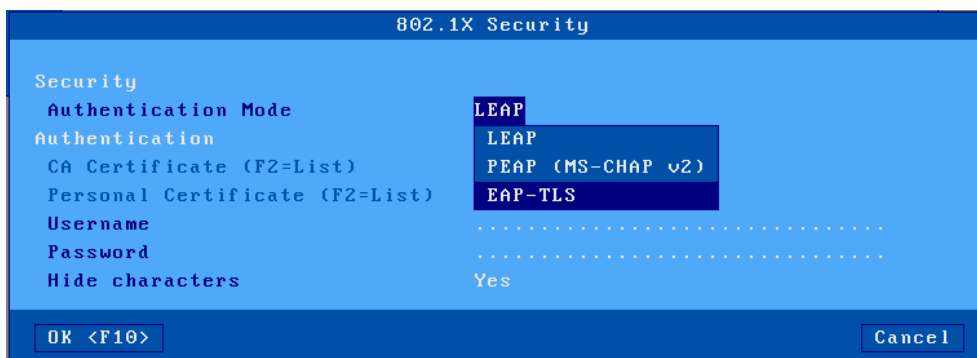
Here a router is defined by:

- its IP address,
- the destination IP address,
- and the type of destination: server or network. In the latter case, the network mask can be specified for sub-netting purposes.

**e) 802.1X security**

The 802.1X protocol allows authentication of the thin client at the Ethernet level. This requires a switch supporting this function and the ability to configure a radius server.

Activate the function to access the Settings dialog box:





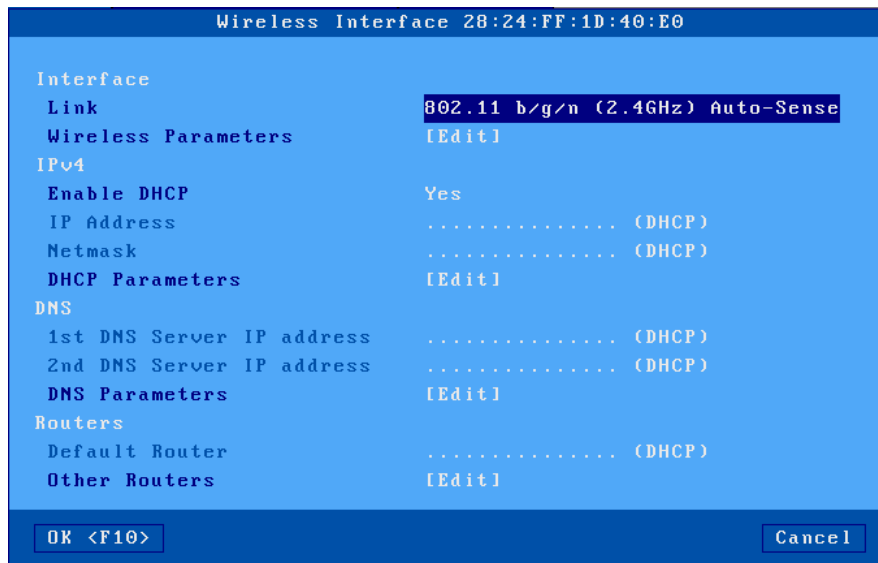
The following table shows for each authentication mode or the necessary parameters:

Authentication Mode	Username	Password	Certificate authority	Certificate staff
LEAP	required	required	---	--
PEAP (MS-CHAP v2)	required	required	optional	optional
EAP-TLS	optional	---	optional	required

For more information, refer to the documentation for the 802.1X protocol and the authentication mode used.

**3.1.3 - 802.11 wireless interface**

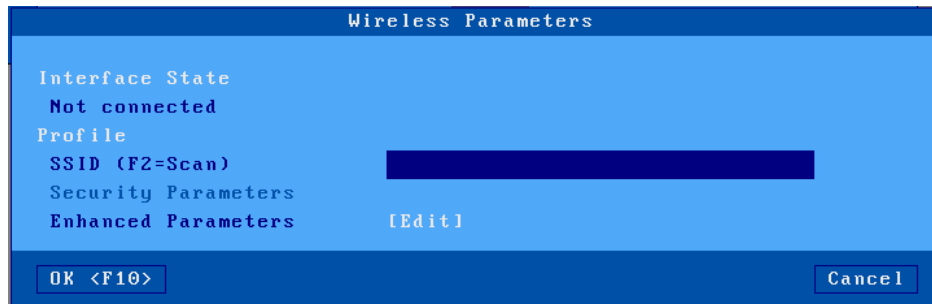
The Wireless interface is configured using the **[Configuration] - [Network] - [Wireless interface] - [Parameters]**. The following dialog box appears (the MAC address of the 802.11 interface is specified in the title bar):



The Connection parameter allows you to choose the operating mode:

- 802.11 b / g / n (2.4 GHz)
- 802.11 a / n (5 GHz)

To access the configuration of the 802.11 connection, click on the [Edit] button in the "802.11 parameters". The following dialog box is displayed:



**Note:** if the interface is connected a [Disconnect] button is available.

The rest of the chapter describes the following operations:

- choice of SSID
- security settings (connection to SSID).
- advanced parameters (roaming for example)

The parameters of the "IPv4", "DNS" and "Routing" sections are the same as those of the wired Ethernet interface. For more information, see chapter [3.1.2](#).

**a) Choice of SSID**

The first step is to enter the SSID of the access point. The SSID can be entered manually or via a scan (provided that the interface is not already connected).

Example of "scan" (<F2> key):

Available Access Points					
SSID	BSSID	Ch	Signal	Security	
<Hidden>	06:1f:33:82:33:9c	11	Low	WPA2-PSK-CCMP	▲
AX_free	4a:98:ac:fe:4d:2c	13	High	WPA-PSK-TKIP+	
Ax_Ap7522_Enterp	74:67:f7:6a:4c:62	11	High	WPA-EAP-TKIP/	
Ax_Ap7522_Enterp156	74:67:f7:6a:4c:63	11	High	WPA-EAP-TKIP/	
Ax_Ap7522_Perso	74:67:f7:6a:4c:61	11	High	WPA-PSK-TKIP/	
CASTEL_PARIS	84:16:f9:6e:a6:d0	1	Low	WPA-PSK-CCMP/	
DanaherNet	28:6f:7f:48:b7:80	1	Low	WPA2-EAP-CCMP	
FreeWifi	4a:98:ac:fe:4d:2d	13	High	.....	
FreeWifi	de:04:54:14:2f:34	3	High	.....	
FreeWifi_secure	de:04:54:14:2f:35	3	High	WPA-EAP-CCMP	
FreeWifi_secure	4a:98:ac:fe:4d:2e	13	High	WPA-EAP-CCMP	
Livebox-c	5c:b1:3e:fd:c7:1c	11	Low	WPA-PSK-TKIP+	
Mi.ALx	9e:63:e5:7e:b7:8b	6	Low	WPA2-PSK-CCMP	
NETGEAR22	80:37:73:fe:2b:84	9	Medium	WPA2-PSK-CCMP	
WINGExpress	74:67:f7:6a:4c:60	11	High	.....	▼

In this list, the hidden SSIDs appear under the name <hidden>. If a hidden SSID is chosen as the SSID, the name of the SSID must be entered manually.

If the chosen SSID appears several times in the list, a dialog box allows you to force (or not) the connection to this particular access point (BSSID forced - see chapter [3.1.3.c](#)).

**b) Security parameters**

Once the SSID has been chosen, select "Security parameters" to configure the access method. The dialog box is as follows:



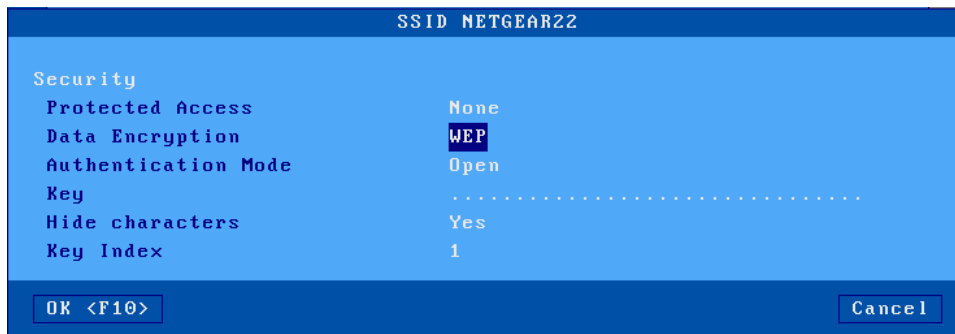
**Note:** if the SSID was chosen via a scan, the parameters are already initialized according to the prerequisites of this SSID.

Choosing a value for "Access Control" changes the options offered. The possible values of "Access control" are:

- **none** : encrypted connection (WEP) or not
- **personal (PSK)**: encrypted connection (WPA / WPA2)
- **Enterprise (EAP)**: authenticated connection (LEAP / PEAP) and encrypted (WPA / WPA2)
- **802.1X** connection authenticated (LEAP / PEAP) and encrypted (WEP)

The rest of the chapter details these access controls.

*b1) "Access control" set to "none"*

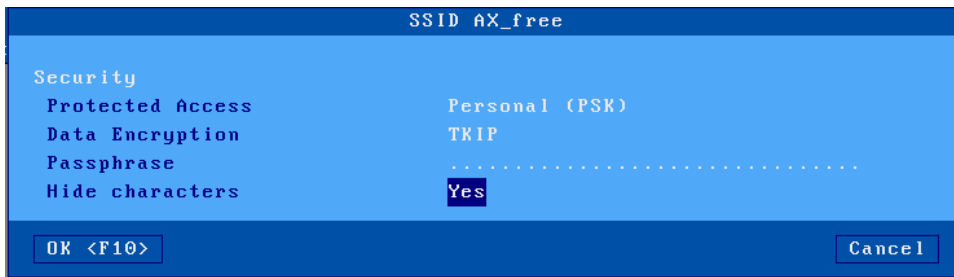


Encryption type	Authentication mode	WEP key required
WEP	Open	yes
	Shared	yes
None	---	---

**Note 1:** a WEP key is a character string 5 or 13 characters long. It can be entered in ASCII or in hexadecimal code (the length is then doubled). For example, the key 12345 in ASCII is set to 3132333435 in hexadecimal

**Note 2:** the thin client only manages one WEP key. If necessary, use the "Key index" parameter (which varies from 1 to 4).

*b2) "Access control" set to "personnel (PSK)"*

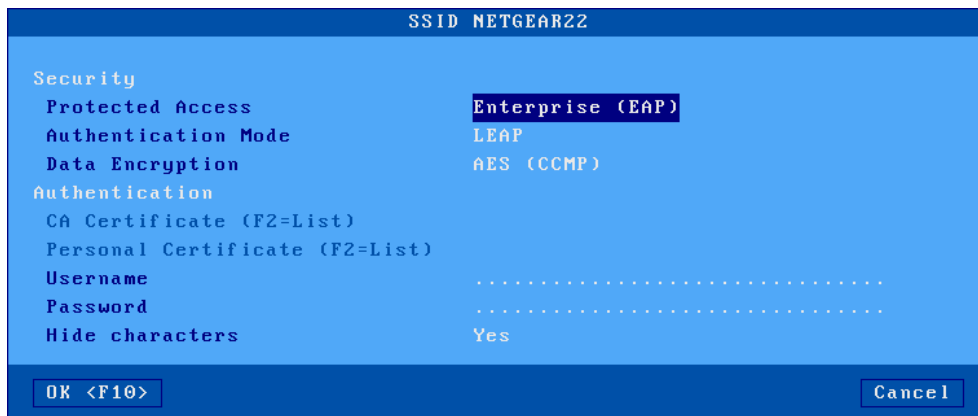


encryption	Passphrase required
AES (CCMP)	yes
TKIP	yes

**Note 1:** "Personal (PSK)" access control is also known as WPA or WPA2. The Axel thin client is able to dynamically choose one or the other of these protocols. If necessary, it is possible to force a protocol through the parameter **"Wireless PSK / EAP version"** in the menu **[Configuration] - [Advanced] - [Tuning] - [Network]**.

**Note 2:** the "passphrase" allows the thin client to calculate the "Pre Shared Key" (PSK). This "passphrase" is between 8 and 63 characters long. But if necessary, it is possible to use the field "passphrase" to directly enter the value of the PSK (32 bytes in hexadecimal notation, ie 64 characters).

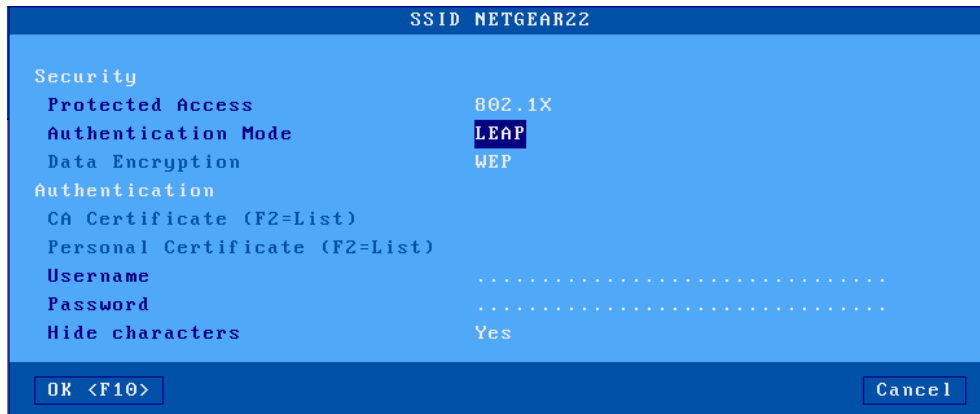
b3) "Access control" set to "company (EAP)"



Authentication mode	Encryption type	Password	certificate
LEAP	AES(CCMP)	required	---
	TKIP	required	---
PEAP (MS-CHAP v2)	AES (CCMP)	required	optional
	TKIP	required	optional
EAP-TLS	AES (CCMP)	--	required
	TKIP	---	required

**Note:** see note 1 of the previous access control regarding the WPA and WPA2 protocols.

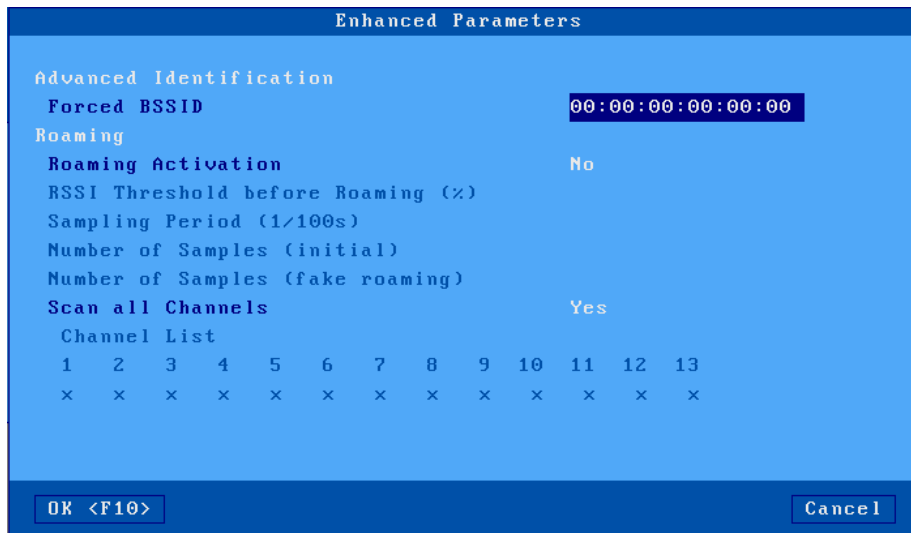
b4) "Access control" set to "802.1X"



Authentication mode	Encryption type	Password	certificate
LEAP	WEP	yes	---
PEAP (MS-CHAP v2)	WEP	yes	optional
EAP-TLS	WEP	---	required

c) **Advanced parameters**

In the 802.11 parameters dialog box, select "Advanced settings". The dialog box is as follows:



- **BSSID forced:** in the case of multiple access points with the same SSID, this parameter allows you to select a particular access point by virtue of its MAC address.
- **Roaming:** this operating mode allows a mobile terminal to automatically disconnect from its access point (from which it is moving away) to reconnect to another access point (closer). If

this disconnection / reconnection is fast enough it will be invisible to the TCP / IP layer. The parameters related to roaming are as follows:

- **RSSI before roaming threshold:** if the average signal quality (RSSI) is below this threshold, the thin client disconnects from the access point to try to find another with a better signal quality.
- The other three parameters are used to calculate the average of the RSSI. For more information, see the organization chart on the next page.
- **Scan all channels:** On connection or after disconnection it is necessary to scan the access points to detect the one with the best signal quality. Exploring all channels takes between 3 and 4 seconds (200ms per channel). To optimize this time and reconnect more quickly, it is possible to specify the channels to be scanned (provided of course that you set this at the access point (s)). In this case, set this parameter to "**no**" and select each channel individually.

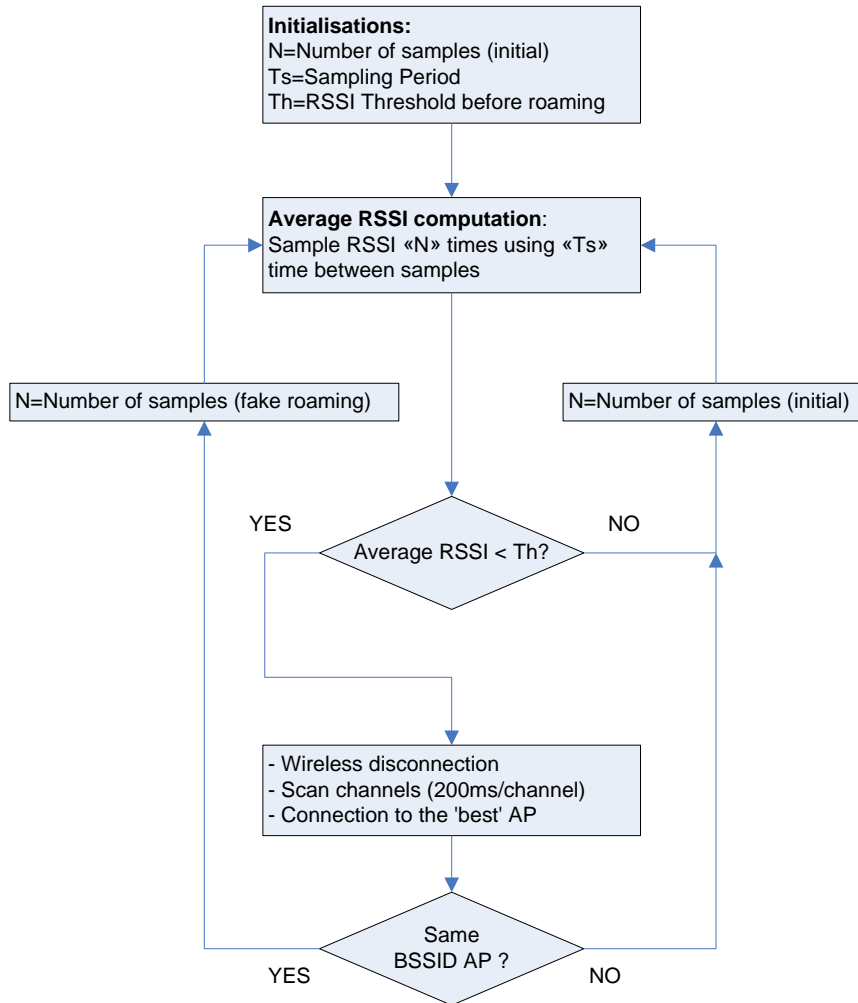
**Notes:**

**a:** The available channels depend on the type of link (2.4 or 5 GHz)

**b:** For Windows servers, in order to avoid disconnections (RDP or ICA) too fast during roaming, it may be interesting to change a value from the following registry:

- **Parameter:** HKEY\_LOCAL\_MACHINE-SYSTEM-CurrentControlSet-Services-Tcpip-parameters-TcpMaxDataRetransmissions
- **Default value:** 5
- **New value:** 20

The following flowchart describes how the thin client calculates the average RSSI. This value is important because if it is lower than the "RSSI threshold before roaming" the thin client disconnects from the current access point:



### 3.1.4 - Server management

A server is a machine (Windows, Unix / Linux, AS / 400 , printer ...) to which the thin client connects. To modify the server table, select the menu **[Configuration] - [Network] - [Servers]**:

IP Address or DNS Name	Friendly Name
192.168.1.199	RDS 2019 server
RDS-BRK1.london.axel.uk	Broker RDS 1
RDS-SERV-2016	RDS 2016 Server
.....	.....
.....	.....
.....	.....
.....	.....
.....	.....
.....	.....

DNS Search Domains

Default Domain      madrid.axel.fr

2nd Domain      .....

3rd Domain      .....

OK <F10>      Delete      Cancel

The definition of a server depends on the use or not of the DNS protocol:

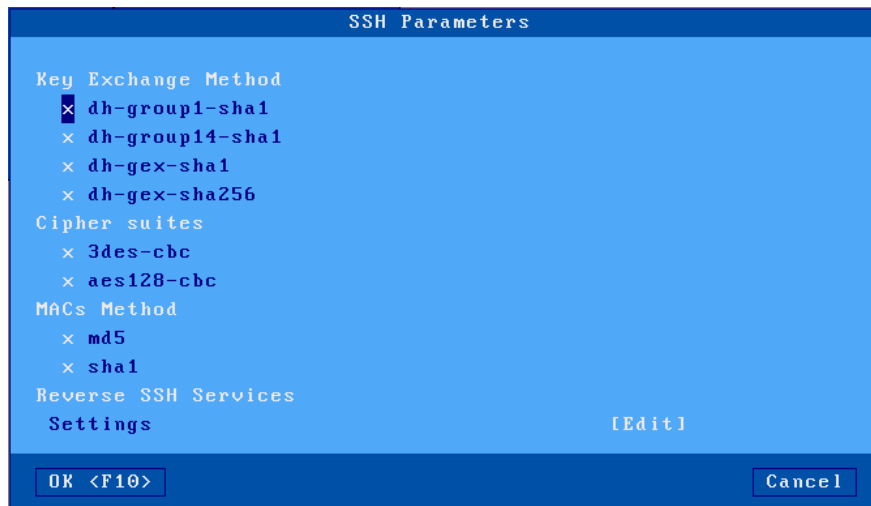
- **no DNS:** a server is defined by an IP address and a friendly name (simple mnemonic) in the example **RDS 2019 server**.
- **with DNS:** the server is defined only by its DNS name and a friendly name. This DNS name can be complete (**RDS-BRK1.london.axel.test**) or not (**RDS-SERV-2016**). The IP address will be automatically found by the thin client (see appendix A.4).
- **Add a server:** move the selection bar to a free entry in the "" column **IP address or DNS name** then enter the "DNS name" or "IP address" of the server, a text name can be added to the right column, it only serves to name the first column more explicitly.  
**Note:** A server can be added directly from the session profile.
- **Deleting a server:** select the [Delete] button and choose the server to delete from the list provided.
- **Modifying a server:** move the selection bar to the column to modify and enter the new value.

The search domains defined in the DNS dialog box are displayed for information (they cannot be modified).



### 3.1.5 - SSH parameters

The parameters are used to modify the security values offered to the server. To modify the SSH parameters, select the menu **[Configuration] - [Network] - [SSH Parameters]**:



For more information on the SSH protocol see paragraph [8.1.2.b](#)

In the event of a connection problem, after checking all the security options as in the window above, check that the following security parameters are present in the configuration file of the "sshd" server, this file is generally located in / etc / ssh, (for Ubuntu, / etc / ssh / sshd\_config):

```
KexAlgorithms diffie-hellman-group-exchange-sha256
Ciphers aes128-cbc
MACs hmac-sha1
```

### 3.1.6 - Reverse SSH

This function allows access to the services (remote control and LPD) of a terminal behind a NAT (and therefore has no public IP address).

With this principle, the thin client opens a connection to an SSH server. Virtual channels are negotiated for each published service (remote control and / or LPD). This allows third-party machines to connect to the SSH server which redirects service requests to the thin client.

The configuration of reverse SSH is accessible via the menu **[Configuration] - [Network] - [SSH parameters]**, you must then confirm with the **[Edit]** button:



Reverse SSH Services

SSH Server

Server

TCP Port

Auto-Connection

Keepalive

Keepalive Value

Reconnection after keepalive

Authentication

Username

Password

Remote TCP Ports for Services

UNC Remote Control

LPD

OK <F10> Cancel

Description of parameters:

- **Server:** IP address or DNS name of the SSH server. This server is not part of the local server list.
- **TCP port:** generally, port 22
- **Username / Password:** authentication to the SSH server
- **Remote control:** TCP port used on the SSH server side to relay this service (0 if the service is not redirected)
- **LPD:** TCP port used on the SSH server side to relay this service (0 if the service is not redirected)

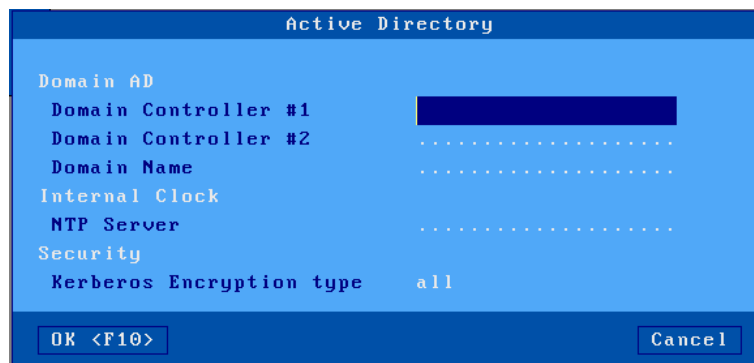
### 3.1.7 - Active Directory

Active Directory can be used to control access to the local desktop of the thin client (see chapter [3.2.8](#)). It can also be used to log in using a smart card to an RDS / TSE session in NLA.

Changing an expired password is not taken into account by the NLA protocol which is used by default to connect to an RDS server (with a PC or with a thin client).

This feature allows changing the password at boot when entering usernames/passwords (like a PC would do).

The configuration of the Active Directory environment is accessible via the menu **[Configuration] - [Network] - [Active Directory]**:



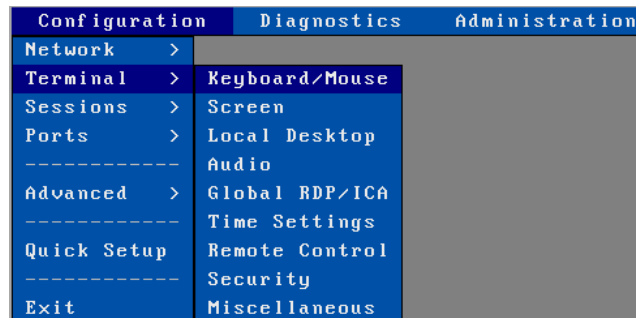
Description of parameters:

- **Domain controller 1:** IP address of the Active Directory domain controller
- **Domain controller 2:** IP address of the controller of a second Active Directory domain if necessary.
- **Domain name:** full name (this is not the NETBIOS domain name)
- **NTP server:** enter the IP address (or DNS name) of the time server (unless this is obtained by the DHCP protocol - See chapter [3.1.2](#))
- **Kerberos Encryption type:** type of encryption negotiated by the thin client.
  - **All:** first negotiation is **AES256\_HMAC\_SHA1** if error then **RC4\_HMAC\_MD5**.
  - **RC4\_HMAC\_MD5:** only RC4\_HMAC\_MD5.
  - **AES256\_HMAC\_SHA1** only AES256\_HMAC\_SHA1.
- A **[TEST]** Button used to check whether the NTP server is available.

**Note:** the parameters of the “AD Domain” cannot be modified (grayed out) if the AD session is in use.

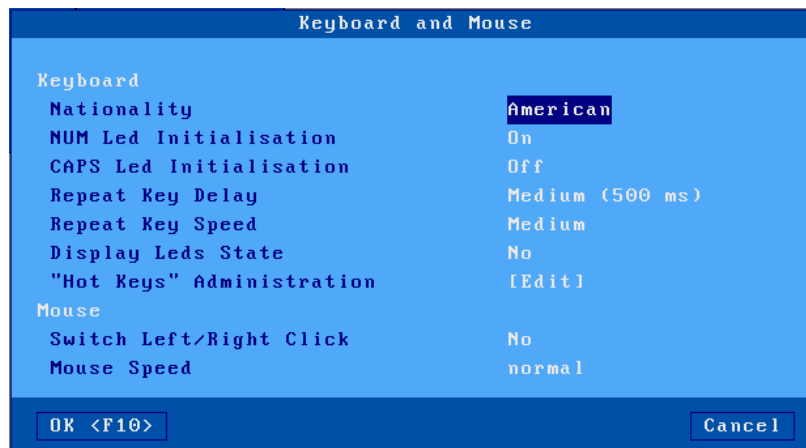
## 3.2 - GENERAL PARAMETERS

These parameters are accessible via the menu **[Configuration] - [Terminal]**:



### 3.2.1 - Keyboard and mouse

Select **[Configuration] - [Terminal] - [Keyboard / Mouse]** :

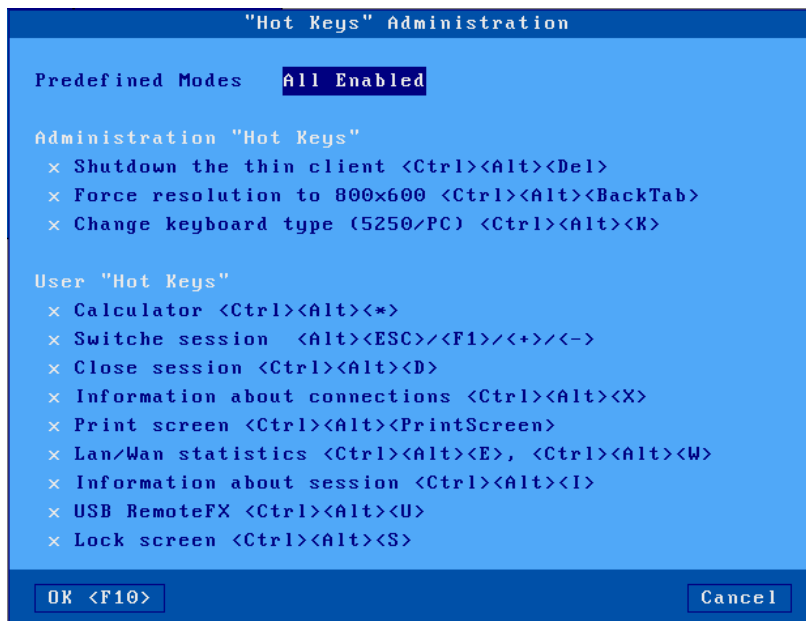


#### a) General keyboard parameters

- **Nationality:** the following list allows you to choose the nationality of the keyboard (some nationalities are only available in the form of options)
- **Initialization led 'Num:** state at power-up
- **Initialization led 'Caps:** state at power-up
- **Repeat key delay:** delay necessary for the transmission for the second time of the code associated with the key on the keyboard currently pressed. The values of this parameter are: never, low (250 ms), medium (500 ms) or high (1 s).
- **Repeat key Speed:** (accessible only if the repeat delay is activated): once key repetition is activated, the code represented by the key pressed is sent regularly. The frequency of this transmission can be Slow, Medium or Fast.
- **Display LED status:** allows you to display in the AXEL task bar the current state of the keyboard LEDs (interesting especially for wireless keyboards which generally do not have integrated LEDs)

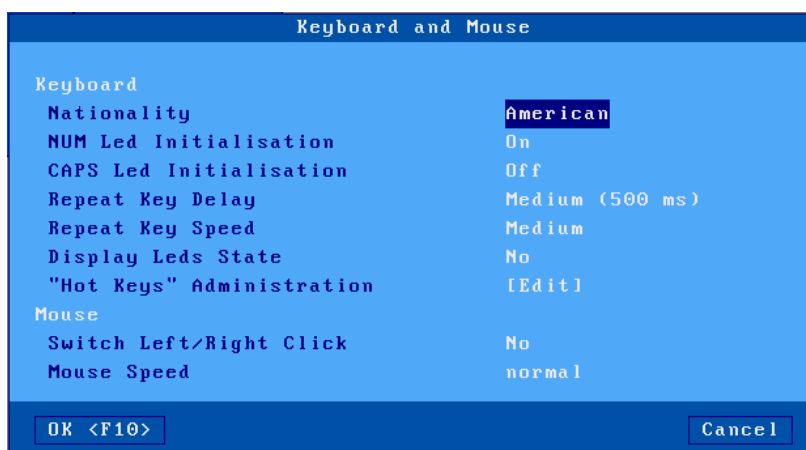
### b) Administration of keyboard shortcuts

Select [Configuration] - [Terminal] - [Keyboard / Mouse] then click on the [Edit] button:



This functionality allows you to prohibit or authorize keyboard shortcuts available on a thin client with the exception of the shortcut which allows access to the setup. This is useful for a thin client in "kiosk" mode accessible to the public.

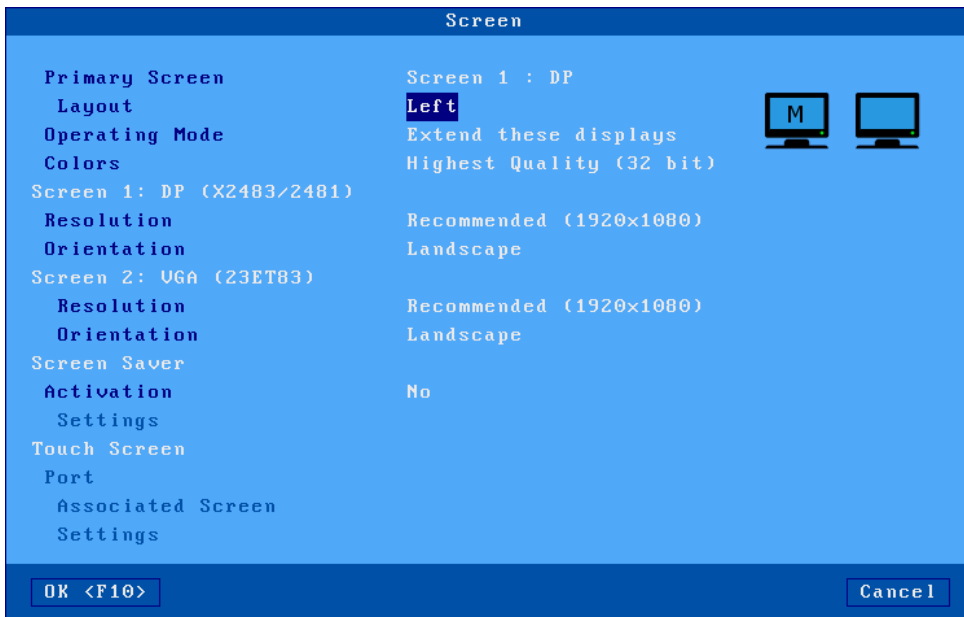
### c) Mouse settings



- **Switch left / right click:** switch the mouse buttons.
- **Mouse acceleration:** may be necessary with large screens.

### 3.2.2 - The screen

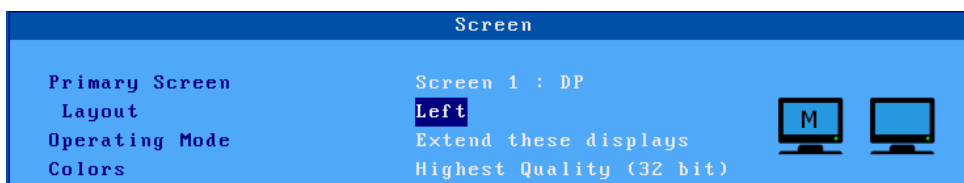
Select [Configuration] - [Terminal] - [Screen]:



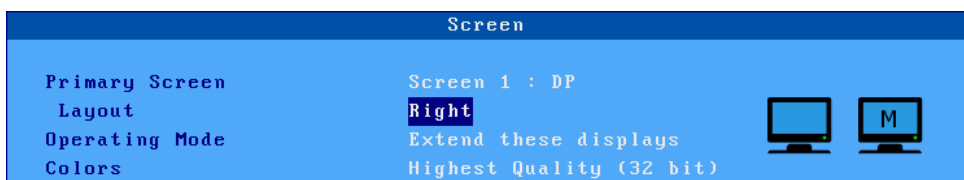
Pictograms located to the right of the window are used to dynamically display the position and orientation of the screens.

#### a) Dual screen management

- **Primary screen:** choice of the screen on which the setup and management information will be displayed. The main screen can be identified by a “M” (like Main) displayed in the center of its pictogram, here on the left.
- **Layout:** Position of the Primary screen. Choice available:
  - Left :



- Right:



- Down:



- **Operating mode:** The available modes are:
  - **Extend these displays:** extended desktop mode with two independent monitors (the resolutions of the two monitors may be different).
  - **Duplicate these displays:** The two monitors display the same thing, in this case the position is not important, and the "parameter **Position** "becomes inaccessible (grayed out).
- **Colors:** is the number of 'bits per pixel'. The available values are 16, 24 and 32 bpp. This number of colors is applied to both two monitors.

**Note:** If there is only one screen connected, these parameters are inaccessible (grayed out) with the exception of the "parameter **Colors**".

**b) Resolution and orientation**

**IMPORTANT:** the connected monitor (s) (VGA or DisplayPort) are detected when the thin client is switched on. If a monitor is changed, the thin client must be rebooted.

**Screen 1** and **Screen 2:** the connector (VGA or DisplayPort) is displayed as well as the screen model:

- **Resolution:** list of resolutions given by the monitor himself.
- **Orientation:** "mode **Landscape**", "**Portrait (Flipped)**" or "**Portrait**".

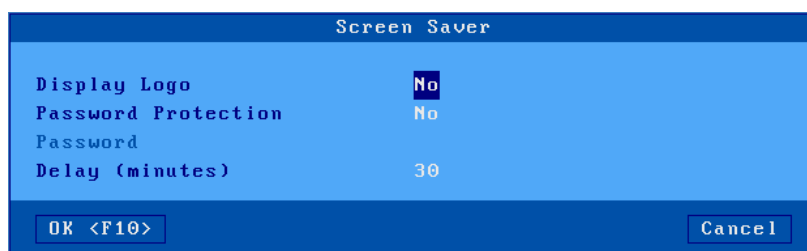
**c) Screen saver**

This function is used to save the monitor by deactivating it after a certain period of inactivity or to lock the screen of the thin client during its use.

The activation (or not) of the screen saver offers three values:

- **no:** inactive function,
- **yes:** the monitor will be reactivated if the keyboard or the mouse is used.
- **yes, local + remote actions:** the monitor will be reactivated if the keyboard or mouse is used or if the display is updated.

Once activated, the screen saver can be configured:



description:

- **Display Logo:** a logo can be displayed on the screen. This logo is displayed on power on of the thin client if no personal logo is loaded in the object store (see chapter [3.6.5](#)).
- **Password protection:** the output of the screen saver can be protected by a local password or by that of the Active Directory logon. For more information on the screen lock, see chapter [4.8.2](#)
- **Delay (minutes):** delay before deactivation or locking of the screen.

#### d) Management of touch screens

There are two types of touch screens managed by Axel thin client, USB-Serial touch screens and USB touch screens.

Generally, the touch screen is managed locally, this means that "touch events" are automatically converted by the thin client into "mouse events". The touch screen is therefore managed without any particular development on the server side.

When the finger touches the touch screen, a "click" event is sent to the server. The type of "click" depends on the type of session:

- 5250 emulation: left "double-click"
- other emulations or protocols: "left click"

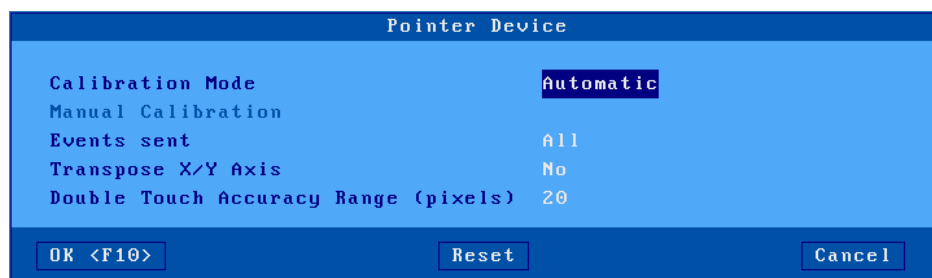
A specific mode in RDP can also be used, it is the "Multi-touch" when the thin client is connected by RDP to an RDS server higher than Windows 2012 or a computer Windows 8 or higher

Description of the parameters:

- **Port:** connection port for a USB-Serial touch screen.  
If a touch screen is connected via USB, this setting is disabled (grayed out).
- **Associated screen:** if two screens are connected, this parameter allows you to select which one is the touch screen.
- **Configuration:** the dialog box displayed depends on the type of touch screen (USB or USB-Serial).

#### d') USB touch screens

the displayed dialog box is as follows:



Parameter description:

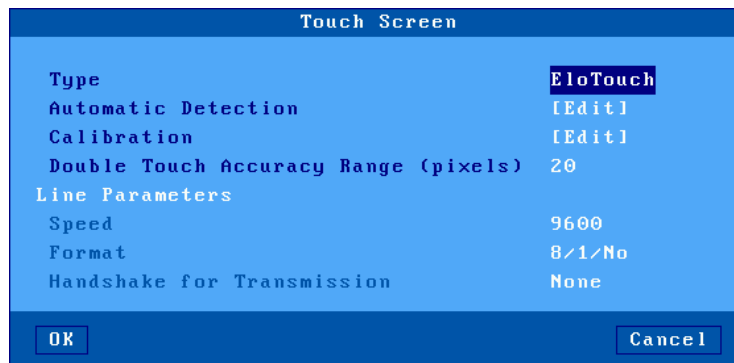
- **Calibration mode:** two possible modes
  - **Automatic** (only if the screen communicates to the thin client the min / max of the touch screen)
  - **Manual:** select the number of calibration points (2, 4 or 9) and the method (linear or not). See below.
- **Manual calibration:** dialog box for calibrating the screen. The principle is to touch the screen at the places where stars appear.
- **Events sent:** two possible modes:



- **Clicks:** only a mouse “click” is sent when the screen is touched.
- **All:** in addition to the “mouse click”, “mouse movement” events are sent until the finger no longer touches the screen.
- **Reverse the X / Y axes:** select “yes” or “no”
- **Double touch precision (pixels):** this parameter allows an easier double-click simulation by defining a target of X pixels square. When the screen is touched twice quickly (less than 0.5 seconds) and the two impacts are in the same area, the thin client generates a double-click event. Otherwise, the thin client generates two simple clicks.

**d”) USB-Serial touch screens:**

the dialog box displayed is as follows:



Parameter description:

- **Type:** selection of the manufacturer of the touch interface: ELOTouch, MicroTouch or Liyitec
- **Calibration:** dialog box for calibrating the screen. The principle is to touch the screen at the places where stars appear.
- **Double touch accuracy (pixels) :** see the USB touch screens chapter above. [3.2.2.c](#) '

### 3.2.3 - The local desktop

When no session is connected the thin client displays a rest screen called "local desktop".

The configuration of the local desktop includes the theme (color, size of the characters ...), the taskbar and the key combinations for changing sessions.

The use of the local desktop is described in chapter [4.3](#).

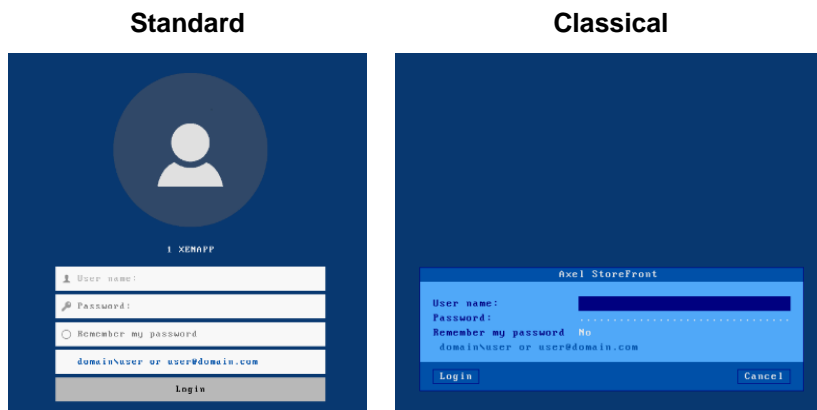
Select [Configuration] - [Terminal] - [Local desktop]:



#### a) Theme

The parameters of the theme are:

**Local login Appearance:**



- **Display Logo:** a logo can be displayed on the screen (at certain predefined positions). If no personal logo is loaded in the object store (see chapter [3.6.5](#)), the Axel logo is displayed.
- **Background color:** to choose from a list of numbers, each number corresponds to a predefined color.
- **Menu color:** four options are available.
- **Character size:** standard or double.

### b) Tasktask Bar

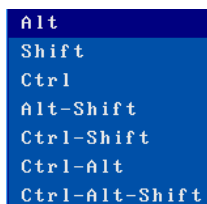
A taskbar at the bottom of the screen can be activated. It allows:

- easily identify the active session.
- view published sessions or applications.
- to change session by means of a mouse click.
- The taskbar settings are:
  - **Displayed for sessions:** this option allows you to display the taskbar when connecting to a session,
  - **Auto Hide:** when the taskbar is activated it is possible to set this mode:
    - **yes:** the taskbar is invisible and only appears when the mouse cursor is left for two seconds at the bottom of the screen.
    - **no:** the taskbar is always displayed.
  - **Appearance:** the “**standard**” style (by default) improves the management of published RemoteApp applications. While the “**classic**” appearance offers compatibility with previous versions of firmware.
  - **Pin sessions** (only for “standard” appearance): by default, the icon of a predefined session is only displayed when the session is connected. If this option is activated, the thin client displays the icons of the predefined sessions (connected or not).
  - **Display labels** (only for “standard” appearance): when this option is activated, the thin client displays the label (in addition to the icon) for each session or application.
  - **Pin the calculator** (only for the “standard” appearance): this option displays an icon for the local calculator in the task bar (see chapter [4.8.6](#)).
  - **Pin the speaker task** (only for the “standard” appearance): this option displays an icon in the bar which allows you to modify the basic volume of the speaker connected to the thin client without having to enter the setup.

### c) Session change keys

Sessions are accessible by key sequence. A session change sequence is composed as follows:

- **introducer:** this key (or this key combination) is chosen from a list:



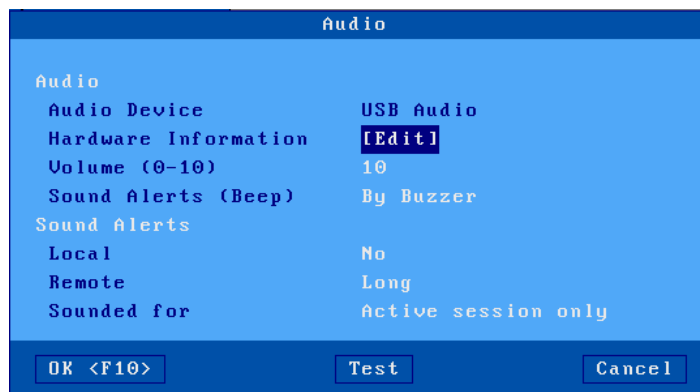
```
Alt
Shift
Ctrl
Alt-Shift
Ctrl-Shift
Ctrl-Alt
Ctrl-Alt-Shift
```

- **session key**: click [Edit] to display the list of configurable keys: desktop **key** (switch to the local desktop of the thin client) or **X session key**(switch to X session).  
By default, the session keys are as follows:



### 3.2.4 - Audio

Select [Configuration] - [Terminal] - [Audio]:



#### a) Audio device

Two types of audio devices can be used, headphones or speakers with 3.5 jack mm or USB audio devices.

The thin client offers a native audio interface with 2 “3.5 mm jack” sockets (HD-Audio). It is also possible to connect a USB audio device (USB Audio), in this case the added device has priority.

The dialog box displays the type of audio interface detected and the following parameters are available:

- **Hardware information**: various information on the device's capabilities.
- **Volume**: local volume adjustment (0 = mute), this is the basic volume which for the RDP and ICA protocols can be modified in the session by Microsoft volume management. It is also possible to modify this base volume outside of the setup, see chapter [3.2.3 b "Pinning the loudspeaker"](#)
- **Sound alerts**: selecting buzzer source: “buzzer” or “audio device”. In the latter case, the audio alerts benefit from the volume adjustment.

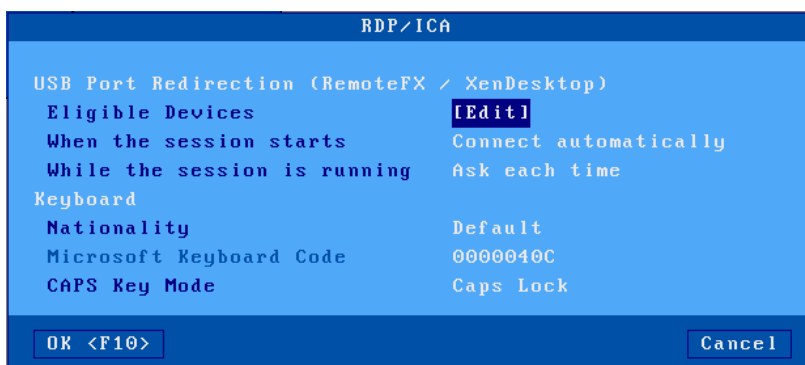
### b) Sound Alerts

An audio alert is a “beep” emitted by the thin client. Two types of audible alerts are available. For each type, the “beep” can be either deactivated or configured (length of the beep):

- **Local:** the thin client emits a beep following an incorrect action.
- **Remote:** the beep is requested by the server.
- **Allowed for:** this parameter allows you to specify whether a remote audible alert is issued for the “**active session only**” or for “**all sessions**”.

### 3.2.5 - Global RDP / ICA

Select [Configuration] - [Terminal] - [Global RDP / ICA]:



### a) RemoteFx or XenDesktop

Redirection from USB ports

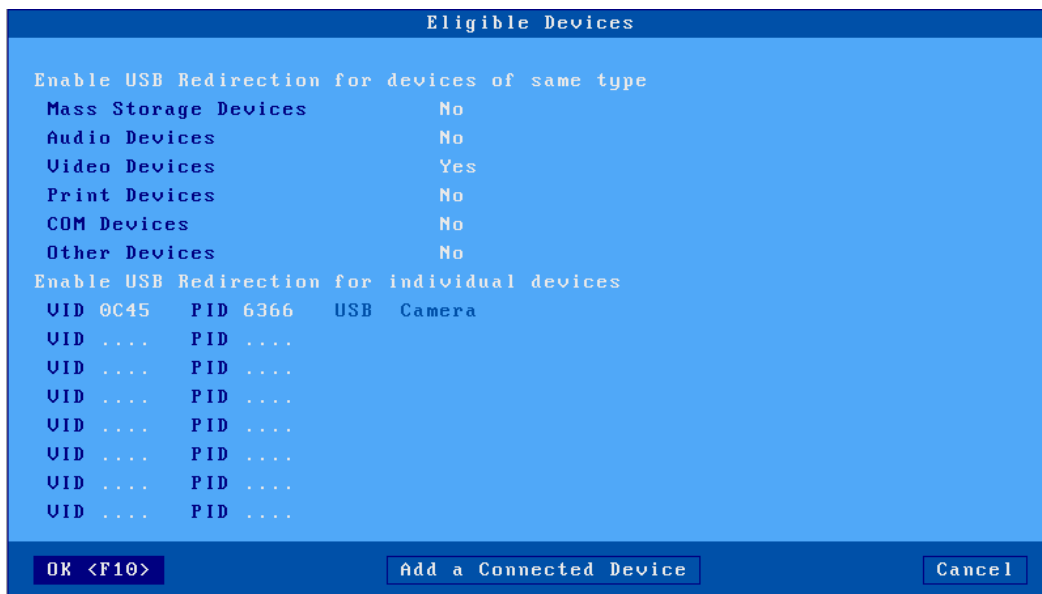
RemoteFx or XenDesktop redirection for USB ports (not to be confused with redirection from devices) allows the thin client to act as a gateway between the USB device and the server. The entire management of the USB device is entrusted to the server.

This only works when the thin client is connected in RDP to a server 2012 (or Windows 8) minimum or in ICA Citrix XenDesktop.

Access to the “” dialog box **Eligible** devices allows you to define which USB devices are eligible for this USB redirection. See next page.

The options “**At the opening of the session**” and “**During the life of the session**” are described in chapter [4.4.6](#).

**Note:** do not forget to also activate USB redirection at the RDP or ICA session level.

**Dialog box to define eligible USB devices:**

Eligibility can be defined by type:

- Mass Storage devices (USB key, hard drive, CD-ROM drive ...)
- Audio devices
- Video devices (webcam)
- Print Devices
- COM Devices
- Other peripherals (other than the above mentioned types, for example a scanner)

Or by **the identifier** USB product: ie the "**Vendor ID**" and the "**Product ID**". These two values can be entered manually or taken from a currently connected product by clicking on the [**Add a connected device**] button.

**Note:** if the value "PID" is left at 0, this means that all the products from the corresponding "VID" are eligible.

**b) Keyboard**

This function allows you to specify to the RDP / ICA server the type of keyboard connected to the thin client:

- **Nationality:** two possible values:
  - **By default:** the nationality of the keyboard is that enabled in the menu [**Configuration**] - [**Terminal**] - [**Keyboard**].
  - **Custom:** the nationality of the keyboard is that corresponding to the value of the 'Microsoft keyboard code' parameter.
- **Microsoft keyboard code:** enter a value (in hexadecimal) of Microsoft keyboard code. (Appendix A.7.4 lists the valid values.)
- **CAPS key mode:** two values: "shift" or "caps".

### 3.2.6 - Date and Time settings

Time management is used to:

- Display the date and time in the taskbar.
- Update the modification dates of files on a USB key
- Automatically restart the thin client at a specific time.
- Check the SSL certificates.

Select [Configuration] - [Terminal] - [Time settings]:



#### **a) Local clock**

The Axcel thin client does not have an internal clock, it does not have a battery. To manage the date and time, the thin client must synchronize with a time server (NTP protocol).

Enter the IP address (or DNS name) of the time server (unless it is obtained by the DHCP protocol - see chapter [3.1.2](#)).

The time and date can be displayed in the task bar of the thin client. The following parameters allow you to choose the display format:

- **Date format:** 'DD / MM / YY' or 'MM / DD / YY'
- **Time format:** 'HH: MM' or 'hh: MM'. (For this second format, the time is displayed modulo 12 with PM or AM afterwards.)

**b) Time zone**

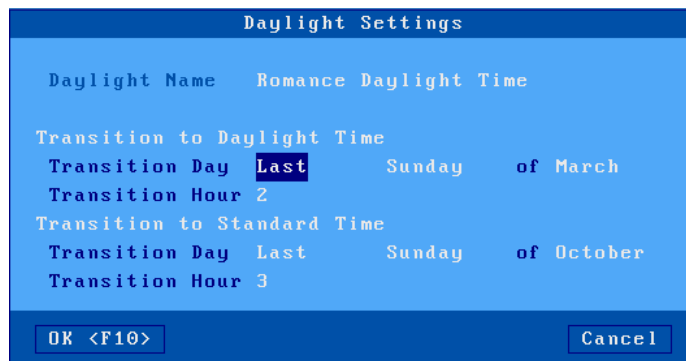
The time and date sent by the time server are in UTC format. To find the local time, the thin client must know:

- time zone (GMT offset)
- and if daylight saving time is managed in this time zone.

**Note:** this information is also used within the RDP / ICA connection. (This allows the Windows server to adjust the date and time of its taskbar). This "time redirection" function must be activated on the Windows server side.

The time zone settings are:

- **GMT time zone:** offset (positive or negative) from the Greenwich meridian.
- **Time zone name:** character string describing the time zone (default: "Romance Standard Time" where Paris is located). This character string must correspond to one of the zone names standardized by Microsoft (beware of upper / lower case). The list is given in appendix A.7.4
- **Daylight saving time adjustment:** allows you to specify whether daylight saving time is managed in the time zone where the thin client is located.
- **Daylight saving time setting:** the following dialog box is displayed (the name of the daylight saving time zone is displayed for information):



Enter the following parameters for each time change:

- **Transition day:** day number, day and month of the time change (for example: last Sunday in March for summer).
- **Transition time:** changeover time without minutes (for example enter 2 for 02:00).

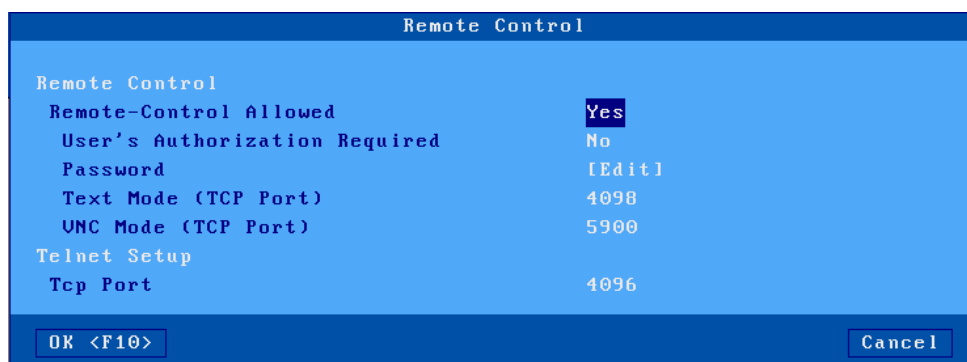
**c) Automatic shutdown and restart**

If an NTP server is declared, it is possible to configure an action: automatic shutdown or "restart" of the thin client (every day or a day of the week at a given time).



### 3.2.7 - Remote control of the thin client

Select the menu [Configuration] - [Terminal] - [Remote control]:



#### a) Remote control

Taking control Remote control allows you to take control of the thin client either for remote administration, either to interact with the user (remote assistance). For more information on remote control see chapter [10.2](#).

Description of parameters:

- **Remote-Control Allowed:** "yes" or "no"
- **User's Authorization Required:** when this option is set to "yes", remote control can only be done if the user of the thin client validates the request. This authorization can be "mandatory" or with "automatic approval" after 30 seconds after the posting of the request, or with "automatic refusal" after this same time.
- **Password:**(optional): the password is requested at the establishment of the session (8 characters maximum).
- **Text mode (tcp port):** connection port for taking control in text mode (setup, telnet, 5250, 3270 ...).  
By default, "4098", "0" prohibits access by this mode.
- **VNC mode (tcp port):** connection port for remote control (Graphics)  
By default, "5900", "0" to prohibit access by this mode.

#### b) Telnet setup

The "telnet setup" function authorizes a telnet client to connect to the thin client. Only the setup is accessible by this function.

The only parameter is the **TCP port:** default "4096", put "0" to prohibit access by this mode. For more information on telnet setup see chapter [10.3](#).

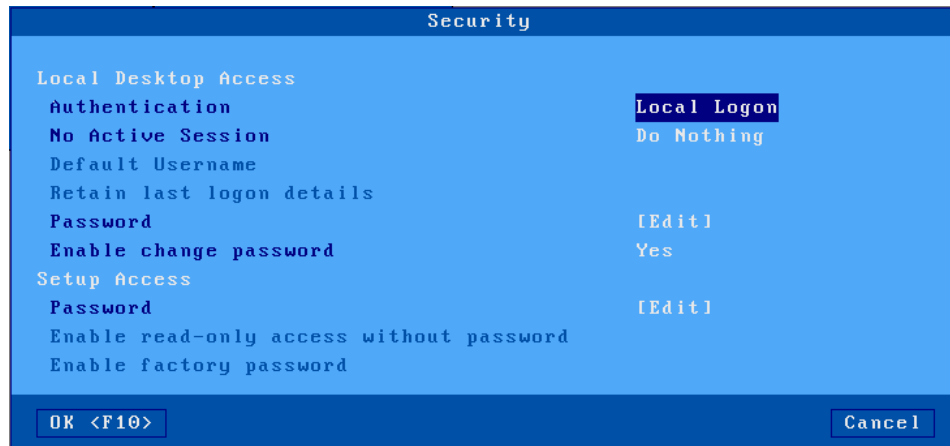
### 3.2.8 - Security

Select menu [Configuration] - [Terminal] - [Security]:

#### a) Access to the local desktop

Access to the **desktop** can be "free", controlled by a "Local logon" or an "Active Directory logon".

##### a.1 - Access by "Local Logon" authentication



Local authentication allows you to configure a local password which will be used to access the thin client. This password can be the one used to log in to your sessions or only for access to the thin client (in this case you will need to enter a new password when connecting the sessions).

At any time, the user can lock their thin client and return to the local logon by simultaneously pressing the [Ctrl][Alt][S] keys.

It is possible to couple this functionality with the screen saver (chapter [3.2.2.c](#)) to set an inactivity timeout which will lock the thin client.

The parameters:

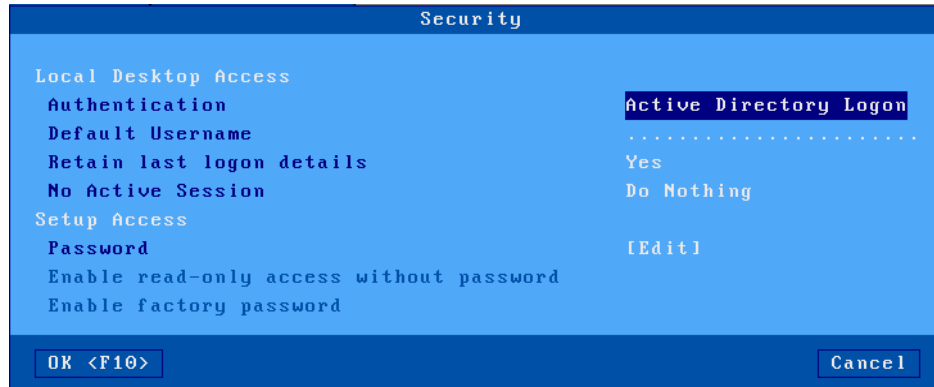
- **No active session:** allows you to configure the behavior of the thin client when no more sessions are connected but at least one session had been connected:
  - **Do nothing:** in this case we return to the local desktop.
  - **Back to logon:** The thin client displays the Active Directory logon again.
  - **Shutdown:** In this case the thin client automatically shuts down.
- **Password:** (maximum 8 characters), local logon password, it will be requested when starting the thin client.
- **Enable to change password:** (default: No), allows the end user to change their password when the thin client starts



If this parameter is set to YES, when displaying the local logon window, an icon at the bottom right of your main monitor allows access to the password change window.

To change the password, the user will first have to enter the current password.

a.2 - Access by "Active Directory" authentication



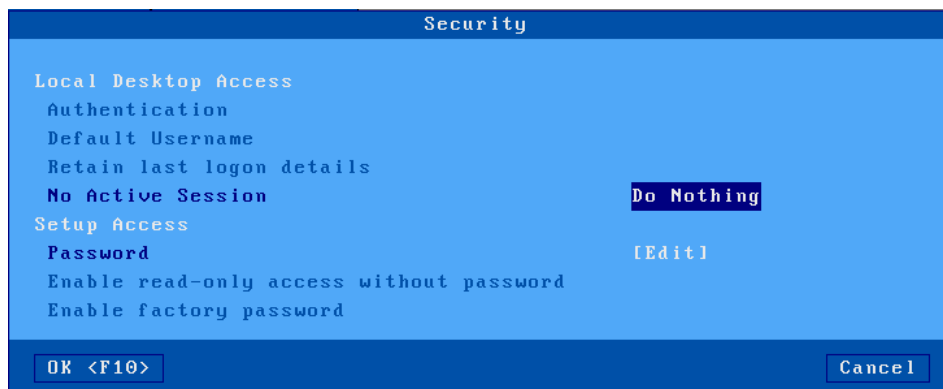
**Warning:** For Active Directory authentication, it is mandatory to configure the Active Directory environment beforehand (see chapter [3.1.7](#)). In this case the Authentication parameter becomes active and allows you to choose the "" option **Active Directory logon**.

The parameters:

- **Default user name:** it will be displayed during logon and can be changed by the user.
- **Remember last logon:** allows to keep in memory the last username entered as long as the thin client is not powered off (the password is never kept).
- **No active session:** allows you to configure the behavior of the thin client when no more sessions are connected but at least one session had been connected:
  - **Do nothing:** In this case we return to the local desktop.
  - **Back to Logon:** The thin client displays the Active Directory logon again.
  - **Shutdown:** In this case the thin client automatically shuts down.

**Note:** the parameters "Authentication" and "Username by default" cannot be modified (grayed out) if AD authentication is in progress'.

a.3 - Free access



The only parameter available in this case is the following:

**No active session:** allows you to configure the behavior of the thin client when no more session is connected but at least one session has already been connected.

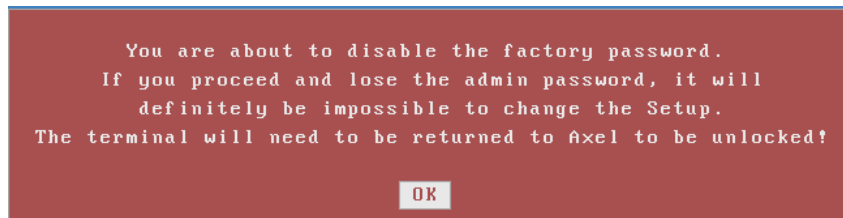
See details of the options in the previous chapter [3.2.8.a.1](#)

**b) Access to the setup with password**

Access to the setup can be controlled by a password. To enter or cancel the password, select **[Edit]**. The following dialog box appears:

The following information must be entered:

- **New password:** enter the password (15 characters maximum)
- **Please confirm:** re-enter the password.
- **Enable read-only access without password** (default "Yes"): when this option is set to "Yes" a "Consultation" button is available in the password input dialog box, it allows you to view all the parameters of the setup but no changes will be kept. If this option is "No", it will not be possible to view the parameters without entering the password.
- **Enable factory password** (default "Yes"):
  - **Yes:** if the password is forgotten, a "factory password" is used to enter the setup. This password is "yaka".
  - **Yes (Factory Settings):** In this case the factory password "yaka" when entered erases all the current parameters and restores the factory setting.
  - **No:** the super password "yaka" will be disabled to enter the setup, only the current password will allow it. In this case a warning box is displayed:



**Caution:** If you do not authorize the factory password, in case of loss of the entered password, you will be obliged to contact your reseller to obtain an "unlock code" which will allow you to regain access to the terminal setup but the current parameters will all be erased and will reset your thin client to factory settings. More information in appendix A.7.7

### 3.2.9 - Miscellaneous

Select the menu [Configuration] - [Terminal] - [Miscellaneous]:



#### a) Text emulation and local printing

The default port is the port used for “screenshots” or by escape sequence printing from text emulations.

Description of the parameters linked to the default port:

- **Default port:** choice a port from the list.
- **Start string for screen printing** (available only if the "default port" is not "none"): character string sent before screen printing.
- **End string prints screen** (available only if the "default port" is not "none"): character string sent after a screen print. For example, "\0C" codes a page break.

**Note:** if the "Choose Portrait / Landscape" parameter is activated (see Appendix A.7.2.d), the "Start prints screen" parameter is replaced by the parameters "Portrait start" and "Landscape start".

#### b) Number format

These two parameters allow the thin client to differentiate between text and number during a copy / paste function from a text session to an RDP / ICA session. (This is useful when the "paste" function is done from a spreadsheet).

The decimal separator can be a period or a comma

The thousand separators can be a period, a comma or a space.

### 3.2.10 - Foot pedal (HID)

The Axel thin client is capable of locally managing a foot pedal. The principle is to associate a keyboard action with each pedal switch

**Note:** this function is available with the firmware option **HID**. The keyboard emulation from the pedal works for RDP, ICA and 5250 sessions.

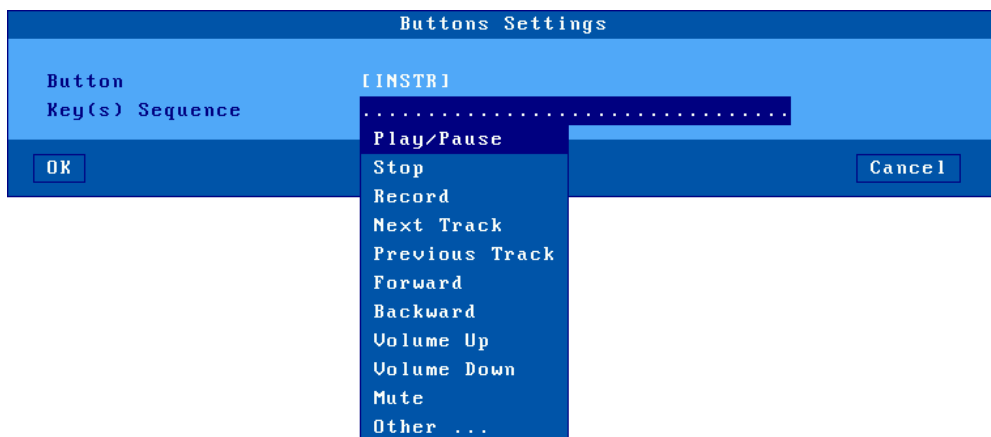
Select the menu [Configuration] - [Terminal] - [Foot Pedal]:



A maximum of 4 buttons can be programmed. Select the button to program. The following is displayed:



The next step allows you to choose an action or by selecting <Other ...> any combination of keys can be associated:



### 3.2.11 – Dictaphone (SMK)

The Axel thin client is able to locally manage the buttons of a dictaphone (Philips SpeechMike and Olympus). The principle is to associate a keyboard action with each button.

**Note:** this function is available with the firmware option **SMK**. Keyboard emulation from the dictaphone works for RDP, ICA and 5250 sessions.

Select the menu **[Configuration] - [Terminal] - [Dictaphone]**

Then the principle is the same as for the foot pedal. See the previous chapter [3.2.10](#).

## 3.3 - SESSIONS

The multi-connection functionality allows up to 6 simultaneous connections to **one or more** servers on the network.

These sessions can be used:

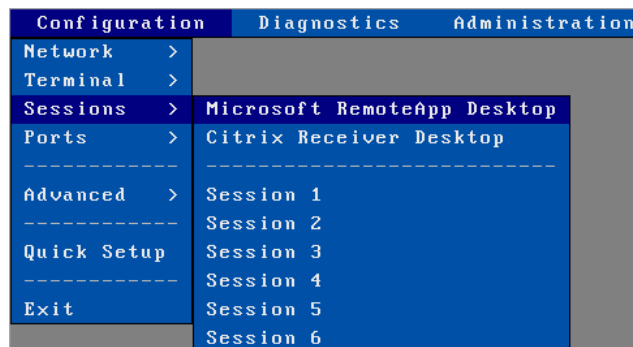
- Either through the RemoteApp or Citrix Receiver desktop
- Either individually by associating a server and a protocol (predefined session) with a session.

### 3.3.1 - Applications desktop (RemoteApp or Citrix Receiver)

The principle is that a user, after local authentication, finds on the desktop of the thin client the icons of the resources published for his user account.

The launch of a published application is done simply by clicking on the corresponding icon. Depending on the operating mode chosen, a dedicated RDP or ICA session is automatically opened for the management of this application.

To configure the application desktop, select the menu **[Configuration] - [Sessions]** and choose either the **[Microsoft RemoteApp desktop]** or the **[Citrix Receiver desktop]**:



Notes:

- To operate, the application desktop must reserve sessions to run the published applications.
- The number of reserved sessions is configurable
- These sessions are reserved from the last session. For example, if three sessions are reserved it will be sessions 4, 5 and 6.

To illustrate this principle here are two examples showing the occupation of the 6 sessions of the thin client.

Example 1: thin client totally dedicated to the "application Desktop"

Reserved	Reserved	Reserved	Reserved	Reserved	Reserved
----------	----------	----------	----------	----------	----------

Example 2: sessions reserved for "application office", VNC and ANSI

VNC	ANSI	Reserved	Reserved	Reserved	Reserved
-----	------	----------	----------	----------	----------

For more information on configuration from the application desktop see chapter [5.3](#).

### **3.3.2 - Predefined**

Select **[Configuration] - [Sessions] - [Session X]** (where **X** session is the session number). A menu is displayed allowing you to select the type of session:

Configuration	Diagnostics	Administration
Network >		
Terminal >		
Sessions >	Microsoft RemoteApp Desktop	
Ports >	Citrix Receiver Desktop	
-----		
Advanced >	Session 1	Microsoft TSE/RDS
-----	Session 2	Citrix Receiver
Quick Setup	Session 3	VMware View Client
-----	Session 4	UNC
Exit	Session 5	5250
	Session 6	3270
		Text Emulation
		None

**Note:** if the session has already been associated with a type of session, the corresponding dialog box is displayed.

#### **a) Type of sessions**

- **Microsoft TSE / RDS:** session to Windows TSE (from NT4 TSE to 2022). For more information see chapter [5.1](#).
- **Citrix Receiver:** session to Metaframe, XenApp / XenDesktop or VDI-in-a-Box servers. For more information see chapter [5.2](#).
- **VMware View Client:** session to a VMware View infrastructure (also called Horizon). For more information see chapter [5.4](#).
- **VNC:** session to Unix / Linux. For more information see chapter [8.2](#).
- **5250:** text mode session to an AS / 400. For more information see chapter [6](#).
- **3270:** text mode session to an OS / 390. For more information on the configuration of this session see chapter [7](#).
- **Text emulation:** networked text mode session (protocols **telnet**, **ssh** or **tty**) or RS232 serial and via a "USB-COM" converter, generally used for connection to Unix / Linux. For more information see chapter [8.1](#).
- **None:** the session is no longer accessible by the user.

#### **b) Duplicate the configuration of a session**

It is possible to duplicate the configuration of a source session to a destination session.

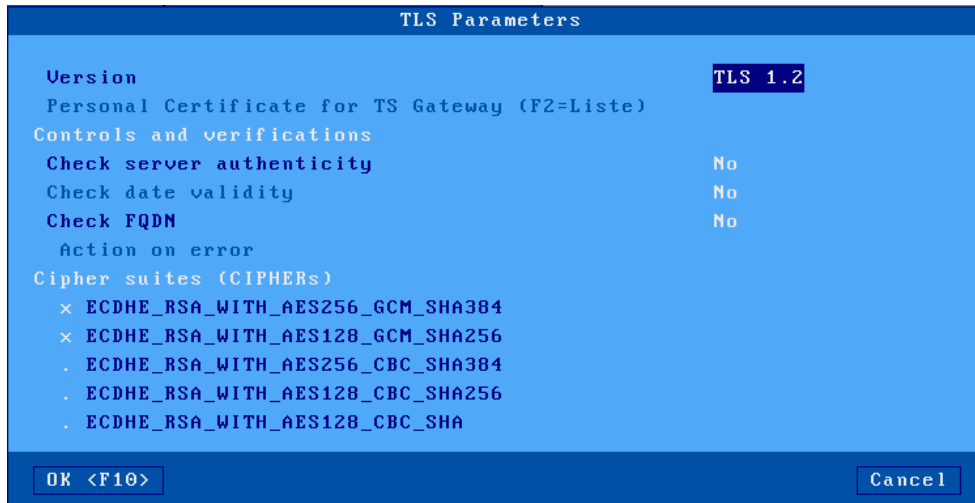


In the menu **[Configuration] - [Sessions]**, select the source session then press **<Ctrl> <C>**. Then select the destination session and press **<Ctrl> <V>**.

After confirmation, the configuration of the source session is applied to the destination session.

**3.3.3 - TLS security**

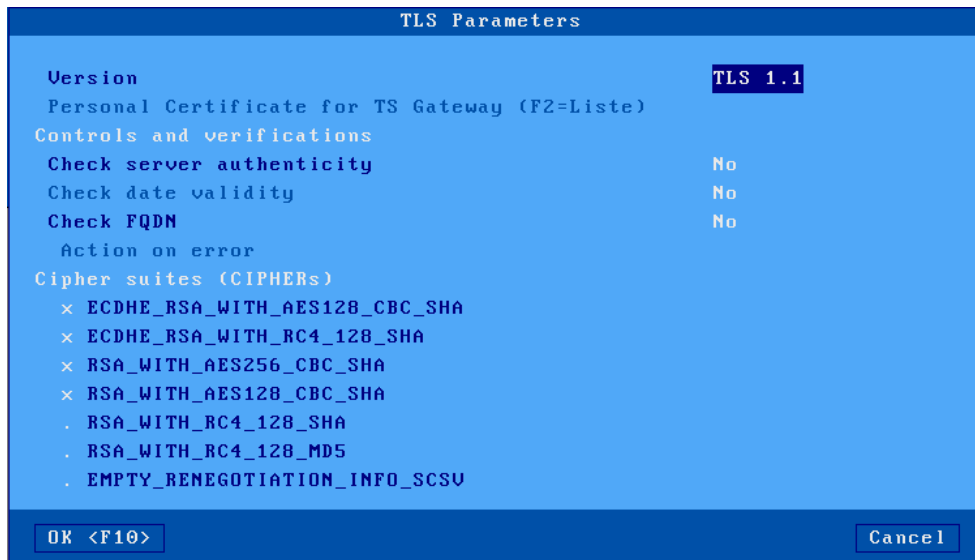
For graphical sessions (Microsoft TSE / RDS, Citrix Receiver, VMware View Client) as well as Microsoft RemoteApp and Citrix Receiver desktops, TLS security is set in the **[Configuration] - [Sessions] - [Session x or Desktop...] - [Connection property] - [TLS Parameters]**:



**a) Version of the TLS client**

The “**version**” parameter allows you to choose the minimum version of the TLS to negotiate with the server: TLS 1.1 or TLS1.2. Depending on the version chosen, the cipher suites differ and the most secure are checked by default.

Example for TLS 1.1:



**b) Personal certificate (optional)**

During the secure connection in TLS, it is possible to send to the server a Personal certificate which will allow the server to authenticate the thin client with certainty. This certificate must first be installed in the thin client's object store (see chapter [3.6.5](#)).

A drop-down list allows you to choose the certificate that will be used for this connection.

**c) Control and verifications**

During a TLS connection, for security reasons, it is preferable to check the server certificate. Certain verifications are only possible if you have a "CA" certificate corresponding installed in the thin client's object store (see chapter [3.6.5](#)).

The first option "**Check server authenticity**" determines whether during a TLS connection (HTTPS, NLA ...) the server certificate is verified. It consists in checking the consistency between the certificate sent by TLS server and the local "CA" certificate.

**Note:** It is possible to install several "CA" certificates in the object store, however it is not necessary to define one at this level, the thin client will choose the one that corresponds to the remote server automatically.

Thereafter, two other verifications can be selected:

- **Check the validity dates:**(active if an NTP server has been declared, see chapter [3.2.6](#)): the verification consists in testing whether today's date is included between the dates "Valid after" and "Valid before" of certificate received from the server.
- **Check the domain name:** Checks that the FQDN name of the TLS server corresponds to the "Common Name" of the installed "CA" certificate.

**In case of error:** allows to set the behavior of the thin client if the server certificate is not valid. For more information see chapter [4.4.3](#).

**d) Authentication and encryption capabilities**

The list of TLS "ciphers" supported by the client is displayed. Check the one or those that will be announced during a TLS connection. By default, they are all checked.

**Note:** If your server is old, you may need to check the ones that are not by default.

## 3.4 - USB MANAGEMENT

### 3.4.1 - Specifications

Technical specifications:

- USB1 and USB2 compatible
- Supported speeds: low-speed (1.5 Mbits), full-speed (12 Mbits) and high-speed (480 Mbits)
- Maximum consumption:
  - **0.5 A** accumulated on the 4 ports on the front panel.
  - **0.5 A** accumulated on the 2 ports on the rear panel.

**Note:** for reasons of power consumption, "non-computer" peripherals (fans, lamps, etc.) are prohibited.

The Axel USB stack supports the following peripherals:

- keyboard (Plug & Play),
- barcode reader (Plug & Play),
- mouse (Plug & Play),
- HUB (Plug & Play),
- touch screen (possibly multi-touch) (Plug & Play),
- printer,
- "USB-COM" or "USB-PARALLEL" adapter,
- storage device (USB key and hard disk formatted in FAT, FAT16 or FAT32, CD / DVD drive type ISO9660),
- smart card reader and tokens,
- audio device,
- Other devices are detected but not managed locally (but they can be supported through the redirection of RemoteFX or XenDesktop USB ports).

**Note:** "USB-COM" also known as "USB-RS232" or "USB-Serial"

Maximum number of peripherals:

- six keyboards or barcode readers,
- three mice,
- two Hubs,
- four "USB-COM" or "USB-PARALLEL" printers or adapters,
- one touch screen,
- one storage device,
- two smart card readers,
- one audio device.

USB devices can be hot-plugged. They are detected dynamically by the Axel thin client. For security reasons, **by default, no device is active without the administrator having authorized it in the setup** except those announced as (Plug & Play) in the list above.

### 3.4.2 - Connecting a USB keyboard

A USB keyboard is automatically recognized by the Axel thin client.

This keyboard uses the general configuration of the thin client at the nationality level, initialization of the LEDs ... For more information, see chapter [3.2.1](#).

**Note:** several keyboards (USB) can be connected. They all share the same configuration (nationality, initialization of the LEDs ...) and can be used simultaneously.

### **3.4.3 - Connection of a USB barcode reader**

A barcode reader is automatically recognized by the Axel thin client. It is managed by the thin client as a local keyboard. For more information, see the previous chapter.

**Note:** In the case of a USB-COM barcode reader, please refer to chapter [3.4.7](#)

### **3.4.4 - Connection of a USB mouse**

A USB mouse is automatically recognized by the Axel thin client. No specific configuration is necessary.

**Note:** several mice (USB) can be used simultaneously.

### **3.4.5 - Connecting a HUB**

A HUB is automatically recognized by the Axel thin client.

No specific configuration is necessary.

### **3.4.6 - Connecting a printer**

A printer is automatically recognized by the Axel thin client, a USB logical port is automatically associated with it, see chapter [3.4.12](#).

You must then configure this printer according to the use required, for this please refer to chapter [3.5.2](#) "Configuration of a printer"

### **3.4.7 - Connection of a USB-COM adapter**

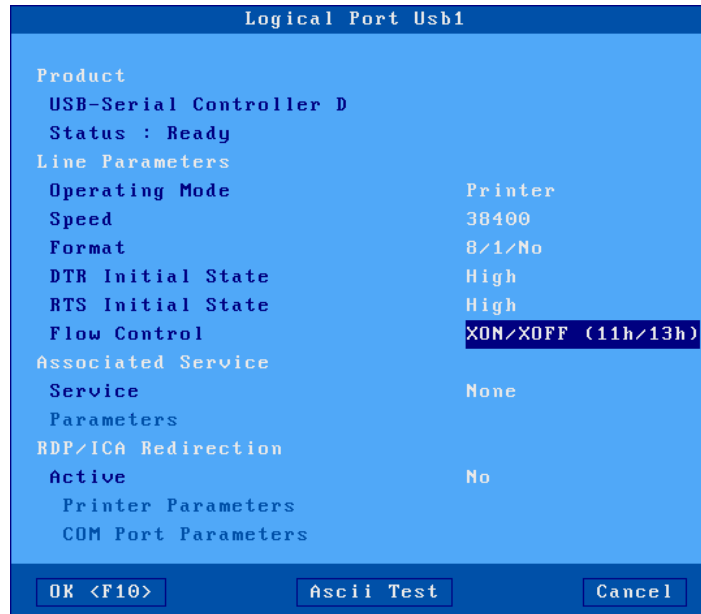
#### ***a) Presentation***

A "USB-COM" adapter sometimes also called "USB-RS232" is generally in the form of a USB cable with one or more DB9 (or DB25) connectors, this allows you to use a serial device when there are no native serial connectors.

However, some USB devices also use this technology, such as barcode readers, touch screens or smart card readers. Despite their USB connection, a virtual serial port must be assigned to them.

### b) Configuration

A USB logical port is assigned to a USB-COM adapter (see attachment and release principles in chapter [3.4.12](#)). For example:



This logical port will allow configuration in terms of line parameters (speed, format ...), network service and RDP / ICA redirection.

Description of the parameters:

- **Operating mode:** the available modes are:
  - **Printer:** communication takes place only from the thin client to the peripheral. Data arriving from the device is ignored (except for flow control characters).
  - **Bidirectional device:** communication in both directions.
  - **ASCII to EBCDIC :** Dedicated to 5250 emulations, this mode allows you to transmit ASCII data received on the serial port by default in the keyboard buffer by transforming them into EBCDIC. This corresponds to the simulation of a keystroke. For this mode, you must set the **"service"** to "none" and configure the logical port as the default port for the thin client (see chapter [3.2.9](#)).
  - **In the sequence.** (only available if the "modeASCII to EBCDIC" ): ASCII character string which can be sent to the device by pressing a programmable key sequence (see chapter [6.1.3.b](#)) "Send Seq. To the.", By Default **[AltGr] - [F2]** ".  
*Example of use: asking the weight of an object on a scale.*
- **Speed:** The value is chosen from a list (from **300** to **115200** baud).
- **Format:** the number of bits, stop bit and parity are to be chosen from a list: 7 or 8 bits, 1 or 2 stop bit and parity (none, even or odd).
- **DTR initial state:** select the state of the signal **DTR** at boot of the thin client "high" or "low".
- **RTS initial state:** select the state of the signal **RTS** at boot of the thin client "high" or "low".
- **Flow control:** flow control used by the device to regulate the flow in the **thin client -> device direction**.
- **Flow control:** (available only for bidirectional operation): flow control used by the thin client to regulate the flow in the direction **peripheral-> thin client**.

- **Associated service** (lpd, tty, prt5250 ...): see chapters [3.5.2](#) and following.
- **RDP / ICA redirection**: see chapter redirection [5.1.6.c](#) for RDP and [5.2.8.c](#) for ICA.

For more general information on USB logical ports, see chapter [3.5.1](#).

### **3.4.8 - Connection of a USB touch screen**

The USB touch screen should be

- a "multi-touch" class. (Management of "multi-touch" only within an RDP session connected to RDS 2012 or Windows 8 minimum).
- a "pointing device" (mouse) class
- a "USB-COM" adapter. In this case, a USB logical port is automatically created (see chapter [3.4.7](#))

In all cases, the configuration of the touch screen is carried out via the menu [Configuration] - [Terminal] - [Screen]. See chapter [3.2.2](#).

### **3.4.9 - Connecting a storage device**

The main types of USB storage devices are:

- USB keys, (memory sticks)
- hard disks,
- CD / DVD drives,
- floppy drives,
- digital cameras if they are detected as a USB class,
- memory card readers (digital camera for example).

**IMPORTANT:** the Axel thin client only supports storage devices formatted in FAT12, FAT16, FAT32 and ISO9660. Other storage devices can be redirected by "RemoteFX USB" or "XenDesktop", see chapter [3.2.5.a](#).

For information, the following table gives for each type of device, the file system generally encountered (X: supported by a PC or Axel, o: supported only by a PC):

Device type	FAT16 or 32	NTFS	ex FAT	ISO 9660	UDF	PIMA	Other
USB key	X	o	o				
Hard drive	X	o	o				
CD / DVD drive				X	o		
Floppy drive	X						
Digital camera	X					o	o
Memory card reader	X						

Unlike a USB printer, it is not necessary to configure each connected storage device. However, the use of a storage device must be configured on two levels:

- **General:** see chapter [3.2.5.a](#) if it is a "USB RemoteFX" or "XenDesktop" redirection.
- **Session:** see chapters [5.1.6](#) for RDP or [5.2.8](#) for ICA

**Note:** activating the task bar (see chapter [3.2.3.b](#)) allows you to view the use of the storage device by means of a colored icon. **It is formally not recommended to disconnect a storage device when it is in use, especially during the writing phase.**

### 3.4.10 - Connection of a USB smart card reader

This function requires smart card readers to be **PC / SC compatible**. The Axel thin client manages **CCID readers**.

Two exceptions made for the **Aladdin** "eToken" reader and the **Renault** "key card" reader which are not CCID but which are managed by the Axel thin client.

**Note:** "card readers **USB-COM**" (for example Sesam Vitale readers) can also be managed by the thin client. This is done through COM RDP / ICA port forwarding or through the "tty" protocol on Unix / Linux. see chapter [3.4.7](#).

For **PC/SC - CCID readers**, the thin client maintains a reader store. This store is accessible via the **[Configuration] - [Advanced] - [Smart card readers]** menu:



A reader is automatically added to the store the first time it is connected to the thin client. The store can hold four readers. To consult or modify the characteristics of a reader, select the corresponding entry:

The parameters associated with a reader are as follows:



- **Reader ID:** non-modifiable parameter composed of "Manufacturer ID" and "Product ID".
- **Vendor Name:** character string returned by the thin client when an application invokes a "SCardGetAttrib (SCARD\_ATTR\_VENDOR\_NAME)" command.
- **IFD Type:** string returned by the thin client when an application invokes a "SCardGetAttrib (SCARD\_ATTR\_VENDOR\_NAME\_IDF\_TYPE)" command.
- **Smartcard Reader Registration:** generally, a reader must be connected to the thin client to be listed by an application ("SCardListReaders" function). Some readers need to be listed even if they are not connected (for example a "token" - reader and smart card integrated in

a kind of USB key). This parameter defines the behavior (Dynamic or Persistent) of the thin client for this reader.

The button **[Delete]** allows you to remove an entry from the store.

Finally, the use of smart card readers must be configured at the level of each RDP / ICA session or desktop. See chapters [5.1.6](#) for RDP and [5.2.8](#) for ICA.

### **3.4.11 - Audio Devices**

A USB audio device is automatically recognized by the Axel thin client.

The use of audio must be configured at each RDP / ICA session. See chapters [5.1.6](#) for RDP and [5.2.8](#) for ICA.

### **3.4.12 - The USB logical USB logical ports**

The ports are used to manage the following devices:

Configuration	Diagnostics	Administration
Network >		
Terminal >		
Sessions >		
Ports >	USB Logical Ports >	Usb1 - COM
-----	Network Printer >	Usb2 - Printer
Advanced >		

- USB printer
- "USB-PARALLEL" adapter
- "USB-COM" adapter



### **a) Attachment of a logical port**

When one of these peripherals is connected for the first time to the thin client, a logical port is automatically assigned to it. Four logical ports are available: Usb1, Usb2, Usb3 and Usb4.

The logical ports already assigned are listed in the menu **[Configuration] - [Ports] - [USB logical ports]**. To obtain information on a device, select its logical port and validate. For example:



The attachment of a logical port to a device is persistent. This means that a device retains its logical port in the following cases:

- if device is turned off or disconnected.
- if the device is disconnected then reconnected even on another USB port.

The release of a logical port must be carried out manually (see subsection 3.4.12. freeing a logical port).

### **b) Configuration of the logical port**

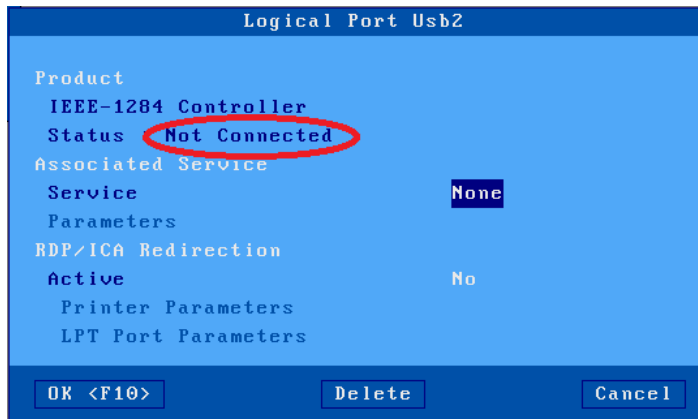
A peripheral connected on a logical port must be configured to be able to function, by default all devices are inactive except those which are "Plug & Play", see the list in chapter [3.4.1](#).

See chapter [3.5.2](#) and following.

### c) Freeing a logical port

If a logical port is no longer used, it must be freed to allow another device to use this port. The release of a USB logical port must be done manually. This operation can only be performed if the USB device is no longer connected.

In the menu **[Configuration] - [Ports] - [USB logical ports]**, select the logical port to be released and confirm. A dialog box of this type is displayed:



In the case where the status of the device is “**not connected**”, the **[Delete]** button allows the logical port to be released.

A freed logical port disappears from the list of ports and becomes available for a future USB device.

#### **3.4.13 - List of connected USB devices**

To view the list of connected devices (supported or not) select the menu **[Diagnostics] - [USB]**. For more information see chapter [9.6](#).

## **3.5 - SETTING AUXILIARY AND LOGICAL PORTS**

The thin client offers two types of ports for the connection of peripherals:

- **Auxiliary ports:** one parallel port, two native serial ports (Aux1 and Aux2).
- **logical USB:** ports: a USB logical port is automatically created when a USB printer or USB-COM adapter is connected to the thin client. A maximum of four logical ports are available (see chapters [3.4.12](#))
- **NET Network:Printer:** a logical port (TCP of Net1 to Net4) manages a network printer (or printer server) in the same way a printer connected to an auxiliary port.

Each of the logical ports of the thin client can be used:

- **by a network service:** (lpd, tty, prt5250 ...): simultaneous management of one or more ports by an independent socket without altering the performance of the current screen session.
- **through an RDP or ICA session:** (see chapters [5.1.6](#) for RDP and [5.2.8](#) for ICA).
- **in transparent mode:** specific to printers, compatibility with software using a printer via escape sequences (as on serial terminals). See the following chapters, for the 5250 emulation chapters [6.1.3.a](#) and [6.3.1.b](#) and for a Telnet or a Serial Session [8.3.4](#).

### 3.5.1 - Port configuration

This chapter gives details for the configuration of each type of port.

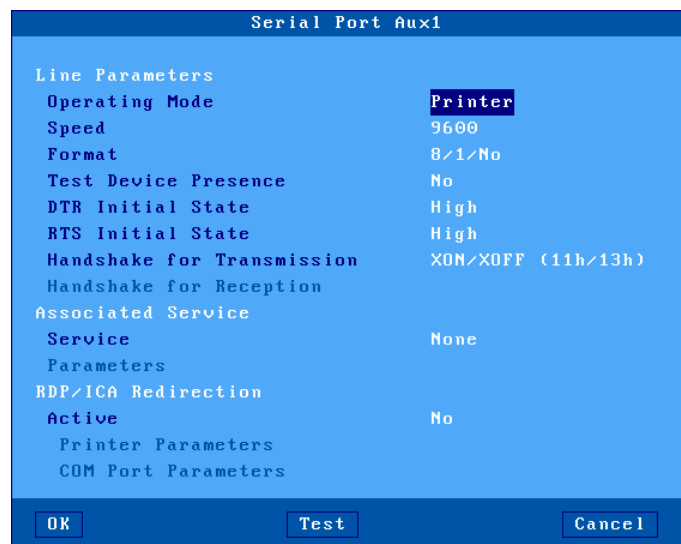
For the selection and configuration of an associated network service, see chapter [3.5.2](#)

**Button [Test]:** for the four dialog boxes described below, this button (present if the device is in "ready" state) is used to test the communication between the thin client and the device. An "ASCII" banner is sent to the port.

**Note:** if the device does not support ASCII format, the banner will not be displayed or printed.

#### a) Setting Serial Ports (G15)

Select the **[Configuration]-[Ports]-[Auxiliary Ports]-[AuxX]** dialog box to configure each auxiliary serial port:



These parameters are:

- **Operating Mode:** three modes are available:
  - **Printer:** data flow takes place one way only (from the AX3000 to the serial peripheral device). However, handshaking between the peripheral and the AX3000 is performed.
  - **Bi-directional Device:** Used to control peripherals such as bar code readers, touch screens, scales etc
  - **ASCII to EBCDIC:** this mode allows ASCII data received by the auxiliary port to be converted to EBCDIC (AS/400) format and be placed in the keyboard buffer. This is useful for connecting PC based peripherals (scanners, scales, etc) to an AS/400 application.  
**Note:** the 'associated service' must be set to 'none' and this port must be set as the AX3000 default auxiliary port (select the [Configuration]-[Terminal]-[Miscellaneous] menu).
- **Aux. Command** (only for "ASCII to EBCDIC" mode): an ASCII character string may be sent to the serial device. This is done by pressing the "Send Aux. Command" keystroke. (AltGr-F2 by default)  
 Example: requesting weight data from scales.
- **Speed:** selected from a list (from 300 to 115,200 bits per second).

- **Format:** data format is selected from a list: data length (7 or 8 bits), stop bit and parity (none, odd or even).
- **Test Device Presence:** the CTS signal can be used by the AX3000 to detect the peripheral's presence.
- **DTR Initial State:** select 'high' or 'low'.
- **RTS Initial State:** select 'high' or 'low'.
- **Handshake for Transmission:** handshake used by the peripheral to control the AX3000's data flow.
- **Handshake for Reception** (available only in bi-directional mode): handshake used by the AX3000 to control the peripheral's data flow.
- **Associated Service** (ldp, prt5250, tty...): see Chapter [3.5.2](#) and following.
- **RDP/ICA Redirection:** see Chapter [5](#).

**b) USB logical ports**

Select the [Configuration] - [Ports] - [USB logical ports] - [UsbX] menu.

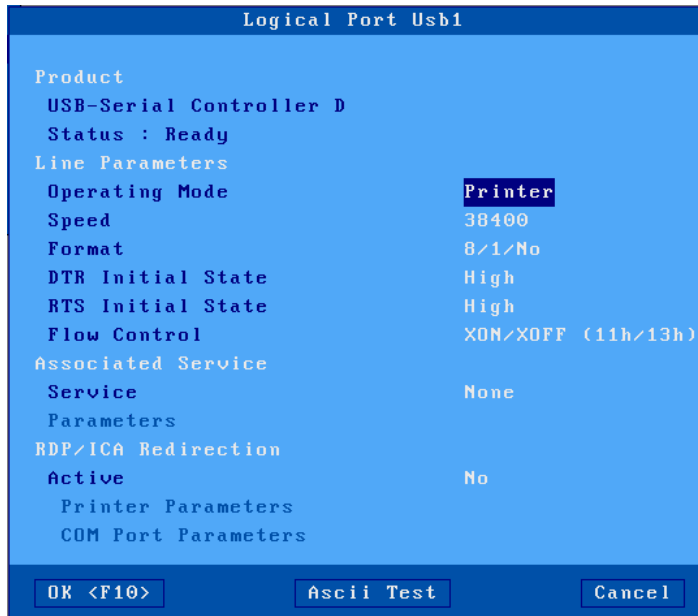
A USB logical port can be associated with a printer or a "USB-COM" adapter or a "USB-PARALLEL" adapter.

Example of a dialog box for a USB printer port or one for a "USB-PARALLEL" adapter:



**Note:** the "Test" button is visible because the device status is "Ready"

Example of a dialog box for a serial USB port:



Explanation of the parameters:

- **Setting the line:**(for "USB-COM" only) see section [3.4.7.b](#).
- **Associated service:**(lpd, tty, prt5250 ...): see chapter [3.5.2](#) and below.
- **RDP / ICA redirection:** see chapter [5](#).

### c) Network printers

Select [Configuration] - [Ports] - [Network printer] - [Netx]:

Description of the parameters:

- **Connection type:** always "raw"
- **Network Printer:** name of the network printer server defined in the server table (see chapter 3.1.4). A new server (DNS) or a new IP address can be entered directly; they will be added automatically to the local server list.
- **TCP port:** the default value is 9100.
- **Inactivity time-out (sec):** Idle time (in seconds) after which the connection between the Axel thin client and the network printer will automatically disconnect.
- **Associated service:**(lpd, tty, prt5250 ...): see chapters [3.5.2](#) and below.
- **RDP / ICA Redirection:** see chapter redirection [5.1.6.a](#) for RDP and [5.2.8.a](#) for ICA.

### 3.5.2 - Configuration of an LPD printer

This chapter describes how to configure a printer managed by the LPD protocol. (other protocols are available):

- **RDP / ICA:** Windows-specific management (see chapter redirection [5.1.6.a](#) for RDP and [5.2.8.a](#) for ICA).
- **Prt5250:** specific management for AS / 400 (see chapter [6.3.1](#)),
- **Prt3270:** specific management for OS / 390 (see chapter [7.3](#)),
- **tty:** specific management for Unix / Linux (see chapter [8.3.1](#)),

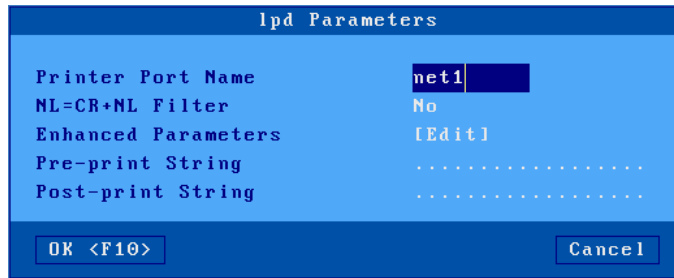
The LPD server embedded on the thin client allows the management of a printer as a system printer across the network.

An LPD printer is characterized by three parameters:

- an IP address (same as that of the thin client),
- a name that identifies the port on which the printer is connected,
- an optional filter which achieves a minimum formatting of the file to be printed (conversion "0Ah" into "0dh" + "0Ah").

To configure the LPD service, select the port (menu **[Configuration] - [Ports] - [xxx]**) enter the following parameters:

- **Service:** select the "service from the list **lpd**".
- **Parameters:** the following dialog box is displayed:



- **Printer port name:** this name identifies the auxiliary port and can represent the name of the remote printer at the operating system level.
- **NL = CR + NL filter:** possible conversion of "0Ah" into "0dh" + "0Ah".
- **Enhanced parameters:** see appendix [A.7.3](#)
- **Pre-print String:** character string sent before printing.
- **Post print String:** character string sent after a print. For example, "\0C" codes a page break.

**Note:** if the "parameter **Choose Portrait / Landscape**" is activated (see Appendix A.7.2), the " parameter **Print start String** is replaced by the "parameters **Portrait start string** " and "**Landscape start String**."

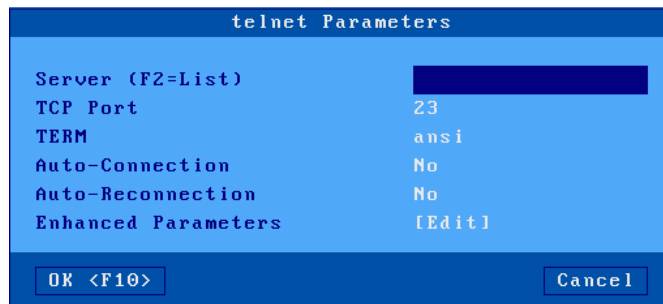
For more information on adding an LPD printer to an operating system, see the chapter relating to the specific operating system.

### 3.5.3 - Configuration of a serial terminal

It is possible to connect a serial terminal to a "USB-COM" adapter. This serial terminal connects to the server via the telnet service. The USB logical port must be configured in the "bidirectional device" operating mode.

To configure the telnet service on the chosen "USB-COM" port, select **[Configuration] - [Ports] - [USB logical ports] - [USBx]** and enter the following parameters:

- **Service:** select the **telnet**.
- **Parameters:** the following dialog box is displayed:



- **Server:** name of the server chosen from the list of servers (see chapter [3.1.4](#)). A new server (DNS) or a new IP address can be entered directly and will be added automatically to the local server list.
- **TCP port:** the default value is **23**.
- **TERM:** value of the TERM variable is negotiated on connection.

- **auto:** if "yes", the Axel thin client automatically opens the session when powered on. Alternatively, the connection can be requested by the user by pressing a key on the keyboard (ie Alt F1)
- **Automatic reconnection:** if "yes", the Axel thin client automatically re-opens a new session opening after a disconnection. Alternatively, the reconnection can be requested by the user by pressing a key on the keyboard.
- **Advanced parameters:** see appendix A.7.3.

### **3.5.4 - Configuration of other devices (tty)**

The "tty" service, available under Unix / Linux, allows bidirectional management of a device.

**Note:** only serial ports are bidirectional. For parallel ports the tty service acts as a unidirectional service.

To configure the "tty" service, select **[Configuration] - [Ports] - [xxx] - [yyy]** and enter the following parameters:

- **Service:** select the "service from the list **tty**".
- **Parameters:** the following dialog box is displayed:

tty Parameters	
Server (F2=List)	[Dark Blue Box]
TCP Port	2048
Auto-Reconnection	No
Enhanced Parameters	[Edit]
<input type="button" value="OK &lt;F10&gt;"/> <input type="button" value="Cancel"/>	

- **Server:** name of the server chosen from the list of servers (see chapter [3.1.4](#)). A new server (DNS) or a new IP address can be entered directly; they will be added automatically to the local server list.
- **TCP port:** the default value is **2048**.
- **Automatic reconnection:** if "yes", the thin client automatically opens the "tty" session after a disconnection. Alternatively, the thin client must be rebooted to open a new connection.
- **Advanced parameters:** see appendix [A.7.3](#).

**Note:** Axel provides software **for Unix / Linux** which allows a pseudo-terminal to be associated with a port managed by the "tty" service. This allows the thin client port to be managed as a local port on the system. For more information, see chapter [8.4](#).

### **3.5.5 - Using a "USB-COM" adapter as the main port for a session**

A screen session can be associated with a USB logical port. This allows an RS232 connection (like a serial terminal) for this session.

As many serial sessions as available multiple "USB-COM" ports can be configured. Serial and TCP / IP sessions can be used simultaneously.

For more information, see chapter [8.1.2.d](#).



**3.5.6 - Other uses (rtty or rsh)**

**a) Use of rtty**

With the "rtty" service, the thin client acts as a server, it is the opposite of the "tty" service described above. It "listens" on a given TCP port. It is therefore possible to establish a connection on this port to transmit (or receive) data.

**Note:** the "rtty" service can also be used with the Axel "axttyd" software in Unix (see chapter [8.4](#)).

To configure the "rtty" service, on the auxiliary port chosen, select **[Configuration] - [Ports] - [xxx] - [yyy]** and enter the following parameters:

- **Service:** select the "rtty" service from the list.
- **Parameters:** the following dialog box is displayed:



- **TCP** port: listening port of the thin client.
- **NL filter = CR + NL:** possible conversion from 0Ah to 0dh 0Ah.
- **New connection always accepted:** defines the behavior of the thin client when an "rtty" connection is already established and a new connection is requested (by the same server or another).
- **Advanced parameters:** see appendix A.7.3
- **Print start** string: character string sent during the "rtty" connection.
- **Print end** string: character string sent during "rtty" disconnection. For example "\ 0C" codes a page break.

**Note:** If the parameter "**SelectPortrait /Landscape**" is on (see Appendix A.7.2), the parameter "**startprinting chain**" is replaced by the parameters "**startPortrait String**" and "**string beginning Landscape**".

**b) Printing with the rsh or rcmd command**

The server embedded on the thin client allows file printing via the rsh command (or rcmd depending on the operating system used).

To configure the rcmd service, on the auxiliary port chosen, select **[Configuration] - [Ports] - [xxx] - [yyy]** and set the service to rcmd. Then enter the value of the printer's name associated with the port.

For more information on the use of rsh according to the operating system used, see chapter [8.3.3](#).

### 3.6 - ADVANCED PARAMETERS AND FUNCTIONS

The menu **[Configuration] - [Advanced]** offers the following functions:

Configuration	Diagnostics	Administration
Network >		
Terminal >		
Sessions >		
Ports >		
-----		
Advanced >	Tuning >	
-----	Auto-Configuration	
Quick Setup	Remote Administration	
-----	Factory settings	
Exit	Local Store	
	Smartcard Readers	

#### 3.6.1 - Tuning

Advanced >	Tuning >	Network
-----	Auto-Configuration	Keyboard/Screen
Quick Setup	Remote Administration	Mass Storage Device
-----	Factory settings	Miscellaneous

This dialog box allows access to a set of parameters whose default values are generally not modified.

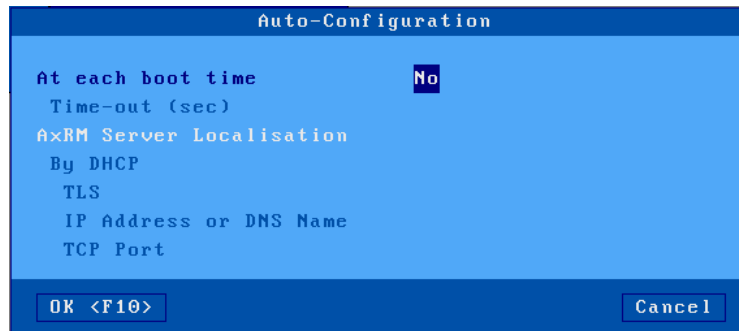
For more information see Annex [A.7.2](#).

#### 3.6.2 - Auto-Configuration at each power-up

-----	Advanced >	Tuning >
-----	-----	Auto-Configuration
Quick Setup	-----	Remote Administration
-----	-----	Factory settings
Exit	-----	Local Store
	-----	Smartcard Readers

The auto-configuration function allows the thin client to check whether a new "firmware" and / or a new configuration file is available on a server. This function is automatically started when the thin client is switched on for the first time or when the thin client is reset to "factory setting". See chapter [2.2](#).

Thereafter, this function can also be activated for each powering up of the thin client:



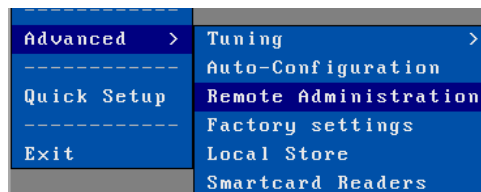
The 'time-out' parameter indicates for how many seconds the thin client tries to obtain a new configuration. If no firmware or configuration is received after this time, the thin client continues the normal boot phase and becomes available to the user.

Two methods are available to determine the location of the AxRM server (IP address and TCP port):

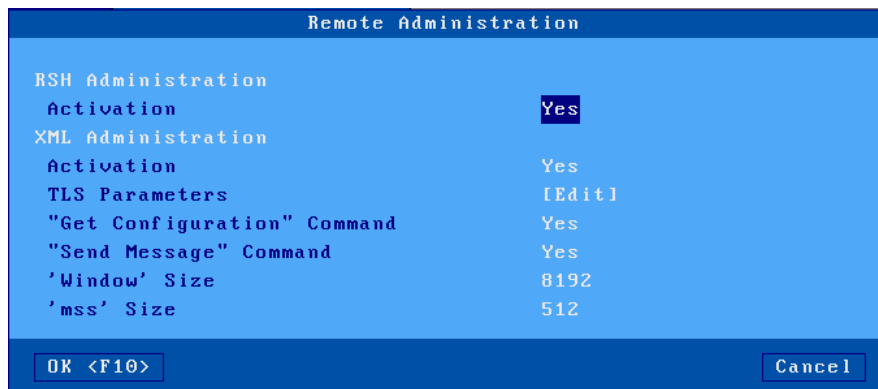
- **Static:** the IP address (or name) and the TCP port are indicated here
- **Dynamic:** (only if the thin client already uses the protocol DHCP to obtain its own IP address): the IP address and the TCP port are given by the DHCP protocol (see chapter [2.2.3](#) which details the criteria for this determination).

For the steps of auto-configuration, see chapter [2.2](#).

### 3.6.3 - Remote administration



This option allows you to customize the remote administration of the thin client:



The administration of the thin client can be done by RSH commands (available on Linux or Windows in command line) or by software administration under Windows (AxRM or Axel Remote

Management), which is available free of charge on the Axel website (<http://www.axel.fr/>). For more information see chapter [10.1](#).

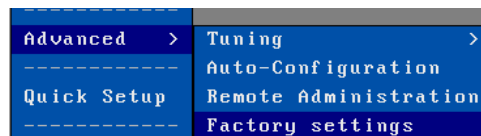
### a) RSH administration

RSH commands can be activated / deactivated.

### b) XML administration

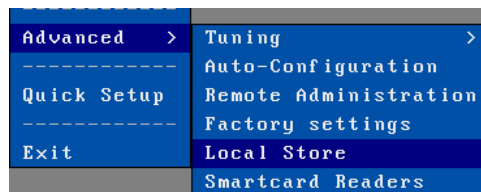
- **Activation:** XML commands can be disabled or forced in a TLS secure channel.
- **"Get configuration"** command: with the value "yes, password required", the execution of this command can be protected by a password (that of the thin client setup) as can the restart, send configuration command or updating the "firmware".
- **"Send message"** command: this command can be disabled or password protected (same as the Get configuration).
- **"Window" and "mss" sizes:** these two values are used for managing the TCP socket of the XML administration protocol.

### 3.6.4 - Factory setting



After confirmation, the current settings are completely erased. The thin client is in the same state as when it was delivered. See annex [A.7.1](#).

### 3.6.5 – Local Store



The Object store is a 256 kb storage space on the thin client. The following types of objects can be stored:

- TSE license: optionally sent during a connection to a TSE / RDS server when this is in "license by device" mode.
- Printer property: optionally sent during a connection to a TSE / RDS server with printer redirection. See chapter [5.1.6](#).
- Logo: this is a JPEG or PNG type image (only one logo can be kept).
- Personal certificate: supported types are PFX, PEM and P12.
- Root certificate (CA): supported types are PEM and CER.
- SSH private key: supported type is PEM

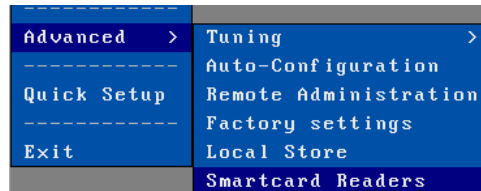
Here is an example of an object store:

Local Store (256Kb)		
Type	Size	Information
Logo	2079	PNG 360x76
Personal Certificate	1226	W2K16_CERT

Exit      Clear All      Add object

- **Adding objects:** the "TSE License" and "Printer properties" objects cannot be added manually. They are issued by a Windows server. The "Logo" and "Certificate" objects are added either from a USB key by the button **[Add Object]**, or via the "AxRM" software. For more information, see the manual *"Axel Remote Management"* available on our website.
- **Deleting objects:** an object can be deleted by pressing the <Delete> key after selecting it. Or the store can be emptied in a single operation by selecting the button **[Clear all]**. These operations can also be performed by the "AxRM" software. For more information, see the manual *"Axel Remote Management"* available on our website.

### **3.6.6 - Smart card readers**



This option allows you to view the smart card readers currently listed by the thin client. For more information, see chapter [3.4.10](#).

## **4 - USING THE THIN CLIENT**

*This chapter describes powering on and off the thin client and the use of multisession.*

## 4.1 - POWER ON

The thin client can be powered up by pressing the on / off button or by the "Wake On Lan" function (if this is authorized - See appendix [A.7.2.a](#)).

The first operation performed by the thin client is to decompress the microcode, load it into memory and initialize (this step is characterized by the display of an AXEL logo on the screen). The rest of the start-up phase depends on the configuration of the thin client.

If the network interface is wired, 802.1X authentication is not active and the IP address is fixed, the thin client has completed the start-up phase after detecting the Ethernet cable. Otherwise, the thin client must perform the following operations:

- **Display the quick setup** (only when switching on for the first time (unconfigured). See chapter [2](#))
- **Connect to the network** (ie detect the Ethernet cable or find the Wi-Fi access point)
- **If necessary, authenticate to the network** (802.1X protocol)
- **Obtain an IP address** (DHCP protocol)

After the start-up phase, the operations performed by the thin client are:

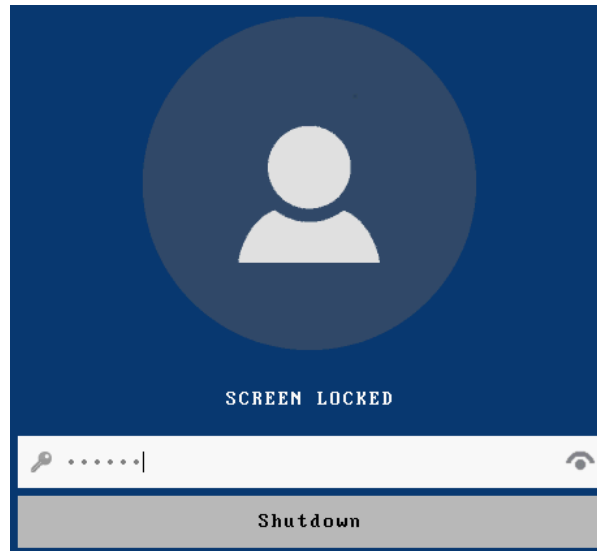
- **Auto-configuration** (only if configured): searches for new firmware and / or configuration available over the network. If this is the case, the thin client may need to reboot several times (for more information see chapter [2.2](#)).
- **Active Directory logon:** if Active Directory authentication is activated, a logon screen is displayed. The user must enter his user's name and password to continue (see chapter [4.2](#)).
- **Auto connection:**
  - screen sessions (if the parameter **auto connection** is set to "yes"). See chapter [4.4](#).
  - auxiliary ports associated with service (telnet, tty or prt5250) if the "Auto" parameter is set to 'yes'.
- If at least one screen session automatically connects, the thin client displays the first active screen session.
- **Local desktop:** if no screen session is connected, the thin client displays the local desktop (see chapter [4.3](#)).


## 4.2 - THIN CLIENT BOOT AUTHENTICATION

If Local logon or Active Directory authentication is activated (see chapter [3.2.8.a](#)), a logon screen is displayed after the thin client starts up.

### 4.2.1 Local Logon

This authentication allows access to thin client sessions to be prohibited without entering a password defined in the setup. This is the window presented when starting the thin client.



It is possible to view the password entered by continuously clicking on the icon  at the end of the entry area.



If the “Allow password change” parameter is set to YES in the setup. When displaying the local logon window, an icon at the bottom right of your main monitor allows access to the password change window.

To change the password, the user will first need to enter the current password.

**Note:** When this window is displayed, it is still possible to enter the setup. It is therefore recommended to secure entry into the setup using a password.

**Tip 1:** You can couple this functionality with the screen saver (See chapter [3.2.2.c](#)) to add a time-out on thin client inactivity.

**Tip 2:** The “Logon Local” can be used to facilitate user authentication if the thin client is located in a closed environment within the company.

The risk of a dictionary type attack on the AXEL thin client being zero, it is not very dangerous for the administrator to configure in the setup a session in “automatic connection” and “automatic login” mode with a user name and a complex password to the server.


In this case, the password “logon Local” can be used as a “Pin code”. The user will then only have to enter the “Pin code” when starting the thin client to automatically authenticate on the server.



### 4.2.2 Active Directory Logon

This authentication can remove the need to authenticate when opening sessions if the “Single Sign On (Active Directory)” option is set at the session level.

- Only a valid authentication gives access to the local office.
- The domain name cannot be changed.
- Password modification is automatically prompted if password has expired (which is not the case for an RDP session if the NLA protocol is required at the server level. See more details on the NLA protocol in chapter [5.1.5](#)).

It is possible to view the password entered by continuously clicking on the icon  at the end of the entry area.

**Tip :** You can couple this functionality with the screen saver (See chapter [3.2.2.c](#)) to add a time-out on thin client inactivity.

The “Active Directory” desktop is closed from the local desktop by clicking on the user icon at the top right. A dialog box invites you to disconnect, the [ESC] key allows you to exit this box.

### 4.3 - LOCAL DESKTOP

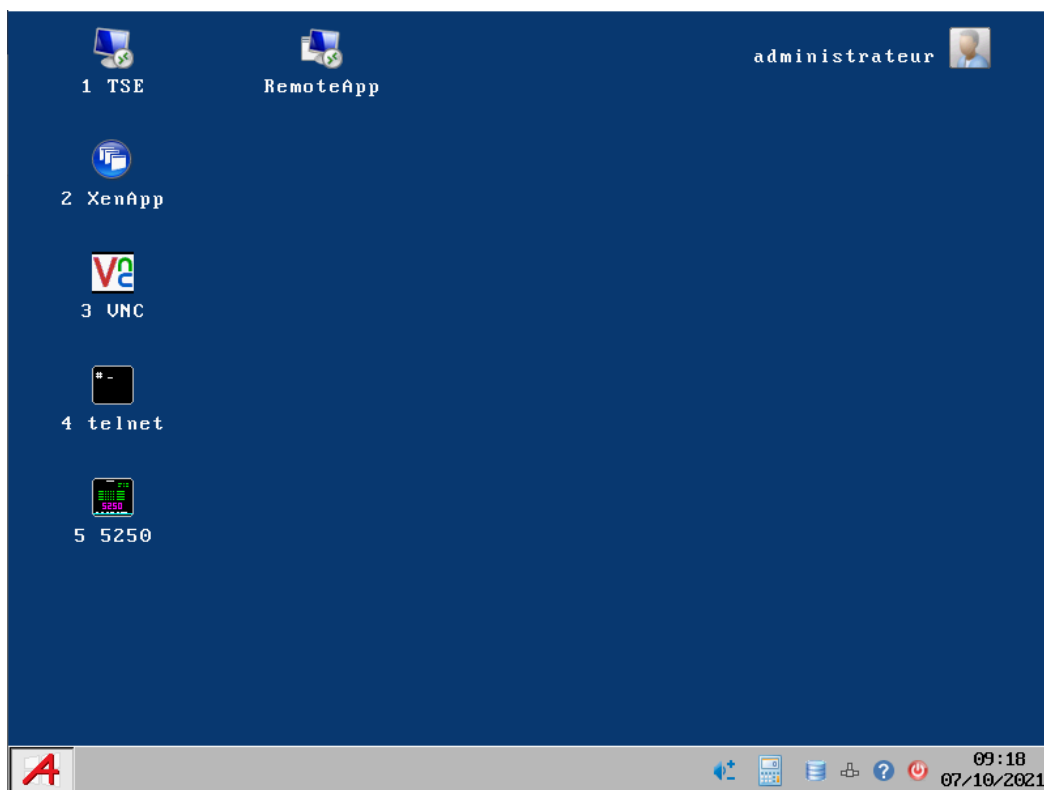
The local desktop is displayed if no session is currently connected or if the user has clicked on the icon at the bottom left to return to the local office.

The appearance of the desktop depends on the style of the taskbar (see chapter [3.2.3](#)).

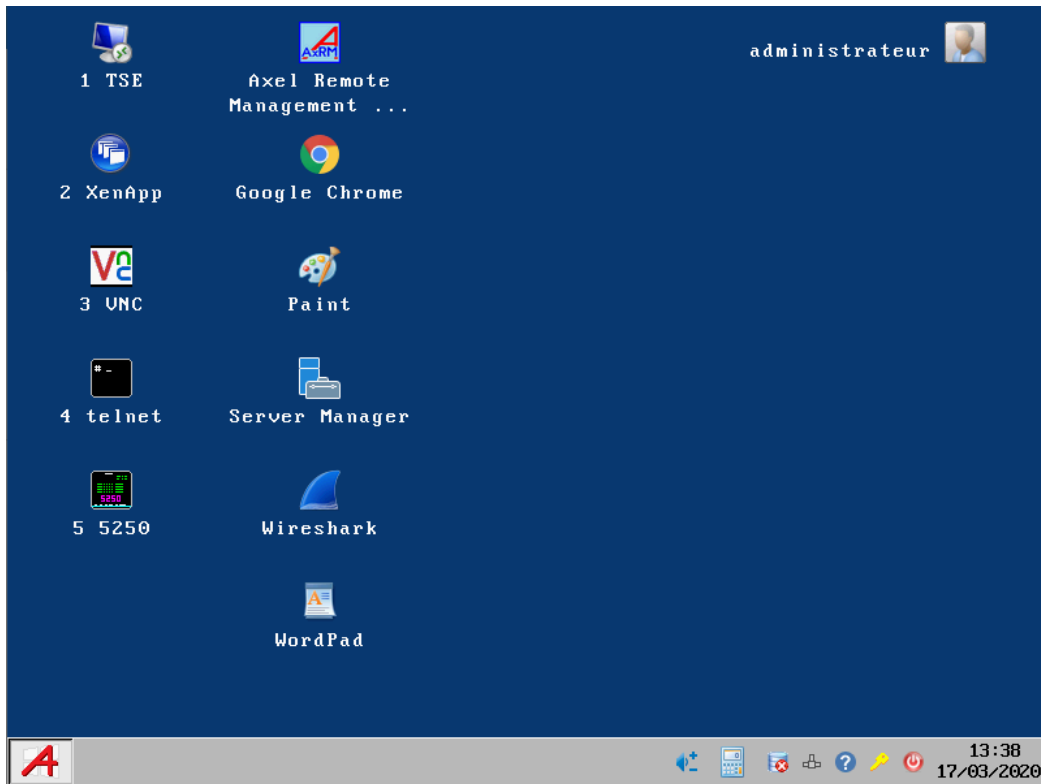
The organization of the local desktop is as follows:

- In the main area, a first column of icons represents the possible predefined sessions (see **table 1**). And a second column shows the icons or the applications available for the RemoteApp or Citrix "applications desktop" if it has been activated.
- A task bar at the bottom of the screen.
- In the case of an Active Directory logon, the name of the user at the top right.

Example of various sessions and a non-active "RemoteApp" desktop:













Example of various sessions and a “RemoteApp” desktop activated by clicking on the icon:



Possible actions:

- Click on an icon or press the associated key combination to open a session.
- Click on an icon in the task bar. See the below.
- Click on the user icon to log out of the Active Directory account.

**Table 1** - lists the icons associated with the types of sessions

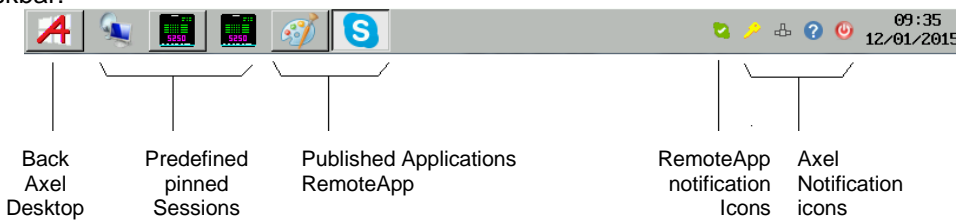
				
Microsoft TSE/ RDS Session	Microsoft RemoteApp Desktop	Citrix Receiver Session	Citrix Receiver Desktop	VDI-in-a-Box Session
				
VMware View Client Session	VNC Session	Systancia AppliDis Session	5252 or 3270 Session	Text Emulation Emulation

### 4.3.1 - "Standard Task Bar"






















The task bar is organized as follows (from left to right):

- An icon allows you to return to the Axel office
- The icons of the connected predefined sessions (with their label if the "Display labels" parameter is activated - see chapter [3.2.3](#)).
- **Note:** all the icons of the predefined sessions (even those not connected) can be displayed if the "Pin sessions" parameter is activated (see chapter [3.2.3](#)).
- Any icons for connected RemoteApp applications.
- Notification icons (see **table 2**)
- Possibly the date and time (see Section [3.2.6](#))

Sample taskbar:



**Table 2** - Axel notification icons in the "standard" taskbar

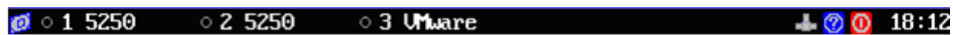
	Turn off the thin client - See chapter <a href="#">4.9</a>
	Obtain information on the thin client (Firmware / Hardware)
	Display the type of network and connection status
	- : 802.11 wireless interface active (no authentication)
	- : 802.11 wireless interface active and authenticated
	- : 802.11 wireless interface not connected
	- : Wired Ethernet interface active (no authentication)
	- : Wired Ethernet interface active and authenticated (802.1X)
	- : Ethernet cable not connected
	Status of the Reverse SSH function.
	- : Reverse SSH active and ready to operate
	- : Authentication problem
	- : At least one service is not active
	Disconnect the current session. Displayed only if the current session is connected. See chapter <a href="#">4.7</a> .
	USB drive indicator. Displayed only if a USB drive is connected.
	- : reading in progress
	- : writing in progress
	- : media absent or format not supported
	Attach or detach devices as part of the USB port redirection.
	Positioned portrait (P) or landscape (L) mode. See Annex <a href="#">A.7.2</a> .
	Adjustment of volume. See chapter <a href="#">4.8.7</a> .

### 4.3.2 - "Classic Task Bar"










The classic task bar is organized as follows (from left to right):

- An icon on the left allowing you to return to the Axel office.
- The name of the predefined sessions with a connection indicator (green if connected)
- Notification icons (see **table 3**)
- Possibly the date and time (see chapter [3.2.6](#))

Example of taskbar:



**Table 3 - Axel notification icons of the 'classic' taskbar**

-  Switch off the thin client - See chapter [4.9](#)
-  Obtain information (Firmware / Hardware)
-  Display of the network type and connection status (see chapter [4.8.1](#))
-  Reverse SSH function status (see chapter [4.8.5](#))
-  Disconnect the current session. Displayed only if the current session is connected. See chapter [4.7](#).
-  USB drive indicator. Displayed only if a USB drive is connected.
  -  : reading in progress
  -  : writing in progress
-  Positioned portrait (P) or landscape (L) mode. See Annex [A.7.2](#).

## 4.4 - SESSION CONNECTION

### 4.4.1 - Activating a session

Activating a session can be done by:

- **The keyboard:** by default, use <Alt> <F> for a predefined session (see chapter [3.2.3](#)) and <Ctrl> <Alt> <O> for the application desktop.
- **Mouse:** click on the corresponding icon in the local desktop or in the taskbar.

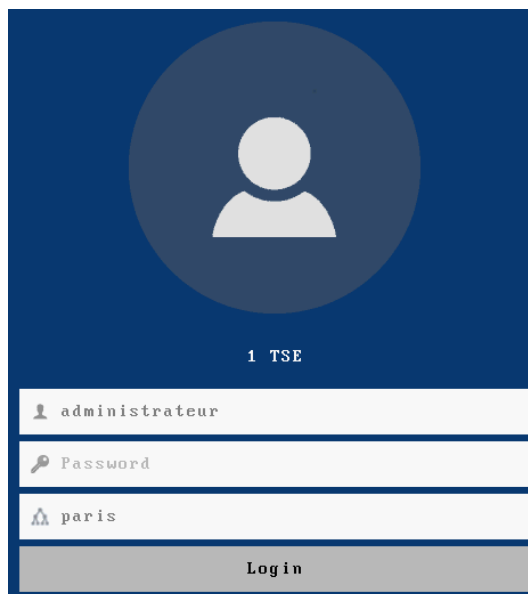
**Note:** if the session to be activated is open access (not associated with a server) a dialog box requesting the connection parameters is displayed:

The server is to be selected from a list. A new server (DNS) or a new IP address can be entered directly; they will be added automatically to the local servers.



### 4.4.2 - Local authentication

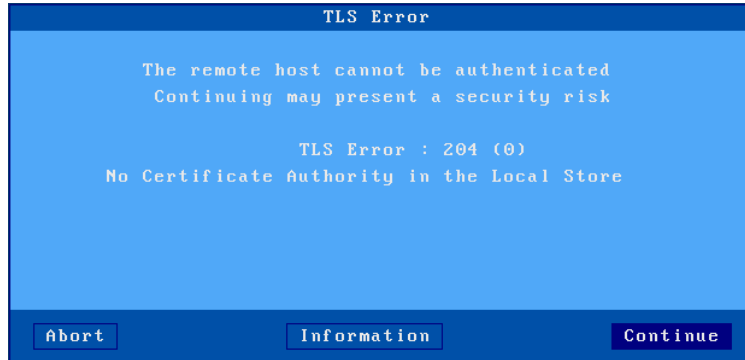
The thin client can display a local authentication request (for example, for the application office, for an RDP session configured with a gateway or a TS broker):



**4.4.3 - Verification of the TLS certificate**

If connected to a TLS server, the thin client, if it is configured to do so (see chapter [3.3.3.c](#)) can check the validity of the certificate by means of an authority certificate (CA) previously installed in the object store. For more information see chapter [3.6.5](#).

If the certificate is not valid a dialog box is displayed. For example:



This dialog box gives the reason for the error and allows you to abandon the connection or continue.

The [option **Continue**] is only available if the "parameter **In the event of an error**"(see chapter [3.3.3.c](#)) is set to "Display an alert".

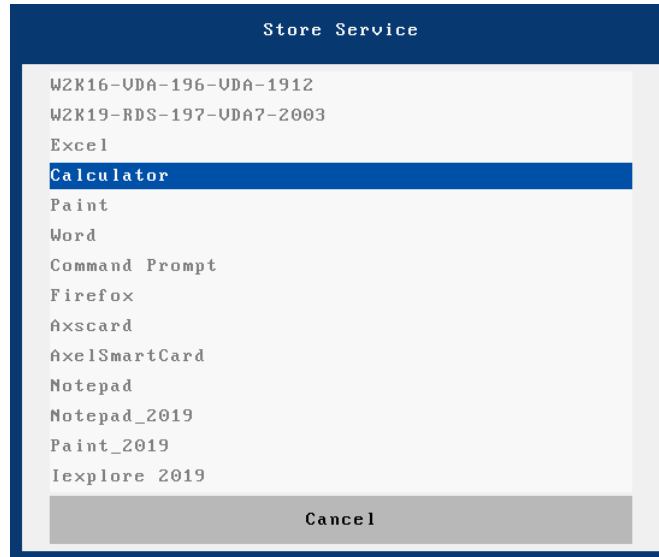
If this parameter is set to "refuse connection" the dialog box is as follows (with no possibility to continue):



In both cases the button [**Information**] allows name of the TLS server and the certificate information for this TLS server to be displayed.

#### 4.4.4 - Possible choice of the published resource

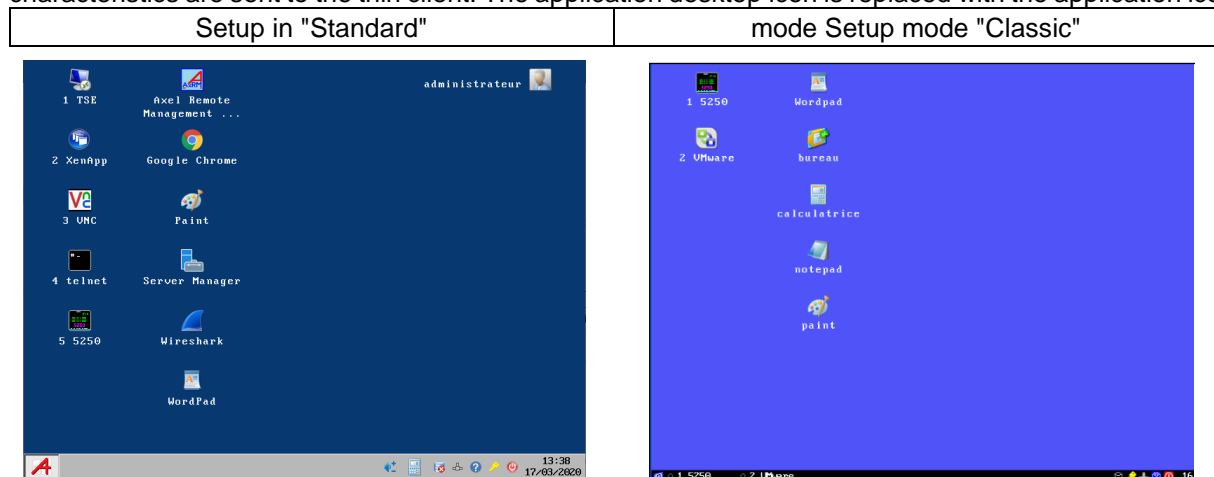
With a predefined session of type "Citrix Receiver" or "VMware View Client", the thin client displays the list of available resources (if none has been previously selected in the setup to auto start):



When one of these remote entries is chosen, the thin client requests from the server the information necessary to open the RDP or ICA session.

#### 4.4.5 - Application desktop Connection

After connection to the application desktop (RemoteApp or Citrix Receiver), the application icons and their characteristics are sent to the thin client. The application desktop icon is replaced with the application icons.



- The “folders” icons represent the possible directories used to prioritize the applications. In a directory, the “.” folder represents the parent directory.
- The “Axel” icon on the left of the task bar allows you to return to the local desktop of the thin client at any time to launch other published applications.
- The <key F5> refreshes the list of icons.



When the user clicks on an application icon, the thin client uses the first free reserved session to launch an RDP / ICA connection. If all of the reserved sessions are in use, the thin client will beep.

#### Information on the RDP / ICA session generated:

- The new RDP / ICA session becomes the current session.
- The RDP / ICA session uses the general operating parameters specified in the setup (encryption, bandwidth ...).
- The screen resolution and number of colors used are those of the local desktop of the thin client.

**Note:** If the “seamless” option is activated, as far as possible the applications are launched in the same session (see paragraph [5.3.2.d](#)).

To launch other applications, it is necessary to return to the local desktop of the thin client. This is done by pressing the <Alt> <Esc> key combination or by clicking on the leftmost icon on the taskbar.

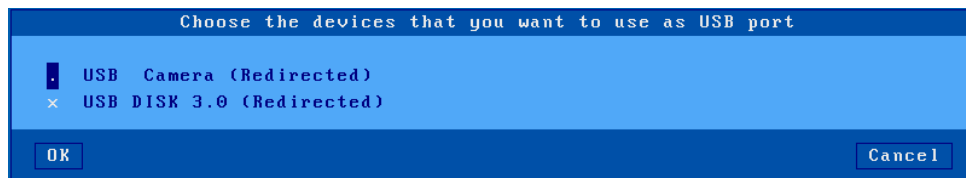
#### 4.4.6 - USB port (RemoteFX or XenDesktop)

**Reminder:** USB redirection is only possible from an RDP / ICA session connected to a RemoteFX server (from Windows 2012) or XenDesktop.

When establishing the RDP / ICA session, the redirection of the eligible USB devices is conditioned by the parameter "At the opening of the session" in [Configuration] - [Terminal- [Global RDP / ICA] dialog box (see chapter [3.2.5](#)).

The values of the "parameter **“The opening of the session”** are:

- **Do nothing:** no eligible device is redirected.
- **Automatically redirect:** all eligible devices are redirected.
- **Ask me each time:** a dialog box listing eligible USB devices is displayed. The user can check or uncheck each device to start or stop redirection. For example:



**Note:** this dialog box is also displayed when a USB device is connected during use if the option "**During the life of the session**" is set or using the key sequence [CTRL] [ALT] [U].

## 4.5 - CHANGING SESSIONS

An important feature of the thin client is the multisession support. After opening a connection to a server, it is possible to establish other connections to other servers (or on the same server).

The session can be changed by:

- **The keyboard:** <Alt> <Fx> for an existing session or to create a predefined session (see chapter [3.2.3.c](#)).
- **The mouse:** click on the corresponding icon in the local desktop or on the label of the session in the taskbar.

If the destination session has not yet been created, it is then connected (see chapter [4.4.1](#)).

## 4.6 - RETURN TO LOCAL OFFICE

The local desktop is automatically displayed if no session is currently connected.

However, it is possible to return to the local desktop at any time, in particular to launch applications from the RemoteApp or Citrix Receiver application office. This is done by pressing the <key combination <Alt> <Esc> or by clicking on the leftmost icon on the taskbar.



## 4.7 - SESSION DISCONNECTION

Disconnection of a session is generally carried out by a system command (which allows the session to be closed properly). For example:

- Windows: select "Logout" from the Start menu.
- Unix / Linux in Telnet or ssh: command "exit" (or <Ctrl> <D>)

Or more radically:

- click the yellow key icon "" on the taskbar. Confirmation is requested.
- press <Ctrl><Alt> <D> (immediate closing, no confirmation).

**Note:** The connection is terminated at the TCP / IP level, which means that the running applications may not be closed on the server side.

The behavior of the thin client after a disconnection depends on the parameter "**Automatic reconnection**" of the session.

If this parameter is set to "**yes**", a connection is re-opened for the session. See chapter [4.4.1](#). If this parameter is set to "**no**", the thin client displays the first session among those still active.

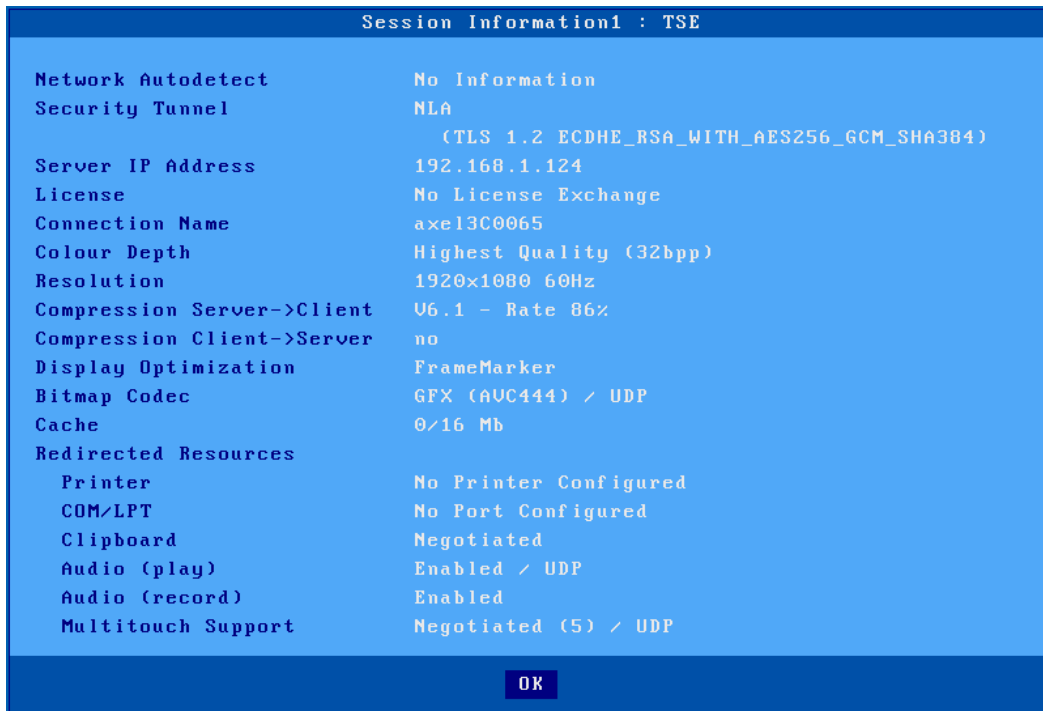
If no session is active, the local desktop is displayed, unless the Local Logon or Active Directory Logon is active, in which case the behavior of the thin client depends on the option "No active session" described in chapter [3.2.8.a](#).

## 4.8 - SPECIAL FUNCTIONS

### 4.8.1 - Information on the current session

Once connected and identified, the key combination <Ctrl><Alt> <I> "i" (as information) provides information on the current session.

The content of the dialog box varies depending on the nature of the session. Example with an RDP connection:



**Note:** This information is sometimes different from that configured in the setup, for certain parameters the server can overrule the terminal's settings.

#### **4.8.2 - Screen Lock**

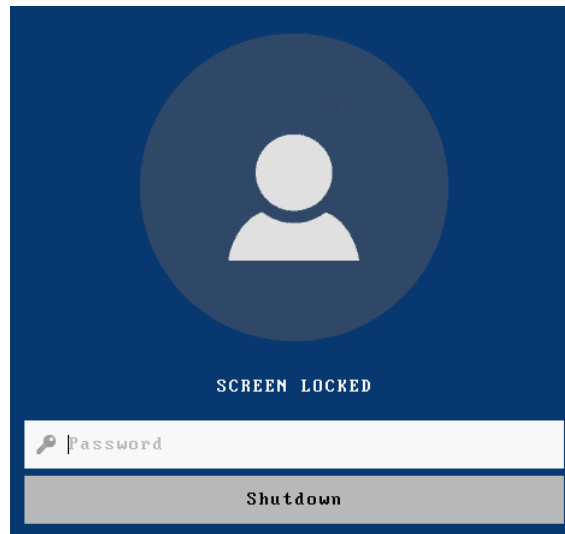
For security reasons, it may be helpful for an operator to lock the screen of the thin client during an absence (rather than logging out).

**Note:** the screen lock means that the screen of the thin client is blank (but the current sessions remain connected). There is no longer the possibility to change session. The only way to regain control is to enter the appropriate password.

The screen lock function is coupled to the screen saver function and must be activated through the setup by the administrator of the thin client (see chapter [3.2.2.b](#)).

A screen can be locked:

- Either **automatically**: after a certain period of inactivity at the level of the thin client (keyboard or screen), the screen goes black with or without logo. Pressing a key reactivates the screen, a dialog box allowing the screen to be unlocked appears.
- Either **manually**: the key combination <Ctrl> <Alt> <S> immediately locks the screen.



When the dialog for unlocking the screen is displayed. Two actions are possible from this dialog:

- Enter the password to unlock the screen. If the Active Directory logon is not used, the password is that of the screen saver. If you forget it, the password for accessing the setup (see chapter [3.2.8](#)) can also be used.
- Reset the thin client. If the password has been forgotten, the only possible operation is to reboot. After the power is returned the administrator can erase or modify the password of the screen saver.

#### **4.8.3 - "Copy / Paste" function**

The thin client offers a "Copy / Paste" function which operates either within the current session but also between different sessions (possibly associated with different protocols) and the setup.

It is therefore possible, for example, to "copy" text from a 5250 session and "paste" it into a Windows session, or vice versa.

##### **a) Copy**

From a Windows session (RDP or ICA):

Use the usual "Copy" function. For example, **<Ctrl> <C>**.

From a VNC session:

The utility "**vnccconfig**" must be launched on the server. Copying is done simply by selecting a text area.

From a text session (5250, 3270, ANSI, VT ...):

To switch to "copy" mode, press **<Ctrl> <C>** (for 5250 or 3270 emulations) or **<Ctrl><Alt> <C>** (for other emulations). The mouse then allows you to select an area. Press **<Enter>** to validate this choice (the content of the zone is copied to the local clipboard) or **<Esc>** to cancel.

**Note:** the "copy" function is only available if this session manages a mouse.

##### **b) Paste**

To a Windows session (RDP or ICA):

Use the usual "Paste" function. For example, **<Ctrl> <V>**.

To a VNC session:


The utility "**vncconfig**" must be launched on the server. Pasting is done by selecting "paste" from the context menu.

To a text session (setup, 5250, 3270, ANSI, VT, WYSE ...):

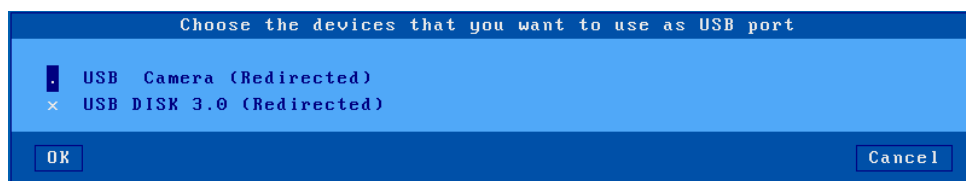
Pressing **<Ctrl> <V>** (for 5250 or 3270 emulations) or **<Ctrl><Alt> <V>** (for other emulations) allows you to paste the contents of the clipboard.

**Note:** for sessions 5250 and 3270, the function **<ZNext>** is sent at the end of each line of the clipboard.

#### **4.8.4 - USB port redirection**

The " " icon in the taskbar or the key combination **<Ctrl><Alt> <U>** displays a dialog box to start or stop the redirection of certain USB devices.

Here is an example of this dialog box:



**Note:** this dialog box is only displayed if the "dialog.**USB port redirection**" function is active within the current RDP / ICA session, and the server accepts this type of redirection.

Eligible USB devices are listed, specifying if they are currently redirected. The user can check (x) or uncheck (.) Each device to start or stop redirection.

**Note:** this dialog box is also displayed when establishing the RDP / ICA session if the option "**At the opening of the session**" is set to "Ask me each time". And it is also displayed when a USB device is connected during use if the "option **During the life of the session**" is set to "Ask me each time". See chapters [3.2.5](#) and [4.4.6](#).

#### **4.8.5 - Reverse SSH**

The " " icon in the task bar displays a dialog box to control the Reverse SSH service.

Various information is displayed in this dialog:

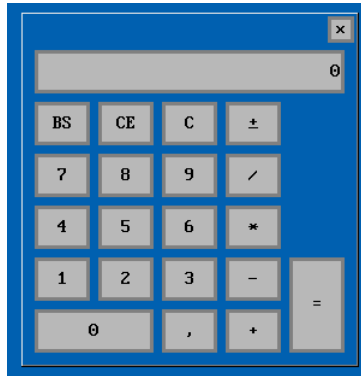
- Connection status: success or failure of the TCP / IP connection to the SSH server
- Service: success or failure of authentication to the SSH server
- VNC remote control: success or failure of the dedicated virtual channel (if requested)
- LPD: success or failure of the dedicated virtual channel (if requested)

**Note:** the [buttons are **Connect**] and [**Disconnect**]used to start or stop the Reverse SSH service.

### 4.8.6 - Local calculator



The "  " icon in the taskbar or the key combination **<Ctrl> <Alt> <\*>** displays a calculator.



This calculator is available from the local thin client desktop or from any active session.

Main features:

- Support of the 4 basic mathematical operations.
- Keyboard or mouse operation
- Exit using the <keys **F10**> or <Esc>
- Available copy / paste functions

### 4.8.7 - Local volume

The key combination **<Ctrl> <Alt> <+>** or **<Ctrl> <Alt> <->** allows to increase or decrease the local volume.




Clicking on this icon when it is positioned in the setup level (see chapter [4.3.1](#)) displays a cursor which allows you to view and modify the local volume.

## **4.9 - SWITCHING OFF OR REBOOT**

### 4.9.1 - Operation carried out locally

Switching off or restarting the thin client can be triggered by:

- the key combination **<Ctrl><Alt> <Delete>**,
- a click on the red "  " icon in the task bar,
- short press on the "button **on / off**" located on the front of the thin client.

A confirmation dialog box appears asking the user to confirm his choice:

- [button **Stop**]: turn off the thin client
- [button **Restart**]

After selecting the choice, the thin client first disconnects all open sessions (screen and auxiliary ports) and then shuts down or restarts.

A setup parameter allows the thin client to be forced to stop without confirmation when the button "**on / off**" is briefly pressed (see Appendix A.7.2.c)

**Note:** it is also possible to force the thin client to switch off by pressing the "on / off" button for 6 seconds. In this case the current sessions are not disconnected and the "Wake On Lan" function will not be available for the next power-up.

#### **4.9.2 - Operation carried out remotely**

The "AxRM" software allows a thin client to be restarted or switched off remotely. (see chapter [8.5](#))

Commands "rsh" also allow these operations (see chapter [8.5](#))

## 4.10 - AVAILABLE KEY COMBINATIONS

The following table lists the key combinations handled by the thin client:

PC	keyboard Keyboard 5250	Comments
<Ctrl> <Alt> <Esc>	<Rest> <Alt> <Config>	Entry in the setup
<Alt> <Fx>	<Alt> <Fx>	Change of session
<Alt> <Esc>	---	Display of the local office
<Alt> <-> / <Alt> <+>	<Alt> <-> / <Alt> <+>	Previous / next session
<Ctrl> <Alt> <O>	<Rest> <Alt> <O>	Office opening applications
<Ctrl> <Alt> <E>	<Rest> <Alt> <E>	Ethernet network Statistics
<Ctrl><Alt> <W>	<Rest> <Alt> <W>	Wireless network Statistics.
<Ctrl> <Alt> <U>	---	Display of the USB ports redirection box
<Ctrl> <Alt> <L>	<Rest> <Alt> <L>	Keyboard LED synchronization
<Ctrl> <Alt> < S>	<Rest> <Alt> <S>	Display of the screen lock box.
<Ctrl> <Alt> <Pause>	<Rest> <Alt> <Pause>	Sending a break signal. (only in telnet / ssh)
<Ctrl> <Alt> <Screen Print>	<Rest> <Alt> <prtsrn>	Hardcopy on the default port
<Ctrl> <Alt> <D>	<Rest> <Alt> <D>	Closing the current session
<Ctrl> <Alt> <K>	<Rest> <Alt> <K>	Changing the keyboard type (PCAS / 400)
<Ctrl> <Alt> <Delete>	<Rest> <Alt> <Delete >	Power off
<Ctrl> <Alt> <i>	---	Display of Information on the current session
<Ctrl> <Alt> <X>	<Rest> <Alt> <X>	Display of current connections (see chapter <a href="#">9.4</a> )
<Ctrl> <Alt> <BackTab>	<Rest> <Alt> <BackTab>	Return to 800x600
<Ctrl> <C> or <Ctrl> <Alt> <C>	<Rest> <C>	Selection and copy of a text box (mouse required)
<Ctrl> <V> or <Ctrl> <Alt> <V>	<Rest> <V>	Paste previously copied text
<Ctrl> <Alt> <-> / <Ctrl> <Alt> <+>	<Rest> <Alt> <-> / <Rest> <Alt> <+>	Decreased or increased audio volume
<Ctrl> <Alt> <*>	<Rest> <Alt> <*>	Calculator display locale

**Note:** key combinations with a blue background can be disabled. See paragraph [3.2.1.b](#).



**- 5 -  
INSTALLATION UNDER  
WINDOWS**

*This chapter describes the installation and use of an Axel thin client under*

This chapter only describes the specifics of the thin client under Windows. For all general statements see the previous chapters.

Connection to a Windows server can be done in two ways:

- **Predefined session:** This is a dedicated connection to a server, a broker or a server farm. The accessed resource can be a desktop or an application. This works for Microsoft TSE / RDS, Citrix Receiver or VMware View Client.
- **Applications desktop:** It allows a user, after authentication, to see on a local desktop the icons of the applications published for his user account. The launch of a published application is done simply by clicking on the corresponding icon. A dedicated RDP or ICA session is automatically opened for the management of this application. This works for Microsoft RemoteApp (2008R2 and later servers) and Citrix Receiver.

The rest of the chapter is composed as follows:

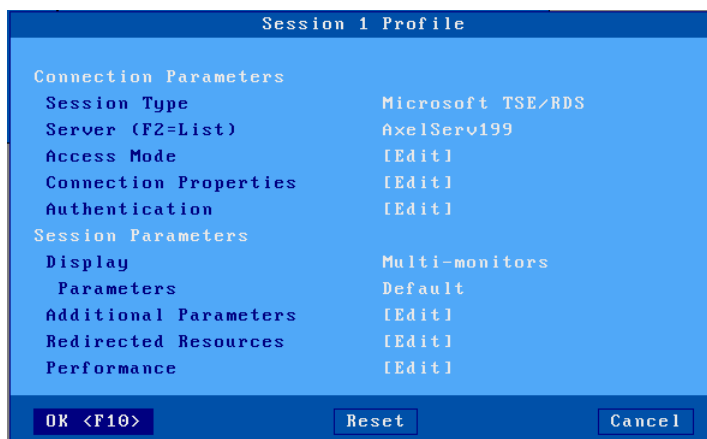
- Microsoft TSE / RDS session. See chapter [5.1](#).
- Citrix Receiver session. See chapter [5.2](#)
- RemoteApp and Citrix Receiver application desktops. See chapter [5.3](#)
- VMware View Client session. See chapter [5.4](#).
- Systancia Applidis session. See chapter [5.5](#)

### 5.1 - MICROSOFT TSE / RDS SESSION

The “compatible RDP” protocol of Axel thin clients enables connections to be made to all types of RDS servers. The following table gives the availability of certain functions depending on the server operating system:

Windows	No. of colors (bits / pixel)	Redirection					
		Printer	Port COM	Audio	USB keyUSB	Chip card reader	port RemoteFx
NT4-TSE	8	-	-	-	-	-	-
2000	8	Yes	-	-	-	-	-
2003	8/15/16/24	Yes	Yes	Sound	-	-	-
2008R2	8/16/32	Yes	Yes	Sound & Microphone	Yes	Yes	-
2012R2 à 2022	16/32	Yes	Yes	Sound & Microphone	Yes	Yes	Yes

To configure a Microsoft TSE / RDS session, select the menu **[Configuration] - [Sessions] - [Session X]** (where X is the session number) in the setup then select the session type "Microsoft TSE / RDS " The following dialog box is displayed:



Update the following parameters:

- **Server:** chosen from the list of servers (see chapter 3.1.4). A new server (DNS) or a new IP address can be directly entered and will be added automatically to the local server list.
- **Access mode:** configuration of a load balancing broker and/or RDS gateway. See chapter 5.1.1.
- **Connection properties:** see chapter 5.1.2.
- **Authentication:** activation of an automatic login procedure and / or automatic application launch. See chapter 5.1.3.
- **Display:** see chapter 5.1.4.
- **Additional parameters:** dialog box offering other RDP parameters (notably encryption and NLA authentication). See chapter 5.1.5.
- **Resource redirection:** dialog allowing redirection of printers and USB ports. See chapter 5.1.6.
- **Performance:** dialog box allowing the management and optimization of bandwidth. See subsection 5.1.7.

### 5.1.1 - Access mode

The following box is displayed:



#### a) Load balancing

The "LoadBalanceInfo" character string lets the thin client connect via a Connection Broker, and be redirected to the most available RDS server of the farm.

The value of "LoadBalanceInfo" can be found in the Connection Broker registry or in a ".rdp" file. For example:

```
loadbalanceinfo:s:tsv://MS Terminal Services Plugin.1.QuickSessionCollection
```

Only the part after the "...: s:" must be entered in the thin client, here the part in red.

**Note:** A default string is proposed which corresponds to the beginning of the standard "LoadBalanceInfo" string proposed by Microsoft, just add append the name of the collection you want to reach.

#### b) RDS or TS gateway

*An RDS gateway allows access to resources (servers / computers) from outside the company without the need to establish a VPN connection.*

The first step is to activate the option "Use a TS gateway server".

The "" option **Name or IP Address** locates the RDS gateway. Its syntax is **server [: port]**

- **server** : name or IP address of the RDS gateway
- **port** : optional TCP port (default **443**)

The 'option **Authentication**' is always set to NTLM.

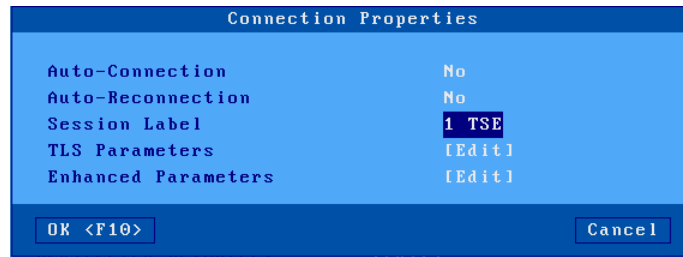
The option **Ignore for local addresses** allows initially a direct connection to the RDS server to be attempted. If this connection fails a second attempt is made through the gateway.

When connecting (HTTPS) to the gateway, a personal certificate may be requested. It is possible to set a personal certificate so it is not requested at each connection (see chapter [3.3.3.b.](#))

**Note:** this parameter is disabled if the object store does not contain a certificate. See chapter [3.6.5.](#)

### 5.1.2 - Connection properties

The following box is displayed:

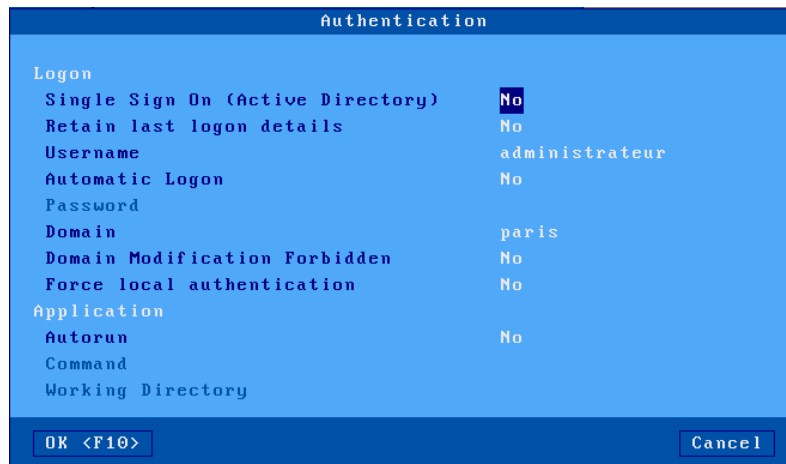


Description of the parameters of this box:

- **Auto-Connection:** if this parameter is set to "yes" the thin client automatically opens the session on boot. Alternatively, the connection must be requested by the user by means of a keyboard or mouse action.
- **Automatic reconnection:** if this parameter is set to "yes", after a disconnection, the thin client automatically re-opens a new session. Alternatively, the reconnection can be requested by the user by means of a keyboard or mouse action.
- **Session label:** This label (14 characters max.) Is used to identify the session at the local desktop or taskbar level.
- **TLS parameters:** Security-related parameters for this connection. See chapter [3.3.3](#).
- **Advanced parameters:** There is generally no need to modify these parameters which are pre-positioned to be the most optimized according to the type of session. See annex [A.7.3](#).

### 5.1.3 - Authentication

The following box is displayed:



**“Logon” section:**

These options are used to configure user authentication:

- **Single Sign On (Active Directory):** allows you to use the Active Directory logon for session authentication. If this option is set to "yes", all the other options in the Logon section are disabled (grayed out).
- **Remember last logon:** Uses the user name and the domain used previously for this session. In this case the following options up to "Prohibit modification of the domain" are disabled (grayed out).
- **Username:** default value proposed on the logon screen.
- **Automatic logon:** if this parameter is 'yes', the thin client presents the user name, password and domain without manual entry.
- **Password:** accessible if "Automatic logon" is "yes".  
Please note: if the password is pre-entered here, the session is not secure.
- **Domain:** default value proposed on the logon screen.
- **Prohibit modification of the domain:** in the case of local authentication (with the Axel logon dialog), modification of the domain name may be prohibited.
- **Local authentication:** activating this option allows you to enter authentication information before establishing the RDP protocol. Authentication can be based on a user name (with password and domain) or a pin code (if smart card redirection is enabled). The answers to this option are: "no", "yes" and "yes, smart card".

**Note:** If the connection is opened with a security level "NLA" or an RDS gateway is used, local authentication is mandatory

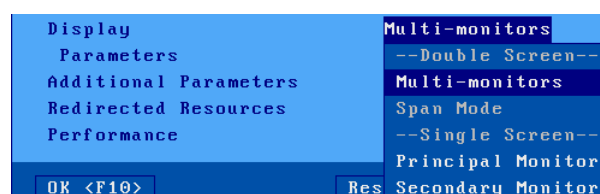
**"Application" section:**

A program can be automatically launched after the logon phase (rather than entering the Windows desktop).

- **Autorun:** the program can be launched in "normal" or "seamless" mode. In seamless mode, part of the windowing is transferred to the thin client and the application icons are displayed in the Axel task bar.
- **Command:** path and name of the program to be executed. As of Windows 2008, this program must be added to the "RemoteApp" programs.  
Example: % SystemRoot% \ system32 \ calc.exe (will automatically launch the Windows calculator).
- **Working directory:** Program working directory.  
Example: D: \

**5.1.4 - Display parameters**

Several modes are available for an RDS session:



- **"Multi-monitor" display** (default): Used to manage the standard Microsoft "multi-screen" when 2 monitors are connected to the thin client (Windows Server 2008 minimum). If only one monitor is connected, if this value is authorized it is possible to add a second monitor later without having to re-configure the thin client.
- **Display "Span mode»:** Available only if the session is not configured in H264 or in Progressive Codec, this is the operating mode which was available on the Windows server

2003 versions, the 2 monitors are seen as one large monitor (ex: 2 monitors of 1920x1080 are seen as a monitor of 3840x1080).

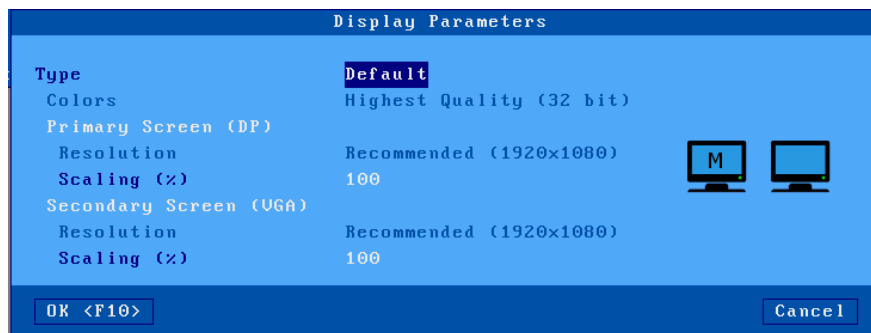
**Note:** In the case of two monitors with different resolutions, the vertical resolution of the smaller of the monitors is used).

- **"Main" or "secondary" monitor display:** Display the session only on one of the two monitors, which allows you to simultaneously display another session on the other monitor. (ex: one 5250 session on 1 monitor and one RDS session on the other)

**Note:** The positioning of the monitors can be modified at a general level, see chapter [3.2.2.b](#)

A dialog box allows you to position the display parameters for the session according to the display mode chosen:

**multi-monitors:**



**extended mode (spanning):**



**Note :** This mode is not available on TSE/RDS (with Progressive and H264 codec)

**main monitor or secondary monitor:**



The parameter "**Type**" offers two values:

- **By default:** the resolution and color values are those set at the general level (see chapter [3.2.2](#)). If one or more of these values are later changed at the general level, the session will inherit the modifications.
- **Custom:** the resolution and color values can be entered independently of those of the general level.

The parameter "**Scaling**" allows you to increase the size of the elements displayed in the session per monitor. The values of the possible percentages are 100, 125, 150, 175, 200.

### 5.1.5 - Additional parameters

The following box is displayed:



Description of the parameters of this box:

- **Minimum security level**, possible values.
  - **Compatible Server**(default): this mode allows you to connect regardless of the server's security level.
  - **NLA (CREDSSP 5 mini)**: the thin client opens a connection with NLA security compatible with CREDSSP 5. If this is refused by the server, an error is displayed and the connection is not made.
  - **NLA**: the thin client opens a connection with NLA security. If it is refused by the server, an error is displayed and the connection is not made.
  - **TLS**: the thin client first opens a connection with this security. If this is refused, a new connection is opened to negotiate a higher security type NLA. If this is refused by the server, an error is displayed and the connection is not made.
  - **RDP**: the thin client first opens a connection with traditional RDP security. If this is refused, a new connection is opened to negotiate security with TLS or NLA.
- **Password change without NLA** (accessible only if the minimum security level is set to NLA): The NLA protocol does not provide for the possibility of changing an expired password,



if it is set to "yes" this parameter gives the possibility for the thin client to connect via SSH to change the expired password. This requires that the server authorizes non-NLA connections.

- **NTLM Version:** NTLM version negotiated with the server (v1 or v2).
- **Encryption**, possible values:
  - **compatible server** (default): the thin client announces all of its encryption capacities to let the server choose the type of encryption.
  - **low level:** connection encrypted in the client-server direction only.
  - **medium level:** encrypted connection, either in the client-server direction, or in both directions.
  - **high level:** encrypted connection in both directions.
  - **fips compatible:** two-way encrypted connection with FIPS algorithms.
- **Connection name:** this character string is used to identify the thin client within the Windows operating system. By default, this name is the name of the thin client (see chapter [3.1.1.a](#)). If the "Terminal name" option is selected in the list of DHCP options, this field is inaccessible.
- **Reconnect if the connection is dropped:** RDP functionality that allows automatic reconnection when connection is lost (a message prevents reconnection with the number of attempts in progress). This does not correspond to the AXEL auto-reconnection function (See chapter [5.1.2](#)).
- **Console mode:** allows you to take control of the main console of the RDS server. (Equivalent to the "/admin" option, formerly "/console" of an RDP client on Windows).
- **Visual optimization:** allows a more fluid display for videos in "RDP" or "RemoteFX Adaptive graphics" especially for those in flash mode, ie YouTube. Not used in H264.
- **Preferred encoding:** this option is only available for a 32bpp connection. The terminal can offer various options but it is the server that decides what to actually use. To view the encoding used by a session, display the information box (see chapter [4.8.1](#)).
- Three possible choices:
  - **RemoteFX Adaptive Graphics**(default): supported from 2012R2
  - **RemoteFX (2008R2):** supported by 2008R2 and possibly 2012R2 according to GPOs
  - **RDP:** supported by all servers.
- **<Ctrl><Alt> <Delete>:** two modes for managing this key combination are available:
  - **local** (default): it is interpreted by the thin client and is used to power off (see chapter [4.9](#))
  - **remote:** it is interpreted by the Windows server (access for example to the task manager).
- **<Scroll Lock> & <Pause>:** whether or not these two buttons are authorized.
- **Default cursor command:** Functionality which authorizes or not to take into account of the RDP "Default cursor" command which can in certain cases be a problem.
- **Audio to buzzer** redirection: this mode allows RDP audio warning to be redirected to the terminal's buzzer.  
**Caution:** Using this function may cause unwanted effects.
- **Session label:** this label appears in the task bar. Two options:
  - **General label:** this is the label as defined in the "Connection property" dialog box, see chapter [5.1.2](#).
  - **Username:** this is the username after authentication.

### 5.1.6 - Resource Redirection

Resources redirection is used to announce the terminal's local resources to the Windows server. These resources are only available to the thin client user.

They are created on the Windows server when the session is connected and removed when the session is disconnected.

The resources managed are:

- **printers:** before being redirected the printer must first be enabled in terms of its physical port connection. See chapter [5.1.6.a](#), then chapter [5.1.6.c](#).
- **Storage devices:** See Chapter [5.1.6.c](#)
- **Smart card:** readers: See Chapter [5.1.6.c](#)
- **Audio management:** See Chapter [5.1.6.c](#)
- the **COM / LPT** ports: Before being redirected COM ports must first be enabled at the physical port. See chapter [5.1.6.b](#) and then chapter [5.1.6.c](#).
- **USB ports:** Must first define a set of eligible USB devices (see Chapter [3.2.5](#)). Then see chapter [5.1.6.c](#)

#### Note on minimum server versions:

- Printer redirection: Windows 2000 server
- USB port redirection: Windows 2012 R2 (or Windows 8) server.
- For other resources a minimum Windows 2003 server is required (and for audio a minimum 2008 server is strongly recommended).

#### a) Declaration of redirected printers

A printer will be automatically integrated into the spooler of the Windows server when the session is connected.

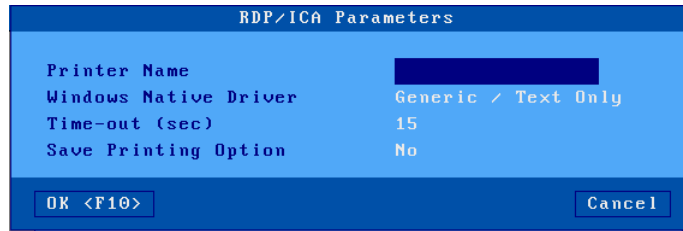
A maximum of four printers can be redirected

Before being redirected, a printer must first be enabled at its connection port. The available ports are USB logical ports and network printers.

Select the printer port dialog box (menu **[Configuration] - [Ports]-[xxx]**). For example, for the Usb1 port:



Set the "Active" parameter to "As Printer". Then select "Printer parameters". The following box is displayed:



Description of the parameters of this box:

- **Printer name:** name of the printer that will be visible on the Windows server.
- **Native Windows Driver:** name of the printer driver. Please note, the exact name of an existing driver installed on the Windows server must be entered, otherwise the printer will not be created.
- **Time-out value (sec):** this parameter represents the time after which a printer error (more paper, printer busy) is reported to the Windows server.
- **Print options cache:** this parameter saves the modifications made to the printer parameters on the Windows server side. If this parameter is "no" the default configuration of the printer will be used. These changes are saved in the object store. See chapter [3.6.5](#).

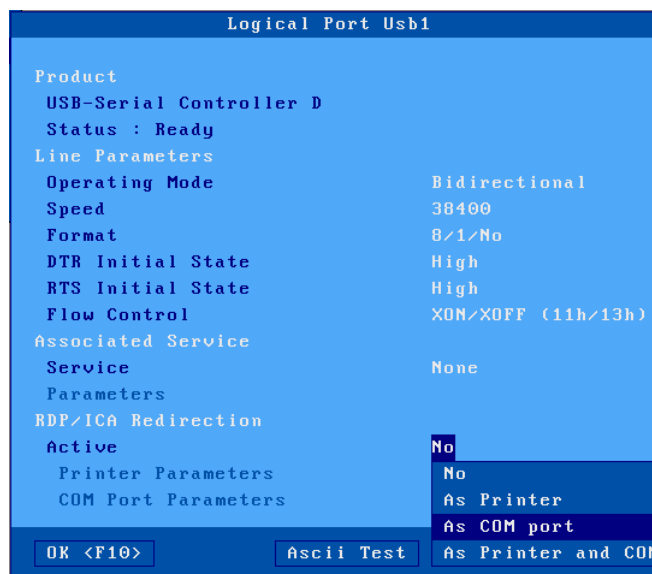
The declaration is finished. To redirect the printer, see chapter [5.1.6.c](#).

☺ :An advanced parameter is used to redirect 2 logical printers for the same physical printer, see Appendix A.7.2.d:

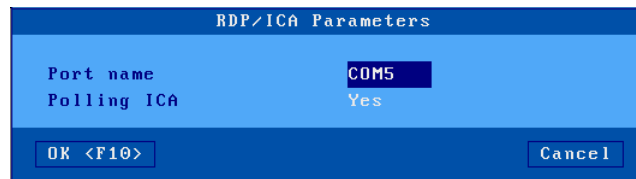
**b) Declaration of redirected COM / LPT ports**

Before being redirected a COM port must be declared. The available ports are USB logical ports and network printers.

Select the COM port dialog box (menu [Configuration] - [Ports]-[xxx]). For example, for the Usb1 port:



Set the "Active" parameter to "COM port" or "printer and COM". Then select "COM Port Settings". The following box is displayed:



Description of the parameters of this box:

- **Name of the redirected port:** choice of the mnemonic under which the TSE server recognizes this port (from COM1 to COM255).
- **ICA polling:** not relevant in TSE

**Note:** in the case of redirection of an LPT port, set the parameter "Activate" to "LPT port" or "printer and LPT". The LPT port configuration dialog only proposes the port name (LPT1 by default).

The declaration is finished. To redirect the COM / LPT port see the next chapter.

### c) Resource redirection

The following box is displayed:



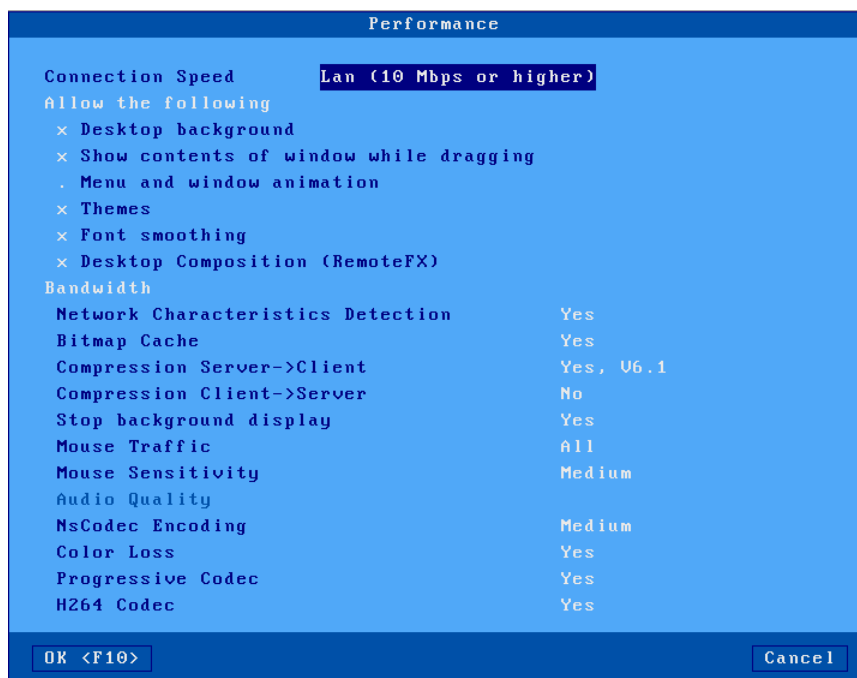
Description of the parameters of this box:

- **Redirected printers:** a list allows you to select the printer(s) to advertise to the Windows server. The list consists of the following entries:
  - **All:** all RDP / ICA printers are redirected.
  - **None:** no printer is redirected.
  - **Printer name (port):** the rest of the list is composed by the name or names of the RDP / ICA printers. This allows you to choose a single printer to redirect.
- **Default printers:** optional redirected printer as default printer.
- **Clipboard:** management of copy / paste intersession.
- **Touch Screen:** Redirection of the touch screen in multitouch mode. If this choice is "no", the screen is not redirected, but it is managed locally like a mouse.
- **Audio:** activation of the classic audio redirection mode ("play-only" or "play and record"). The audio quality (and therefore the necessary bandwidth) can be set in the 'Bandwidth' dialog box. See the next chapter. A "play on remote computer" mode allows audio to be redirected to the server speaker.
- **USB drive:** activation of storage device redirection. Access authorization is specified in parentheses (see chapter [A.7.2.c](#)).

- **Smartcard:** activation of smartcard reader redirection.
- **Auto-Connection:** Auto-connection of session when a smart card is inserted
- **COM / LPT ports:** a list allows you to select the COM port(s) to offer to the Windows server. The list consists of the following entries:
  - **All:** all ports are redirected.
  - **None:** no ports are redirected.
  - **xxx port:** the rest of the list is composed by the COM or LPT. This allows you to choose a single port to redirect.
- **USB ports (RemoteFX):** activation or deactivation of the USB RemoteFX redirection (works only from W2012-R2 server or a Windows 8. For more information on eligible devices see chapter [3.2.5.a](#).
  - **Include audio management (Lan):** this option allows you to manage audio in "USB port redirection" mode as opposed to classic mode (see above). In this case the audio device is dedicated to this session and "audio" parameter is greyed out.

### 5.1.7 - Performance

The following box is displayed:



The first parameter is used to set the "**Connection speed**" (Lan, Wan ...). This parameter is sent to the server at the time of the connection, which allows it to adapt the connection to the chosen speed.

Depending on this choice, user experience features are enabled or not by default. To authorize a functionality, place an "x" in front of the corresponding parameter:

- **Desktop Background:** sets whether or not the user can choose his wallpaper.
- **Show content of windows while dragging:** the user can choose to display the content of windows when moving or resizing.
- **Menus and windows animation:** the user can choose to have animated menus
- **Themes:** the user can choose a different theme (ie a desktop appearance) than the default theme.
- **Font Smoothing:** better appearance of fonts.

- **Desktop composition (RemoteFX)** (only available with RemoteFX - See chapter [5.1.5](#)): allows you to get the maximum experience of the Aero theme (transparent window border, 3D selection of applications, display of a thumbnail in the taskbar ...).

These features must also be authorized at the Windows server level and are generally very bandwidth intensive.

**Note:** if the 'Connection speed' option is set to 'auto-detection', these parameters are not taken into account. It is the server which automatically determines the value of each.

Description of the 'Bandwidth' parameters of this dialog box:

- **Network characteristics detection:** this option allows the server to evaluate the bandwidth and RTT (Round Trip Time). The detected values are displayed in the session information box (see chapter [4.8.1](#))  
**Note:** this parameter is forced to "yes" if the "Connection speed" option is set to "auto-detection".
- **Bitmap cache:** activating the bitmap cache allows the thin client to store images (icons, buttons, etc.) in memory for later retrieval. This optimizes the performance of the thin client and decreases the traffic between the server and the thin client. The three possible values are:
  - **no:** no cache
  - **yes:** the cache is initialized for each session
  - **yes, permanent** (default): the content of the cache is not erased at the end of a session. This can save bandwidth for the next session.
- **Compression Server-> Client:** enabling compression reduces the amount of data sent from the server to the client. Possible values: "no", "yes, V5.2", "yes, V6.0", and the default value "yes, V6.1". This last value allows the thin client to advertise all supported types.
- **Compression Client-> Server:** enabling compression reduces the amount of data sent by the client to the server.
- **Stop background display:** with "RemoteFX Adaptive Graphics" encoding, the display of an RDP session that is not displayed continues to be updated. It is possible to deactivate this to optimize the bandwidth. The data flow is stopped when the session is not in the foreground and resumed when the session returns to the foreground. The screen display is then redrawn by the server because it was not maintained when in back ground.
- **Mouse traffic:** the possible responses are:
  - **all:** standard behavior; all mouse events (clicks and movements) are sent to the Windows server.
  - **clicks:** only click events are sent to the Windows server. Interesting in the case of a slow connection, this significantly reduces the bandwidth. However, the appearance of the mouse cursor is not updated in real time.
- **Mouse sensitivity:** with a "low" mouse sensitivity, fewer mouse events are sent to the Windows server. This optimizes the bandwidth but the mouse appears more jerky.
- **Audio quality:** audio quality has an impact on bandwidth. In case of remote connection, it is preferable to set a "low" audio quality.
- **NsCodec encoding:** (32 bpp only): this encoding optimizes bandwidth and it is possible to choose a "medium" or "high" quality.
- **Color loss:** (32 bpp only): this capacity allows the server to optionally optimize bandwidth by reducing the quality of a bitmap.
- **Progressive codec:** (RemoteFX Adaptive Graphics only): this capacity makes it possible to optimize the bandwidth by displaying certain bitmaps in several passes (each step increases the quality of the bitmap).
- **H264 codec:** This codec is especially relevant for displaying video, it allows the thin client to play a full screen video smoothly.

For this it is helpful that the management of the H264 is configured on the server and that the server has a dedicated graphics card (s) so as not to be completely saturated by sending the video.

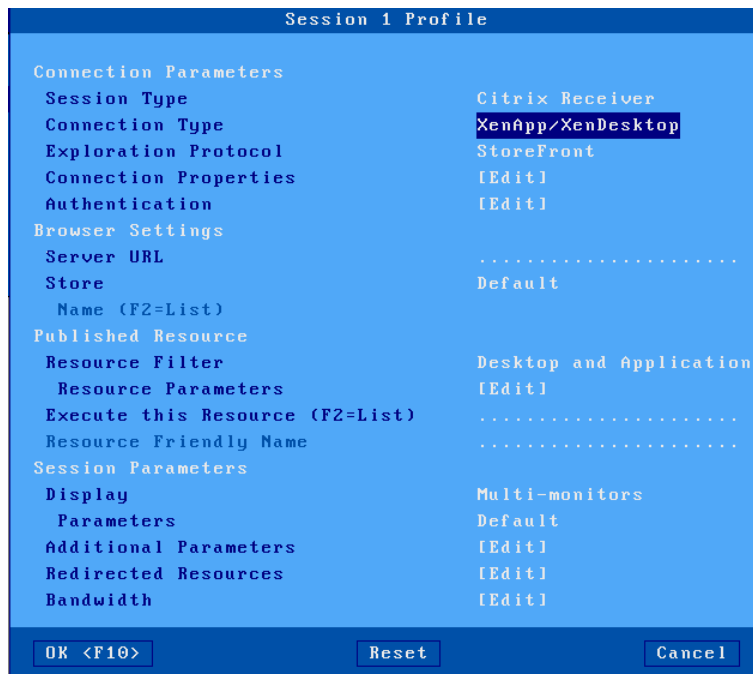
**Note:** Only one session (selectable) can be configured to use H264, by default it is the first.

**Attention:** This Codec do not match with the 1920x1200 graphical resolution

## 5.2 - CITRIX RECEIVER SESSION

The "ICA compatible" protocol of Axel thin clients makes it possible to establish connections on Metaframe XP, Presentation server 4, Presentation server 4.5, XenApp, XenDesktop and VDI-in-a-Box servers.

To configure a Citrix Receiver session, enter the setup, select the menu **[Configuration] - [Sessions] - [Session X]** (where X is the session number) and select the "Citrix Receiver" session type. The following dialog box is displayed:



The 4 sections of this dialog box are described in the following chapters.

### 5.2.1 - "Connection parameters and Browser Settings" section

- Connection types: A Citrix Receiver session can be associated with one of the following connection types:
  - **XenApp / XenDesktop**: resource management is carried out using the "StoreFront", "WEB Interface" or "TCP / IP + http" protocols.
  - **Metaframe**: resource management is carried out using the "WEB Interface" or "TCP / IP + http" protocols.
  - **VDI-in-a-Box**: desktop management is only carried out using the "WEB Interface" protocol.
  - **Direct access**: Direct access to server or VDA. See chapter [5.1.2.d](#).
- **Exploration protocol**: These protocols are detailed on different chapters "StoreFront" see [5.2.1.a](#), "WEB Interface" see [5.2.1.b](#) and "TCP / IP + http" see [5.2.1.c](#).
- **Connection properties**: see chapter [5.2.4](#).
- **Authentication**: see chapter [5.2.5](#).

#### a) StoreFront protocol

The recent versions of Citrix are all based on the StoreFront protocol.

Here is part of the displayed dialog box:





**Server URL:** the syntax is [https://]server[: port]

- **https:** use is optional (by default http)
- **server:** name or IP address of the server **StoreFront** or the **Citrix Gateway**
- **port:** optional TCP port (default 80 for http and 443 for https)

**Store:** a StoreFront can host several stores. The store name can be chosen in different ways:

- **Default:** the first store found will be used
- **Choose now:** the store name is freely entered or selected from a list (F2). Local authentication may be necessary (user name, password and domain) to access the published resources (enumeration and launch). See chapter [5.2.2](#).
- **Choice at connection:** All stores are displayed in a list at each connection.

**b) WEB Interface and VDI-in-a-Box protocols**

**Important:** On the Citrix farm, the WEB Interface must be configured with a site **PNAgent**.

Here is part of the displayed dialog box:



**Server URL:** the syntax is [https://]server[:port] [/config].

- **https:** use is optional (by default http)
- **server:** name or IP address of the WEB interface server
- **port:** optional TCP port (default 80 for http and 443 for https)
- **/ Config:** optional path to find the configuration file (by default "/Citrix/PNAgent/config.xml")

Local authentication is required (user name, password and domain) to access the published resources (enumeration and launch). See chapter [5.2.2](#).

**c) TCP / IP + HTTP protocol**

This is the old method of accessing the farm which is carried out by one of the farm's servers on the XML port. Pre-authentication can be used (username, password and domain) to filter resources (enumeration and launch).

Here is part of the displayed dialog box:



**Server and XML port** : the syntax is server [: port]

- **server**: name or IP address of one of the servers on the farm
- **port**: optional XML port (default 80)

**Note** : the value of the XML port can be found in the Citrix administration console or in the registry: [HKLM] - [System] - [Current Control Set] - [Services] - [Ctxhttp] - [TCPPort].

**d) Direct access**

This type of connection allows you to open a Citrix session on one of the farm's servers (without going through the publication of resources).

This is the displayed dialog box:

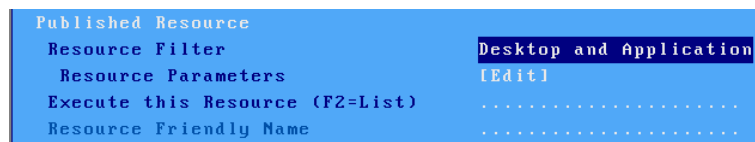


**Server**: chosen from the list of servers (see chapter 3.1.4). A new server (DNS) or a new IP address can be entered directly, which will automatically add the server list.

**5.2.2 - "Published Resource " section**

A published resource can be a Citrix desktop or application.

This is part of the displayed dialog box:



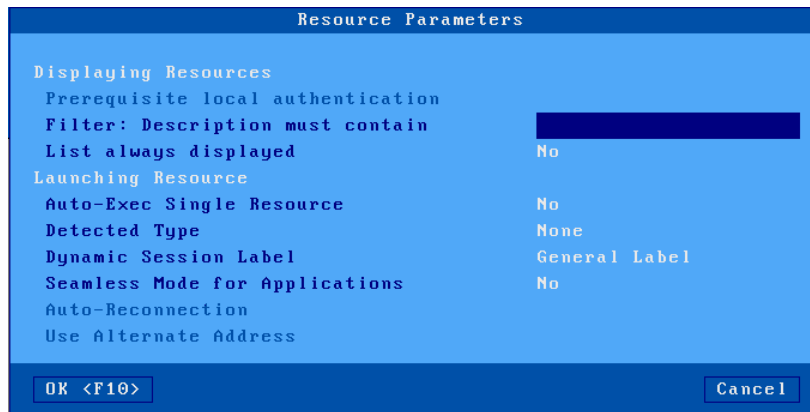
**Note**: the published resource capacity is not available for the "Direct access" connection type.

**Resource filter:** depending on the type of session and connection, the resources can be sorted by different values

- **Desktop and applications:** StoreFront", "WEB Interface" and "TCP / IP + http"
- **Desktop only:** "StoreFront", "WEB Interface", "TCP / IP + http" and "VDI-in-a-Box".
- **Application only:** "StoreFront", "WEB Interface" and "TCP / IP +http".
- **Servers:** "TCP / IP + http".

**Execute this resource:** allows you to specify a resource to run when opening the Citrix session. If the resource name is empty, a list of resources will be displayed on connection. The name of the resource can be entered manually or retrieved from a list (by pressing <F2>).

The content of the list is set by the "Resource parameters" dialog box:



### ***Resource display.***

These parameters are used for the enumeration of resources:

- **Prerequisite local authentication:** The advantage of local authentication is to display the resources accessible to a given user (and not all the resources defined in the farm). This authentication, optional in "TCP / IP + http", is mandatory in "StoreFront" and "WEB Interface".
- **Filter:** the description must contain: this parameter allows you to filter the published resources by listing only those whose "description" contains the character string entered.
- **List always displayed:** This option allows a resource has been selected, to display the list of resources with this resource selected by default.

### ***Launching Resource.***

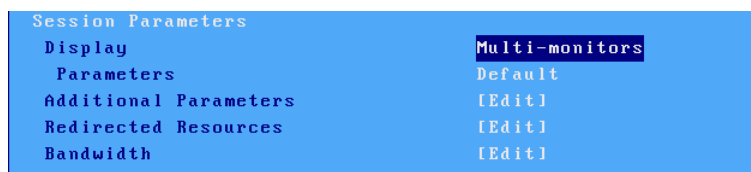
These parameters are used during the execution of a resource:

- **Auto-Exec single resource:** when the list of available resources has only one entry, this single resource can be executed automatically
- **Type detected** (available if local authentication is active): the "disconnected" and "disconnected and active" sessions can be listed. The "Automatic reconnection" parameter allows you to execute them automatically.
- **Dynamic Label sessions** the label appears in the taskbar and the local office. Two possibilities:
  - **General label:** this is the label defined in the "property" dialog box Connection
  - **Username:** this is the username after authentication
- **Applications in seamless mode:** seamless mode is when part of the windowing function is passed to the thin client (for example, the application icons are displayed in the Axel task bar).

- **Use secondary IP address:** activate this parameter to manage address translation (NAT). For more information, see note CTX039746 in the Citrix knowledge base.)

### 5.2.3 - “Session Parameters” section

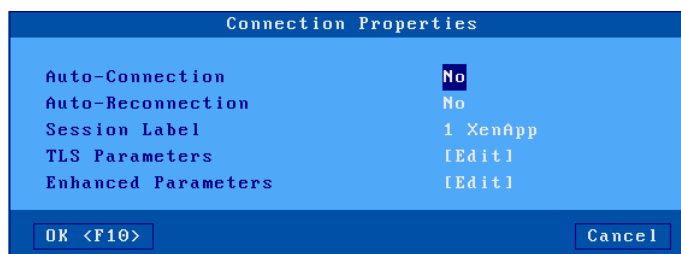
Here is the part of the box displayed dialog:



- **Display Parameters:** see chapter [5.2.6](#).
- **Additional parameters:** other parameters (connection name, time zone management, etc.). See chapter [5.2.7](#).
- **Redirecting Resources:** setting the redirection of printers and auxiliary ports. See chapter [5.2.8](#).
- **Bandwidth:** Dialog for managing and optimizing bandwidth. See chapter [5.2.9](#).

### 5.2.4 - Connection properties

The following box is displayed:

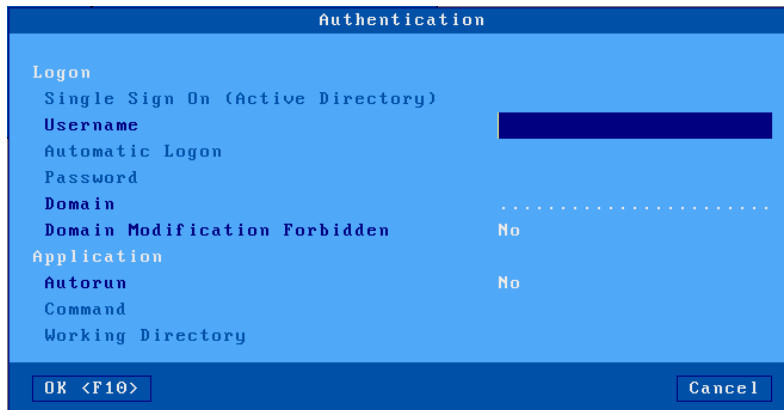


Description of the parameters of this box:

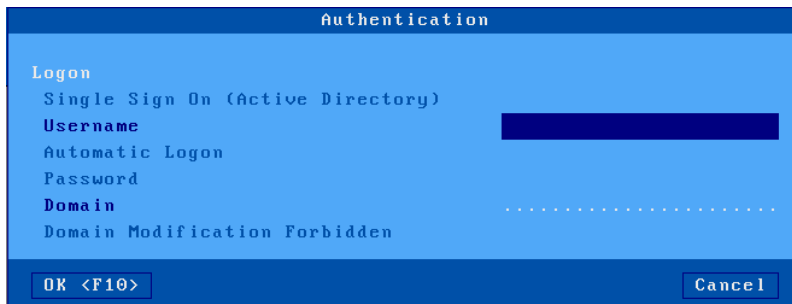
- **Auto-Connection:** if this parameter is set to 'yes', during power-up, the thin client automatically opens the session. Otherwise, the connection must be opened by the user.
- **Automatic Reconnection:** if this parameter is set to 'yes', after a disconnection, the thin client automatically opens a new session. Otherwise, this reconnection must be opened by the user.
- **Session Label:** The label (14 characters max) is used to identify the session on the office or the taskbar.
- **TLS Parameters:** Security-related parameters for this connection. See chapter [3.3.3](#).
- **Enhanced Parameters:** There is generally no need to modify these parameters which are pre-set to be optimized for the type of session selected. See annex [A.7.3](#).

**5.2.5 – Authentication**

The dialog box varies depending on the Connection type:



Type "Direct Access"



Other types of connection

**"Logon" section:**

These options are used to configure user authentication:

- **Single Sign On (Active Directory):** allows you to use the Active Directory logon for session authentication. If this option is set to "yes", all the other options in the Logon section are disabled (grayed out).
- **User Name:** default user offered on the login screen. (Can be left blank)
- **Logon Automatic:** if "yes", the login process is automated.
- **Password:** accessible if "Automatic logon" is "yes". Password can be pre-entered
- **Domain:** default value proposed on the logon screen.
- **Prohibit modification of the domain** (not available for StoreFront): in the case of local authentication (with the Axel logon dialog), modification of the domain name may be prohibited.

**"Application" section** (only for the "Direct access" type):

A program can be automatically launched after the logon phase (rather than entering the Windows desktop).

- **Autorun:** An application can be launched in normal or 'seamless' mode. (In seamless mode, part of the windowing is transferred to the thin client)
- **Command:** path and name of the program to be executed.  
Example: % SystemRoot% \ system32 \ cmd.exe
- **Working directory:** Program working directory.

Example: D: \

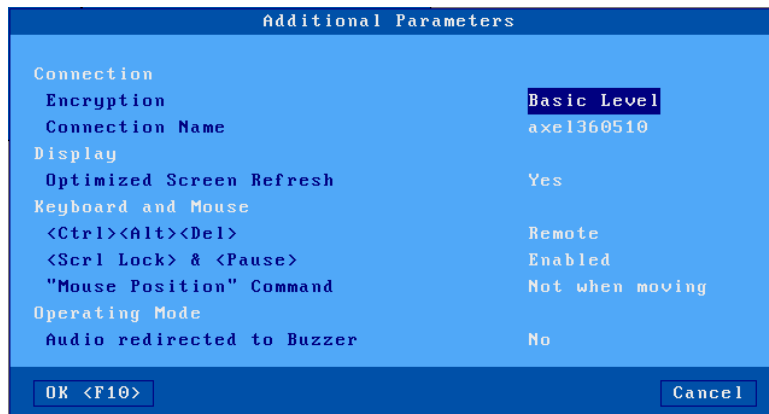
### 5.2.6 - Display parameters

Refer to chapter [5.1.4](#) "

Display parameters" of a TSE / RDS session, the parameters are identical.

### 5.2.7 - Additional parameters

The following box is displayed:



Description of the parameters of this box:

- **Encryption:** the types of encryptions managed by the thin client are:
  - "Basic level ": Metaframe default encryption.
  - "RC5": RC5 encryption with key lengths from 40 to 128 bits
- **Connection Name:** This character string identifies the thin client to Windows (see the environment variable "CLIENTNAME").  
**Note:** By default, this is the name of the thin client (see chapter [3.1.1.a](#)). If the "Terminal name" option is selected in the list of *DHCP options*, *this field is inaccessible*.
- **Optimized screen refresh:** allows a more fluid display for videos (especially for those in flash mode, ie YouTube).
- **<Ctrl><Alt> <Delete>:** two modes for managing this key combination are available:
  - "Local": interpreted by the thin client and is used to power off (see chapter [4.9](#))
  - "Remote": interpreted by the Windows server (access for example to the task manager).
- **<Scroll Lock> & <Pause>:** activate or not these two keys
- **"Mouse Position commands:** the Citrix server sends regular cursor positioning Mouse commands. By default, the thin client ignores these commands if the user is moving the mouse. For compatibility issues with certain software, it is possible to set this option to "Always accepted".
- **Audio redirected to buzzer:** this mode redirects RDP audio commands to the thin client's buzzer.  
**Caution:** Using this function may cause unwanted effects

## 5.2.8 – Resource Redirection

Resource redirection is used to announce one or more local resources to the Windows server. These resources are only available to the thin client user. They are created on the Windows server when the session is connected and removed when the session is disconnected.

The resources managed are:

- **printers:** before being redirected printer must first be enabled in terms of its physical port connection. See chapter [5.2.8.a](#) then chapter [5.2.8.c](#).
- The **COM / LPT ports:** before redirecting a port must first be enabled at the physical port. See chapter [5.2.8.b](#) then chapter [5.2.8.c](#) and [5.2.8.d](#).
- **Storage devices:** see Chapter [5.2.8.c](#)
- **Smart Card Readers:** see Chapter [5.2.8.c](#)
- **Audio Management:** see chapter [5.2.8.c](#)

### a) redirected printers

Refer to Section 5.1.6.a

"Declaration of redirected printers" identical to TSE / RDS printer redirection. To redirect the printer, see chapter [5.2.8.c](#).

### b) Declaration of redirected COM / LPT ports

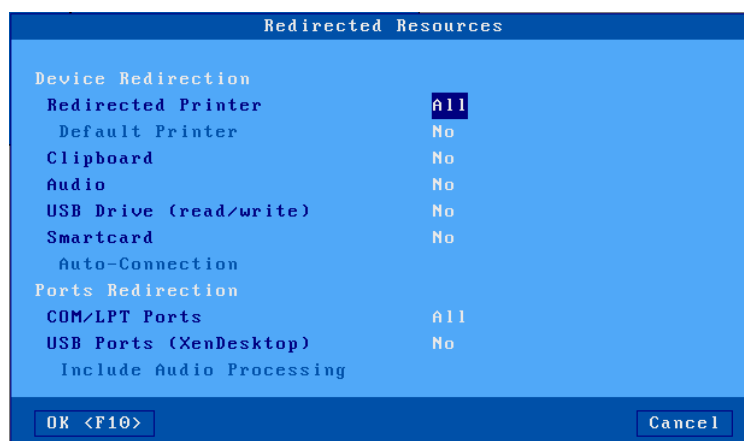
Before being redirected a COM port must be declared. The available ports are USB logical ports and network printers. Refer to chapter [5.1.6.b](#).

Declaration of redirected COM / LPT ports" is the same as with a TSE / RDS session. To redirect the COM port, see the following chapter [5.2.8.c](#). Then chapter [5.2.8.d](#) for port reassignment.

### c) Redirecting resources

To redirect resources within a session, select the session profile (menu **[Configuration] - [Sessions]-[Session X]**).

In this box, select 'Resource Redirection'. The following box is displayed:



Description of the parameters:

- **Redirected printers:** Allows you to select the printer (s) to redirect to the Windows server. The list consists of the following entries:
  - **all:** all RDP / ICA printers are redirected.
  - **none:** no printer is redirected.
- **Printer name (port):** the rest of the list is composed by the name or names of the RDP / ICA printers. This allows you to choose a single printer to redirect.
- **Default printer:** select of one of the redirected printers as default printer.
- **Clipboard:** for "copy / paste" between sessions.
- **Audio:** activation (play-only or play and recording). The audio quality (and resulting bandwidth) can be set in the 'Bandwidth' dialog box. See the next chapter.
- **USB drive (read/write):** activation of storage device access is specified in parentheses (see chapter [A.7.2](#)).
- **Smart cards:** activation of smart card reader redirection.
- **Auto-Connection:** Automatically connected when a smart card is inserted into the Card reader
- **COM/LPT ports:** a list allows you to select the port or ports to be announced to the Windows server. The list consists of the following entries:
  - **all:** all RDP / ICA ports are redirected.
  - **none:** no port is redirected.
  - **xxx (port):** a list is shown allowing you to choose the port to redirect.
- **USB ports (XenDesktop):** whether or not to activate USB redirection under Citrix. For more information on eligible devices see chapter [3.2.5](#).
- **Include audio processing:** always disabled with Citrix.

#### d) Reassignment of COM / LPT ports

Once redirected, the COM ports of the thin client must be assigned to the COM ports of the Windows server. This connection is not automatic. It must be performed **from** the ICA thin client, after the logon, using the "commands **change client**" or "**net use**".

Example: for COM4 port of the server becomes COM1 port of the thin client

```
net use com4: \\ client \ com1:
or
changes client com4: com1:
```

**Note:** this assignment is only valid for this thin client. In this example, COM4 port is not visible to other users.

☺ : Modification of a user account to automatically launch the "command net use":

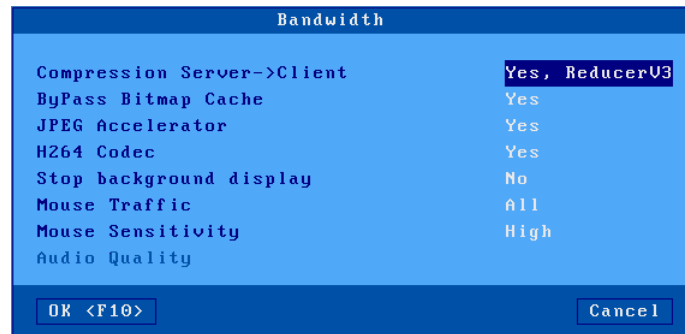
- Create a Netlogon directory and make it shareable.
- Create in the Netlogon.directory a file "Myscript.bat" Insert into this file "net use" command.
- In the properties of the user profile, select the 'profile' tab and enter "myscript.bat" in the "logon script" field.

For more information, search for "Netlogon" in Windows Help.



### 5.2.9 - Bandwidth management

The following box is displayed:



Description of the parameters:

- **Compression servr -> Client:** enabling compression allows the Windows server to optimize bandwidth. The "Reducer V3" option can also contribute in some cases.
- **Bypass Bitmap Cache:** this option allows the server to display bitmaps directly without having to store them in the cache beforehand. The thin client announces this feature, it is the server which decides whether it is used or not.
- **JPEG Accelerator:** activating this function announces to the Windows server that the thin client is able to decode and display JPEG files. This optimizes bandwidth.
- **Stop Background display:** with XenApp / XenDesktop, the display of a session in the background is still updated. It is possible to deactivate this to optimize the bandwidth. The data flow is stopped when the session is in the background and resumed when the session returns to the foreground.
- **Mouse Traffic:** the possible options are:
  - **all:** standard behaviour; all mouse events (clicks and movements) are sent to the Windows server.
  - **clicks only:** click events are sent to the Windows server. This significantly decreases the bandwidth. However, the appearance of the mouse cursor is not updated in real time.
- **Mouse sensitivity:** with "low" mouse sensitivity, fewer mouse events are sent to the server. This optimizes the bandwidth the mouse appears more jerky.
- **Audio quality:** quality has an impact on bandwidth. In case of remote a connection it may be preferable to set a low quality.

## 5.3 - REMOTEAPP AND CITRIX RECEIVER OFFICES

Two operating modes for the application office:

- **RemoteApp**: connection to a Microsoft 2008R2 server minimum
- **Citrix Receiver**: connection to a Citrix farm.

The principle the user, after authentication, finds the icons of the applications published for his user account on the desktop of the thin client.

The launch of a published application is done simply by clicking on the corresponding icon. Depending on the operating mode chosen, a dedicated RDP or ICA session is automatically opened for the management of this application.

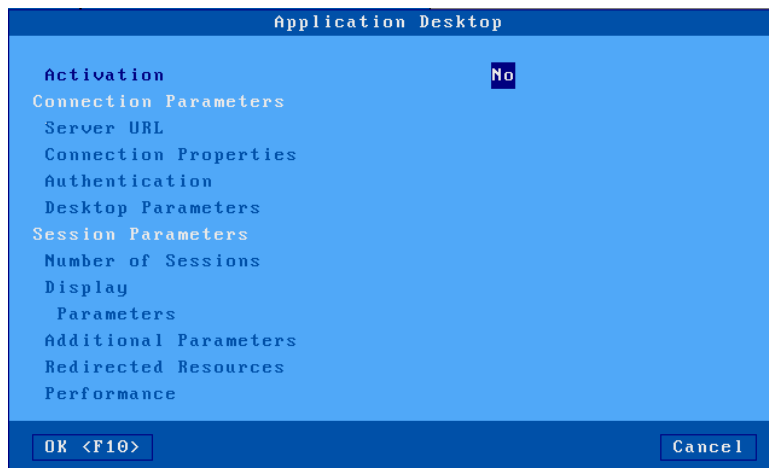
**Note:** for more information on this concept see chapter [3.3.1](#).

### 5.3.1 - Activation of the "Application desktop"

Enter the setup of the thin client (**<Ctrl><Alt> <Esc>**). The configuration of the application desktop is accessible via the menu **[Configuration] - [Sessions]**. Select either **[Microsoft RemoteApp Desktop]** or **[Citrix Receiver Desktop]**.

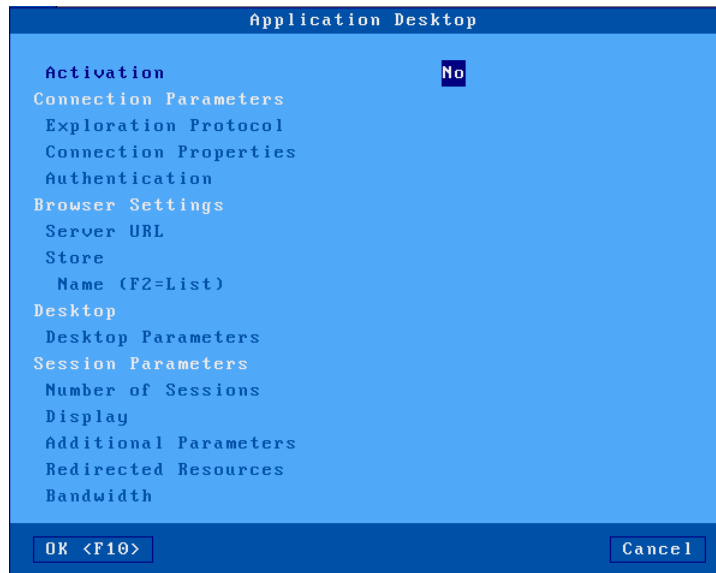
**Note:** only one type of desktop (RemoteApp / Citrix Receiver) can be activated at a time.

For a Microsoft RemoteApp desktop, the following dialog box is displayed:



Set "Activation" to "yes" to activate the configuration parameters.

For a Citrix desktop, the following dialog box is displayed:



Set "Activation" to "yes" to activate the configuration parameters.

**5.3.2 - "Connection parameters" section**

Here is part of the displayed dialog box:

For a Microsoft RemoteApp desktop



For a Citrix desktop



**a) Exploration protocol and server**

The parameter **Exploration protocol** is available only for Citrix (for more information, see chapter [5.2.1](#)). The options are:

- **StoreFront**: standard access to XenApp / XenDesktop of current release.
- **WEB Interface**: access to a Citrix WEB Interface server where a "PNAgent" site has been defined.
- **TCP / IP + HTTP**: access to an old Citrix farm through its XML port.

The description of the location of the server depends on the exploration protocol:

For "RemoteApp" offices

- **Server URL:** the syntax is [https: //] server [: port] [/ config].
  - **https:** use is optional (by default http)
  - **server:** name or IP address of the server
  - **port:** optional TCP port (default 80 for http and 443 for https)
  - **config:** optional path for the configuration file.  
Default: /Citrix/PNAgent/config.xml for "Citrix WEB Interface"

For "Citrix StoreFront" or "WEB Interface" desktops

- **Server URL:** the syntax is [https: //] server [: port] [/ config].
  - **https:** use is optional (by default http)
  - **server:** name or IP address of the server
  - **port:** optional TCP port (default 80 for http and 443 for https)
  - **config:** optional path for the configuration file.  
Default: /Citrix/PNAgent/config.xml for "Citrix WEB Interface"

For "Citrix TCP / IP + http" offices

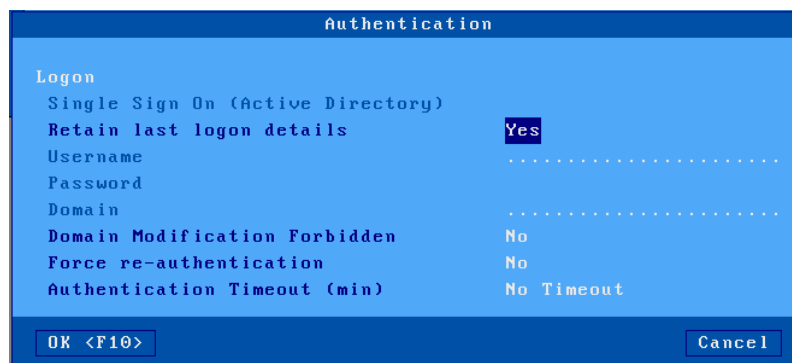
- **Server and XML Port:** the syntax is server [: port].
  - **server:** name or IP address of the server
  - **port:** optional XML port (default 80)

### ***b) Connection properties***

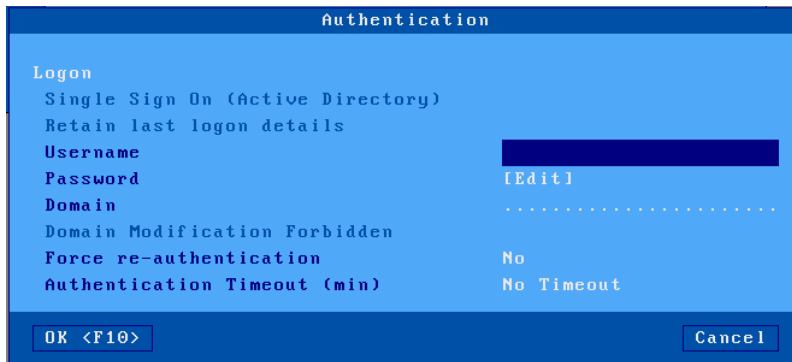
Refer to chapter [5.1.2](#) "Connection properties" of a TSE / RDS session, the parameters are identical.

### ***c) Authentication***

The following box is displayed for a Microsoft RemoteApp desktop:



The following box is displayed for a Citrix desktop:



Description of the parameters of this box:

- **Single Sign On (Active Directory):** allows the use of the Active Directory logon for session authentication. If this option is set to "yes", all the other options in the Logon section are disabled (grayed out).
- **Retain last logon details** (RemoteApp only): Lets the last used user name and domain to be prompted.
- **Username:** default value proposed on the logon screen.
- **Password:** if the password is entered, the logon will be done automatically.
- **Domain:** default value proposed on the logon screen.
- **Domain Modification Forbidden:** this parameter is used to prohibit the user from changing the domain name.
- **Force re-authentication:** if this option is activated, the user will have to authenticate each time a published application is launched (either user name or pin code).
- **Authentication timeout (min):** if a deadline is specified, the thin client will log out to the desktop after this deadline. A new logon will be necessary.

**d) Desktop Parameters**

The following box is displayed for a Citrix desktop:



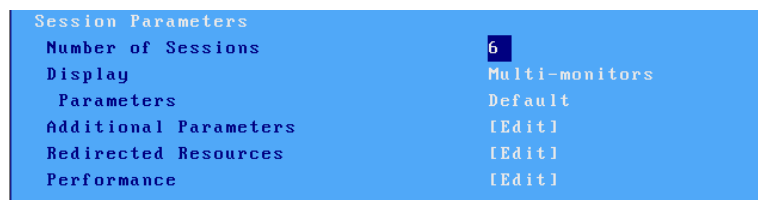
Description of the settings for this box:

- **Filter: description must contain:** (only for Citrix): this parameter makes it possible to filter the published applications by listing only those whose description contains the character string entered.
- **Number of Rows for display of names:** specifies the number of lines (between 1 and 5) used to display the name of the application under its icon.

- **Resource filter:** allows you to filter desktops and applications.
- **Resource display Mode:** if the "desktop and applications" resource type is selected, this parameter is used either to display resources at the same level or in two different directories.
- **Auto-Exec Single Resource:** if after the application desktop logon, only one published resource is listed, this parameter allows it to be automatically executed.
- **Automatic Sessions Reconnection:** (only for Citrix and if the previous parameter is not activated): this parameter also called "smooth roaming", allows a user to find his sessions when he reconnects from another workstation. Reconnected sessions can be of the "disconnected" or "disconnected and active" type.
- **Force one resource per session:** if this parameter is active, each execution of a published application generates the creation of an RDP / ICA session (6 maximum). Otherwise, the thin client tries to reuse an existing RDP / ICA session to launch the application in "seamless" mode (if the application is not a "desktop" and if a session is already connected to the same server).
- **Dynamic session label** (only if the previous parameter is not activated): this label appears in the taskbar. Four possibilities:
  - **General Label:** this is the label defined in the "Connection property" dialog box
  - **First Application Label:** it is the name of the first application launched in the session
  - **Last application Label:** this is the name of the last application launched in this session
  - **Server Name:** this is the DNS name or the IP address or the name in the server table.
- **Use Alternative Address** (Citrix TCP / IP + HTTP only): activate this parameter to manage address translation (NAT). For more information, see note "CTX039746" in the Citrix knowledge base.

### 5.3.3 - "Session parameters" section

Here is part of the dialog displayed for a Microsoft RemoteApp desktop:



Description of the parameters of this box:

- **Number of sessions:** number of RDP / ICA sessions reserved for published applications created from the desktop of the thin client.
- **Display:** Refer to chapter [5.1.4](#) "Display parameters" of a TSE / RDS session, the parameters are identical.

The following parameters are used by RDP / ICA sessions to run published applications.

- **Additional parameters:** see chapter [5.1.5](#) for RemoteApp and [5.2.7](#) for Citrix.
- **Redirected Resources:** see chapter [5.1.6](#) for RemoteApp and [5.2.8](#) for Citrix.
- **Performance** or **Bandwidth:** see chapter [5.1.7](#) for RemoteApp and [5.2.9](#) for Citrix.

Notes:

- After validation, the sessions reserved for the application desktop become inaccessible.
- Activating the application desktop activates the taskbar. This allows you to switch sessions and return to the local desktop of the thin client with the mouse.

## 5.4 - "VMWARE VIEW CLIENT" SESSION

A "VMware View Client" session allows the thin client to be integrated into a VMware workstation virtualization environment with the "RDP" connection protocol.

### 5.4.1 - Configuration of the session

To configure enter the setup (<Ctrl><Alt> <Esc>) then **[Configuration] - [Sessions] - [Session X]** (where X is the session number) and select the session type "VMware View Client". The following dialog box is displayed:

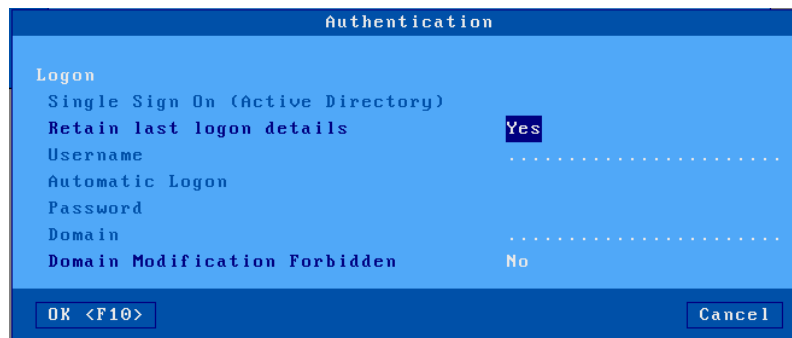


Enter the following parameters:

- **Server URL:** the syntax is [https: //] server [: port].
  - **https:** use is optional (by default http)
  - **server:** name or IP address of the View server
  - **port:** optional TCP port (default 80 for http and 443 for https)
- **Connection properties:** see chapter [5.1.2](#).
- **Authentication:** activation automatic login procedure. See subsection [5.4.1.a](#).
- **Menu of available offices:** dialog allowing the configuration of the menu where the list of virtual offices will be displayed. See sub chapter [5.4.1.b](#).
- **Display parameters:** see chapter [5.1.4](#).
- **Additional parameters:** dialog box for certain RDP parameters. See chapter [5.1.5](#).
- **Resource redirection:** configuration of the redirection of certain resources (printers, USB drives, etc.) See chapter [5.1.6](#).
- **Performance:** dialog box allowing the management and optimization of bandwidth. See chapter [5.1.7](#).

### a) Authentication

The authentication dialog box is as follows:

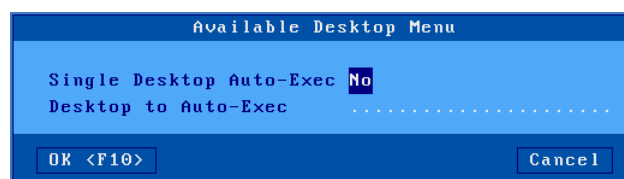


Description of the parameters of this box:

- **Single Sign On (Active Directory)**: allows you to use the Active Directory logon for session authentication. If this option is set to "yes», all the other options in the Logon section are disabled (grayed out).
- **Retain last logon details**: allows saving the user's name and domain used previously on the login screen.
- **Username**: default value of the user's name proposed.
- **Automatic login**: if this parameter is "yes", the login phase is automated and the password can be entered.
- **Password**: accessible if "Automatic login" is "yes".
- **Domain**: default value proposed on the logon screen. (Use capital letters)
- **Domain Modification Forbidden**: this parameter is used to prohibit the user from entering a different domain name.

### b) Menu of available offices

After authentication, the list of available offices is displayed. This dialog box allows the configuration of this list:



In the case where the list of offices has only one entry, the parameter **Auto-exec single desktop** allows this desktop to be automatically selected to establish a connection. This avoids presenting a single item list to the user.

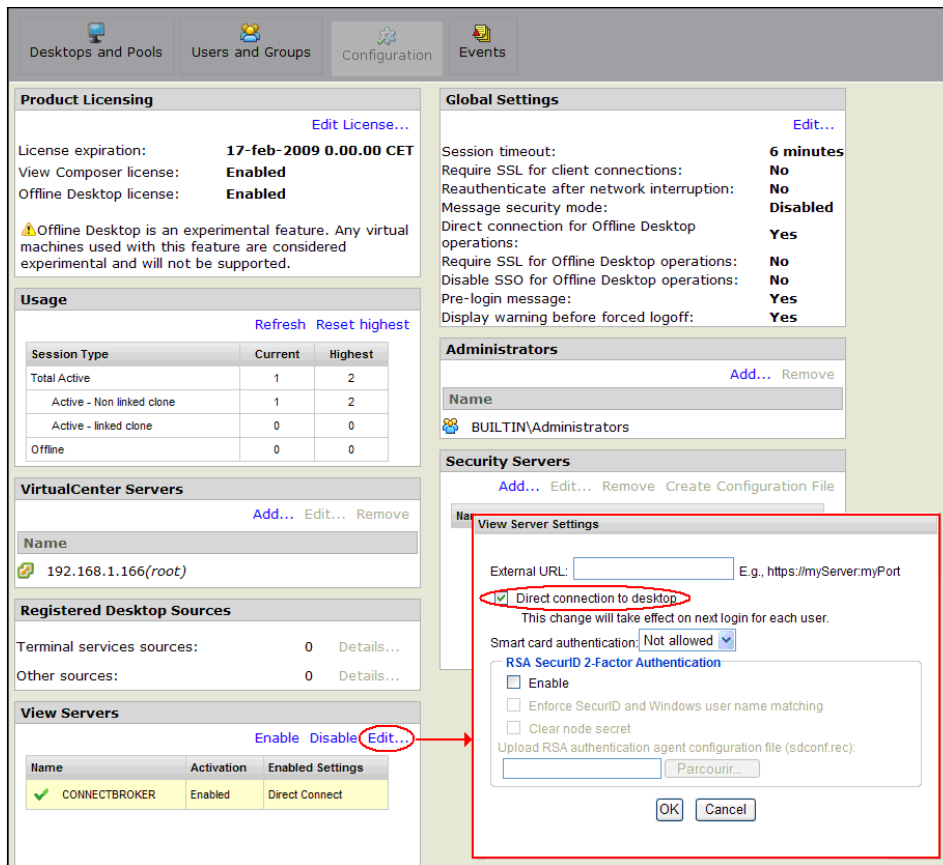
The "parameter **Auto-exec of this desktop**" allows you to specify a desktop name. If this desktop is in the list, it is automatically run.

### 5.4.2 - Configuration of the 'View Manager

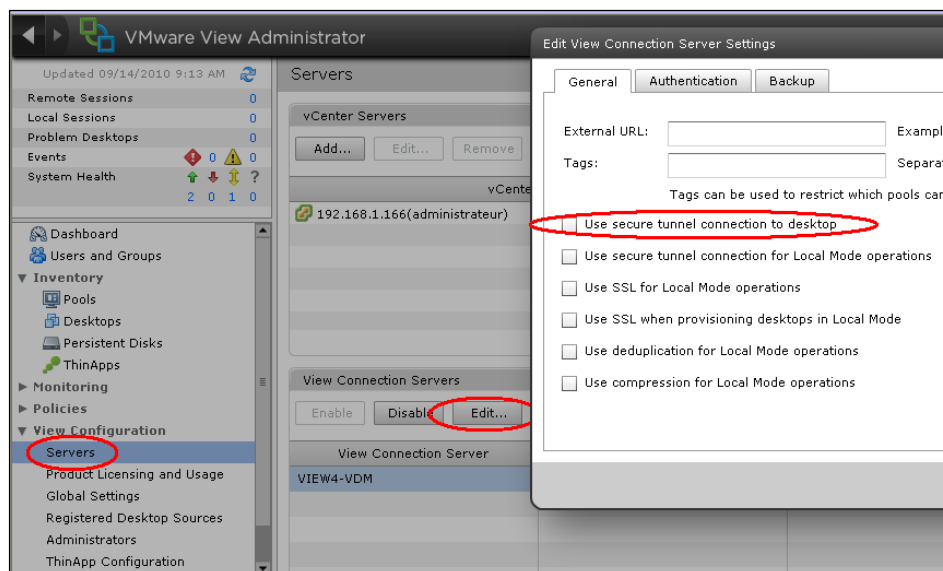
To use an Axel thin client the '**Direct connection to the desktop**' must be activated. (after the authentication phase, the thin client no longer goes through the 'View Manager ". To check (or modify) this parameter, enter the "View Manager" configurator and go to the "View server" configuration.

With VIEW 4, activate the "Direct connection to desktop" option:

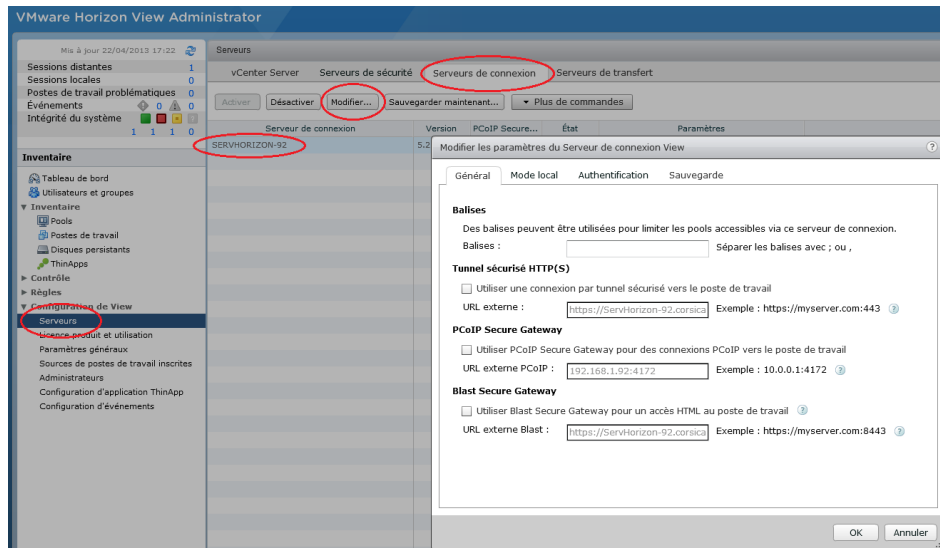




With VIEW 4.5, deactivate the "Use secure tunnel connection to desktop" option:



With "VIEW Horizon", deactivate the "HTTP (S) secure tunnel" option:

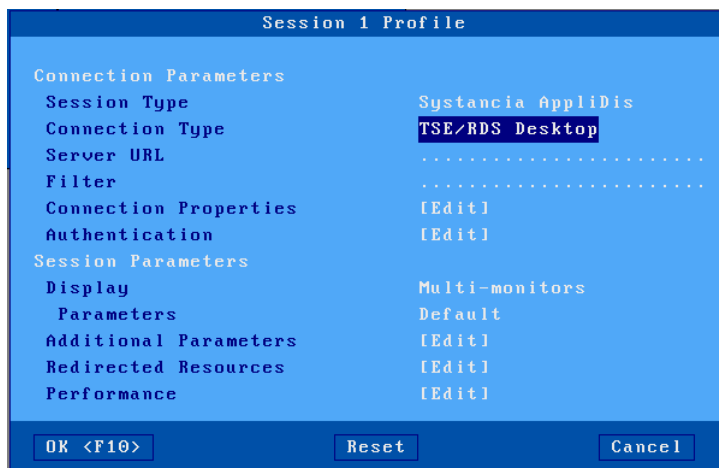


### 5.5 - "SYSTANCIA APPLIDIS" SESSION

The AppliDis solution allows simplified administration of TSE / RDS servers. The Axel thin client offers a dedicated session type.

**This type of session is only available with firmware option "APD",** please contact us to obtain this type of firmware if necessary.

To configure enter the setup (<Ctrl><Alt> <Esc>) select the menu **[Configuration] - [Sessions] - [Session X]** (where X is the session number) and select "Systancia AppliDis" session. The following dialog box is displayed:



Enter the following parameters:

- **Connection type:** choice from a list:
  - **TSE / RDS desktop:** for connections on servers using only AppliDis load balancing
  - **Virtual Desktop:** a secure desktop with applications opened only by the icons and the Systancia menu
  - **Session marker:** allows you to track an application (and not a desktop) and retrieve it regardless of the TS server where it is run.

- **Server URL:** the syntax is [https: //] server [: port].
  - **https:** use is optional (by default http)
  - **server:** name or IP address of the View server
  - **port:** optional TCP port (default 80 for http and 443 for https)
- **Connection properties:** see chapter [5.1.2](#).
- **Authentication:** see chapter [5.1.3](#).
- **Display parameters:** see chapter [5.1.4](#).
- **Additional parameters:** dialog box for certain parameters of the RDP protocol. See chapter [5.1.5](#).
- **Resource redirection:** configuration of the redirection of certain resources (printers, USB drives, etc.) See chapter [5.1.6](#).
- **Performance:** dialog box allowing the management and optimization of bandwidth. See chapter [5.1.7](#).

## 5.6 - PRINTER MANAGEMENT

The thin client offers USB logical ports and network printers. The independent management of these ports makes it possible to connect several printers to the thin client (4 maximum).

In addition to printer redirection protocols specific to RDP or ICA protocols, the AXEL thin client integrates the LPD protocol. This protocol is available with most operating systems and allows you to manage one or more printers connected to the thin client as system printers. Printers are managed by the spooler and accessible to all authorized users.

**Note:** The same printer can be managed simultaneously by LPD and RDP redirection.

The main characteristics of each protocol:

### ***LPD protocol:***

- The printer is visible to all users who have the right to use it.
- The printer is permanent in the server spooler.
- Adding the printer must be done by the administrator at the server level.
- The printer's name is fixed.
- The printer is available when the thin client is turned on and is accessible to all users.
- The data stream is not compressed.
- The multiplexing of the data stream is ensured by TCP / IP.

### ***RDP / ICA protocol:***

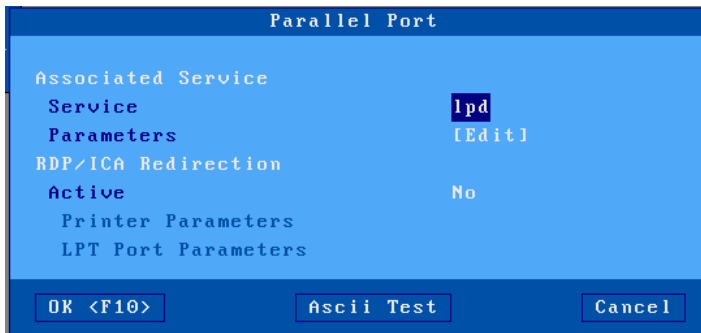
- The printer is only visible to the user of the terminal.
- The printer is only present in the server spooler when the RDP or ICA session is connected
- The addition of printer (s) is automatically performed by the thin client during the RDP or ICA connection.
- The name of a printer is not fixed. It is composed by: "terminal name / printer name / session X" (the session number may vary and does not depend on the thin client).
- The data stream is compressed.
- Multiplexing the data flow (screen / printer) is ensured by RDP or ICA.

The rest of the chapter details the configuration of an LPD printer. For the RDP redirection protocol see chapter [5.1.6](#) and for the ICA protocol see chapter [5.2.8](#).

**5.6.1 - Configuring the thin client**

To configure the LPD service:

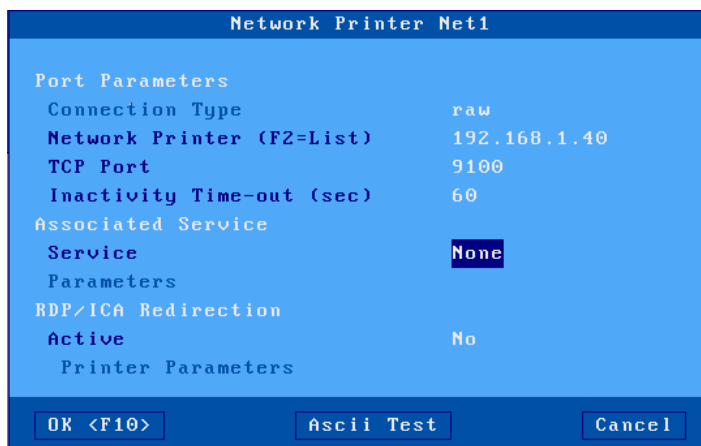
[Configuration]-[Ports aux.]-[xxx]-[yyy]



Or [Configuration] - [Ports] - [USB logical ports] - [USB x]



or [Configuration] - [Ports] - [Network printer] - [Net x]



In the case of the network printer, configure:

- **Network printer:** Enter the name or IP address of the network printer.
- **TCP port:** by default, "9100"
- **Inactivity time-out:** default "60" seconds

Then enter the following parameters:

- **Service:** select the "service from the list **lpd**".
- **Network service settings:**
  - **Printer port name:** this name identifies the auxiliary port and normally represents the name of the queue at the operating system level.
  - **NL filter = CR + NL:** default "no".
  - **Advanced parameters:** see appendix A.7.3.
  - **Print start string:** generally left empty, allows you to send a character string at each start of print.
  - **Print end string:** generally left empty, allows a character string to be sent at the end of each print.

**Note 1:** if the "Choose Portrait / Landscape" parameter is activated (see Appendix A.7.2), the parameter "**Print start string**" is replaced by the parameters "**Portrait start chain**" and "**Landscape start chain**".

**Note 2:** if the auxiliary port used is a serial port, enable the operating mode in "**printer**".

### 5.6.2 - Configuration of a Windows 2016, 2022 server or Windows 11

To create a printer, in the "control panel -> Devices and printers"

- Click on "**Add a printer**", a search for printers is automatically launched, but the server will not find it.
- Click on the link "**The printer that I want isn't listed**"
- In the displayed dialog box, activate "**Add a local or network printer with manual settings**"
- Click on **[Next]**.
- In the new dialog box, activate "**Create a new port**". In the proposed list select "**Standard TCP / IP port**".
- Click on **[Next]**.
- In "**Host name or IP address**" enter the DNS name of the thin client or its IP address, leave the Port name as Windows suggests, then **uncheck** the "**Query the printer and automatically select the driver to use**"
- Click on "**Next**", a search will be carried out without success (wait for the end).
- A new window offers two types of devices, **select "Custom"**, then click **[Settings ...]**
- In the box that appears select the "Protocol **LPR**" then in "**Queue name**" enter the name of the printer port defined in the setup of the thin client (example "**usb1**")

Configure Standard TCP/IP Port Monitor

Port Settings

Port Name: 192.168.1.239

Printer Name or IP Address: 192.168.1.239

Protocol

Raw  LPR

Raw Settings

Port Number: 9100

LPR Settings

Queue Name: usb1

LPR Byte Counting Enabled

SNMP Status Enabled

Community Name: public

SNMP Device Index: 1

OK Cancel

**Please note:** the case of the characters and the spaces are important.

- Click the button **[OK]**
- Click on **[Next]**
- Choose the driver for this printer from the list provided, if it does not exist it must be installed.
- Then finish the installation with the selected parameters.

Once the printer has been created, all print jobs to this printer are automatically redirected to the thin client.

**- 6 -**  
**INSTALLATION UNDER OS / 400**

This chapter describes the specifics of the thin client under OS / 400. For all general settings (network environment, configuration of auxiliary ports, use of multisession ...), see the previous chapters. The thin client supports both 5250 screen sessions (tn5250 protocol) and printers (Prt5250 or LPD protocols).

## 6.1 - 5250 SCREEN SESSION

The IBM 5250 emulation developed by Axel is based on IBM-3477-FC. It is an emulation of "TN5250" type which can be "tunneled" in a TLS pipe for more security.

It offers all the characteristics of a 5250 terminal. Specifically:

- the extended telnet 5250 protocol (TN5250E): complies with RFCs 1205 and 2877 (negotiation of the name and type of the terminal, etc.),
- color management,
- 80x24 and 132x27 screen formats,
- management of the ZIO line.

### 6.1.1 - Configuration of the session

To configure the profile of a session, select the menus **[Configuration] - [Sessions] - [Session X]** (where X is the session number). The following dialog box is displayed:

Session 1 Profile	
<b>Connection Parameters</b>	
Session Type	5250
Protocol	TN5250
Server	no server
Connection Properties	[Edit]
Authentication	[Edit]
<b>Session Parameters</b>	
Terminal name (DEVNAME)	.....
Display Parameters	[Edit]
Additional Parameters	[Edit]
Key Mapping	[Edit]
Palette	[Edit]
<input type="button" value="OK &lt;F10&gt;"/> <input type="button" value="Reset"/> <input type="button" value="Cancel"/>	

Description of the parameters:

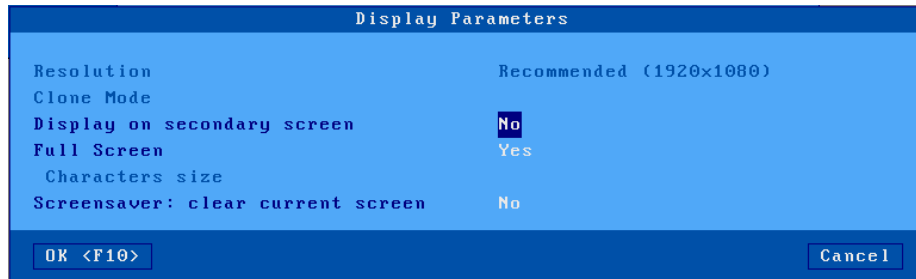
- **Type of session:** select "5250"
- **Protocol:** Two choices are possible, "TN5250" unsecured mode or "TN5250-TLS" mode "tunneled" in a TLS pipe.
- **Server:** chosen from the list of servers (see chapter 3.1.4). A new server name (accessible by DNS) or a new IP address can be directly entered, they will be added automatically to the local servers list.
- **Connection properties:** see chapter 6.1.5.
- **Authentication:** Auto-Sign On procedure (see chapter 6.1.4).
- **Terminal name (DEVNAME):** name to be assigned to session 5250. If this name is left empty, the name is dynamically chosen by the OS / 400 system at the time of connection (ex: QPADEV001).
- **Display parameters:** for more information see the following chapter.
- **Additional parameters:** dialog box allows changing the behavior of the emulation (see chapter 6.1.3.a).
- **Programmable sequences:** dialog box for reprogramming key combinations (see chapter 6.1.3.b).
- **Palette:** setting the emulation colors (see chapter 6.1.3.c).



Validate the dialog box then exit / saving. The thin client is ready.

### **6.1.2 - Display parameters**

The following box is displayed:



Description of the parameters:

- **Resolution:** information of resolution is selected in **[Configuration] - [Terminal] - [Screen]**
- **Display on the secondary screen:** By default, a 5250 session is displayed on the main monitor, but when 2 monitors are connected, it is possible to configure the session on the secondary screen.
- **Full screen:** two values:
  - "Yes": the session occupies the entire screen and the font size automatically adapts to the resolution according to the number of rows / columns.
  - "No": the session is displayed in windowed mode and the size of the characters can be selected.
- **Character size** (only when "Full screen" is disabled): two values: "standard" (8x16) or "large" (16x32).

**Note:** for more information, see Annex [A.7.5](#).

### **6.1.3 - Parameters for 5250 emulation**

Certain parameters can be modified. Enter the setup then select the session profile **[Configuration] - [Sessions] - [Session X]**

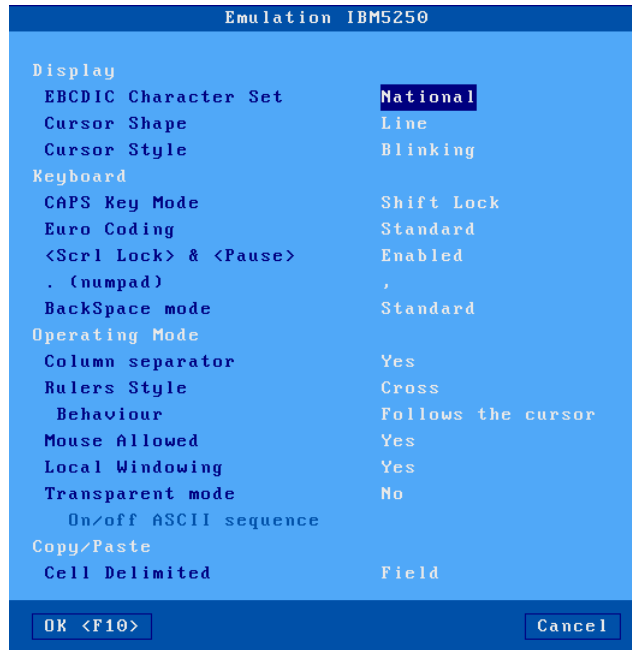
Three groups of parameters allow the configuration of 5250 emulation:

- **additional parameters:** emulation behavior.
- **programmable sequences:** assignment of 5250 functions to any combination of keyboard keys.
- **palette:** default color change.

**a) Additional parameters**

Many parameters are available to customize the behavior of the 5250 emulation.

The following box is displayed:



Description of the parameters:

- **Character set:** the possible values are:
  - **National** (the characters depend on the nationality of the keyboard),
  - **Multinational.**
  - **a particular nationality** (French, American ...).
- **Cursor shape:** line, half-block or block.  
**Note:** the shape of the cursor can also be selected from session 5250 by pressing <Alt> <F11> (or <Alt Gr> <F11> on a PC keyboard).
- **Cursor style:** fixed or flashing.
- **CAPS key mode:** behavior when CAPS LOCK is set:
- **Caps:** pressing an alphabetical key sends the corresponding capital letter. Unlocking is carried out by pressing <CAPS>.
  - **Shift:** pressing a key sends the same character that would be sent by pressing [Shift] and this key. Unlocking is carried out by pressing [Shift].
  - **Capital letters:** pressing a key sends the capital letter of this key if possible (A, É, ...). Otherwise, non-capital key is sent. The [Shift] key works the same way as [CAPS]. Unlocking is carried out by pressing [CAPS].
  - **Caps +:** same functioning as the mode [Shift] with in addition the taking into account of ALL the keys of the keyboard.
- **Euro coding:** management of the Euro symbol. Three possible answers:
  - **no:** no management of the Euro,
  - **standard:** the Euro symbol replaces the international currency symbol '₣' (generally EBCDIC code 9Fh),
  - **personalized:** enter the EBCDIC code of the Euro symbol (decimal notation).
- **<Scroll Lock> & <Pause>:** whether or not these two buttons are authorized
- **. (Numpad):** value returned by pressing the <key. > the numeric keypad. Two possible values: period (.) Or comma (,).
- **Backspace mode:** two possible values are:

- **standard**: move the cursor to the left
- **deletion**: deletion of the character to the left of the cursor
- **Column separator**: two possible values are:
  - **no**: the attribute "column separator" is not managed,
  - **yes**: the attribute "column separator" is displayed but, due to VGA constraints is displayed in the form of an underline.
- **Type of crosshairs**: the "Line" function allows you to locate the cursor position in relation to the other characters displayed. Three types are available:
  - **cross**: a horizontal and vertical line cross at the cursor position,
  - **horizontal**: a horizontal line is displayed on the same line as the cursor,
  - **vertical**: a vertical line is displayed in the same column as the cursor.This function is activated or deactivated from session 5250 by pressing the key <Alt Gr> <F12>.
- **Behavior**: parameter defining the behavior of the cursor marker. Two possible answers: "follows the cursor" or "fixed".
- **Mouse allowed**: activation or not.
- **Local windowing**: window display mode. Two possible answers:
  - **no**: the windows are displayed with the original characters ("." and ":"),
  - **yes**: the windows are displayed with "real frames".
- **Transparent mode active**: transparent mode allows data to be sent in ASCII to auxiliary ports (serial, parallel, etc.). For more information see chapter [6.2.5.c](#).  
The 3 possible values are:
  - **no**: inactive mode,
  - **yes**: the data is coded in ASCII.
  - **yes, hexa**: the data is only coded in hexadecimal.
- **ASCII sequence on / off**: transparent mode starts and end sequence. For more information see chapter [6.2.5.a](#).
- **Cell delimiter**: allows you to choose how to **copy / paste** a table.

### b) Programmable sequences

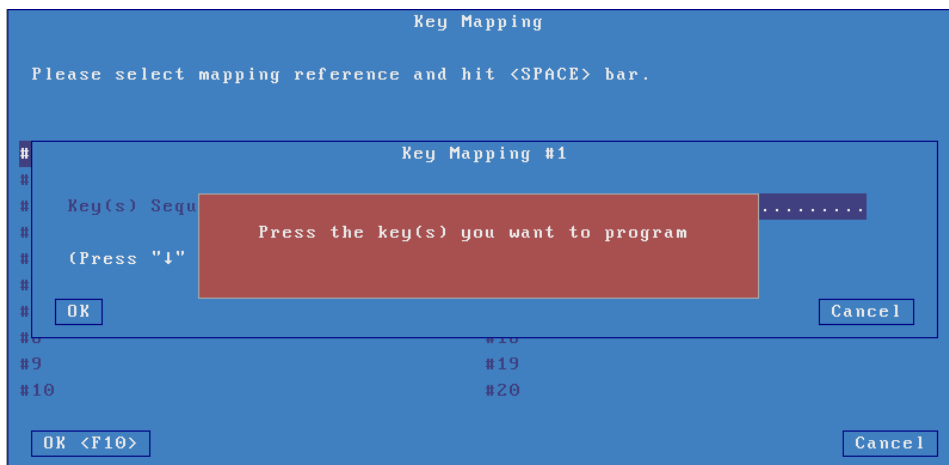
This function allows you to associate “5250 commands” and / or a character string with any key or combination of keys.

The following box is displayed:



The thin client authorizes the programming of 20 key sequences (from # 1 to # 20).

Select the sequence number to program. The following display is made:



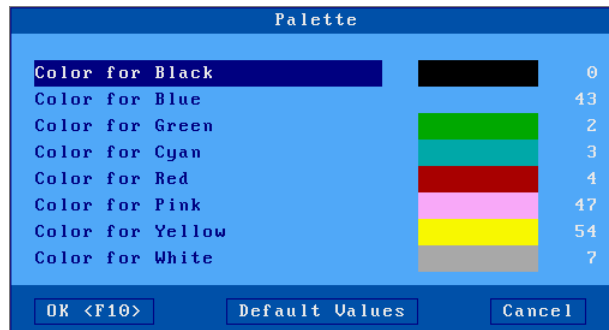
Press the key or combination of keys to be programmed. Then select the "Associated command" parameter. Enter a character string and / or a 5250 command (press [**Down arrow**]> to bring up the list of commands):



Finally, validate the current sequence.

**c) Palette**

The "Palette" allows you to change the default allocation of colors received from the server (for example, displaying blue when black received from the server). The following box is displayed:



Select one of the 8 colors and assign it a new color.

**6.1.4 - Authentication (Auto-SignOn)**

The following box is displayed:



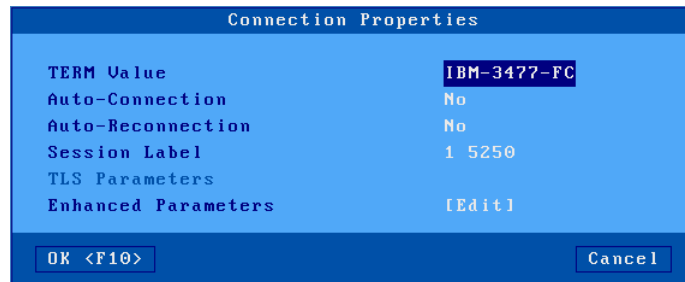
This dialog box contains the parameters of the SignOn screen displayed during connection:

- **Username:** Enter the username
- **Password:** accessible if "Username" is not empty.
- **Program / Procedure** (accessible if "Username" is not empty).
- **Menu** (accessible if "User name" is not empty).
- **Current library** (accessible if "Username" is not empty).

**Please note:** the Auto-SignOn function must be authorized at AS/400 level. The variable **QRMTSIGN** must be set to **"\* VERIFY"** (CFGTCP command).

### 6.1.5 - Connection properties

The following box is displayed:



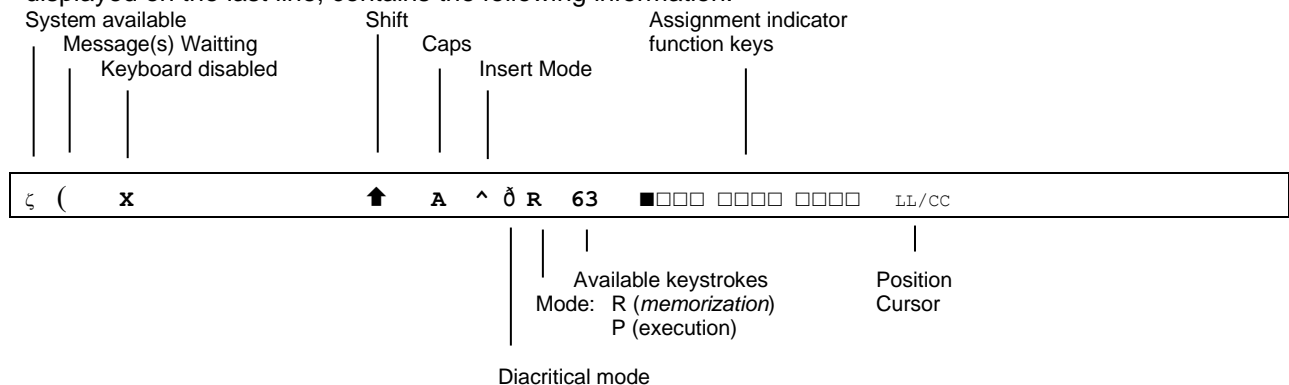
Description of the parameters of this box:

- **Value of the TERM variable:** "IBM-3477-FC" is the default value.
- **auto:** if this parameter is set to "yes" during power-up, the thin client automatically triggers the opening of the session. Otherwise, this connection must be requested by the user by means of a keyboard or mouse action.
- **Automatic reconnection:** if this parameter is set to "yes", after a disconnection, the thin client automatically triggers a new session opening. Otherwise, this reconnection must be requested by the user by means of a keyboard or mouse action.
- **Session label:** This label (14 characters max.) is used to identify the session at the local desktop or taskbar level.
- **TLS parameters:** (only available if the protocol used is TN5250-TLS) see chapter 3.3.3
- **Advanced parameters:** see appendix A.7.3LIGHT

## 6.2 - USE OF THE CLIENT

### 6.2.1 - ZIO: 5250 status line

The ZIO (Operator Information Zone) is a status line specific to a 5250 session in progress. The ZIO, displayed on the last line, contains the following information:



The following table lists the symbols that can be displayed in the ZIO.

Symbol	Name	Description
ζ	System ready	The host system is operational and available
(	Message (s) pending	This symbol, accompanied by an audible signal, indicates that one or more messages from the host system are pending.
x	Entry locked	The thin client refuses the data entered on the keyboard This symbol is displayed when: <ul style="list-style-type: none"> <li>- other data is being processed</li> <li>- the host system is heavily used</li> <li>- the host system has detected an error</li> </ul>
↑	Shift	The <Shift> key is currently pressed
A	Caps Lock	The keyboard is now locked in upper case (key<CAPS>)
^	insert	The insert mode is active(<insert>key)
ø	Diacritical mode	The diacritical mode is active. This mode is automatically activated when a character entered is being typed (^ + e = ê)
R	Recording	The thin client is in Recording mode (see chapter <a href="#">6.2.3</a> )
P	Play	The thin client is in Play mode (see chapter <a href="#">6.2.3</a> )
LL/CC	Position of the cursor	The values LL and CC indicate respectively the coordinates row / column of the cursor



**6.2.2 - Equivalence of the 5250 keyboard with the PC / AT keyboard**

List of functions 5250:

<b>Function 5250</b>	<b>Keyboard 5250</b>	<b>Keyboard PC / AT</b>
Help	<Help>	<Alt Gr> <F1>
System Call	<Shift> <Attn>	<Shift> <Esc> or <AltGr> <ImpEcr>
Attention	<Attn>	<Esc> or <Alt Gr> <Pause>
Character Euro	<Alt> <E>	<Alt Gr> <E>
Zone start	<Alt> <Trait>	<Start>
Down scroll	<Shift> <↓>	<Top page> or <Shift> <↓>
Up scroll	<Shift> <↑>	<Bottom page> or <Shift> <↑>
Right quick	shift <Shift> <→>	<Shift> <→>
Left quick	shift <Shift> <←>	<Shift> <←>
Duplication	<Dup>	<Shift> <Insert>
Erase all fields	<Alt> <EffEc>	<Pause>
Erase end of zone	<Effac>	<End>
Enter	<Enter>	<Enter>
Macro execution	<Exec>	<Alt Gr> <F5>
F1 ... F12	<F1> ... <F12>	<F1> ... <F12>
F13 ... F24	<F13> ... <F24>	<Shift><F1>...<Shift> <F12>
Shape cursor (cf. chap. <a href="#">6.1.3</a> )	<Alt> <F11>	<Alt Gr> <F11>
Hexa	<Alt> <Help>	<Alt Gr> <F7>
Printing (local mode in PC850)	<Rest><Alt> <Impr>	<Ctrl> <Alt> <Screen>
Print (Print Host mode)	<Print>	<Screen>
Macro storage	<Memor>	<Alt Gr> <F4>
Restore	<Rest>	<Left Ctrl>
Crosshair (see chapter <a href="#">6.1.3</a> )	<Trait>	<Alt Gr> <F12>
Back Margin	<↵>	<Right Ctrl>
Front	<→  >	tab<Tab>tab
Back	<  ←> or <Shift> <→  >	<Shift> <Tab>
Zneg	< Zneg>	<-> (numpad)
Zpos	<Zpos>	<+> (numpad)
Zsuiv	<Zsuiv>	<Entr> (numpad)

**List of Axel functions: Axel**

<i>function</i>	<i>Keyboard 5250keyboard Thin</i>	<i>PC / AT</i>
client shutdown	<Rest><Alt> <Suppr>	<Ctrl><Alt> <Suppr>
Configuration (setup)	<Rest><Alt> <Config>	<Ctrl > <Alt> <Esc>
Disconnecting from the session	<Rest><Alt> <D>	<Ctrl><Alt> <D>
Sending data to the aux port.	<Right Alt> <F2>	<Alt Gr> <F2>

**6.2.3 - Programming of function keys (Record/Play)**

This function is used to record frequently used key sequences and to assign them to the function keys. The stored sequences can then be executed at any time.

The data assigned to a function key is saved in non-volatile memory. This means that turning off the thin client does not affect the contents of the soft keys.

This allows programming of the 24 function keys from (<F1> to <F12> and from <Shift> <F1> to <Shift> <F12>).

**Reminder:** The keys <Alt Gr> <F4 > and <Alt Gr> <F5> correspond to the <Record> and <Play> keys on an AS400 keyboard:

**a) Programming of a key**

The programming of these keys is done in "run-time". This means that once connected, it is enough to activate a "memorization" mode then to type the sequence of keys to register to program a function key.

Here are the operations required to program a key:

- press <Alt Gr> <F4> to enter programming mode,
- press the function key to program (<F1> to <F12> or <Shift> <F1> to <Shift> <F12>),
- type the keystroke to register,
- press <Alt Gr> <F4> to end the programming mode.

Notes:

- Memory limitation: 256 keystrokes maximum per function key.
- To erase the content of a previously programmed key, simply save an empty sequence.

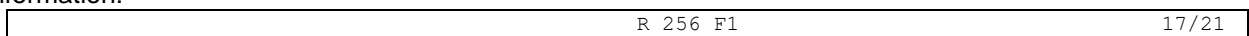
Example of programming a function key:

1 - Press <Alt Gr> <F4> to activate the "Store" mode. The ZIO goes into reverse video and displays the following information:

- the number of memorable keystrokes for the thin client
- the 24 squares represent the programmable function keys, a solid square represents an already programmed function key.



2 - Press the function key to program. The ZIO goes into normal mode and then displays the following information:



**Note:** the "R" indicates the "Record" mode, the 2nd field indicates the number of recorded keystrokes for the key and the 3rd field indicates the key being programmed.

3 - Tap the key sequence to memorize.

4 - To stop the storage mode, press <Alt Gr> <F4>.

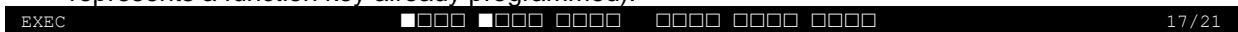
**b) Execution of a key**

To execute the programmed sequence of a function key, perform the following operations:

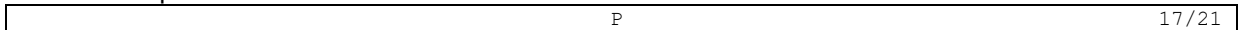
- press <Alt Gr> <F5> to enter the execution mode,
- press the function key to execute (<F1> to <F12> or <Shift> <F1> to <Shift> <F12>),
- the keystroke is executed.

Example of execution of a function key:

1. Press <Alt Gr> <F5> to activate the "Play" mode. The ZIO goes to reverse video and displays the following information (the 24 squares represent the programmable function keys, a solid square represents a function key already programmed):



2. Press the function key to execute. The ZIO goes into normal mode and the 'P' indicator is displayed. The sequence is executed:



**Note:** during "Process" mode, keyboard buffering is disabled.

**6.2.4 - The mouse**

**Note :** the mouse must be activated beforehand. See chapter [6.1.3](#).

Four actions are possible with the mouse:

- **left click**, two possibilities depending on the nature of the character string located under the mouse cursor:
  - If this string is the label of a function key, this function key is issued (keystroke simulation).
  - Otherwise the position of the text cursor is updated.
- **double left click**, two possibilities depending on the nature of the character string located under the mouse cursor:
  - If this string is the label of a function key, this function key is issued (keystroke simulation).
  - Otherwise this string is emitted followed by <Enter> (simulation keystroke).
- **right click**: roll up emission (keyboard keystroke simulation).
- **right double-click**: emission of roll down (keyboard keystroke simulation).

Note on the identification of the character string under the mouse cursor:

The delimiters of this string are:

- the video attributes,
- and the following EBCDIC codes: 00, 40, 4A, 4B, 4C, 4D, 4E, 5A, 5C, 5D, 5E, 60, 61, 6B, 6E, 6F, 7A, 7E, C0 and D0.

Example for the string "F3 = Exit":

- left click or left double click on "F" or "3": emission of <F3>
- double-click on "E": emission of "Exit" then <Enter>.

### **6.2.5 - Transparent mode**

The purpose of this function is to allow developers to send **ASCII characters** directly to the auxiliary and logical ports of the thin client

Transparent mode can be used:

- **from a screen session** (see chapter [6.1.3](#)): the characters are redirected to the specified resource. Example: management of a scales in association with the "ASCII to EBCDIC" function.
- **from a printer session** (see chapter [6.3.1](#)): characters are sent to the port of this session.

#### ***a) Introduction sequence***

Activate the transparent mode and select the introduction sequence (default value: "@% @")

**Note:** it is important to choose a sequence sufficiently complex not to inadvertently receive it in a standard display or editing flow.

#### ***b) Operating rules***

The transparent mode obeys the following rules:

- For "Screen" sessions, the mechanism is activated by sending the introduction sequence (for example "@% @") followed by the printing port number:
  - 0: default port.
  - 1 to 3: not used for this model
  - 4 to 5: network printers (Net1 and Net2 respectively)
  - 6 to 9: USB logical ports (respectively Usb1, Usb2, Usb3 and Usb4)
  - 10 to 11: network printers (Net3 and Net4 respectively)
- For "Printer" sessions, the mechanism is activated by sending the introduction sequence alone.
- In both cases, the mechanism is deactivated following receipt of the introduction sequence a second time.
- The transformation is based on the ASCII table (PC 850) which is used for the ASCII to EBCDIC function.

#### ***c) Character or hexadecimal mode***

The thin client offers two types of transparent mode:

- **Character mode** : ASCII characters and ASCII codes in hexadecimal can be mixed in the data stream. A hexadecimal notation is preceded by the character "/" and must be followed by two characters (between **0 and F**).  
Example: "Esc AB <RC>" is coded "\ 1BAB \ 0D"
- **Hexadecimal mode** : there are only hexadecimal ASCII codes written on 2 characters (between in the data stream **0 and F**).  
Example: "Esc AB <RC>" is coded "1B41420D"

**d) Examples**

In the following examples the introducer is "@% @"

**Example 1:** To a Screen session, character mode

When the thin client receives in EBCDIC:

"@ % @ / 1Bat / 2F @% @" (either in hexadecimal: 44 6C 44 F1 61 F1 C2 81 A3 61 F2 C6 44 6C 44)

The thin client sends in ASCII on the port "Aux1":

"<ESC> at /" (Either in hexadecimal: 1B 61 74 2F).

**Example 2:** Towards a Printer session, character mode

When the thin client receives in EBCDIC:

"@% @ / 1Bat / 2F @% @" (either in hexadecimal: 44 6C 44 61 F1 C2 81 A3 61 F2 C6 44 6C 44)

The thin client sends in ASCII on the port of this printer session:

"<ESC> at /" (ie in hexadecimal: 1B 61 74 2F).

**e) Management of DTR and RTS signals**

The principle of transparent mode can also be used to control the status from a screen session of outgoing DTR and RTS signals.

The syntax of the command is as follows:

- @DTR Port Action"
- @RTS Port Action"

Where:

- **Port:** see the port numbers defined above
- **Action:** if 0 the signal is lowered otherwise it is raised

**6.3 - PRINTER MANAGEMENT**

The thin client offers USB logical ports and network printer ports. The independent management of these ports makes it possible to connect several printers to the thin client.

These printers are managed using one of these two protocols:

- **Prt5250:** this service (RFC 2877) is specific to the OS / 400 system. A printer controlled by this service is seen as a system printer.
- **LPD:** this service (RFCs 1048 and associated) is present on most operating systems (Unix / Linux, NT ...). The main advantage of this service is that it allows sharing a printer between different systems. LPD service brings the following restrictions:
  - manual declaration at OS / 400 level,
  - management of an "outqueue" (and not of a "device"),
  - resumption in case of limited error (resumption of the complete job).

Generally, the "protocolPrt5250" is used (no printer declaration is necessary at OS / 400 level). On the other hand, the LPD protocol allows sharing of the printer by different operating systems. Use the protocol that best meets your needs.

### 6.3.1 - Configuration and use of a PRT5250 printer

#### a) General configuration

To configure the printer on an auxiliary port, enter the setup of the thin client and select [Configuration] - [Ports] - [xxx] - [yyy].

In the dialog box displayed, set the "associated service" parameter to "Prt5250". Then select "Network service" to bring up the following dialog box:

Description of the parameters:

- **Server:** chosen from the list of servers (see chapter 3.1.4). A new server name accessible by DNS or a new IP address can be directly entered; they will be added automatically to local servers.
- **Advanced parameters:** see the following sub-chapter
- **Printer name (DEVNAME):** name of the printer unit at AS / 400 level.
- **Message Queue (MSGQNAME):** name of the operating message queue linked to the printer on the AS / 400.
- **Message library (MSGQLIB):** name of the operating message library on the AS / 400.
- **Host font (FONT):** font identifier (3, 4 or 5 digits).
- **ASCII / Host conversion (TRANSFORM):** forced to "yes", this is the only possible method of operation.
- **Printer model (MFRTYPMDL):** enter the name of the required printer driver available on the server (examples: "\*NONE", "\* HP4", "\* NECP2" ...)
- **Drawer 1 (PPRSRC1):** paper source 1 (choice from a list).
- **Drawer 2 (PPRSRC2):** paper source 2 (choice from a list).
- **Envelope magazine (ENVELOPE):** type of envelope from paper source 3 (choice from a list).
- **ASCII 899 Code Page (ASCII899):** Indicates whether the "ASCII 899" code page is installed for the printer.
- **Personalization object (WSCSTNAME):** qualified name of a personalization object to be associated.
- **Personalization library (WSCSTLIB):** name of the personalization library on the AS400.

## b) Enhanced parameters

The following box is displayed:

Enhanced Parameters	
TCP Port	23
TERM	IBM-3812-1
Auto-Connection	Yes
Auto-Reconnection	Yes
Enhanced Parameters	[Edit]
Transparent mode	No
On/off ASCII sequence	
<input type="button" value="OK &lt;F10&gt;"/> <input type="button" value="Cancel"/>	

Description of the parameters:

- **TCP port:** AS / 400 telnet port. Generally, 23.
- **TERM:** never change this value.
- **auto:** if this parameter is set to 'yes', during power-up, the thin client automatically opens the session.
- **Automatic reconnection:** if this parameter is set to 'yes', after a disconnection, the thin client automatically triggers a new session opening.
- **Advanced parameters:** see appendix A.7.3
- **Transparent mode active:** transparent mode allows data to be sent in ASCII to the auxiliary port of the session. The possible values are:
  - **no:** inactive mode,
  - **yes:** the data is coded in ASCII.
  - **yes, hexa:** the data is only coded in hexadecimal.
- **ASCII sequence on / off:** transparent mode start and end sequence. For more information see chapter [6.2.5.a](#).

## c) Use

The "Prt5250" service is a client-type network service. This means that when the thin client is powered up, any port associated with the "" Prt5250 "service automatically establishes a connection on the appropriate AS / 400 server.

At OS / 400 level, the printer is available as soon as the connection "Prt5250" is established.

A printer connected by the "Prt5250" service on the Axel thin client, is considered as a standard printer of the OS / 400 system. It is therefore managed (start, stop ...) through the menu control of printers.

```
====> GO PRINTER
```

**d) In the event of a problem ...**

- Quick test to check the whole connection:
  - In the thin client setup, select the menu **[Configuration] - [Ports] - [xxx]**. In the displayed dialog box select the button **[Test]**.
  - A banner should be printed.  
#####  
### AXEL PRINTER TEST ###  
#####
- If the printer is not "seen" by the AS / 400 spooler, several causes are possible. To find out the reason for a 5250 connection failure, enter the setup of the thin client, and select the menu **[Diagnostics] - [Connection states]**:

AUXILIARY PORTS			
Port	Service	State	Other Information
Usb2	prt5250		192.168.1. 192.168.1.17 23 ..... (....)

Refresh Close Connections Exit

In the dialog box displayed, click the button **[Refresh]**. Check the information displayed on the line corresponding to the printer port, in particular the return number in parenthesis at the end of the line.

- If there is nothing on the line, check that the server name is entered correctly.
- If the status keeps changing from "CLOSED" to "CONNECTED" and there is no return number (in parenthesis at the end of the line), this means that the unit name is already used for a connection of the same type.
- Here are the main return numbers (in parenthesis at the end of the line):
  - **1902**: (Session successfully started), **the connection is correctly established**.
  - **8903** (Device not valid for session): the printer name is already used for a different type of connection.
  - **8925** (Creation of device failed): when creating the printer, at least one parameter is incorrect (ex: printer model does not exist).
  - **8928** (Change of device failed): when modifying the printer (reconnecting with new parameters), at least one parameter is incorrect (ex: nonexistent printer model).
  - **8930** (Message queue does not exist): the message queue or its library does not exist.
  - **AX01** (Terminal type not recognized): the TERM variable of the thin client's auxiliary port (by default "IBM-3812-1") is not recognized by the server.

**Note:** the full list of possible errors is given in "RFC 2877".

**6.3.2 - Configuration and use of an LPD printer**

Configure the auxiliary port as specified in chapter [3.5.2](#)

Then create a printer within your system with the following command (in this example "AXPRT01" is the name of the printer):

```
====> CRTDEVPRT DEVD(AXPRT01) DEVCLS(*VRT) TYPE(3812) MODEL(1) FONT(11)
```

To make this printer associated with the thin client by LPD, modify its "output queue" (outqueue) OS / 400 level:

```
====> CHGOUTQ OUTQ(AXPRT01) RMTSYS(*INTNETADR) RMTPRTO('USB1') CNNTYPE(*IP) DESTTYPE(*OTHER)
TRANSFORM(*YES) MPRTYPMDL(*NECP2) INTNETADR('192.168.1.240')
```



Description of the command parameters:

- **AXPRT01**: name of the output queue
- **USB1**: Name of the printer port in the setup of the thin client ("USB1" is only one example). **Attention capital required both in the setup and here.**
- \* **NECP2**: type of remote printer (here a NEC type P2).  
For certain printers (labels, bar codes, etc.), for which there are no defined models, you can use the type "\*\* **NONE**".
- **192.168.1.240**: IP address of the thin client.

**Note:** if the editor is not started automatically, use the "STRRTWTR" command.

At OS / 400 level, the printer is actually an "outqueue". It is therefore not possible to manage it as a device (in particular it is impossible to start or stop the printer).

## 6.4 - TO GO FURTHER ...

Reconnection problems may appear, in the event that the thin client session has a name (DEVNAME) and that this thin client has been turned off without logging out cleanly.

This problem is due to a TCP / IP server being unable to detect in real time the existence of a TCP / IP device. The OS / 400 "believes" that a previous session of the thin client is still active and therefore refuses the connection of this "second" session.

The solution is to activate an automatic cleaning mechanism (**keepalive**) which regularly checks the state of the devices to which sockets are assigned (ie TCP / IP connections). These automatic checks are triggered after a certain period of inactivity of the device. They release the socket and the thin client name assigned to a non-responding network device.

**Note:** The OS / 400 command is `netstat` used to check the status of the sockets.

The command used to modify it is as follows (xxx is expressed in minutes):

```
====> CHGTELNA TIMMRKTIMO (xxx)
```

Stop and restart the telnet server:

```
====> ENDTCPSVR SERVER (*TELNET)
====> STRTCPSVR SERVER (*TELNET)
```

**CAUTION:** in the case of connections by router, the use of a "keepalive" with a short delay (2 minutes for example) can prevent routers from hanging up the telephone line.

**- 7 -**  
**INSTALLATION UNDER OS/390**

This chapter covers AX3000 installation under OS/390 zSeries.

This chapter is dedicated to the operation of the AX3000 in the OS/390 environment. For more general information about the AX3000 (network and session settings, instructions for users, etc) please refer to the previous chapters.

## 7.1 - 3270 SCREEN SESSION

The IBM 3270 emulation type developed by Axel provides all the features of an IBM 3270 terminal. Especially:

- -The 3270 telnet protocol (TN3270): compliant with the RFC 1646,
- -Enhanced 3270 telnet protocol (TN3270E): compliant with the RFC 2355,
- -The device type negotiated by the AX3000 is IBM-3278-2-E:
  - -Color support,
  - -Screen sizes: 80x24, 80x32, 80x43 and 132x27,
  - -3270 status line.

### 7.1.1 - Setting a Session

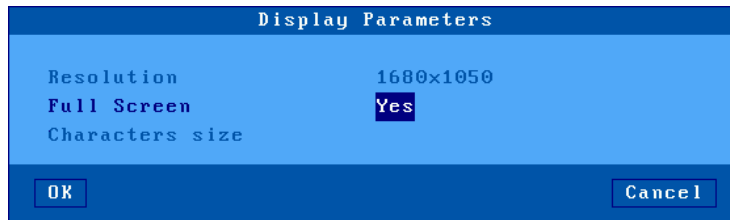
To set a profile session, enter the AX3000 Set-Up and select the **[Configuration]-[Sessions]-[Session X]** menu (where X is the session number to be configured). The following box is displayed:

These parameters are:

- **Type:** select "3270"
- **Server:** selected from the server table (see Chapter [3.1.4](#)). A new server can be added by selecting 'IP address' or 'Server Name'.
- **Connection Properties:** see Chapter [7.1.4](#)
- **Terminal Name (DEVNAME):** this optional name identifies the terminal connection at the OS/390 level.
- **Display Parameters:** see the next chapter.
- **Additional Parameters:** lets certain emulation parameters to be changed. See Chapter [7.1.3](#).
- **Key Mapping:** lets any keys to be remapped. See Chapter [7.1.3](#).
- **Palette:** lets emulation colors to be remapped. See Chapter [7.1.3](#).

### **7.1.2 - Display Parameters**

The following box is displayed:



These parameters are:

- Resolution: For information only. This is the resolution selected in the [Configuration]-[Terminal]-[Screen] menu.
- **Full Screen**: two possible values:
  - 'Yes': the session is displayed on the entire screen and the character size is automatically adapted to the resolution and the number of lines/columns.
  - 'No': the session is displayed in a 'Window' mode and the character size can be customized.
- **Character Size** (Only when 'Full Screen' is disabled): Two possible values: 'standard' (8x16) or 'double' (16x32).  
**Note:** for more information, please refer to Appendix A.7.5.

### **7.1.3 - Customizing the 3270 Emulation**

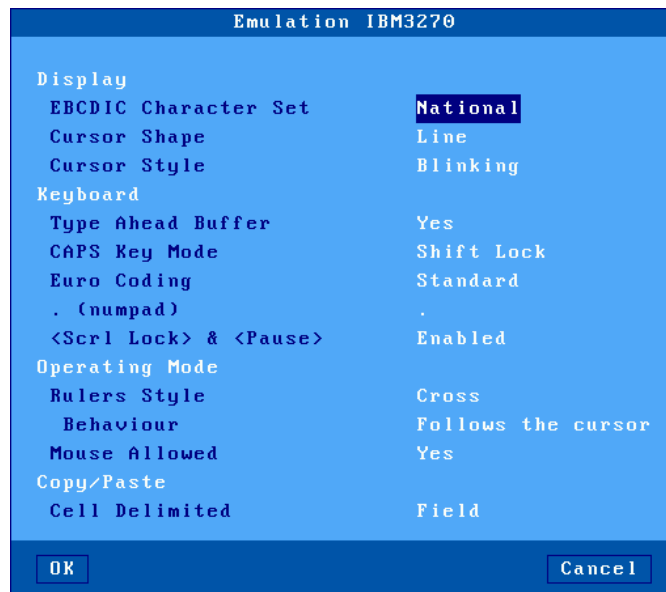
Various 3270 emulation parameters can be modified but generally the default values are the most suitable.

To customize the 3270 emulation, enter the AX3000 Set-Up and select the session profile (**[Configuration]-[Sessions]-[Session X]** menu). Three groups of parameters control 3270 emulation settings:

- Additional Parameters: 3270 emulation behavior,
- User-defined Sequences: mapping 3270 functions to any PC keyboard keys.
- Palette: remapping emulation colors.

### a) 3270 Emulation Additional Parameters

The following box is displayed:



These parameters are:

- **Character Set:** the possible values are:
    - National (characters are keyboard nationality dependent),
    - Multinational.
    - A specific keyboard nationality (American, French...).
  - **Cursor Shape:** Line, Half-Block or Block.
  - **Cursor Style:** Blinking or Steady
  - **Type Ahead Buffer:** enable/disable the keyboard buffer.
  - **CAPS Key Mode:** set the CAPS LOCK to behave in either of two ways:
    - Caps Lock: only alphabetical keys are affected. To unlock, press the <CAPS> key.
    - Shift Lock: each key sends either the corresponding upper-case letter or the shifted (upper) character. To unlock this mode, press the <Shift> key.
    - Uppercase: each key sends the upper character if it is present. Otherwise, this is the lower character (upper-case letter if possible) which is sent. <Shift> key acts in the standard way (whatever the CAPS key). To unlock this mode, press the <CAPS> key.
    - Caps Lock +: same as 'Shift Lock'. But in addition, ALL the keys supported (including <Esc>, function keys...).
  - **Euro Coding:** Euro symbol support. The three possible values are:
    - No: no specific processing is done
    - Standard: The Euro symbol replaces the international currency symbol '¤' within the current character set.
    - Custom: any character can be replaced by the Euro symbol within the current character set (use the decimal notation to enter the Euro EBCDIC code).
  - **. (numpad):** the two available values are the dot (.) and the comma (,).
  - **<Scroll Lock> & <Pause>:** enable or disable these two keys
  - **Rulers Style:** the "rule" function allows the cursor to be located easily among other characters. Three types of rules are available:
    - Cross: a horizontal line and a vertical line indicate the cursor location,
    - Horizontal: a horizontal line is displayed at the cursor line,
    - Vertical: a vertical line is displayed at the cursor column.
- Press <Alt Gr><F12> to enable/disable the rule function from a 3270 session.

- **Behavior:** the two values are: "follows the cursor" or "fixed"
- **Mouse Allowed:** enable/disable the mouse within this session
- **Cell Delimited:** Cut & Paste behavior.

**b) Remapping 3270 Functions to any PC Keyboard keys**

This allows any key to be remapped to any 3270 function and/or character string.

The following box is displayed:



Up to 20 sequences can be remapped (from #1 to #20).

To program a new sequence (or to modify an existing one) select the sequence number. The following dialog box is displayed:



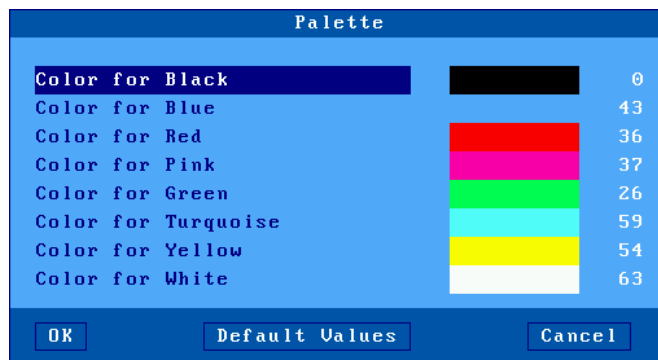
Enter the keystroke to be remapped. Then enter a character string and/or press <Down Arrow> to select through a list the associated 3270 function.



**c) Palette**

This allows default emulation colors to be remapped to any color.

The following box is displayed:

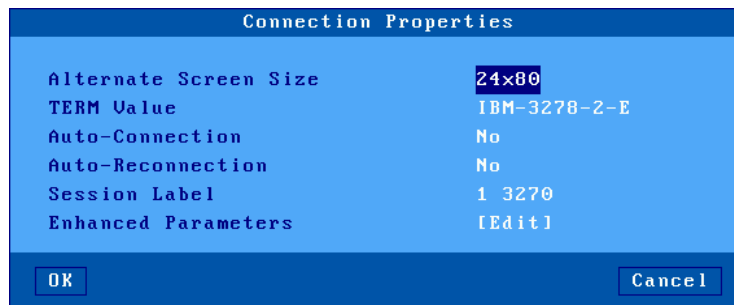


Select one of the 8 emulation colors and associate it with another color.



### 7.1.4 - Connection Properties

The following box is displayed:



These parameters are:

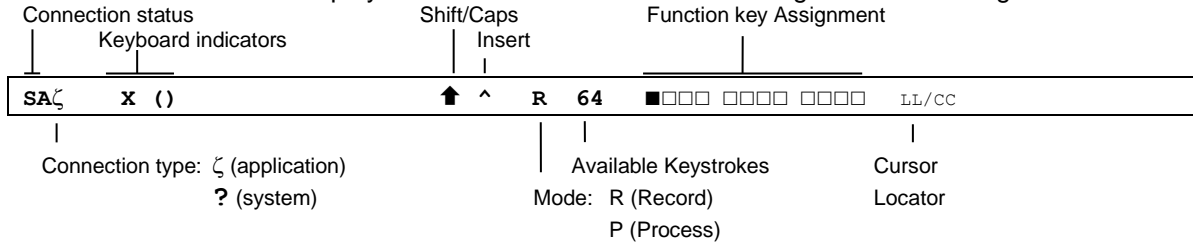
- **Alternate Screen Size:** possible values are 24x80, 32x80, 43x80 and 27x132. This value set-up a TERM default value.
- **TERM Value:** terminal capabilities. Default value is IBM-3278-2-E.
- **Auto-Connection:** if this parameter is set to 'yes', the connection will be automatically established when the AX3000 is powered. Otherwise, the user can press <Alt><Fx> to establish the connection.
- **Auto-Reconnection:** if this parameter is set to 'yes', a new connection is automatically established after a disconnection. Otherwise, the user can press <Alt><Fx> to establish a new connection.
- **Session Label:** this character string (11 characters max.) is used to identify the session within the local desktop or in the taskbar.
- **Enhanced parameters:** see Appendix A.7.3.

## 7.2 - USING THE THIN CLIENT

### 7.2.1 - The 3270 Status Line

**Note:** the 3270 status line is different than the AX3000 TCP/IP status line.

The 3270 status line is displayed at the bottom of the screen and gives the following information:



The status symbols are described in the following tables.

#### Connection Symbols

Symbol	Meaning
S	Connection with host is established
A	Connection is non-SNA
ζ	Connection to an application (Lu-Lu)
?	Connection to the system (not an application)

#### Keyboard Symbols

Symbol	Meaning
X ( )	Keyboard is disabled
X	Only <Enter> is disabled
X ⚠ >	Error: too much data entered. Press <Reset>
X ⚠ NUM	Error: numeric value must be entered. Press <Reset>
X ⚠ ← →	Error: invalid cursor position. Press <Reset>

#### Mode Symbols

Symbol	Meaning
↑	<Shift> is currently pressed or the keyboard is in Caps Lock mode
^	The insert mode is enabled (<Inser> key)
R	The "Record" mode is set (see Chapter 6.2.3)
P	The "Process" mode is set (see Chapter 6.2.3)
LL/CC	LL and CC indicate the row and column where the cursor is located

### 7.2.2 - Using a PC/AT Keyboard (102/105 keys)

The IBM 3270 emulation enables a PC/AT keyboard to be used for operation as a 3270 terminal.

The first twelve 3270 function keys are accessed through <F1> to <F12>. The F13 to F24 function keys are accessed through <Shift><F1> to <Shift><F12>.

The following table lists the other useful keys:

3270 Functions	PC/AT keyboard
Fast cursor move to right	<Alt><right arrow>
Fast cursor move to left	<Alt><left arrow>
Backspace	<BackSP>
Tab	<Tab>
BackTab	<Shift><Tab>
Home	<Home>
Newline	<Enter>
EOF	<End>
Erase Input	<Alt><End>
Insert mode	<Inser>
Delete	<Del>
Duplicate	<Shift><Inser>
Field Mark	<Shift><Home>
System	<Alt><Syst> or <Shift><Esc>
Attention	<Alt><Pause> or <Esc>
Reset	<Ctrl left>
Clear	<Pause>
PA1	<PgUp>
PA2	<PgDn>
PA3	<Shift><PgUp>
PF1	<F1>
PF13	<Shift><F1> or <Esc>
Enter	<Right Ctrl> or <Num Entr>
<Record>	<Alt Gr><F4>
<Exec>	<Alt Gr><F5>
Euro Symbol	<Alt Gr><E>
Rule	<Alt Gr><F12>

### 7.2.3 - Programming Function Keys (Macro Feature)

The Axel 3270 emulation allows function keys to be programmed. For example, a series of keystrokes can be recorded and played back by pressing a single key.

The recorded data is stored in non-volatile memory so is not affected by switching off.

Recorded keystrokes can be assigned to any of the twelve function keys (<F1> to <F12>).

#### a) Programming a Function Key

To record a series of keystrokes, proceed as follows:

- Press <Alt Gr><F4> to set the record mode,
- Press any of the 12 function keys to which you want to assign,
- Type the key sequence you want to save,
- Press <Alt Gr><F4> to exit the record mode.

#### Notes:

- Memory usage: maximum 256 keystrokes recorded per function key.
- To delete a recorded function key, you have to record an empty key sequence.

Example:

- 1 - Press <Alt Gr><F4> to set the Record mode. The 3270 status line is set in reverse video mode and the following information is displayed (the 12 boxes are the 12 function keys, a solid box means that data is recorded):

```
MEMOR          ■□□□ □□□□ □□□□          17/21
```

- 2 - Press one of the function keys (from <F1> to <F12>). The 3270 status line is set in normal mode and the following information is displayed:

```
R 256 F1          17/21
```

**Note:** 'R' indicates the Record mode. The second field is the maximum keystrokes that can be recorded for this session. The third field is the selected function key.

- 3 - Type the key sequence.
- 4 - To exit the Record mode, press <Alt Gr><F4>.

#### b) Processing a Key Sequence

To execute a series of keystrokes that have been recorded:

- Press <Alt Gr><F5> to set the Process mode,
- Press the recorded function key, (from <F1> to <F12>)
- The key sequence is processed.

Example:

- 1 - Press <Alt Gr><F5> to set the Process mode. The 3270 status line is set in reverse video mode and the following information is displayed (the 12 boxes are the 12 function keys, a solid box means that data is recorded):

```
EXEC          ■□□□ □□□□ □□□□          17/21
```

- 2 - Press the recorded function key (from <F1> to <F12>). The 3270 status line is set in normal mode and the following information is displayed (the 'P' symbol indicates the Process mode). The key sequence is processed:

```
P          17/21
```

**Note:** during the process mode, the input is inhibited.

### 7.3 - 3270 PRINTER

Auxiliary ports (2 serial for the G15), USB ports and logical ports (USB and TCP) are provided. These ports are independently controlled so multiple printers can be attached to the AX3000.

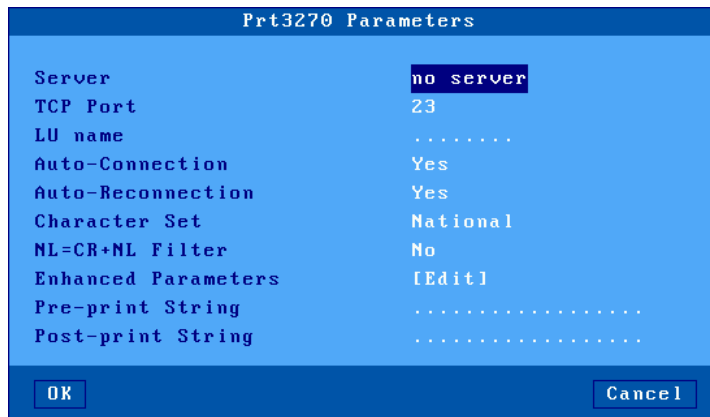
These printers can be controlled by one of two protocols:

- **Prt3270:** a printer controlled by this service is seen as a standard spooled system printer device.
- **LPD:** this service (RFCs 1048 and related) is provided as a standard feature by major operating systems (Unix/Linux, NT, etc.). The main benefit of this protocol is an LPD printer can be shared by different operating systems.
  - manual declaration at IBM server level,
  - management of an "outqueue" (and not of a "device"),
  - recovery in case of error is limited (recovery of the entire job).

This chapter describes only the Prt3270 protocol.

To set the Prt3270 service, enter the AX3000 Set-Up and select **[Configuration]-[Aux. Ports]-[xxx]**.

In the displayed box, set the "Associated Service" to "Prt3270", then select "Net Service Parameters". The following box is displayed:



These parameters are:

- **Server:** selected from the server table (see Chapter 3.1.4). A new server can be added by selecting 'IP address' or 'Server Name'.
- **TCP PORT:** telnet port of the S/390 server. Default is 23.
- **LU Name:** system printer name.
- **Auto-Connection:** set to yes.
- **Auto-Reconnection:** set to yes.
- **Character Set:** the possible values are:
  - National (characters are keyboard nationality dependent),
  - Multinational.
  - A specific keyboard nationality (American, French...).
- **NL=CR+NL Filter:** The line feed character (0Ah) can be mapped to carriage return + line feed (0Dh + 0Ah),
- **Enhanced parameters:** see Appendix A.7.3.
- **Pre-print String:** character string sent before the printing.
- **Post-print String:** character string sent after an the printing (for example "\0C" is a form feed)

**Note 1:** If "Choose Portrait/Landscape" is enabled (see Appendix A.10.2), the parameter "**Pre-print String**" is replaced by the two parameters "**Portrait Pre-print String**" and "**Landscape Pre-print String**".

**Note 2:** if the auxiliary port used for printing is a serial port, set the 'Printer' operating mode and set the associated parameters (baud rate, handshake, etc).

## 7.4 - REMOTE ADMINISTRATION

A Windows administration utility (AxRM or Axel Remote Management) is available free on the Axel Web site. See Chapter [10.1](#).

**- 8 -**  
**INSTALLING UNDER UNIX/LINUX**

This chapter covers AX3000 installation under Unix/Linux.

## 8.1 - TEXT MODE SESSION (TCP/IP OR SERIAL MODE)

### 8.1.1 - Setting a Session Profile

To set the profile of a session, enter the AX3000 Set-Up and select the **[Configuration]-[Sessions]-[Session X]** menu (where X is the session number to be configured). The following box is displayed:

Session 1 Profile	
Connection Parameters	
Session Type	Text Emulation
Emulation	ANSI
Protocol	telnet
Server	no server
Connection Properties	[Edit]
Session Parameters	
Display Parameters	[Edit]
Additional Parameters	[Edit]
Editing Keyboard Table	[Edit]
Key Mapping	[Edit]
Coloring Mode	Disabled
Coloring Mode Settings	
Palette	[Edit]

Buttons: OK, Reset, Cancel

These parameters are:

- **Session Type:** select 'Text Emulations'.
- **Emulation:** see Chapter [8.1.3](#)
- **Protocol:** select 'telnet', 'tty', 'ssh' or 'serial'. (See Chapter [8.1.2](#))
- **Server:** selected from the server table (see Chapter [3.1.4](#)). A new server can be added by selecting 'IP address' or 'Server Name'.
- **Connection Properties:** see Chapter [8.1.8](#)
- **Display Parameters:** see Chapter [8.1.4](#).
- **Additional Parameters:** allows certain emulation parameters to be changed. (See Chapter [8.1.5](#))
- **Editing Keyboard table:** allows certain keys to be remapped. (See Chapter [8.1.5](#))
- **Key Mapping:** allows all of the keys to be remapped. (See Chapter [8.1.5](#))
- **Coloring mode:** allows monochrome applications to be displayed in color. (See Chapter [8.1.6](#))
- **Palette:** lets colors to be remapped. (See Chapter [8.1.5](#))



### 8.1.2 - Protocols: telnet, tty, ssh, ssh2 or serial

Connecting a character-based session can be done:

- Either in TCP/IP mode via **telnet**, **tty** or **ssh2** protocols
- Or in serial mode (RS232) by using a USB-Serial adaptor

#### a) The TELNET Protocol

The telnet server is a standard module of the Unix/Linux TCP/IP stack. The AX3000 can immediately open a client telnet session, without any additional software or alteration to the Unix/Linux settings.

Main characteristics of a telnet session:

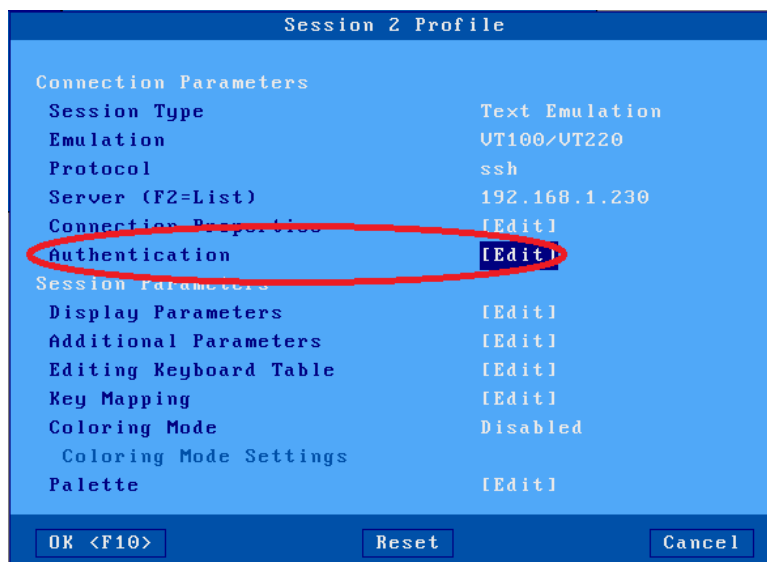
- Dynamic allocation of pseudo-terminals (pty),
- System access is controlled by a 'login', which is generated by the telnetd daemon,
- The value of the TERM environment variable is negotiated after the login stage. (See Chapter [8.1.8](#) for default TERM values.)

#### b) The SSH Protocol

An SSH connection can be considered as an encrypted telnet connection. Main characteristics are:

- Dynamic allocation of pseudo-terminals (pty),
- System access is controlled by a 'login', which is generated by the sshd daemon (available with most versions of Unix/Linux),
- The value of the TERM environment variable is negotiated after the login stage. (See Chapter [8.1.8](#) for default TERM values.)

When the "ssh" protocol is chosen, a new line "Authentication" is added to the session profile:



Select the menus **[Configuration]-[Sessions]-[Session X][Authentication]** to access the authentication window:

This window is used to manage authentication with or without private key. In case of a private key, a PassPhrase is requested instead of the password.

- **User name:** User name
- **SSH key name:** Name of the private key that must be installed in the object store beforehand, see chapter [3.6.5](#)
- **Password** or **PassPhrase:** Password in the case of a simple connection, PassPhrase in case of a connection with private key.

**Note:** The Axel SSH client is compliant with OpenSSH.

### c) The TTY Protocol

The tty server is an Axel proprietary protocol. Additional software is required (see Chapter [8.4](#)).

Main characteristics of a tty session:

- Pre-defined allocation of pseudo-terminals (pty),
- UNIX access is controlled by a 'login', which is generated by the init daemon (controlled by the **/etc/inittab** file).

The Unix/Linux host must run the AXEL tty server daemon (**axttyd**). The configuration file **axttyd** must contain a list of AX3000 sessions and the ptys associated with each.

Each session is identified by the name of the AX3000 (from the **/etc/hosts** file) and a special keyword (**sessx** where **x** is the session number). For example:

```
axel1    sess1    /dev/ptyp12    /dev/ttyp12
axel1    sess2    /dev/ptyp13    /dev/ttyp13
axel2    sess2    /dev/ptyp2     /dev/ttyp2
```

A thin client session controlled by the tty server acts as a serial terminal attached to a multi I/O board. The **/etc/inittab** file must therefore be modified to launch the **getty** command for each pseudo-terminal.

Example for SCO Unix: get a login on **/dev/ttyp12**:

```
p12:23:enable:/etc/getty -t60 /dev/ttyp12 m
```

This modification will take effect after invoking the following command:

```
# init q <RC>
```

For more information about the Axel tty server, refer to Chapter [8.4](#).

#### d) Serial Ports and USB-COM adaptors

The Axel thin client supports both TCP/IP and serial RS232 (G15) connections.

To establish a serial connection, the session 'Protocol' must be set to 'serial'. Then set 'Main Serial Port' to a native serial port or an USB serial port.

The selected auxiliary port is set-up through the **[Configuration]-[Ports]-[xxx]-[yyy]** menu (see Chapter [3.5.1](#)).

#### 8.1.3 - Selecting the Emulation

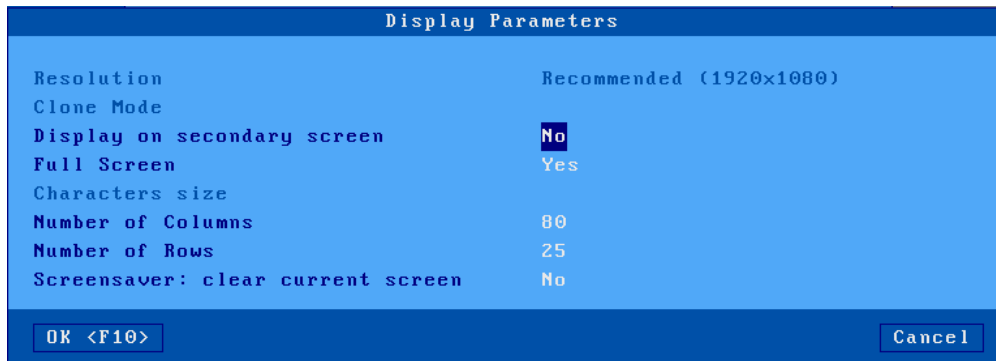
The available emulations are:

ANSI	ANSI DOS
SCO OPENSERVER	UNIX SCO 3.2.2
UNIX SVR4	UNIX SCO 3.2.4
ANSI RS 6000	XENIX SCO
UNIXWARE 7	ANSI DATA GENERAL
LINUX	ANSI INTERACTIVE
UT100/UT220	AT0300
UT52	PRISM
WYSE 50/60/120	THEOS
ADDS UP-A2 Enhanced	OS2 POLYMOD2
ADDS UP-60	SM9400
3151	SM9412
Other ...	TWIN SERVER
	PROLOGUE 3
	TUI 950
	AMPEX+
	QUT119+
	C332

**Note:** selecting emulation sets the value of the TERM environment variable (see Chapter [8.1.8](#)). This value can be modified later if necessary.

### 8.1.4 - Display Parameters

The following box is displayed:



These parameters are:

- **Resolution:** For information only. This is the current resolution selected in the [Configuration]-[Terminal]-[Screen] menu.
- **Display on the secondary screen:** Show on secondary screen: By default, a text session is displayed on the main monitor of the thin client, but when 2 monitors are connected on the thin client, it is possible here to configure the session on the secondary screen.
- **Full Screen:** two possible values:
  - 'Yes': the session is displayed on the entire screen and the character size is automatically adapted to the resolution and the number of lines/columns.
  - 'No': the session is displayed in a 'Window' mode and the character size can be customized.
- **Character Size** (Only when 'Full Screen' is disabled): Two possible values: 'standard' (8x16) or 'double' (16x32).
- **Number of Columns:** three possible values: 40, 80 or 132.
- **Number of Rows:** enter a value between 24 and 44.
- **Screensaver:** clears the current screen: Force a "clear screen" as soon as the screen saver function is activated (see chapter [3.2.2.b](#)). This very special feature ensures that when reactivating the screensaver, the data displayed will only be those received after the reactivation.

**Note:** for more information, please refer to Appendix A.7.5.

### 8.1.5 - Customizing the Emulation

Various emulation parameters can be modified but generally the default values are the most suitable. Three groups of parameters control emulation settings:

- **Additional Parameters:** emulation behavior.
- **Editing Keyboard Table:** associating character strings to certain keyboard keys.
- **Key Mapping:** associating character strings to any keyboard keys.
- **Palette:** remapping emulation colors.

### a) Emulation Additional Parameters

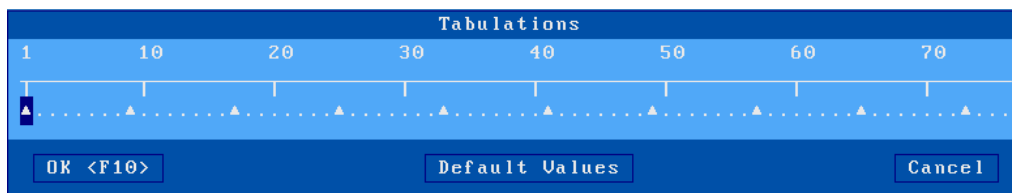
The following box is displayed:



These parameters are:

- **Character Set:** the available character sets depend on which emulation is selected.
- **Vertical Scrolling:** whether the AX3000 display scrolls, when the cursor is moved down passed the bottom of the screen:
  - Yes: the display scrolls up
  - No: the cursor re-appears on the first (top) line.
- **Wrap:** behavior of the AX3000 when the cursor reaches the last column of the screen:
  - Yes: the next characters wrap round onto the start of the next line
  - No: each new character overwrites the last character on the line.
- **CR=CR+LF:** AX3000 behavior when 0x0Dh is received:
  - Yes: 0x0D is mapped to 0x0D and 0x0A
  - No: no specific processing is done
- **Cursor Shape:** Line, Half-Block and Block.
- **Cursor Style:** Blinking or Steady.
- **Attributes Mode:** VGA monitor mode. The two values are "color" and "monochrome" (which allows underline attribute to be displayed).
- **Enhanced Mode:** enable or disable the display of double-size characters or color underline attribute.
- **Blink Allowed:** if blink attribute is disabled, 16 background colors can be used (instead of the 8 normally available).
- **Ignore Blank Atb** (WYSE emulation only): if 'yes', the blank attribute is not processed (example: normal+blank=normal).
- **End Sequence:** to stop transparent printing mode
- **Coding:** two keyboard modes are available (ASCII and scancode).
- **CAPS Key Mode:** set the CAPS LOCK to behave in either of three ways:
  - Caps Lock: each alphabetical key sends the corresponding upper case letter. To unlock this mode press the <CAPS> key.
  - Shift Lock: each key send the same character sent by pressing <Shift><This key>. To unlock this mode press a <Shift> key.
  - Uppercase: each key send the upper character if it is present. Otherwise, this is the lower character (upper-case letter if possible) which is sent. <Shift> key acts in the standard way (whatever the CAPS key). To unlock this mode press the <CAPS> key.

- Caps Lock +: same as 'Shift Lock'. But in addition ALL the keys supported (including <Esc>, function keys...).
- **Composed Characters:** this parameter (only available in ASCII mode) sets the keyboard behavior for diacritical characters (for example: ^ + e = ê):
  - No: no specific processing is done
  - Local: composite characters are locally processed by the AX3000
  - Remote: SCO specific mode (mapchan).
- **Euro Coding:** this parameter is only available if the current character set is not PC858 or ISO8859-15 (These 2 character sets include the Euro symbol). The three values are:
  - No: no specific processing is done
  - Standard: the Euro symbol replaces the international currency symbol '¤' within the current character set.
  - Custom: any character can be replaced by the Euro symbol within the current character set (use the decimal notation to enter the Euro ASCII code).
- **<Scroll Lock> & <Pause>:** enable or disable these two keys
- **Tabulations:** a dialog box appears in which tab stops can be set.



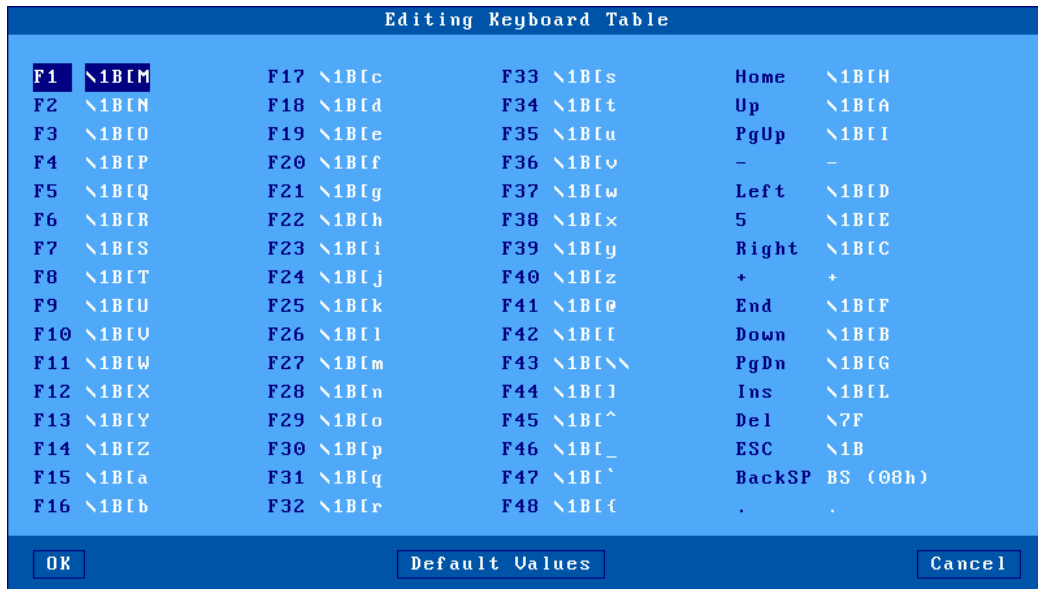
- **Init String:** this character string is sent when the session (telnet or tty) is established.
- **Answer Back:** session identifier (max 10 character.).
- **Monitor Mode:** the monitor mode is used to examine the data received by the AX3000:
  - No: monitor mode disabled.
  - Yes, hexadecimal value
  - Yes, symbol
- **Remote Terminal Set-Up:** enable or disable the use of escape sequences to set thin client parameters from the host computer.
- **Mouse Allowed:** enable/disable the mouse within this session.
- **Nulls Suppress (WYSE emulation only):** if 'yes', bytes with ASCII code set to zero are skipped.

**b) Editing Keyboard Table**

This dialog box allows certain keys to be remapped. This function is only available in keyboard ASCII mode.

**Note:** to remap keys not shown below use the "Key Mapping" function described in the next chapter.

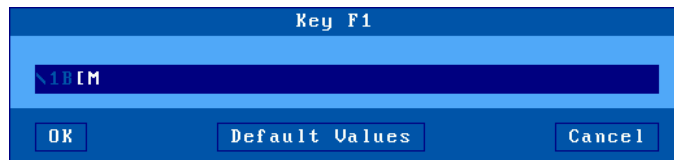
The following box is displayed:



There are three groups of programmable keys:

- From F1 to F48: function keys used singly or with a modifier key. Example for ANSI emulations:  
 F1 to F12: <F<sub>x</sub>>                      F13 to F24: <Shift><F<sub>x</sub>>  
 F25 to F36: <Ctrl><F<sub>x</sub>>              F37 to F48: <Ctrl><Shift><F<sub>x</sub>>
- Numeric pad with Number Lock off
- Special keys: Esc, Backspace and the 'dot' of the numeric pad.

To enter a programmable key value, select this key label. The following dialog box is displayed:



The main field is used to enter the programmable key value. ASCII codes lower than 20h can be entered as 'xx' (where xx is the hexadecimal value of the ASCII code).

**Note:** for the 'Backspace' key and the numeric pad dot, a toggle is only available (two possible values for each key).

Memory usage is limited to 256 bytes maximum per key.

**c) Key Mapping**

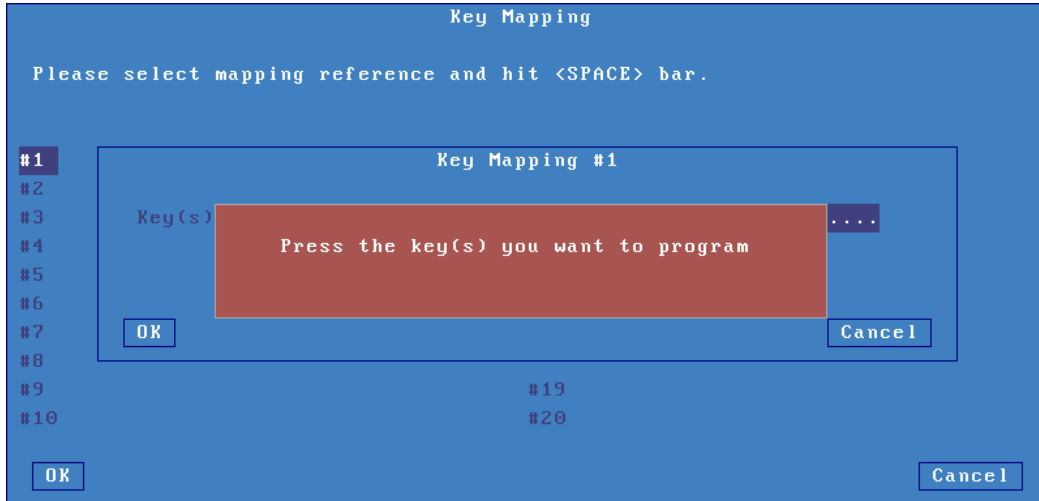
This function allows any key to be remapped into any value (only available for ASCII keyboard mode)

Select "Key Mapping" within the 'Session Profile' box and press <Space> to display the following box:

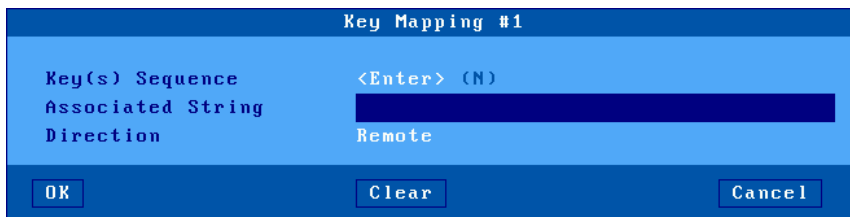


Up to 20 sequences can be remapped (from #1 to #20).

To program a new sequence (or to modify an existing one) select the sequence number. The following dialog box is displayed:



Press keystroke to be remapped). The following dialog box is displayed:



Other parameters:



- **Key(s) Sequence:** keystroke to be remapped
- **Associated String:** enter the value associated with the key sequence. ASCII codes lower than 20h can be entered as '\xx' (where xx is the hexadecimal value of the ASCII code).
- **Direction:** two possible values:
  - Remote: when the key sequence is pressed, the 'Associated String' is sent to the server.
  - Local: when the key sequence is pressed, the 'Associated String' is interpreted by the thin client (as if the string had been sent by the server).

#### **d) Palette**

This allows default emulation colors to be remapped to any color.

Within the 'Session Profile' box, select 'Palette'. The displayed box allows the 16 emulation colors to be remapped to another color.

#### **8.1.6 - Coloring Mode**

A background color, plus a foreground color for each monochrome character attribute or graphics character, may be set through the Coloring Mode. This function allows monochrome applications to be displayed in color.

The "**Coloring Mode**" parameter offers 2 values:

- **Standard:** 6 coloring attributes
- **Enhanced:** 16 coloring attributes

To customize the coloring mode, select the "**Coloring Mode Settings**" parameter. The displayed dialog box allows coloring attributes to be associated with a foreground and background colors.

#### **8.1.7 - Underline Attribute Management**

The reverse video attribute, the bold attribute and the blinking attribute are supported by all VGA monitors. However, the underline attribute is only supported by monochrome VGA monitors.

If the underline attribute is essential with a color VGA monitor, one of the following three methods can be used, but note that each entails the loss of some other display capability.

##### ***a) Using the Session as a Monochrome Session***

Set the **Attribute Mode** parameter to **monochrome** (see Chapter [8.1.5](#)).

##### ***b) Using the Coloring Mode***

The AX3000 coloring mode is used to provide different foreground and background colors for each monochrome attribute. So although no underline appears on the screen, normal and underlined text can be distinguished by different background colors.

The benefit of this method is that the coloring mode is specific to a single session. Sessions with different colors, or with the native colors of a software package, can be run on the same AX3000.

For more information about "coloring mode", see Chapter [8.1.6](#).

### c) Using Underline Attribute in Color Mode

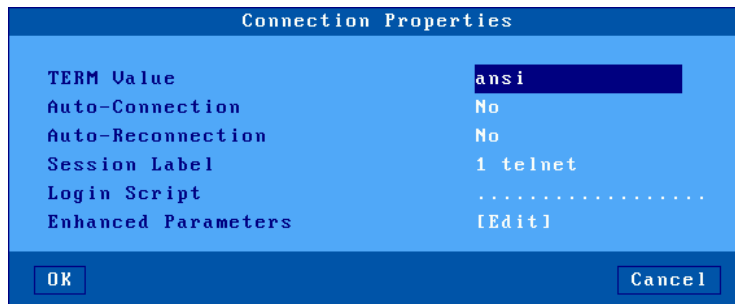
An AX3000 set-up parameter allows the underline attribute to be displayed in color mode, but this disables the bold attribute.

This is a good way to display underlining if the bold attribute is not used by the software in question.

Enter the AX3000 set-up and set for the required session the '**Enhanced Mode**' parameter to '**Yes**'. See Chapter [8.1.5](#).

### 8.1.8 - Connection Properties

The following box is displayed:



These parameters are:

- **TERM Value** (telnet and ssh2 protocols). The default TERM value depends on the selected emulation.
- **Auto-Connection**: if this parameter is set to 'yes', the connection will be automatically established when the AX3000 is powered. Otherwise, the user can press <Alt><Fx> to establish the connection.
- **Auto-Reconnection**: if this parameter is set to 'yes', a new connection is automatically established after a disconnection. Otherwise, the user can press <Alt><Fx> to establish a new connection.
- **Session Label**: this character string (11 characters max.) is used to identify the session within the local desktop or in the taskbar.
- **Login Script**: a "login script" can be set to automatically enter user names and passwords at the login prompt. See Chapter [8.1.9](#).
- **Enhanced parameters**: see Appendix [A.7.3](#).

### 8.1.9 - Login Script

The "login script" can be set to automatically enter user names and passwords at the login prompt.

#### a) Enabling a Login Script

To associate a login script with a session, within the 'Session Profile' box select "Connection Properties". In the displayed box (see Chapter [8.1.8](#)) select "Login Script".

The login script is a character string with the following characteristics:

- Maximum 60 characters.
- The string is composed of tokens. The NULL character (encoded by \00) is used as a token-separator. A string must contain an even number of tokens.
- Any character except a NULL can compose a token.
- A string can contain as many tokens as needed.
- Odd tokens are characters expected by the AX3000.
- Even tokens are characters sent by the AX3000 after the expected token has been received.

A login script looks like:

```
aaaaaa\00bbbbbb\00cccccc\00dddddd
```

#### b) Example

With the following script:

```
login:\00root\0D\00password:\00mypwd\0D
```

When the session is opened (<Alt><Fx>), the AX3000 acts as:

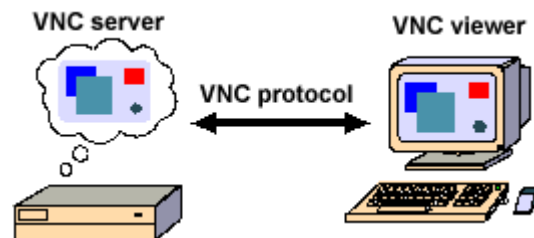
- Waiting for "**login:**".
- After "**login:**" has been received, the AX3000 sends "**root**" + <CR>. **Note:** as for the programmable keys, ASCII codes lower than 20h can be entered as 'xx' (where xx is the hexadecimal value of the ASCII code. Examples: Escape is \1B and <CR> is \0D.
- Waiting for "**password:**".
- After "password:" has been received, the AX3000 sends "**mypwd**" + <CR>.

**Note:** whilst a login script is running, the AX3000 keyboard is locked. In the event of a problem (wrong expected token), press <Esc> to skip the login script and to unlock the keyboard.

## 8.2 - GRAPHICAL MODE SESSION (VNC)

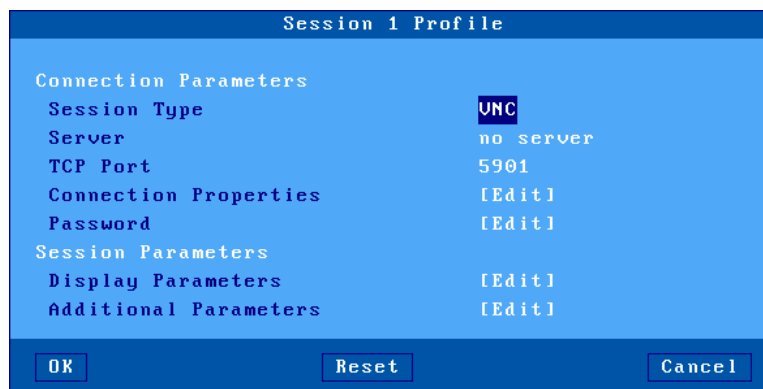
The VNC protocol enables a remote graphical display on the Axel-VNCviewer. The image is constructed, maintained and updated within the Unix server's frame buffer, and transmitted across the TCP/IP network.

**Note:** this protocol is public and the associated software is free. For more information please see <http://www.realvnc.com/>



**CAUTION:** Not to be confused with its opposite, the “VNC server” integrated in the AXEL thin client which allows a client to take control remotely (See chapter 10.2).

To set-up a VNC session, select **[Configuration]-[Sessions]-[Session X]** (where X is the session number). The following dialog box is displayed:

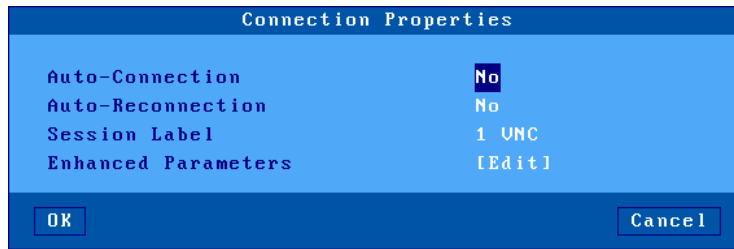


Set the following parameters:

- **Session Type:** select 'VNC'
- **Server:** selected from the server table (see Chapter [3.1.4](#)). A new server can be added by selecting 'IP address' or 'Server Name'.
- **TCP Port:** numeric value associated with the display (see Chapter [8.2.1](#)).
- **Connection Properties:** see next chapter.
- **Password:** this allows the optional VNC connection password to be stored (Note: this is the VNC password - not the user password).
- **Display Parameters:** see Chapter [8.2.2](#).
- **Additional Parameters:** lets certain VNC parameters to be changed. See Chapter [8.2.3](#).

**8.2.1 - Connection Properties**

The following box is displayed:



These parameters are:

- **Auto-Connection:** if this parameter is set to 'yes', the connection will be automatically established when the AX3000 is powered. Otherwise, the user can press <Alt><Fx> to establish the connection.
- **Auto-Reconnection:** if this parameter is set to 'yes', a new connection is automatically established after a disconnection. Otherwise, the user can press <Alt><Fx> to establish a new connection.
- **Session Label:** this character string (11 characters max.) is used to identify the session within the local desktop or in the taskbar.
- **Enhanced parameters:** see Appendix [A.7.3](#).

**8.2.2 - Display Parameters**

The following box is used to set the display parameters for the session:



- **“Primary” or “secondary”** monitor display: When 2 monitors are connected to the thin client, this parameter is used to display the session only on one of the 2 monitors, which possibly allows another session to be simultaneously displayed on the other monitor. (ex: 1 VNC session on 1 monitor and 1 RDS session on the other)
- **Multi-monitor:** the 2 monitors are seen as a single large monitor (eg 2 1920x1080 monitors are seen as a 3840x1080 monitor) (?)

- **Parameters:**



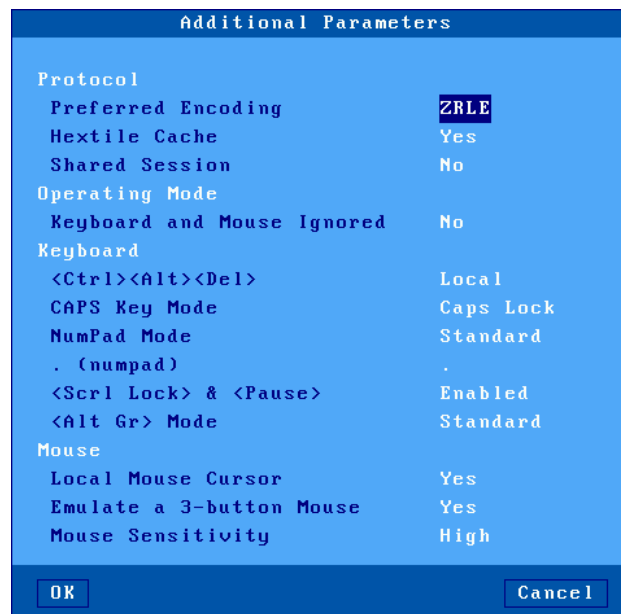
This box allows display settings (resolution, number of colors and frequency) to be set. The availability of these parameters depends of the Type value:

- **Dynamic:** The Resolution is given by the Xvnc server when the session is established. If supported, it's accepted by the thin client. Else default value (from general level) is used.
- **Default:** the three parameters (resolution, colors and frequency) are issued from general settings (see Chapter 3.2.2). When general settings are modified, these three parameters are automatically updated with new values.
- **Customized:** the three parameters are independent from general settings.

**Note:** the "Dual Monitor" option is always disabled.

### 8.2.3 - Additional Parameters

The following box is displayed:



These parameters are:

- **Preferred Encoding:** the 'encoding' is the data format used by the VNC server to send graphical data to the thin client. Supported encodings are:
  - Hextile: original encoding supported by all VNC server versions.
  - ZRLE: newer and higher performing encoding but is only supported by a RealVNC server V4. In addition, ZRLE graphical data may be compressed.
- **Hextile Cache:** when this parameter is disabled, display updates are directly done on the screen itself. Else a display update is first built in memory and then displayed. The global

performance is the same whatever the method. But the thin client is more comfortable to be used when the 'Cache Hextile' is enabled.

- **Shared Session:** this allows multiple VNC thin clients to share the same graphical display (i.e. the same server frame buffer).
- **Keyboard and Mouse Ignored:** if 'yes' all parameters related to mouse and keyboard are disabled. The thin client no longer sends mouse/keyboard event to the VNC server.
- **<Ctrl><Alt><Del>:** there are two modes for this keystroke:
  - Local: the keystroke is handled by the AX3000 and is used to shutdown the thin client (see Chapter 4.9)
  - Remote: the keystroke is handled by the VNC server.
- **CAPS Key Mode** : set the CAPS LOCK to behave in either of three ways:
  - Caps Lock: each alphabetical key sends the corresponding upper case letter. To unlock this mode press the <CAPS> key.
  - Shift Lock: each key send the same character sent by pressing <Shift><This key>. To unlock this mode press a <Shift> key.
  - Uppercase: each key send the upper character if it is present. Otherwise, this is the lower character (upper-case letter if possible) which is sent. <Shift> key acts in the standard way (whatever the CAPS key). To unlock this mode press the <CAPS> key.
  - Caps Lock +: same as 'Shift Lock'. But in addition ALL the keys supported (including <Esc>, function keys...).
- **Numpad Mode:** this parameter sets the type of keyboard event sent when pressing a key of the numpad:
  - Standard: keyboard events are thus defined by the RFB protocol.
  - ASCII: keyboard events are the same than the top row keys (above QWERTY). With this mode an application can't distinguish if the pressed key belong or not to the numpad. This mode may be required for some JAVA-based applications.
- **. (numpad):** the two available values are the dot (.) and the comma (,).
- **<Scroll Lock> & <Pause>:** enable or disable these two keys
- **<Alt Gr> Mode:** this parameter sets the type of keyboard event sent when pressing <Alt Gr> (located at the right of the space bar):
  - Standard: the keyboard event is AltGr.
  - Ctrl+Alt: the keyboard events are <Ctrl> and <Alt> (left of the space bar).
- **Local Mouse Cursor:** if 'no', the mouse cursor is fully handled by the VNC server. If 'yes', the behavior depends on the VNC server version:
  - Xvnc V3: as above the mouse cursor is handled by Xvnc. In addition the local mouse cursor location is indicated by a little square pointer (2x2 pixels). This can be useful when the local mouse cursor location is different from the VNC cursor location (for example when the Unix/Linux server or the network is overloaded).
  - Xvnc V4: the mouse cursor is handled by the AX3000. With a low-bandwidth, this allows the mouse cursor to be more reactive.
- **Emulate a 3-button Mouse:** if 'yes', the mouse middle button is emulated by clicking both left and right buttons.
- **Mouse Sensitivity:** This setting varies the sample rate of the mouse. If the sensitivity is increased the mouse movement will be more fluid, but also network activity is increased.

## 8.3 - CONTROLLING PRINTERS

Auxiliary ports 2 serial (G15), logical USB ports and network printer ports are provided by the AX3000. These ports are independently controlled so multiple printers can be attached to the AX3000.

A printer is generally controlled by a network service:

- **tty protocol:** this is an Axel proprietary protocol. A printer controlled by the tty protocol is seen as a local printer.
- **LPD protocol:** this service (RFCs 1048 and related) is provided as a standard feature by major operating systems (Unix/Linux, Windows, etc.). The main benefit of this protocol is an LPD printer can be shared by different operating systems.
- **rsh command:** this command allows the contents of a file to be redirected over the network.

In addition, a printer can also be controlled in "transparent mode" (by embedded escape sequences, like a printer attached to a serial terminal).

The following covers the tty protocol, the rsh command and the transparent mode. For more information about LPD printers, refer to Appendix A.3.

### 8.3.1 - The tty Protocol

The tty server is an Axel proprietary protocol. An additional piece of software is needed (see Chapter 8.4).

The Unix/Linux host must run the AXEL tty server daemon (`axttyd`). The configuration file `axttyd` must contain a list of AX3000 auxiliary ports and the pttys associated with each.

Each auxiliary port using the tty protocol (see Chapter 3.5.4) is identified by the name of the AX3000 (from the `/etc/hosts` file) and a special keyword. For example:

<code>axel1</code>	<code>aux1</code>	<code>/dev/ptyp12</code>	<code>/dev/ttyp12</code>
<code>axel1</code>	<code>aux2</code>	<code>/dev/ptyp13</code>	<code>/dev/ttyp13</code>
<code>axel2</code>	<code>parallel</code>	<code>/dev/ptyp2</code>	<code>/dev/ttyp2</code>

An auxiliary port controlled by the tty server is seen as a Unix/Linux local port (like a multi I/O board).

Data can be sent to an auxiliary port by:

- Either a redirection to the ttyp (example: "cat file > /dev/ttyp12")
- Or declaring a local printer attached to the ttyp (/dev/ttyp12). This printer is used through the `lp` command.

### 8.3.2 - The LPD Protocol

Set the auxiliary port as shown in Chapter 3.5.2.

Use the appropriate UNIX system management tool to add a remote printer. At least, two parameters are requested:

- The name of the remote host: enter the AX3000's hostname (refer to **/etc/hosts**),
- The name of the printer: this is the **Printer Port Name** entered when the AX3000 was set up.

Run the `lp` command to use this printer.

**Note:** some options of the `lp` command (number of copies, banner, etc) cannot be used, because the AX3000 is not a UNIX server and has no hard disk on which to run a spooler.



### **8.3.3 - The rsh Command**

The rsh command (or rcmd on SCO OpenServer) can be used to print a file.

The rsh parameters are:

- The hostname or the IP address of the device,
- A keyword which is the AX3000 auxiliary port name. This name has been set through the AX3000 Set-Up (see Chapter [3.5.6](#)).

To print a file, the rsh command reads data from 'standard input' (`stdin`) and sends this data to one of the AX3000's auxiliary ports. For example:

```
$ rsh axname parallel < file <CR>
```

In this example, `axname` is the name of the AX3000 (refer to `/etc/hosts` file) and `parallel` is the Printer Port Name of the AX3000 auxiliary port.

### **8.3.4 - Using Transparent Mode**

One of the auxiliary or logical ports should be selected as the default printer port which will be controlled by escape sequences.

Select the **[Configuration]-[Terminal]-[Miscellaneous]** dialog and set the 'default printer port'.

This default port can only be used if no network service (`lpd`, `tty`, etc) is currently using it.

**Note:** the default printer port is also used to perform local printing of the screen using the **<Prt Scr>** key

## **8.4 - THE AXEL TTY SERVER**

### **8.4.1 - Overview**

The TTY server emulates a multi i/o board connection over a TCP/IP connection. For example using this service a remote printer attached to an Axel thin client is accessed by Unix as a local printer via `/dev/tty4`, which may be preferable over using LPD in certain circumstances. Similarly the Axel thin client can be accessed via a predetermined and fixed `/dev/tty`, which in certain cases may be preferable over using telnet.

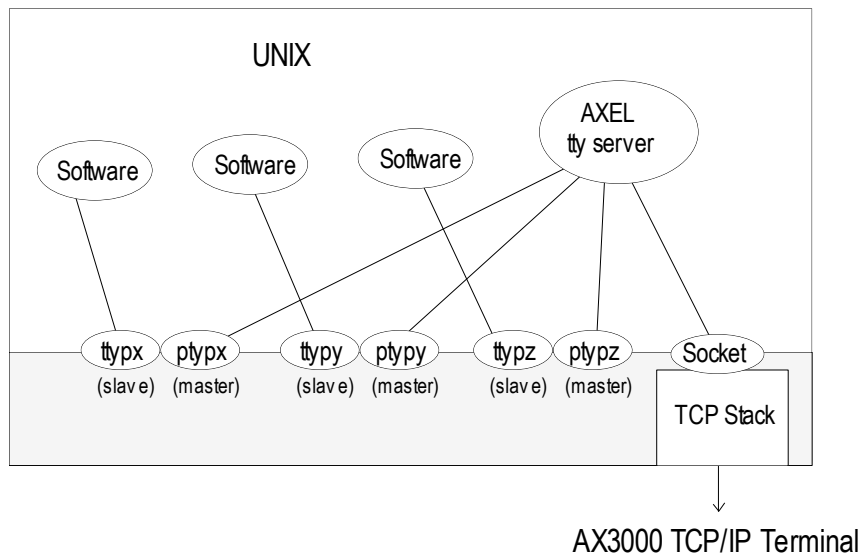
The AXEL tty server is a UNIX daemon (`axttyd`). The `axttyd` daemon must be used with the AX3000 `tty` or `rtty` network service.

The AXEL tty server creates a 'pipe' between pseudo devices on the UNIX host (`/dev/ttypx`) and AX3000 resources (sessions and/or auxiliary ports). This 'pipe' lets Unix treat the Axel sessions and auxiliary ports as local resources.

**Note about pseudo-terminals:** a pseudo-terminal is composed of two parts: a master file and a slave file. UNIX supports two possible styles for naming pttys:

- One master and X slaves (AT&T style): the master filename is **/dev/ptmx** and the slave filenames are **/dev/pts/xxx** (where **xxx** is a number).
- X masters and X slaves (Berkeley style): the master filename is **/dev/ptypxxx** and the slave filenames are **/dev/ttypxxx** (where **xxx** is the same number for master and slave).

The following drawing shows the Unix/Linux mechanisms:



#### 8.4.2 - Installing an AXEL tty server

Copy to **/etc** and rename as **axttyd** the appropriate binary. Example for IBM AIX:

```
# cp axttyd.AIX /etc/axttyd <CR>
```

**Note:** the source file and the **makefile** are also provided. If the binary file required for your operating system is not provided, it can be generated.

Copy the AXEL association file (**axfile**) into the **/etc** directory:

To launch the AXEL tty server automatically, whenever the host is booted, copy into the boot directory the **S91axel** file (for Unix) or the **S91axtty** file (for Linux).

The **S91axel** or **S91axtty** files launch the AXEL tty server. If parameters other than the default are required, this command line can be edited.

### 8.4.3 - Using an AXEL tty server

#### a) Overview

The AXEL tty server uses a configuration file which lists all authorized associations between AX3000 resources and UNIX ptty. Each entry in this file contains four parameters:

- AX3000 hostname (see **/etc/hosts**)
- The AX3000 resource, which depends on which network service is used:
  - tty on thin client session: **sess1** to **sess6**
  - tty on auxiliary port: **aux1**, **aux2** and **parallel**,
  - tty on logical USB port: **usb1** to **usb4**,
  - tty on logical TCP port: **net1** to **net4**,
  - rtty: encoded by a TCP port
- The master file of the pty (**/dev/ptty** or **/dev/ptmx**)
- The slave file of the pty (**/dev/ttyp**, **/dev/pts/xxx** or a link file automatically created by **axttyd**).

For example:

#AX3000	Resource	Master	Slave
axel1	aux1	/dev/ptyp12	/dev/ttyp12
axel1	aux2	/dev/ptmx	/dev/pts/13
axel2	2050	/dev/ptyp0	/dev/ttyp0
axel2	sess1	/dev/ptmx	/dev/axel
axel2	sess2	/dev/ptyp2	/dev/ttyp2

#### Notes:

- Lines beginning with '#' are ignored.
- Association lines 1, 2, 4 and 5 use the tty service, and association line 3 uses rtty service.
- Association line 4 uses a link file (**/dev/axel**). This file is linked with an undefined slave ttyp (**/dev/pts/xxx**). This link file is automatically created when **axttyd** is run.

Errors (syntax error, unknown AX3000 hostname, pty not available, etc) are recorded in a log file.

### **b) Running the Axel Tty Server**

The command to start the AXEL tty server is:

```
/etc/axttyd [-f file] [-l log] [-n port] [-hbFUk] &
```

- -b: use a buffer for received data.
- -f: configuration file (default: /etc/axfile).
- -F: tty buffers are flushed when the tty connection is established.
- -h: on-line help.
- -l: log file (default: /tmp/axttylog).
- -n: TCP port (default: 2048) for connections using the tty service.
- -U: only unidirectional dataflow is supported. Data from the network is dropped.
- -k: turn-off keepalive function.

**Note:** take care to add the '&' character at the end of line.

The AXEL tty server can be started either from the UNIX command line or at boot time (from **S91axel** or **S91axtty**).

All authorized associations, connections and disconnections will be recorded in the specified log file.

#### **8.4.4 - The axttyd Mechanism**

The axttyd daemon performs the following steps:

- **init stage:** association file checking (errors are reported in the log file) and associated pty opening (masters and slaves),
- **rtty stage:** for each rtty association, a child process is created. Each child process listens on the associated pty. When data is received a socket is opened on the AX3000 auxiliary port. Bi-directional communication is then enabled. If no data is sent or received for any one minute interval, the connection is closed. It will be opened again, the next time data is received from the pty.
- **tty stage:** when all the rtty child processes are created, the axttyd daemon listens on the TCP/IP socket (generally 2048). For each connection request (from an AX3000 tty service), a child process is created. This process controls communication between the pty and the AX3000 resource (session or auxiliary port).

### **8.4.5 - Uninstalling**

Remove the AXEL files and kill the AXEL tty server process (signal TERM):

```
# kill -TERM pid<CR>
```

where `pid` is the process ID of the AXEL tty server.

### **8.4.6 - In Event of Problems...**

In event of difficulties please consult the logfile (`/tmp/axttylog`) and to read the last messages.

#### ***a) Message "Cannot bind TCP port"***

The message indicates the axtty TCP port (2048 by default) is currently in use. This port must be released.

#### ***b) Message "Waiting for connections from TCP/IP socket"***

Initialization is correct and completed. The Axel tty server is now waiting for incoming connections. Check thin client settings (specially the tty auto-connection parameter). Possibly a firewall is blocking communication from the thin client to the server.

## **8.5 - REMOTE ADMINISTRATION**

### **8.5.1 - AxRM Software**

Axel's Windows administration utility (AxRM or Axel Remote Management) is available free on the Axel Web site. See Chapter [10.1](#).

### **8.5.2 - Using Unix/Linux Commands**

The rsh command can be used to run remote commands (get set-up, reboot...) onto the thin client. Available administration commands are described in Appendix [A.6](#).

In addition, a telnet server is embedded on the Axel thin client. This allows the thin client Set-Up remote control.



**- 9 -**  
**TOOLS AND STATISTICS**

*This chapter describes the embedded Axel Thin Client tools.*

The interactive set-up provides the following administration features:

- Using a memory stick to transfer a configuration file
- Updating the thin client firmware (memstick or network)
- Ping command
- Connection management
- Interface information
- USB device list

## 9.1 - HANDLING A CONFIGURATION FILE WITH A MEMSTICK

A configuration file is a text file. It can list some or all AX3000 set-up parameters.

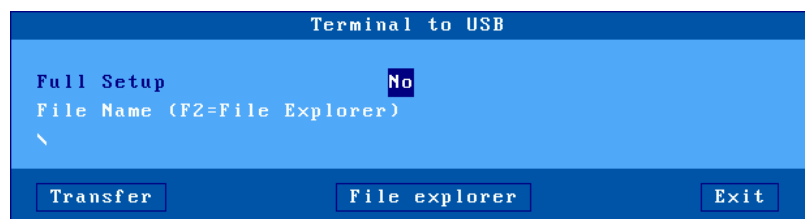
For more information about the configuration file format, see the Chapter [10.4.2](#).

The configuration file management can also be done remotely. See Chapter [10](#).

### 9.1.1 - Obtaining and Storing the Configuration File

The configuration file can be obtained from a pre-configured.

Select the **[Upgrade]-[Config File]-[Terminal to USB]** menu from the AX3000 set-up. The following box is displayed:



When **'Full Set-Up'** option is selected, all non-used thin client parameters will be included (as comments) in the configuration file.

The configuration filename can be manually entered or located with the [File Explorer] button.

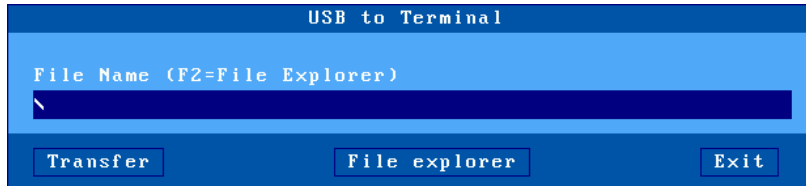
Click the [Transfer] button to launch the operation.



### 9.1.2 - Send a Configuration File to the Thin Client

A configuration file can be sent to the thin client.

Select the **[Upgrade]-[Config File]-[USB to Terminal]** menu from the AX3000 set-up. The following box is displayed:



The configuration filename can be manually entered or located with the [File Explorer] button.

Click the [Transfer] button to launch the operation.

**IMPORTANT:** the thin client will automatically reboot after this operation.

## 9.2 - UPDATING THE FIRMWARE

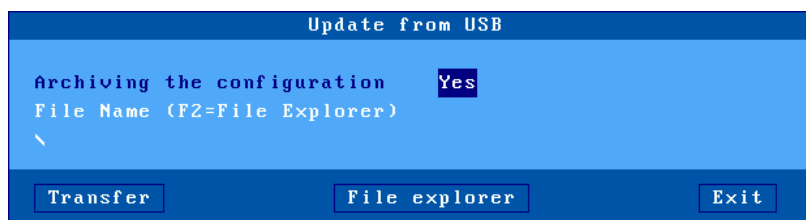
The thin client firmware can be updated. This can be done:

- Remotely with the AxRM software. See Chapter [10](#).
- From a USB memstick.
- With the bootp/tftp protocol.

All Axel products have an 'FK' (Firmware key) number. **It is important that the firmware file and Axel hardware have the same FK number.** If not, the update will fail.

### 9.2.1 - From a MemStick

Select the **[Upgrade]-[Firmware]-[Update from USB]** menu from the AX3000 set-up. The following box is displayed:



When 'Archiving the configuration' option is selected, before the firmware upgrade, the configuration file will be stored at the memstick root (the filename is the thin client MAC address).

The firmware filename can be manually entered or located with the [File Explorer] button.

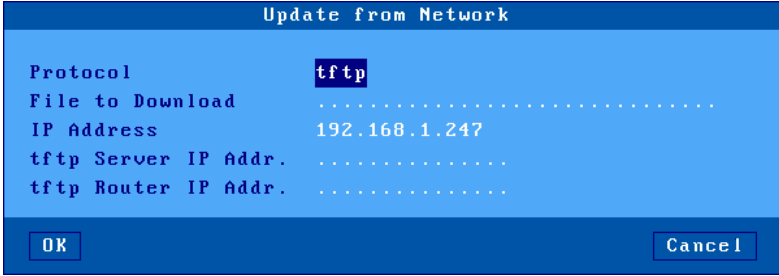
Click the [Transfer] button to launch the operation.

**IMPORTANT:** the thin client will automatically reboot after this operation.

The configuration is not sent automatically to the thin client after the firmware update.

### 9.2.2 - With bootp/tftp Protocols

Select the **[Upgrade]-[Firmware]-[Update from Network]** menu from the AX3000 set-up. The following box is displayed:



```
Update from Network
Protocol          tftp
File to Download  .....
IP Address        192.168.1.247
tftp Server IP Addr. ....
tftp Router IP Addr. ....
OK                Cancel
```

Firmware can be updated in one of two ways:

- **tftp** protocol: the operator must enter the location of the firmware file.
- **bootp and tftp** protocol: this is an automatic procedure. The necessary parameters will already be available from a bootp server.

**Note:** AxRM can act as a bootp/tftp server

**IMPORTANT:** the thin client will automatically reboot to perform this operation.

### 9.3 - THE PING COMMAND

The ping command is used to check for the presence of a live TPC/IP device. Select the **[Diagnostics]-[Ping]** dialog from the AX3000 set-up, then select the server name from the list or enter the IP address or the DNS name of the server.

## 9.4 - CONNECTION MANAGEMENT

Connection failures are often caused by incorrect settings.

### 9.4.1 - Global Connection List.

Select the **[Diagnostics]-[Connections]** dialog to check the status of all defined connections:

Connections							
SESSIONS							
#	Type	State	Server	Host IP Addr.	Port	Miscellaneous	
1	TSE	Connected		192.168.1.156	3389	.....	
2	telnet	Connected		192.168.1.181	23	IBM5250	
3	telnet	Connected		192.168.1.150	23	ANSI	
AUXILIARY PORTS							
Port	Service	State	Other Information				
Aux1	prt5250	Connected	as400	192.168.1.181	23	AXELPRN	(1902)
Aux2	None	Closed					
PARA	None	Closed					
Net1	None	Closed					
Net2	None	Closed					
Net3	None	Closed					
Net4	None	Closed					

Refresh      Close Connections      Exit

**Note:** 'outside' the set-up, use <Ctrl><Alt><X> displays this box.

For each session, the following information is displayed:

- **No:** session number.
- **Type:** main values are TSE, ica, telnet, tty, vnc...
- **State:** the possible values are:
  - Established: the session is connected,
  - Closed: the session has ended,
  - Syn sent: connection request in progress,
- **Time Wait:** connection close in progress.
- **Server and IP Addr Host:** the associated host.
- **Port:** the TCP port used for the session (this is usually 23 for telnet, 2048 for tty and 59xx for vnc).
- **Configuration:** the associated pre-defined configuration.
- For each auxiliary port, the following information is displayed:
- **Port:** the name of the port: Aux1, Aux2, PARA (parallel), Usb1 to Usb4, Net1 to Net4
- **Service and Other:** information about the associated network service:
  - lpd: printer port name and optional filter,
  - rcmd: printer port name,
  - telnet: associated host, TCP port, TERM and connection flags,
  - tty: associated host, TCP port and connection flag,
  - prt5250: associated host, TCP port, printer name and AS/400 connection status,
  - printd or rtty: TCP port and optional filter.

- **State:** see above for the possible values.

A connection can be manually closed by selecting the [CLOSE CONNECTION] button.

**Note:** to refresh the information displayed, select the [REFRESH] button.

**9.4.2 - "TCP Server" and "TCP Client" Connection Information**

To go further with connection information, two additional statistics dialog boxes are available:

- **TCP server:** contains information about connections where the AX3000 is acting as a server (lpd, rty and rcmd).
- **TCP client:** contains information about connections where the AX3000 is acting as a client (telnet, tty, rdp, ica and vnc).

These statistics show the following:

- Information about connections
- Values of counters

These dialog boxes are accessed by the **[Diagnostics]-[Statistics]-[TCP xxx]-[yyy]** menu.

Example of a TCP client connection box:

TCP/Client Statistics							
Who	Type	State	Local Socket	Remote Socket	Rcv-Q	Snd-Q	
S1	Rdp	Connected	192.168.1.245:1389	192.168.1.156:3389	0	0	
S2	Telnet	Connected	192.168.1.245:1025	192.168.1.181:23	0	0	
S3	Telnet	Connected	192.168.1.245:1403	192.168.1.150:23	0	0	
aux1	Pr5250	Connected	192.168.1.245:1032	192.168.1.181:23	0	0	

Refresh Exit

Description of the information given within this box:

- **Who:** AX3000 resource involved in the connection: S1 (session 1), ..., S8 (session 8), Aux1, Aux2, PARA (parallel), Usb1 to Usb4, Net1 to Net4.
- **Type:** network service being used (telnet, tty, etc).
- **State:** the possible values are:
  - Established: the session is connected,
  - Closed: the session has ended,
  - Syn sent: connection request in progress,
  - Time Wait: connection close in progress.
- **Local Socket:** IP address and TCP port for the AX3000.
- **Remote Socket:** IP address and TCP port for the host.
- **Rcv-Q:** number of bytes received by the AX3000 and not yet processed
- **Snd-Q:** number of bytes not yet sent to the host

Example of a counter box:

TCP/Client Statistics			
<b>GENERAL</b>		<b>ERRORS</b>	
Sent Connection Requests	0	Bad CRC	0
Sent Reset Frames	0	Bad Length	0
Received Broadcasts	0		

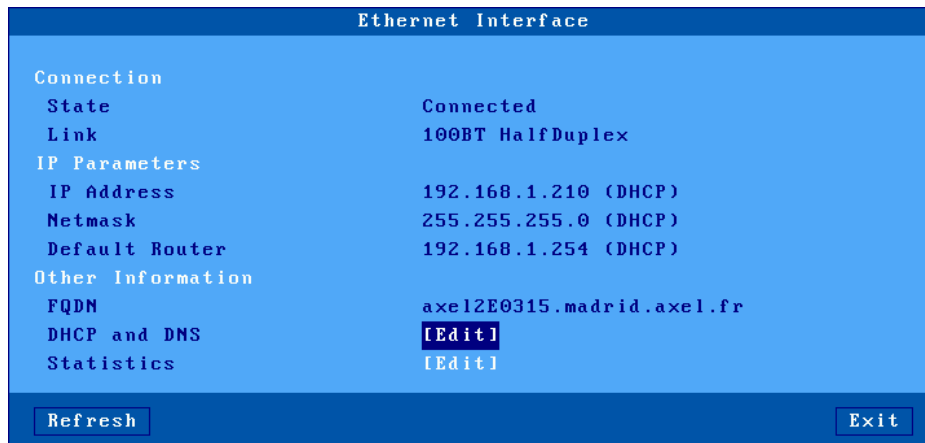
Refresh Exit

**9.5 - ETHERNET INTERFACE INFORMATION**

**9.5.1 - Ethernet Interface**

**a) State**

The following information is displayed when selecting the **[Configuration]-[Network]-[Ethernet Interface]-[State]** menu:



**Note:** this information is automatically updated every 5 seconds. To force an update, use the [Refresh] button.

In the above dialog box, the following information is given:

- **Link:** speed and type the network interface (useful when set in auto-sense mode).
- **IP parameters:** IP address, netmask and default router
- **FQDN:** thin client full name
- **DHCP and DNS:** Information DHCP and DNS, See Chapter [9.5.1.b](#)
- **Statistics:** Lan Statistics from boot, See Chapter [9.5.1.c](#)

## b) DHCP/DNS

The DHCP/DNS box is the following:



In the above dialog box, the following information is given:

DHCP client:

- **State:** the current DHCP state. The possible states are:
  - **selecting:** searching a DHCP server (broadcast)
  - **requesting:** requesting an IP address from the DHCP server which answered 'selecting'
  - **bound:** search has been successfully completed (IP address has been set)
  - **free:** DHCP protocol is not enabled or DHCP protocol failed
  - **renewing:** renewing the leased IP address to the DHCP server which answered 'selecting'
  - **rebinding:** renewing the leased IP address to any DHCP server (broadcast)
- **DHCP Server:** IP address of the DHCP server.
- **Lease Time (seconds):** amount of time of the leased IP address. For BOOTP protocol, the value is 'infinity'.
- **Remaining Lease:** remaining time before lease expires. For BOOTP protocol, the value is 'infinity'.

DNS Server Update by the Terminal:

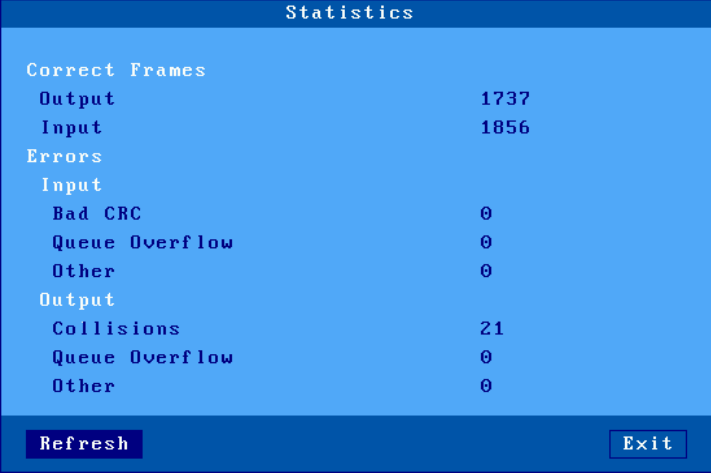
- **Update Type:** information about the DNS server update when updated by the thin client. Main values are:
  - **None:** no update
  - **Direct / Reverse:** both types are done by the thin client.
  - **Direct / Reverse (by DHCP):** direct update done by the thin client and reverse update done by the DHCP server
- **Status:** the possible update values are:
  - **None:** no update (not requested)
  - **Done:** update succeeded
  - **Failed:** update failed
  - **Pending:** update in progress
  - **Dhcp:** update done by the DHCP server (the thin client had been informed to forgive the update)

DNS cache:

- **DNS cache state:** allows you to view or delete DNS cache entries. If the DNS cache is disabled or if no entry is listed, this option is not accessible.

**c) Statistic**

The statistics box is the following:



The screenshot shows a window titled "Statistics" with a blue background. It displays network statistics in a list format. The "Correct Frames" section shows 1737 Output and 1856 Input. The "Errors" section is divided into "Input" and "Output" categories, with various error types like "Bad CRC", "Queue Overflow", and "Collisions" all showing a count of 0. At the bottom, there are "Refresh" and "Exit" buttons.

Statistics	
Correct Frames	
Output	1737
Input	1856
Errors	
Input	
Bad CRC	0
Queue Overflow	0
Other	0
Output	
Collisions	21
Queue Overflow	0
Other	0

**Correct Frames:** "Output" and "Input" are the number of correct frames (transmitted and received)

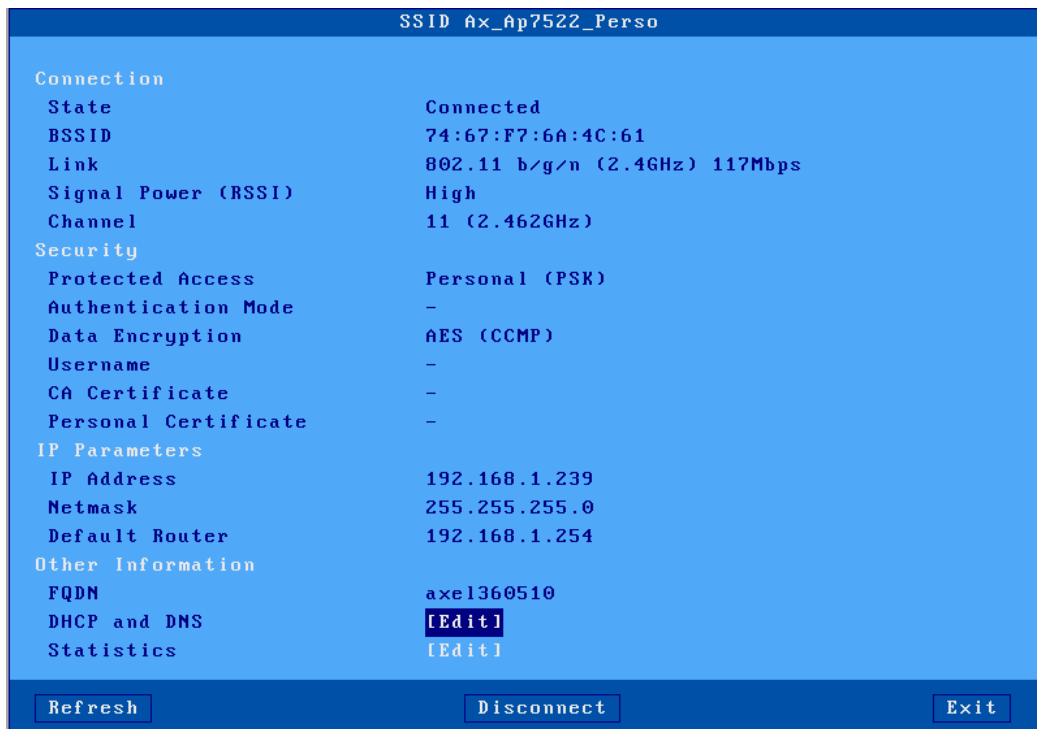
**Errors:** this section gives the type and the number of errors. No errors should be shown in a good working environment/healthy network.



## 9.5.2 - Wireless Interface

### a) State

The following information is displayed when selecting the **[Configuration]-[Network]-[Wireless Interface]-[State]** menu:



**Note:** this box information is automatically updated every 5 seconds. To force an update, use the **[Refresh]** button.

When the wireless interface is connected, the 802.11 information available is:

- **BSSID:** access point MAC address.
- **Link:** protocol and current speed.
- **Signal power** (reception)
- **Channel:** channel number and frequency
- **Security**
  - Access control: PSK personnel, company (EAP) or 802.1X
  - Authentication mode: LEAP, PEAP (MS-CHAP v2), EAP-TLS
  - Encryption type: EAS (CCMP), TKIP
  - Username: username used for authentication (if necessary).
  - Authority certificate: CA used for verification (if necessary).
  - Personal Certificate: Certificate used for authentication (if necessary).

For more security information see chapter [3.1.3.b](#)

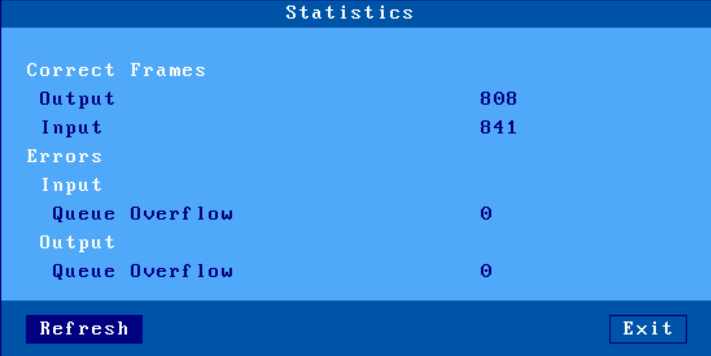
For other information (IP Parameters and Other Information) see chapter [9.5.1.a](#)

**Note:** this dialog box is also accessible by the key sequence **<CTRL> <ALT> <W>** if it is not disabled during setup (see chapter [3.2.1.b](#))

The DHCP/DNS box is similar to the Ethernet dialog box, see chapter [9.5.1.b](#).

### c) *Statistic*

The statistics box is the following:



Statistics	
Correct Frames	
Output	808
Input	841
Errors	
Input	
Queue Overflow	0
Output	
Queue Overflow	0

Refresh Exit

## 9.6 - USB STATISTICS

The [Diagnostics]-[USB] menu lists the connected USB devices. For example:



USB Devices List	
2	USB SmartCard Reader
4	PS2 to USB Adapter
4	PS2 to USB Adapter
4	PS2 to USB Adapter
4	PS2 to USB Adapter
1	DataTraveler 2.0

Refresh Exit

For each line the number is the USB physical port number. The associated label is given by the USB product itself. If the USB product is supported, more information can be obtained by clicking the product name.

**- 10 -**  
**REMOTE ADMINISTRATION**

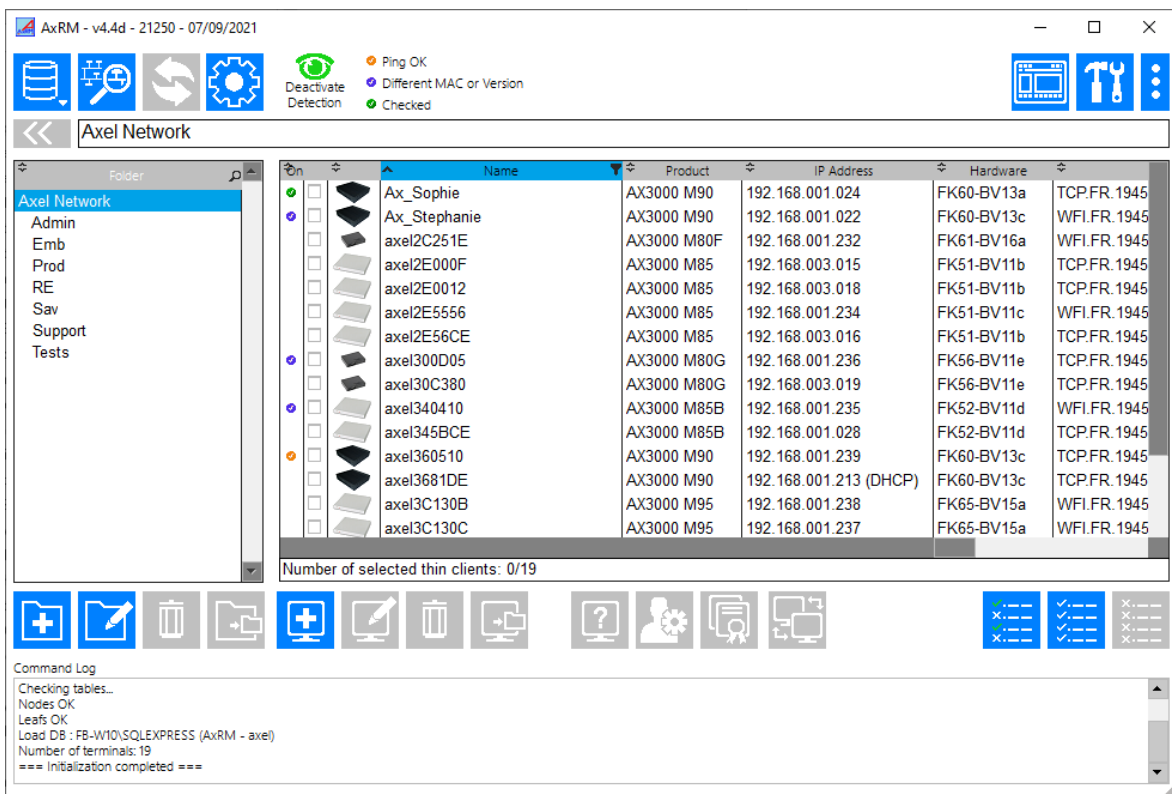
This chapter covers remote administration of the TCP/IP AX3000.

Four types of operations are provided by the remote administration:

- The use of AxRM,
- The remote control,
- The interactive telnet setup,
- The batch set-up (getting and sending a set-up file)

### 10.1 - AXRM: THE AXEL MANAGEMENT SOFTWARE

A Windows administration utility (AxRM or Axel Remote Management) is available at no charge from the Axel Web site (<http://www.axel.com>):



The AxRM software allows system administrators to manage and configure Axel TCP/IP products remotely over a network. The remote Axel device is selected by its IP address or network name. (The

software can also assign an IP address to a newly installed thin client that has not had an IP address set)

AxRM is an abbreviation for Axel Remote Management software.

AxRM is used for:

- Obtaining hardware and firmware revision levels
- Obtaining Ethernet and serial line configuration
- Obtaining network and device statistics
- Obtaining set-up configuration
- Rebooting the peripheral
- Remotely configuring a peripheral
- Downloading firmware,
- Entering the interactive set-up via a telnet client.

It is also possible:

- To build and manage a thin client database,
- To compile a list (batch) of commands to run consecutively,
- To download a firmware through BOOTP,
- To set IP addresses by using the device MAC address.
- Repair thin clients that have lost their firmware (bootp error)

For more information about the AxRM utility, read the manual "*Axel Remote Management*".

## 10.2 - REMOTE CONTROL

This functionality allows an administrator to remotely take control of a thin client. The administrator can passively watch the users screen or actively take control with his own keyboard for various support or administration purposes.

**Note:** the remote-control function must be enabled on the thin client (see below)

To set-up the remote control function, select the menu **[Configuration]-[Terminal]-[Remote Control]**. For more information, please refer to Chapter [3.2.7](#).

Three remote control modes are available:

- **Telnet mode:** This mode allows you to interactively modify the setup of a thin client remotely from a classic "telnet" or from AxRM. The default port is "4096" but it can be changed see chapter [3.2.7.b](#).  
In this mode, the mouse is not managed, the setup is displayed simultaneously on the thin client and it is not possible to interact with the sessions. This mode uses very little bandwidth.
- **Text mode:** This mode allows you to interactively modify the setup of a thin client remotely, and to interact on "text" type sessions only. It can only be implemented with the

administration software "AxRM" or directly with its external component "AxViewer". This mode uses very little bandwidth.

- **VNC mode:** It allows full access to the thin client (setup and interaction with any type of session), it can be implemented directly by a classic VNC client or by the "AxRM" or "AxViewer" software.

The advantage of "AxRM" or "AxViewer" software is that they allow the use of keyboard shortcuts (eg <CTRL> <ALT> <ESC> to enter the setup) which is not the case with a classic VNC client.

Based on the VNC protocol, this mode is very bandwidth-intensive.

Use AxRM to take the control of the thin client. See Chapter [10.1](#).

### 10.3 - INTERACTIVE TELNET SET-UP

The AX3000 interactive set-up can be accessed through a telnet session. A specific TCP port is used.

The default value of this TCP port is 4096. This value can be changed. See Chapter [3.2.7](#).

We strongly advise using AxRM to open the telnet setup (see Chapter [10.1](#)). But any telnet client could be used with the correct arguments as below

- ANSI emulation (with color support)
- TERM value: "ansi"
- Screen size: 80x25
- Scrolling mode disabled

#### Notes:

- To disable the telnet set-up, set the TCP port to 0.
- When the telnet set-up is running, the set-up is also displayed on the target thin client. The keyboard of the target thin client is locked.
- The AX3000 telnet server supports the keepalive mechanism (value 3 minutes). In event of network incident, the set-up will be automatically ended and the keyboard of the target thin client will be unlocked.
- The possible connection errors are:
  - The interactive set-up is already in use on the target thin client.
  - The client telnet arguments as given above are not set.

## 10.4 - BATCH REMOTE SET-UP

This feature enables an AX3000 to be set up remotely, using the remote administration command.

### 10.4.1 - AX3000 Remote Set-Up

A text file (provided as an argument to the remote administration command) defines the value of some or all set-up parameters. It can either be:

- Created with a text editor
- Obtained by a remote administration command on an AX3000 already set-up.

We strongly advise using AxRM to operate with the batch setup (see Chapter [10.1](#)), but the native rsh system commands can be used.

The remote administration command parameters are:

- The name or the IP address of the AX3000,
- A command: one of the 3 following keywords:
  - **setup\_send** : set-up an AX3000,
  - **setup\_get** : get an AX3000 configuration,
  - **ax\_reboot** : reset an AX3000.

Example for obtaining a set-up:

```
# rsh axname setup_get > /tmp/file<CR>
```

Example for sending a set-up:

```
# rsh axname setup_send < conf_file
```

Example for rebooting a thin client (required after sending a set-up):

```
# rsh axname ax_reboot
```

See Appendix A.6 for more information about administration command.

### 10.4.2 - Configuration File Format

A configuration file can list some or all AX3000 set-up parameters. And it begins with the label 'BEGIN\_AX\_SETUP' and ends with the label 'END\_AX\_SETUP'.

Example:

```
BEGIN_AX_SETUP V1.1
# this is a comment
tcp_host1_name=vangogh
...
END_AX_SETUP
```

**Note:** lines beginning with '#' are treated as comments and ignored.

When a configuration file is obtained from an AX3000, the inactive parameters (undefined hosts, print server unused, coloring mode disabled, etc) are commented out.

#### a) Header

```
BEGIN_AX_SETUP V1.1
#####
#          TCP/IP AX3000 Platine Terminal          #
#          #                                       #
# Ethernet address: 00:A0:34:20:27:10             #
# Firmware: FK18.BV2.1a/TCP.FR.1236b.STD         #
# 12354                                           #
#####
#
RESET_CMOS
```

**Note:** the RESET\_CMOS command allows all the set-up parameters (except the AX3000 IP address) to be reset. This line can be deleted or set as a comment.

**b) Substitution Commands**

axname_encoding_string=	(yes   no)
-------------------------	------------

Enabling "axname\_encoding\_string" allows some set-up parameters to contain 'substitution commands'. This allows variables such as the thin client name and the session number. The substitution is done when a set-up file is sent to the thin client.

☺ : this function is useful when multiple thin clients are configured with the same set-up file, but each thin client requires certain unique parameters.

**Notes:**

- It works only through the remote set-up function. (It's not available with the interactive set-up).
- Some set-up parameters are not supported by this function: the thin client name, the passwords, the pre and post-printing sequences and the transparent mode sequences.

The substitution commands are:

- <\$> is the parameter "tcp\_axname"
- <#> is the session number (1 to 6) or the port number (AUX1=1, AUX2=2, PARALLEL=3, NET1=4, NET2=5, NET3=6, NET4=7, USB1=8, USB2=9, USB3=10, USB4=11).
- <\$(X,Y)> is an "tcp\_axname" sub-string (start X, length Y).

**Notes:**

- If X is greater than the "tcp\_axname" length, the substring is empty.
- If X+Y is greater than the "tcp\_axname" length the substring is truncated.
- In event of syntax error the substitution is not done.

**Example:** if the thin client name is "axel201234":

```
TERM<$(7,4)>           => TERM1234
TERM<$(7,10)>          => TERM1234
TERM<$(20,7)>           => TERM
TERM<$(20,A)>           => TERM<$(20,A)>
<$(1,2)><$(7,4)>-<#>    => ax1234-2 (ex.: session 2 or AUX2)
```

**c) End of File**

The configuration file must be ended with the label 'END\_AX\_SETUP'



**APPENDIX**

The following appendices give information about:

- A.1 - Using the AX3000 interactive set-up
- A.2 - Network overview (Ethernet address, IP address and routers)
- A.3 - DHCP protocol
- A.4 - DNS protocol
- A.5 - Axel DHCP Option
- A.6 - Administration command list
- A.7 - Going further...
- A.8 - Hardware and firmware information

## A.1 - USING THE INTERACTIVE SET-UP

### A.1.1 - Entering the Set-Up

The following can be used to enter the AX3000 interactive set-up:

- Using <Ctrl><Alt><Esc> from the thin client
- Using the AxRM remote control command. See Chapters [10.1](#) and [10.2](#).
- Using Telnet to access the thin client remotely. See Chapter [10.3](#).

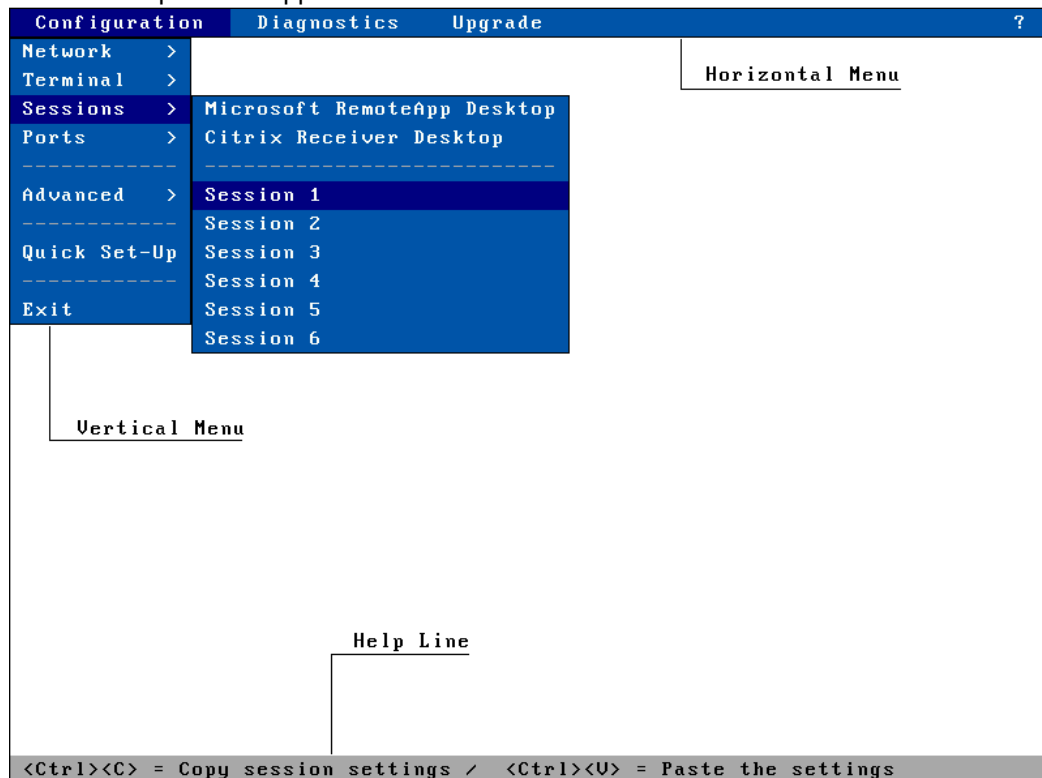
**Note:** the set-up can be password-protected, in which case the password must be entered to access the quick set-up dialog box. For more information, see Chapter [3.2.8](#).

### A.1.2 - Navigation

The AX3000 set-up comprises a horizontal general menu, with drop down vertical menus.

A help line is located in the bottom of the screen.

The AX3000 set-up screen appears as follows:



### **a) The Horizontal General Menu**

Move through the menu with horizontal arrow keys. A different vertical menu will be displayed automatically as each item is traversed.

### **b) Vertical Menus**

Move through vertical menus with vertical arrow keys. Confirm the selected command by pressing **<Enter>** or **<Spacebar>**.

**Note:** the symbol '>', beside a vertical menu item, indicates that it is a sub-menu.

### **c) Dialog Boxes**

Use the **<Tab>** or **<↓>** to move to next field or button. Use the **<Shift><Tab>** or **<↑>** to move to previous field or button.

Two types of fields are distinguished in a dialog box:

- Button: press **<Enter>** or **<Spacebar>** to perform the associated action.
- Parameter: two types of value occur:
  - A free value (numeric or character string): the data capture mode is automatically enabled (see the next chapter).
  - A discrete value: press **<Spacebar>** to show the permitted values or to display a list of values. Move through lists with vertical arrow keys; confirm the selected value by pressing **<Enter>**. Press **<Esc>** to cancel.

#### **Notes:**

- Pressing **<Enter>** on a 'Parameter' field allows the default button ([OK], [Next]...) to be selected.
- Pressing **<F10>** allows selecting the 'default' button. Or, if this button is already selected, perform the associated action.

Select the [OK] button to save modifications and exit the dialog box. Select the [Cancel] button or press **<Esc>** to exit the dialog box without saving modifications.

### **A.1.3 - Enter Data**

When a 'free value' parameter field is selected, a value must be entered (it cannot be selected from a list).

**Note:** to indicate 'free value' mode, the cursor blinks at the beginning of the field.

During this mode the following keys are enabled:

- **<Tab>**, **<↓>**, **<Shift><Tab>**, **<↑>**: valid the value and move to the next/previous field.
- **<Esc>**: abandon your changes
- **<←>** and **<→>**: move the cursor within the character string
- **<Home>** and **<End>**: move the cursor directly to the beginning or the end of the string
- **<Del>**: delete the character at the cursor position
- **<Backspace>**: delete the character before the cursor position
- **<Insert>**: one of two editing modes (Insertion/Overwrite)

To enter characters with an ASCII code lower than 20 hexadecimal, use a backslash ('\') before the hexadecimal value. For instance, the 'Esc z' sequence can be encoded by '\1Bz'.

**Note:** when the character string is longer than the length of the field, two indicators are displayed at the left and at the right of the field.

#### **A.1.4 - Special Notation**

The set-up is a sequence of menus and sub-menus. Define an action by the path followed through the set-up tree (hierarchy), using the following notation:

**[item1]-[item2]-[action]**

For example, to perform the above **action**, select **item1** in the main menu, then select **item2** in the sub-menu.

#### **A.1.5 - Exiting the set-up**

To exit the set-up, select **[Configuration]-[Exit]**.

If changes have been made while in the set-up, a dialog box appears:

- Select [Yes] to save the modifications and exit the set-up. The new AX3000 settings will then be stored in NVRAM (non-volatile memory).
- Select [No] to abandon your changes and exit the set-up.

## **A.2 - NETWORK OVERVIEW**

### **A.2.1 - Ethernet Addresses**

Axel thin clients (like other devices equipped for Ethernet networking) have a unique hardware address which is issued by the manufacturer and cannot be modified. This address is in the form of six hexadecimal bytes, separated by colons:

AX3000 Ethernet address format:

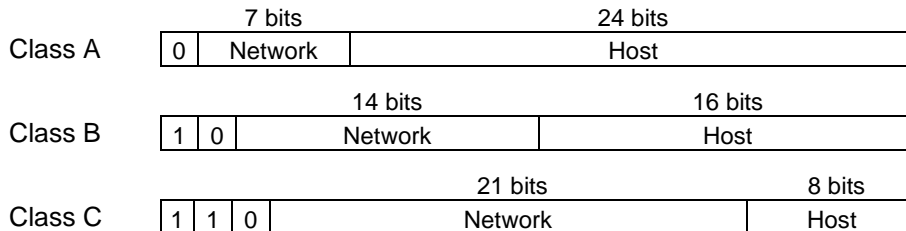
**00:A0:34:xx:xx:xx**

Select the **[?]-[Information]** command in the horizontal menu of the AX3000 set-up to see the AX3000 Ethernet address.

### A.2.2 - IP Address

Every device connected to an Ethernet network must have a single 32-bit address which encodes both the network and the host ID. Internet addresses (sometimes called «IP addresses») are usually written as four decimal numbers separated by decimal points ('.' character).

There are three main classes of IP address:



Thus every IP address occupies 4 bytes and contains both:

- A network address, and
- A host address.

Note: all devices attached to the same network must have the same class and the same network address. Each must have a different host address.

**For example:** an AX3000 connected, over a network, to a host with an IP address 192.1.168.40 (class C: three bytes for the Network address) must have the three first bytes of its address set to 192.1.168. The fourth byte cannot be equal to 40.

### A.2.3 - Router

Depending on the network topology, the AX3000 and the host may be installed on different physical networks and linked through one or several routers.

Two types of router can be used to access remote networks:

- A default router: this router knows how to reach many remote networks.
- Specific routers: in charge of one remote network.

The default router is only identified by an IP address.

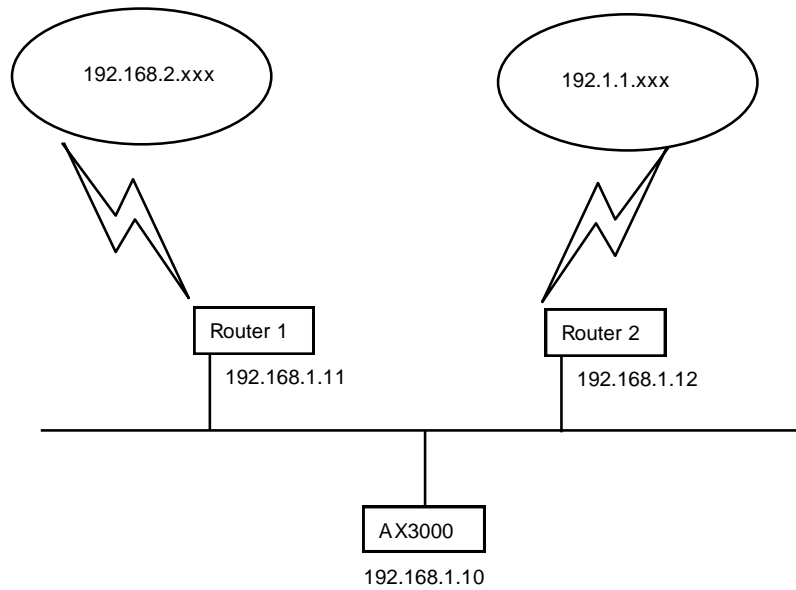
The specific routers are identified by the following parameters:

- **Router IP address:** this router must be connected to the same network as the AX3000.
- **Destination IP Address:** IP address of the host or the network to be reached.
- **Destination Type:** two values:
  - **Host:** the destination is a single host,
  - **Network:** the destination is a whole local network (the class mask is applied to this IP address).

#### **Notes:**

- At the AX3000 level, the routing algorithm uses a specific router to reach the destination. If no specific router fits, the default router is used.
- The AX3000 doesn't support ICMP REDIRECT requests (dynamic routers are not supported).

**Example 1:** router 1 is used to reach the 192.168.2.xxx network and router 2 is used to reach the 192.1.1.xxx network:



The AX3000 route table will show the following:

Other Routers			
Gateway IP addr	Target IP addr	Target Type	Netmask
192.168.1.11	192.168.2.0	Network	255.255.255.0
192.168.1.12	192.1.1.0	Network	255.255.255.0
.....	.....	.....	.....

Buttons: OK, Delete, Cancel

**Example 2:** router 1 is used to reach both networks (192.168.2.xxx and 192.1.1.xxx):

The AX3000 route table is:

Routers	
Default Router	192.168.1.11
Other Routers	[Edit]

Buttons: OK, Cancel

## A.3 - THE DHCP PROTOCOL

DHCP (Dynamic Host Configuration Protocol) is an industry standard protocol that lets a DHCP server (Unix, Windows, AS/400, etc.) allocate temporary IP addresses and other network parameters to thin clients and PCs when they are powered on. This can greatly simplify managing large networks.

### A.3.1 - Overview

Here is a brief description of Axel's implementation DHCP:

- At boot time the AX3000 broadcasts DHCP requests to find the DHCP server.
- If a DHCP server is found and correctly set-up, an IP address, and subsequently other parameters are given to the AX3000.
- Before accepting the IP address the AX3000 can be set to check that the IP address given really is free (ARP protocol).
- The IP address offered is given temporarily. This duration is called the 'Lease Time'.
- If a lease time has been entered through the AX3000 Set-Up, this lease time is offered to the DHCP server, which may or may not accept this value.
- The AX3000 is expected to renew its lease before the lease expires. Once the lease has expired the AX3000 is no longer permitted to use the assigned IP address.
- Generally an IP address is dynamically assigned out of a pool of IP addresses. However static IP addresses can be associated to AX3000s (for instance when the AX3000's print server is used). This association is performed either by using the AX3000 Ethernet address or by using a 'Client Identifier' (which is a character string entered through the AX3000 Set-Up).
- The DHCP protocol can be considered as a superset of the BOOTP protocol. IP addresses can also be offered to AX3000s by a BOOTP server (in this case the 'lease time' is infinite).
- The AX3000 DHCP client protocol is compliant with RFCs 1533 and 1541.
- This section deals only with the AX3000 DHCP protocol use. To set-up and enable a DHCP server please read your operating system's manual.

### **A.3.2 - Setting-Up the AX3000**

DHCP protocol is set through either the AX3000 Quick Set-Up or the AX3000 Interactive Set-up. For more information, see Chapters [2](#) and [3](#).

### **A.3.3 - Using the AX3000**

If the DHCP protocol is enabled the AX3000 automatically requests an IP address on boot, the message 'DHCP in progress' is displayed on the bottom of the screen.

**Note:** the search can be aborted by entering the set-up.

If a DHCP (or BOOTP) server is available an IP address is given after a few seconds. This dialog box is then cleared and the AX3000 follows its normal behavior: either the set-up idle is displayed (no automatic session is set) or an automatic connection is opened.

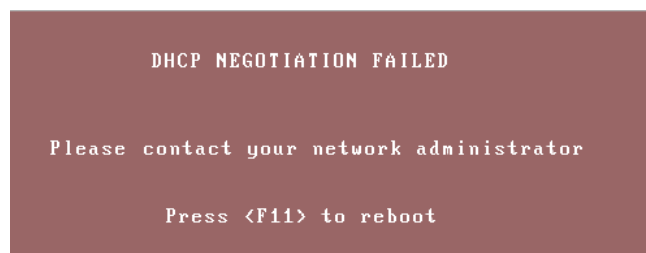
Further 'lease time' re-negotiations are totally invisible to the AX3000 user. Only error messages are displayed (see next chapter).

**Note:** enter the set-up to find out the AX3000 IP address or other parameters offered by the DHCP server.

### **A.3.4 - Errors**

#### ***a) Boot Time Failure***

The AX3000 automatically searches for a DHCP server on booting. If after 30 seconds no DHCP (or BOOTP) server answers the following dialog box is displayed:



At these stage two options are available:

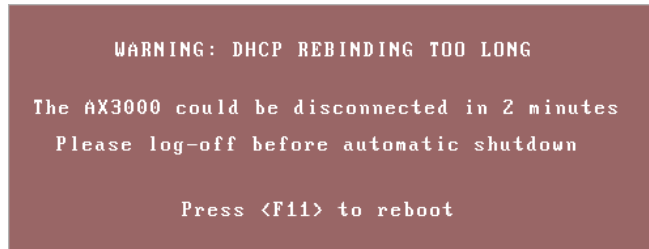
- <F11>: rebooting the AX3000 to run the DHCP search again.
- <Ctrl><Alt><Esc>: entering the set-up to modify AX3000 settings.



### b) Re-negotiation Failure

The lease time must be regularly re-negotiated (except if the IP address has been offered by a BOOTP server).

If a re-negotiation fails the following dialog box is displayed:



This indicates that in two minutes the AX3000 will no longer be permitted to use the leased IP address and the session will be terminated.

If after these two minutes, the re-negotiation has still failed, an error box is displayed and all current sessions (telnet, tty, lpd, etc.) are closed (i.e. lost). And the thin client is shutdown.

**Note:** the AX3000 Trace Mode allows a trace of data exchanged between the AX3000 and the DHCP server (see Chapter [3.1](#)). This is useful to diagnose problems.

## A.4 - THE DNS PROTOCOL

The DNS protocol (Domain Name System) allows names to be 'resolved' by the AX3000. Resolving is retrieving an IP address associated with a name.

### A.4.1 - Overview

A domain (computer network) can be considered as a tree, with branches (nodes) such as hubs, switches, routers, print servers etc, and leafs, for example PCs, thin clients and printers.

The domain system makes no distinction between the use of interior nodes and leafs, and this documentation uses the term "nodes" to refer to both. (I.e. any network resource).

Each node has a name (**Label**) which must be unique to other nodes at the same level, but not necessarily unique within the whole network.

#### **Label syntax:**

- Permissible characters are letters (a..z to A..Z), numbers (0..9) and the hyphen (-).
- A Label must begin by a letter and be ended by a letter or a number.
- The resolution is not case-sensitive.

The domain name of a node is the list of the labels on the path from the node to the root of the tree. A dot is used to separate each label. Two types of host names can be distinguished within the AX3000:

- **A full name:** one or more dots are included in the name.
  - Example: "www.axel.com"

- **An incomplete name:** no dots are used. The resolution procedure concatenates another character string to this name (the default DNS domain name). For more information see Chapter [3.1.2](#).
  - Example: "as400" is concatenated with "servers.axel.com" to create a full name of "as400.servers.axel.com"

A host name is only resolved if the IP address is needed. (i.e. to open a session or to ping).

**Note:** a name is resolved for each connection attempt, even if its IP address has been obtained by a previous resolution.

## **A.4.2 - Resolving a Name**

### ***a) Resolution Strategy***

To resolve a name, a DNS request is sent by the AX3000. A DNS request contains the destination DNS server IP address and the name to be resolved.

To resolve a name possibly more than one DNS request is needed (if one or more default DNS domains are defined). The resolution process is stopped either when the AX3000 receives a positive response from a DNS server (success: an IP address is associate to this name) or when all the DNS requests has been sent and no positive response has been received (failure: the name is not resolved).

The order of the requests sent to resolve a hostname is called the resolution strategy.

The resolution strategy depends on both:

- Whether or not a domain name is declared,
- Whether the name to resolve is complete.

If no default DNS domain is defined in the AX3000 Set-Up, the resolution is done with the name itself regardless of whether the name is full or not.

If one or more default DNS domains are defined, the resolution strategy depends on the name:

- **Full name:** the resolution is first done with this name. If unsuccessful new resolutions are performed by concatenating the full name with the defined DNS domains.
- **Incomplete Name:** the resolutions are first done with the defined default DNS domains. If unsuccessful a new resolution is performed with this incomplete name.

**Example of name resolutions:** looking at the host table in Chapter [3.1.3](#) the name resolution attempts are:

- **as400:** this is not a full name; the resolution is first made with the first DNS domain (as400.servers.axel.com). Then, in event of failure, with the second DNS domain (as400.terminals.axel.com). Then, in event of failure, the resolution is made with the name itself (as400).
- **linux:** an IP address is associated. No DNS resolution.
- **www.axel.com:** this is a full name. The resolution is first made with the name itself (www.axel.com). Then, in event of failure, the resolution is made with the first DNS domain

(www.axel.com.servers.axel.com). Then, in event of failure, with the second DNS domain (www.axel.com.terminals.axel.com).

### ***b) Resolution Method***

To resolve a name, the AX3000 sends DNS requests to the DNS server(s).

If a DNS server sends back a positive response, then the IP address is found and the resolution operation is completed. If not two cases of failure are possible:

- **Receiving a negative response:** the name is not known by this DNS server. The AX3000 will retry with a new DNS request or with the second DNS server.
- **No response (time-out):** after a few seconds the DNS server has not sent back a response. The AX3000 resends the same request to the DNS server.

**Note:** after 4 time-out errors on the same DNS server, this server is "removed" from the resolution operation.

**Note:** if a response previously considered as a time-out error is received, this response is treated as a valid response (positive or negative).

The AX3000 requests a recursive search to the DNS servers (and not iterative search). This means that the DNS server must search itself for a DNS server which is able to resolve the required name.

The resolution operation depends on the number of DNS servers. These are the steps for a one-server resolution and a two-server resolution.

#### **One DNS Server:**

1. A DNS request is sent to the server.
2. In event of no response, this request is sent again (4 times max.).
3. In event of negative answer, the resolution is aborted.
4. If other requests can be sent (default DNS domains are defined), go back to step 1.

#### **Two DNS Servers:**

1. A DNS request is sent to the server 1.
2. In event of no response from server 1, this request is sent to the server 2.
3. In event of no response from server 2, go back to step 1 (4 times max.).
4. In event of negative answer from any server, the resolution is aborted.
5. If other requests can be sent (using default DNS domains are defined), go back to step 1.

**Example:** looking at the screen shots of the Chapter [3.1](#), these are the DNS requests sent to resolve "as400" with 2 DNS servers and 2 default DNS domains (of course this process is stopped if one DNS server sends back a positive response):

1. "as400.servers.axel.com" to DNS server 1
2. "as400.servers.axel.com" to DNS server 2
3. "as400.terminals.axel.com" to DNS server 1
4. "as400.terminals.axel.com" to DNS server 2
5. "as400" to DNS server 1
6. "as400" to DNS server 2

### ***c) Messages Displayed on the AX3000 Screen***

To open a session the AX3000 must resolve the host name (if no IP address has been associated through the set-up).

This is a screen-shot example when the resolution successes:

```
Connecting to as400.servers.axel.com:23 (Telnet)...
Session number 1
Resolving...
Resolved: 192.168.1.180
Connected
```

**Explanation:** the AX3000 attempts to resolve "as400.servers.axel.com". The resolution process returns the IP address which is 192.168.1.180.

In the event of a problem, the "Resolved: a.b.c.d" message is replaced by an error message. For example:

```
Connecting to as400.servers.axel.com:23 (Telnet)...
Session number 1
Resolving...
Srv: domain not found
Press <Ctrl><Alt><Shift><D> to close this session
```

**Error messages:** error messages reported by the DNS server begins with Srv. Error messages from the thin client begin with "Loc". The main messages are:

- **Srv: domain not found:** the name doesn't exist within this domain.
- **Srv: refused query:** the DNS servers refuses to respond to the request. This could be due to a DNS server security function.
- **Loc: no DNS server defined:** no DNS server has been defined through the AX3000 Set-Up.
- **Loc: name syntax error:** the syntax of the name to resolve is not correct (for example two consecutive dots: as400.servers).
- **Loc: timeout:** no DNS server responds
- **Loc: no memory:** due to a temporary memory overload, the AX3000 can not process the name resolution. Retry later.

When the resolution fails, the session must be manually closed. This is done by pressing <Ctrl><Alt><Shift><D>.

#### **A.4.3 - Publishing the Thin Client Name**

The thin client name may be registered with the DNS server. This can be done by the DHCP server or by the thin client itself.

##### ***a) By the DHCP Server***

**Important:** the DHCP server must support the DDNS (Dynamic DNS) function.

To register the thin client name by the DHCP server:

- Enable the DHCP protocol
- Set "DNS Server Update" to "by the DHCP server"

Because the DNS server is updated by the DHCP server the information about the type ("direct" or "direct / reverse") and the result (success or failure) of the DNS update is not returned to the thin client.

##### ***b) By the Thin Client***

The thin client can register itself. The thin client behavior depends on the value of "DNS Server Update" option:

- **By the terminal:** the thin client updates the DNS server only if the DHCP server is agreed.

- **By the terminal (forced):** whatever the DHCP server information, the thin client updates the DNS server (use carefully).  
According to the option 'Update Type', the thin client updates "direct (A)" or "Direct (A) and Reverse (PRT)" DNS server records.  
For a "Direct (A)" update, two entries are added in the DNS server database:
  - A "Host" type entry, containing the thin client IP address,
  - A "Text" type entry, containing the thin client signature.

**Note:** the DNS server will be updated only if the thin client name is a full name: ended by a DNS domain (i.e. FQDN).

For a "Reverse (PRT)" update, one entry is added: a "Pointer" type entry, containing the thin client's full name.

**Note:** the signature allows the thin client to check its "Host" type entry. If the check fails (i.e. no associated signature or wrong associated signature) the thin client's behavior during the DNS server update depends on the value of the set-up parameter "**Action on Error**" (see Chapter [3.1](#)):

- **Display an error:** a red dialog box is displayed. The user may reboot the thin client or enter the set-up.
- **Continue the update:** the entries ("Host", "Text" and "Pointer") are overwritten.
- **Cancel the update:** the DNS update is aborted but the thin client is available for use.

The type ("direct" or "direct / reverse") and the result (success or failure) of the DNS update are returned to the thin client and are available in the thin client set-up. See chapter [9.5](#).

## A.5 - SETTING-UP AXEL DHCP OPTIONS

In addition to the standard options (IP addresses, DNS server...), the DHCP server can be used to communicate manufacturer specific information (vendor option).

With Axel, a vendor option can be used to specify the network location (IP address and TCP port) of the AxRM auto-configuration service.

The Axel options are contained within the range of numbers from 231 to 240. The 'type' is always 'character string'. The format of the entry is as follows:

- Entry starts with a keyword followed by one or more parameters.
- The symbol ":" is used as separator.

**Note:** In contrast to some implementations Axel uses a 'keyword' rather than a specific number. The actual number (231 to 240) is irrelevant so any non-conflicting number in this range can be used.

### **A.5.1 - 'axrm serv' Option: XML auto-configuration**

The 'axrm serv' option specifies the network location (IP address and TCP port) of the AxRM auto-configuration service in XML mode.

The format is as follows:

```
axrm serv:param1:param2
```

The parameters are:

- The IP address or DNS name of the AxRM server
- The XML port AxRM is listening on (by default 80)

### **A.5.2 - 'axrm servssl' Option: XML-SSL auto-configuration**

The 'axrm servssl' option specifies the network location (IP address and TCP port) of the AxRM auto-configuration service in XML-SSL mode.

The format is as follows:

```
axrm servssl:param1:param2
```

The parameters are:

- The IP address or DNS name of the AxRM server
- The XML-SSL port AxRM is listening on (by default 443)

**Note:** when the both options 'axrm serv' and 'axrm servssl' are published, the 'axrm servssl' is used in priority.

## A.6 - RSH ADMINISTRATION COMMAND LIST

Several administration commands are offered by the AX3000. These commands are launched by using a remote administration command (**rsh** for example) which is available as standard features from most major operating systems.

The following table lists the available AX3000 administration commands:

Command	Description
ax_reboot	Rebooting the AX3000. Example: rsh ax3000 ax_reboot [password]
ax_sinit	Resetting an AX3000 resource (screen session or aux. port) Example: rsh ax3000 ax_sinit [password] sess1
setup_get	Requesting the AX3000 Full Set-Up. Example: rsh ax3000 setup_get > file
setup_get	Requesting the AX3000 Set-Up with only significant options. Example: rsh ax3000 setup_get > file
setup_get_lite	Requesting the AX3000 Set-Up. Example: rsh ax3000 setup_get > file
setup_send	Setting-up the AX3000 through a text file. Example: rsh ax3000 setup_send [password] < file
ax_download	Requesting an AX3000 firmware downloading. Example: rsh ax3000 ax_download [password] 192.1.1.1 file
ax_version	Requesting the AX3000 firmware revision. Example: rsh ax3000 ax_version
ax_getstat	Requesting the AX3000 statistics. Example: rsh ax3000 ax_getstat
ax_switch	Switching to a screen session. Example: rsh ax3000 ax_switch sess1

**Note:** these commands are also available with uppercase characters (ax\_version and AX\_VERSION are the same command).

## A.7 – TO GO FURTHER ...

### A.7.1 - Reload Factory Settings

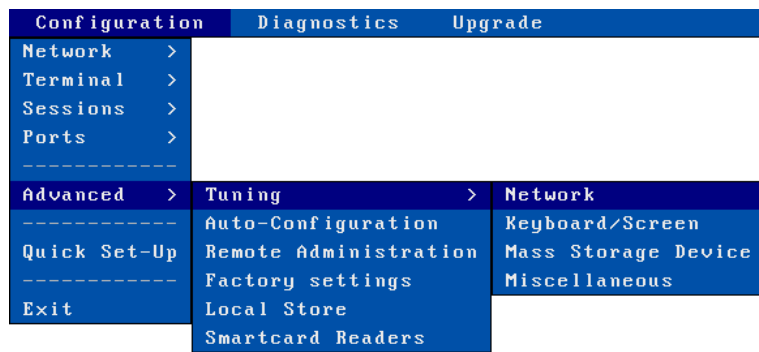
The menu **[Configuration]-[Advanced]-[Factory Settings]** allows, after confirmation, thin client factory settings to be reloaded. **The current configuration is lost.**

On next boot, the Quick Set-Up will be displayed and the Auto-Configuration service will be started (see Chapter 2).

### A.7.2 - General Level: Advanced Parameters

This chapter describes special AX3000 operating parameters. Usually the default values are suitable.

All these general parameters are located in sub-menus from **[Configuration]-[Advanced]-[Tuning]**:



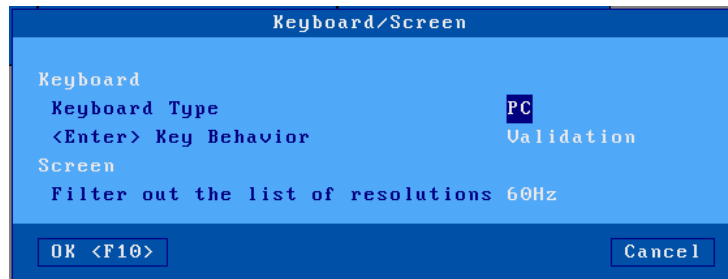
### a) Network Menu



- **DNS Cache:** this option allows the thin client to maintain a DNS cache.
- **IP Address Set by Ping:** this parameter allows or disables the AX3000 IP Address to be set by a ping command. (See Appendix A.8.6.)
- **Allow Network Discover:** by default, SNMP requests are supported by Axel thin clients. This allows thin clients to be discovered by AxRM (the Axel administration software). This parameter can be used to disabled the SNMP support.
- **MTU:** set the Maximum Transfer Unit value (Ethernet layer).
- **TCP SACK Enabled:** this is an optimization to improve performance in the event of TCP packet loss (see RFC 2883).
- **Wake-on-lan Enabled:** (default no) this option allows the thin client to be powered on remotely. The supported method is magic packet (UDP)
- **Wireless PSK/EAP version:** see Chapter 3.1.3 section d).
- **Show Connection Messages:** turn on/off verbose mode when a connection is established.
- **Net Tracer:** turn on/off network trace messages.
- **DNS Trace Mode:** turn on/off DNS trace messages.
- **DHCP Trace Mode:** turn on/off DHCP trace messages.
- **'Window' and 'mss' Size:** these values are used for tuning the TCP socket of the XML administration protocol.



**b) Keyboard/Screen Menu**



**Keyboard Type:** by default **PC** keyboards (102/105 keys) are supported by the AX3000, but other keyboards type are available for special use:

- AS400 (F24): 122-keys keyboard (24 function keys) for 5250 emulation,
- ANSI (F20): keyboard with 20 function keys for VT220 emulation.

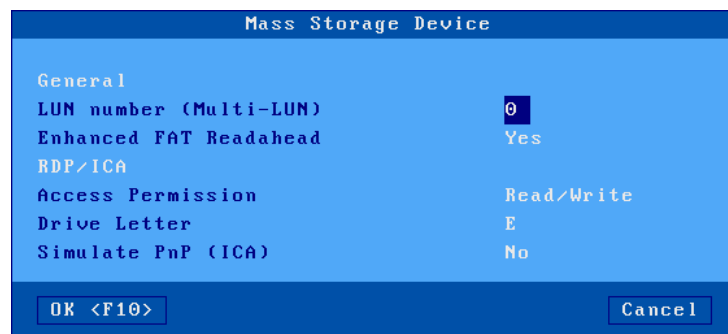
**Note:** Do not experiment with keyboard types – i.e. if you do not have an AS400 keyboard do not select AS400

**<Enter> Key Behavior:** this option allows the <Enter> key mode to be set. This mode is used with when a logon box is displayed and managed by the thin client:

- Validation: pressing <Enter> performs the same action as clicking the [OK] button,
- Browsing: pressing <Enter> jump to the next field.

**Filter out the list of resolutions:** when the thin client is started, a resolution list is announced by the monitor(s). A frequency is associated with each resolution. To prevent a too long resolution list, resolutions can be filtered out with the frequency (60Hz or 75Hz).

**c) Mass Storage Device Menu**



**LUN Number:** some USB drives may be formatted in multi-LUN mode (multiple partitions). But the Axel Thin Client handles only a single LUN. This option allows the LUN number to handle to be selected. (If the LUN Number is too high, the LUN #0 will be used).

**Enhanced FAT Readahead:** this option allows performances to be increased. It can be disabled.

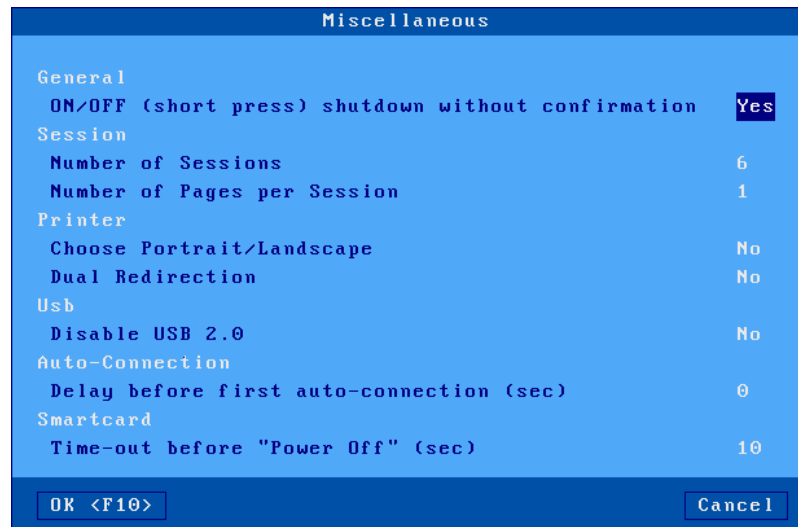
External USB mass storage devices (memory sticks, hard drives, CD/DVD readers...) are redirected to the Windows/Citrix server and are seen as local drives

The USB drive parameters are:

- **Access Permission:** 'Read Only' and 'Read/Write'
- **Driver Letter:** mnemonic given to the Windows server.

**Simulate PnP (ICA):** hot plug is not supported by old Citrix versions. This option allows a redirected USB mass storage to be announced even if no physical device is plugged.

#### d) Miscellaneous Menu

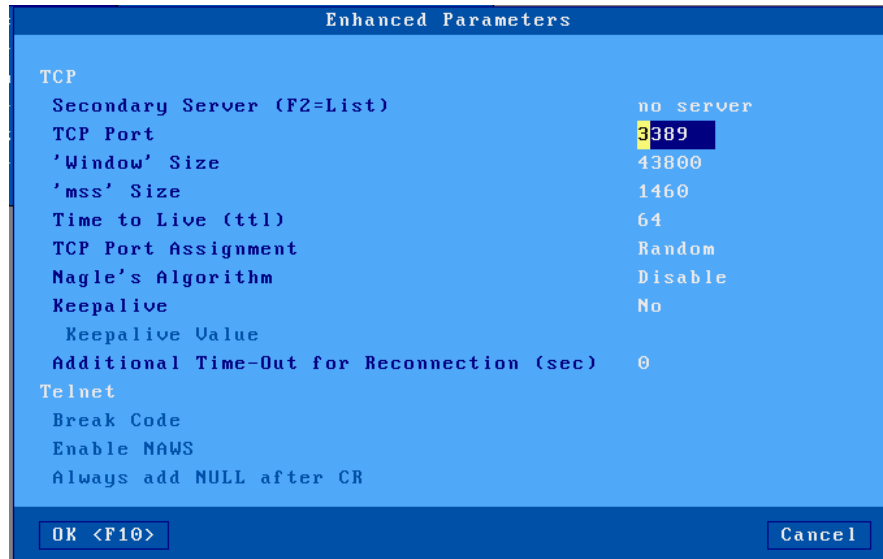


- **Shutdown the terminal without confirmation:** the terminal can be shutdown by pressing briefly the power button. In this case, when this option is set to 'No', a confirmation will be displayed.
- **Number of Sessions:** this parameter is the maximum number of concurrent connections. Its value is from 1 to 6.
- **Number of Pages per Session:** this parameter allows multi-page support. This may be used by legacy text application under Unix/Linux.  
**Important:** the 'Number of Sessions' multiplied per the "Number of Pages per Session" must not exceed 6.
- **Choose Portrait/Landscape:** when this option is set, printer string sequences can be entered for the "default printer port" and printer services (LPD, Prt3270...). These sequences allow a portrait/landscape mode to be selected via a thin client taskbar icon (see Chapter 4.3).
- **Dual Redirection:** this option allows 2 logical printers to be created per RDP/ICA redirected printer.
- **Disable USB 2.0:** for compatibility reasons with some old USB devices, this option allows the USB 1.1 protocol to be forced on one USB port (among the 6 available ports). This port is located on the top of the rear panel.
- **Delay before first auto-connection:** Delay in seconds before the first session auto-connection after starting the thin client. Given that AXEL thin clients restart very quickly, it is sometimes necessary to add a delay before the first connection to avoid errors linked to the previous connection which has not yet been released by the server.
- **Time-out before "Power Off":** Time-out in seconds before sending power-off command to the smart card (to avoid problems linked to sending it too quickly), 0 = power-off command never sent.

### A.7.3 - Session Level: Enhanced Parameters

Each session (screen or auxiliary port) offers enhanced parameters. These parameters are available through the "Connection Properties" box (depending on the session type this box is located in the [Sessions]-[Session x] menu or the [Aux. Ports]-[xxx] menu).

This is an example of the dialog box:



Notes:

- The available parameters depend on both the connection type (screen or auxiliary port) and the associated protocol.
- New values are used for the next TCP/IP connection (no need to power-cycle the AX3000).

#### a) 'Secondary Server' Parameter

A secondary server allows the user to select on which server the session is connected to. The server is chosen when the session is established. A mini-menu is displayed.

#### b) 'TCP port' Parameter

This parameter is the server TCP port on which the session is connected. The default value depends on the current protocol.

#### c) 'mss' and 'Window' Parameters

These two parameters are the AX3000 resources allocated to telnet and tty screen sessions for receiving network data:

- **mss** (maximum segment size) is the largest segment of TCP data. This size is negotiated with the server at the connection time.
- **window** is the reception windows size (i.e. the size of the buffer on which the TCP data is stored).

It is not advisable to modify these two values unless the input data flow is not continuous (i.e. the data flow pauses and resumes regularly during scrolling).

**d) 'Time to Live' Parameter**

This parameter controls the 'to live' time of the datagram to prevent it being looped forever due to routing errors. Routers decrement the TTL of every datagram as it traverses from one network to another. When its value reaches 0 the packet is dropped.

This parameter doesn't impact the AX3000 performance.

**e) 'TCP port Assignment' Parameter**

The AX3000 resources (screen sessions and auxiliary ports) are identified by numeric values called TCP ports.

The TCP port assignment can be either random or fixed. The default value depends on the current network service.

The random method means the AX3000 TCP ports are different after every re-boot. On booting the AX3000 generates a new base value. This value (x) is between 1024 and 3072. For each session a range of 8 TCP ports is given: session 1 = (x...x+7), session 2 = (x+8...x+15)... When a connection is established the next port of the associated range is used. After 8 connections, the same TCP port of a range is re-used.

The main benefit of this method is that if the AX3000 is suddenly powered off (power cut for example), at the next boot time, the connections are immediately accepted by the server. (i.e. the sessions are hooked on different sockets because the TCP ports are different). However this does create 'phantom' sessions, as the initial sessions are still active from the server's perspective, and must be killed by the server.

This can be done with the 'keepalive' process, manually killing or rebooting.

In some situations it may be beneficial to have always the same TCP port for an AX3000 resource (to avoid phantom sessions or to identify connections). This is the fixed port assignment. With this method the AX3000 resources are always:

- session 1 = 1024, ..., session 8 = 1031,
- aux1 port = 1032, aux2 port = 1033, parallel port 1034.
- net1 = 1035, ..., net4 = 1038,
- usb1 = 1039, ..., usb4 = 1042.

**f) 'Nagle's Algorithm' Parameter**

The Nagle's Algorithm controls behavior of the output network dataflow of a TCP/IP device. This algorithm allows the number of datagrams sent by the AX3000 to decrease. However a certain latency may be noticeable due to the caching of data before transmission.

This algorithm is disabled to prioritize performance. However some operating systems require this function to be enabled.

**g) 'Keepalive' Parameter**

The keepalive is a mechanism that allows the AX3000 to regularly check its TCP/IP connection status.

In event of network incident, the AX3000 is able to detect this incident and to close the related TCP/IP connections. This mechanism is also useful when DSL connections are used (the AX3000 IP address is reset on time per day).

By default the keepalive function is disabled.

The keepalive function is set in minutes.

**Note:** with ISDN routers (which automatically drop the phone line) this regular data flow will prevent the router from hanging-up. In this scenario the keepalive can cause expensive phone bills.

**h) 'Additional Time-Out for Reconnection (sec)' Parameter**

When a session is set in 'auto-reconnection' mode, the reconnection is attempted immediately after the disconnection.

If needed, this option allows this reconnection to be delayed.

**i) 'Break Code' Parameter**

For the telnet session, the **<Ctrl><Alt><Pause>** hotkey sends a 'break' code to the host. This break code is defined by the RFC 854, this is 'IAC BREAK'.

If needed, this break code value can be modified. The extra values are:

- AO (Abort Output),
- IP (Interrupt process),
- None (<Ctrl><Alt><Pause> generates no code).

**j) 'Enabling NAWS' Parameter**

The NAWS function (Negotiate About Window Size - RFC 1073) is an optional feature negotiated when the telnet session established. It allows the thin client screen format (line x row) to be indicated to the server (when the session is established or at any time when the screen format is modified).

This parameter allows this function to be disabled: some telnet servers don't correctly support the NAWS function.

**k) 'Always add NULL after CR' Parameter**

This option allows being compliant with different telnet server implementation (about ASCII mode).

**l) 'National Language Negotiation' Parameter**

This option is only available with 5250 emulation. It allows some environment variables (KBDTYPE, CODEPAGE and CHARSET) to be set.

## A.7.4 - Keyboard Codes and Time Zone Names for RDP/ICA Sessions

### a) Keyboard Codes

For RDP/ICA sessions a Microsoft keyboard code can be specified. (See Chapter [3.2.5](#)) This code allows a keyboard nationality to be negotiated with the TSE server.

The following table lists the available keyboard codes:

Keyboard nationality	Code	Keyboard nationality	Code
Afrikaans	0436	Icelandic	040F
Albanian	041C	Indonesian	0421
Arabic - United Arab Emirates	3801	Italian - Italy	0410
Arabic - Bahrain	3C01	Italian - Switzerland	0810
Arabic - Algeria	1401	Japanese	0411
Arabic - Egypt	0C01	Korean	0412
Arabic - Iraq	0801	Latvian	0426
Arabic - Jordan	2C01	Lithuanian	0427
Arabic - Kuwait	3401	Macedonian (FYROM)	042F
Arabic - Lebanon	3001	Malay - Malaysia	043E
Arabic - Libya	1001	Malay - Brunei	083E
Arabic - Morocco	1801	Maltese	043A
Arabic - Oman	2001	Marathi	044E
Arabic - Qatar	4001	Norwegian - Bokml	0414
Arabic - Saudi Arabia	0401	Norwegian - Nynorsk	0814
Arabic - Syria	2801	Polish	0415
Arabic - Tunisia	1C01	Portuguese - Portugal	0816
Arabic - Yemen	2401	Portuguese - Brazil	0416
Armenian	042B	Raeto-Romance	0417
Azeri - Latin	042C	Romanian - Romania	0418
Azeri - Cyrillic	082C	Romanian - Moldova	0818
Basque	042D	Russian	0419
Belarusian	0423	Russian - Moldova	0819
Bulgarian	0402	Sanskrit	044F
Catalan	0403	Serbian - Cyrillic	0C1A
Chinese - China	0804	Serbian - Latin	081A
Chinese - Hong Kong SAR	0C04	Setsuana	0432
Chinese - Macau SAR	1404	Slovenian	0424
Chinese - Singapore	1004	Slovak	041B
Chinese - Taiwan	0404	Sorbian	042E
Croatian	041A	Spanish - Spain	0C0A
Czech	0405	Spanish - Argentina	2C0A
Danish	0406	Spanish - Bolivia	400A
Dutch - Netherlands	0413	Spanish - Chile	340A
Dutch - Belgium	0813	Spanish - Colombia	240A
English - Australia	0C09	Spanish - Costa Rica	140A
English - Belize	2809	Spanish - Dominican Republic	1C0A
English - Canada	1009	Spanish - Ecuador	300A
English - Caribbean	2409	Spanish - Guatemala	100A
English - Ireland	1809	Spanish - Honduras	480A
English - Jamaica	2009	Spanish - Mexico	080A
English - New Zealand	1409	Spanish - Nicaragua	4C0A
English - Philippines	3409	Spanish - Panama	180A

English - South Africa	1C09
English - Trinidad	2C09
English - United Kingdom	0809
English - United States	0409
Estonian	0425
Farsi	0429
Finnish	040B
Faroese	0438
French - France	040C
French - Belgium	080C
French - Canada	0C0C
French - Luxembourg	140C
French - Switzerland	100C
Gaelic - Ireland	083C
Gaelic - Scotland	043C
German - Germany	0407
German - Austria	0C07
German - Liechtenstein	1407
German - Luxembourg	1007
German - Switzerland	0807
Greek	0408
Hebrew	040D
Hindi	0439
Hungarian	040E

Spanish - Peru	280A
Spanish - Puerto Rico	500A
Spanish - Paraguay	3C0A
Spanish - El Salvador	440A
Spanish - Uruguay	380A
Spanish - Venezuela	200A
Southern Sotho	0430
Swahili	0441
Swedish - Sweden	041D
Swedish - Finland	081D
Tamil	0449
Tatar	0444
Thai	041E
Turkish	041F
Tsonga	0431
Ukrainian	0422
Urdu	0420
Uzbek - Cyrillic	0843
Uzbek - Latin	0443
Vietnamese	042A
Xhosa	0434
Yiddish	043D
Zulu	0435

**Note:** this list can be found on the MSDN Microsoft site

**b) Name of Time Zone**

For the RDP/ICA time redirection, a time zone name must be given (see Chapter 3.2.6). This **case-sensitive** name must belong to the following Microsoft list:

Hours	Name
(GMT-12:00) International Date Line West	Dateline Standard Time
(GMT-11:00) Midway Island, Samoa	Samoa Standard Time
(GMT-10:00) Hawaii	Hawaiian Standard Time
(GMT-09:00) Alaska	Alaskan Standard Time
(GMT-08:00) Pacific Time (US and Canada)	Pacific Standard Time
(GMT-07:00) Mountain Time (US and Canada)	Mountain Standard Time
(GMT-07:00) Chihuahua, La Paz, Mazatlan	Mexico Standard Time 2
(GMT-07:00) Arizona	U.S. Mountain Standard Time
(GMT-06:00) Central Time (US and Canada)	Central Standard Time
(GMT-06:00) Saskatchewan	Canada Central Standard Time
(GMT-06:00) Guadalajara, Mexico City...	Mexico Standard Time
(GMT-06:00) Central America	Central America Standard Time
(GMT-05:00) Eastern Time (US and Canada)	Eastern Standard Time
(GMT-05:00) Indiana (East)	U.S. Eastern Standard Time
(GMT-05:00) Bogota, Lima, Quito	S.A. Pacific Standard Time

(GMT-04:00) Atlantic Time (Canada)	Atlantic Standard Time
(GMT-04:00) Caracas, La Paz	S.A. Western Standard Time
(GMT-04:00) Santiago	Pacific S.A. Standard Time
(GMT-03:30) Newfoundland and Labrador	Newfoundland and Labrador Standard Time
(GMT-03:00) Brasilia	E. South America Standard Time
(GMT-03:00) Buenos Aires, Georgetown	S.A. Eastern Standard Time
(GMT-03:00) Greenland	Greenland Standard Time
(GMT-02:00) Mid-Atlantic	Mid-Atlantic Standard Time
(GMT-01:00) Azores	Azores Standard Time
(GMT-01:00) Cape Verde Islands	Cape Verde Standard Time
(GMT) Dublin, Edinburgh, Lisbon, London	GMT Standard Time
(GMT) Casablanca, Monrovia	Greenwich Standard Time
(GMT+01:00) Belgrade, Bratislava, Budapest	Central Europe Standard Time
(GMT+01:00) Sarajevo, Skopje, Warsaw	Central European Standard Time
(GMT+01:00) Brussels, Madrid, Paris...	Romance Standard Time
(GMT+01:00) Amsterdam, Berlin, Bern, Rome	W. Europe Standard Time
(GMT+01:00) West Central Africa	W. Central Africa Standard Time
(GMT+02:00) Bucharest	E. Europe Standard Time
(GMT+02:00) Cairo	Egypt Standard Time
(GMT+02:00) Helsinki, Kiev, Riga, Sofia...	FLE Standard Time
(GMT+02:00) Athens, Istanbul, Minsk	GTB Standard Time
(GMT+02:00) Jerusalem	Israel Standard Time
(GMT+02:00) Harare, Pretoria	South Africa Standard Time
(GMT+03:00) Moscow, St. Petersburg...	Russian Standard Time
(GMT+03:00) Kuwait, Riyadh	Arab Standard Time
(GMT+03:00) Nairobi	E. Africa Standard Time
(GMT+03:00) Baghdad	Arabic Standard Time
(GMT+03:30) Tehran	Iran Standard Time
(GMT+04:00) Abu Dhabi, Muscat	Arabian Standard Time
(GMT+04:00) Baku, Tbilisi, Yerevan	Caucasus Standard Time
(GMT+04:30) Kabul	Transitional Islamic State of Afghanistan Standard Time
(GMT+05:00) Ekaterinburg	Ekaterinburg Standard Time
(GMT+05:00) Islamabad, Karachi, Tashkent	West Asia Standard Time
(GMT+05:30) Chennai, Kolkata, Mumbai	India Standard Time
(GMT+05:45) Kathmandu	Nepal Standard Time
(GMT+06:00) Astana, Dhaka	Central Asia Standard Time
(GMT+06:00) Sri Jayawardenepura	Sri Lanka Standard Time
(GMT+06:00) Almaty, Novosibirsk	N. Central Asia Standard Time
(GMT+06:30) Yangon Rangoon	Myanmar Standard Time
(GMT+07:00) Bangkok, Hanoi, Jakarta	S.E. Asia Standard Time
(GMT+07:00) Krasnoyarsk	North Asia Standard Time
(GMT+08:00) Beijing, Chongqing, Hong Kong	China Standard Time
(GMT+08:00) Kuala Lumpur, Singapore	Singapore Standard Time
(GMT+08:00) Taipei	Taipei Standard Time
(GMT+08:00) Perth	W. Australia Standard Time
(GMT+08:00) Irkutsk, Ulaanbaatar	North Asia East Standard Time
(GMT+09:00) Seoul	Korea Standard Time
(GMT+09:00) Osaka, Sapporo, Tokyo	Tokyo Standard Time
(GMT+09:00) Yakutsk	Yakutsk Standard Time
(GMT+09:30) Darwin	A.U.S. Central Standard Time
(GMT+09:30) Adelaide	Gen. Australia Standard Time



(GMT+10:00) Canberra, Melbourne, Sydney	A.U.S. Eastern Standard Time
(GMT+10:00) Brisbane	E. Australia Standard Time
(GMT+10:00) Hobart	Tasmania Standard Time
(GMT+10:00) Vladivostok	Vladivostok Standard Time
(GMT+10:00) Guam, Port Moresby	West Pacific Standard Time
(GMT+11:00) Magadan, New Caledonia	Central Pacific Standard Time
(GMT+12:00) Fiji Islands, Kamchatka	Fiji Islands Standard Time
(GMT+12:00) Auckland, Wellington	New Zealand Standard Time
(GMT+13:00) Nuku'alofa	Tonga Standard Time

Note: this list can be found on the MSDN Microsoft site.

### **A.7.5 – Displaying Text Session in Graphics Mode**

Previously Axel used the legacy method to display text sessions (telnet, 5250, 3270...) based on columns and rows (80x25, 132x25...) and a specific resolution.

We are changing the way we display text because:

- Many new TFT monitors no longer support the specific resolution required (720x400) - or if they do the characters are blurry and jittery
- Many monitors have a slight delay when changing session of different resolutions. Using graphics resolutions lets Windows and telnet sessions use the same resolution.
- Most new monitors are widescreen, and the legacy characters, designed for aspect ratio 4/3 can be distorted when 'stretched' on a wide screen monitor.

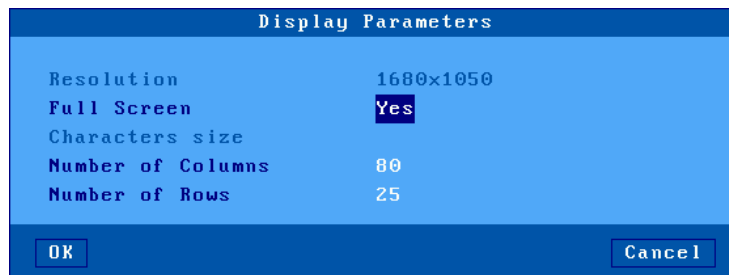
The solution is to use graphics resolutions for text displays. This addresses the first two points above; the character issue is covered below.

The challenge is fitting characters designed for aspect ratio of 4/3 onto a 16/9 screen without creating distortion and keeping the characters aesthetically acceptable.

To resolve this issue we offer two variables:

- Full screen or part screen (window).
- Options for character size and space between characters.

Below is the dialogue box showing the options – also see chapters [6.1.3](#), [7.1.2](#) and [8.1.4](#):



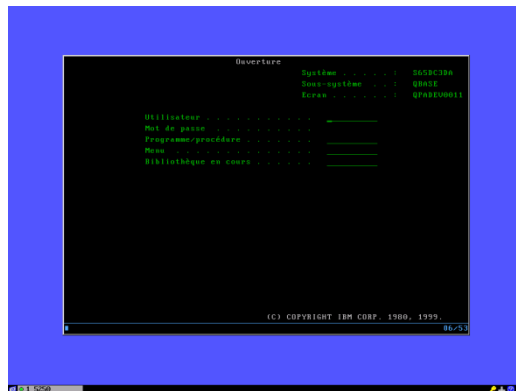
#### **a) Full Screen Mode**

To provide similar appearance to legacy screens a full screen mode is offered: the session is displayed on the entire screen and the character size is automatically adapted to the resolution and the number of lines/columns.

When the full screen mode is not selected the thin client calculates the optimal spacing between characters and a window is displayed:

- The background color is selected through the menu [Configuration]-[Terminal]-[Local Desktop]. (See Chapter [3.2.3](#))
- A grey-light frame surrounds the session.
- And the character size can be customized. (See next sub-section)

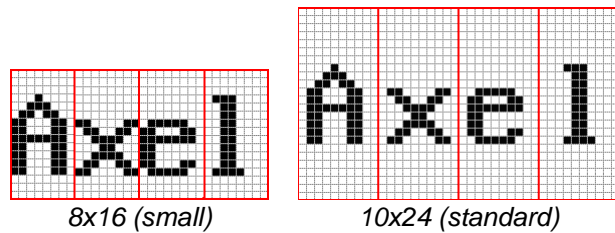
Example:



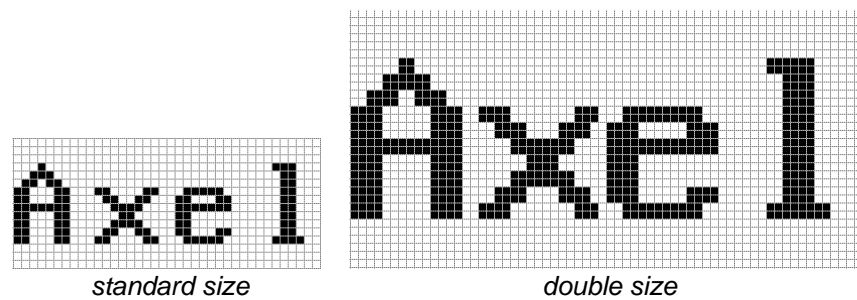
**b) Size and spacing of characters**

The thin client has a single font (size 8x16 pixels), but two options:

- **Inserting spaces around character** (horizontal and vertical) to 'pad' the character



- **Doubling the size of the character** – each pixel mapped to 4 pixels



### c) Information about Current Session

The <Ctrl><Alt><I> keystroke allows an information box to be displayed.

For example:

```

Information session 1 : TSE

Network Autodetect          No Information
Security Tunnel             NLA
                             (TLS 1.2 RSA_WITH_AES256_CBC_SHA)
Server IP Address          192.168.1.124
License                     No License Exchange
Connection Name            axel365EE4
Colour Depth               Highest Quality (32bpp)
Resolution                 1920x1080 60Hz
Compression Server->Client  U6.1 - Rate 2%
Compression Client->Server no
Display Optimization       FrameMarker
Bitmap Codec               GFX (AUC444)
Cache                      0/16Mb
Redirected Printer         Not Requested
Redirected COM/LPT         Not Requested
Redirected Clipboard       Not Requested
Redirected USB MemStick    Not Requested
Redirected Smartcard       Not Requested
Redirected Audio (play)    Not Requested
Redirected Audio (record)  Not Requested
USB Port Redirection       Not Requested
Multitouch Support         Negotiated (2)

OK

```

#### A.7.6 - Setting the IP Address by a PING Command

A new feature with version 'e' firmware enables the system manager to remotely assign an initial IP address to a brand new thin client, or remotely change an existing IP address.

The procedure is to manually modify the ARP table of your computer (Unix, Linux, Windows...). An ARP table entry is composed of IP addresses and Ethernet MAC addresses. The command below associates an arbitrary IP address to the thin client's hard coded MAC address. The MAC address is printed on the base of each thin client. With its updated ARP table your computer is able to access the AX3000. To set the new IP address the thin client must be pinged a multiple times.

#### Using under Unix/Linux:

Run the following command to associate the AX3000's Ethernet address xx:xx:xx:xx:xx:xx with the IP address a.b.c.d (this command updates the ARP table):

```
# arp -s a.b.c.d xx:xx:xx:xx:xx:xx
```

Run a ping command:

```
# ping a.b.c.d
```

The first ping requests are not acknowledged. But after few seconds the AX3000 is rebooted and replies the ping requests. The AX3000 is now set with the a.b.c.d IP address.

**Using under Windows:**

☺: Windows administration s/w (AxRM or Axel Remote Management) is available free on the Axel Web site. See Chapter [10.1](#).

The procedure is the same as Unix/Linux except for the Ethernet address notation ('-' are used as separators instead of ':'). The command is:

```
C:\> arp -s a.b.c.d xx-xx-xx-xx-xx-xx
```

Run one or more ping commands (4 ping requests are sent by ping command):

```
C:\> ping a.b.c.d
```

**Note:** if required this function can be disabled by setting the 'IP Addr. Set by Ping' parameter to 'no'. For more information, refer to Appendix A.7.2.

## A.8 - HARDWARE AND FIRMWARE INFORMATION

To obtain the thin client's firmware and hardware revisions, use one of the following:

Use the AxRM utility - "Get Terminal Information" command,

Enter the AX3000 **interactive set-up**, and select [?]-[Information],

Get the AX3000 set-up by issuing the **setup\_get** remote command (the revision is included in the text file banner):

Example: rsh axname setup\_get > file

Use the following **ax\_version** remote command to get the revision directly:

Example: rsh axname ax\_version

### A.8.1 - Hardware Information

The AX3000 hardware information is **FKx-BVyyy**:

- **FKx** is the circuit board code (FK stands for Flash Key)
- **BVyyy** is the boot code version (the boot code is the non-erasable part of the flash memory)

There are currently following different generations of hardware in the field:

FK3, FK5 & FK11: models 55, 55E and 56

FK7: models 65

FK13: models 65 and 65E

FK14: models 65/65E (PS/2 mouse)

FK15: models 60/60E

FK16: 75/75B/75E

FK17: models 65B (10/100BaseT)

FK18, FK19 & FK40: models 75C

FK20 & FK45: models 65C

FK30 & FK31: models 70W

FK35 & FK36: models 70F

FK41: models 75D

FK51: models 85

FK52: models 85B

FK55: models 80F

FK56 & FK59: models 80G

FK57: models 80WMS

**FK60 & FK61: models 90**

**FK65: models 95**

**Note:** the correct firmware file must be downloaded for your AX3000 hardware. Example: if **FK60** firmware file is downloaded into **FK61** hardware, the download process will fail.

### A.8.2 - Firmware Information

The firmware version is **FCT.NA.yywwi:STD**

Firmware	WFI.FR.1945a:STD-BFT
----------	----------------------

- **FCT** is the AX3000 operating mode (TCP or WFI)
- **NA** is the firmware nationality (code is ISO compliant). The main nationalities are:
  - XX: International (except for the following countries)
  - BR: Brazil
  - CZ: Czechoslovakia
  - DE: German
  - DK: Denmark
  - EE: Estonia
  - FI: Finland
  - FR: France
  - GR: Greece
  - IS: Iceland
  - PL: Poland
  - PT: Portugal
  - RU: Russia
  - SI: Slovenia
  - SK: Slovakia
  - TR: Turkey
- **yywwi** is the year and the week number of the firmware creation following by an alphabetical index (for instance: 1945a, year “2019”, week “45” index “a”).
- **STD** stands for 'Standard'. In event of firmware option additional codes follow: **HID** (FootControl), **SMK** (SpeechMike)....

**Note:** three parameters depend on the firmware nationality:

- The set-up message nationality (FR: French messages, DE, German messages, other: English messages),
- The possible presence of a national keyboard and associated character set. For instance, the Turkish environment (keyboards and character set) is only available with the 'TR' firmware.
- The default keyboard nationality (FR: France, DE: German, XX: North American, TR: Turkey, etc).

### A.8.3 – Compilation Index

The compilation index corresponds to the compilation number in the same version, these indices do not correspond to a “major” change in functionalities, they are generally corrections which are made over time and feedback from customers.

It is the “comp” parameter which corresponds to this index, it is made up of 2 numbers:

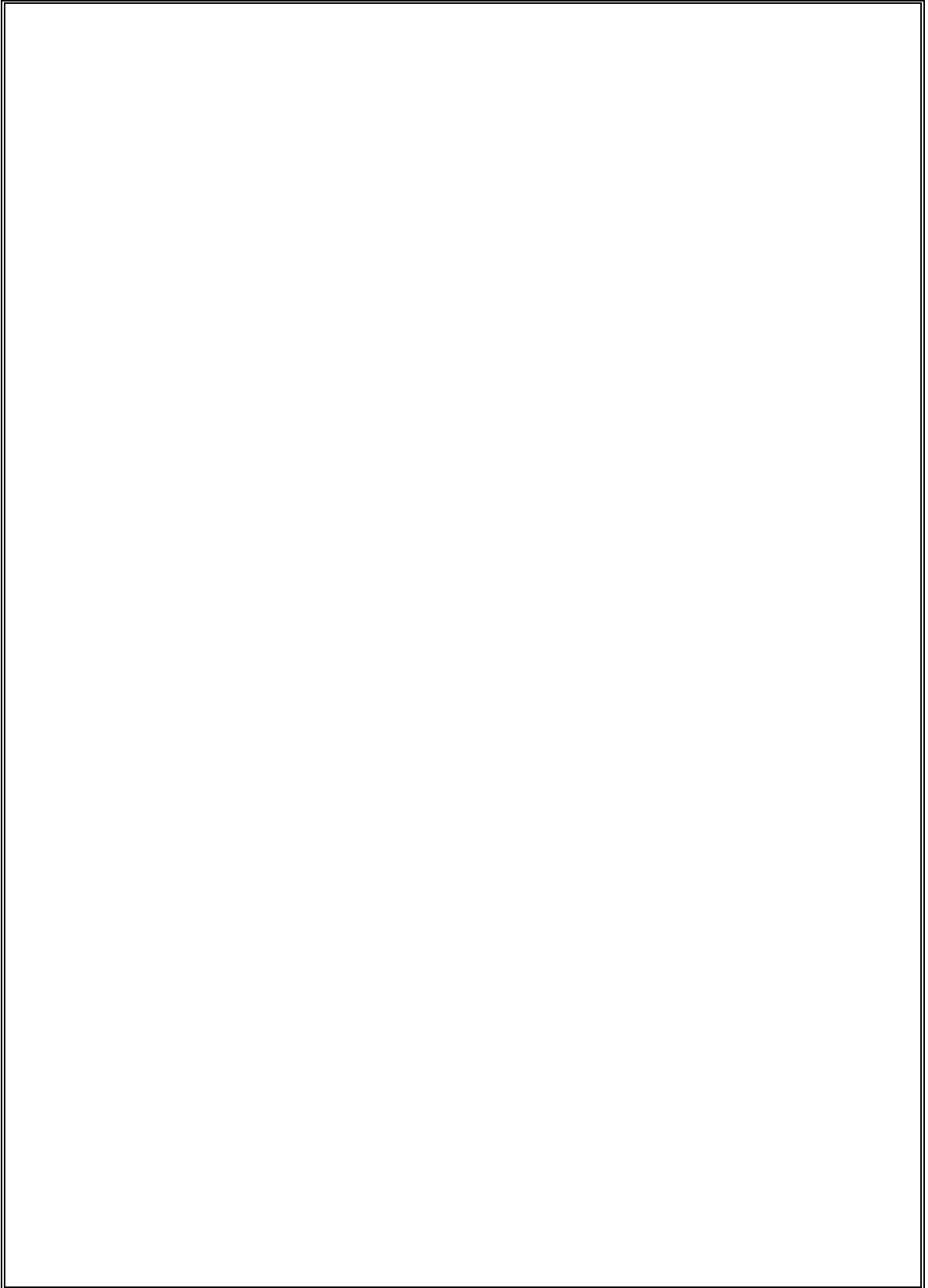
Comp	20146 (20111)
------	---------------

- **xxxx** code the index of the “term” part of the firmware (here 20146)
- **yyyy** code the index of the « tcp » part of the firmware (here 20111).





## PERSONAL NOTES

A large, empty rectangular box with a thin black border, occupying most of the page below the title. It is intended for the user to write their personal notes.

AXEL

14 Avenue du Québec  
Bât. Kentia - BP 628  
91962 Courtabœuf cedex - FRANCE  
Tél: +33(0)1 69 28 27 27 - Email: [info@axel.fr](mailto:info@axel.fr)