Xcalibur Global 1.2

Evaluation Kit Manual

XCALIBUR GLOBAL

Management Software

Written By: Chip PC Training Dep.
December 2007

www.chippc.com

Chip PC
Technologies

Contents

1 General

Xcalibur Global version 1.2 is an industry leading management software that lowers the organization's TCO and increases its network security by efficiently managing multiple thin client devices and users from a central location.

The combination of ***Chip PC***'s leading thin-clients, with their advanced image and Plug-ins, together with the Xcalibur Global management platform provides a complete thin client solution for a wide variety of organizations.

Xcalibur Global is capable of mapping both the organizational structure of the enterprise as well as its physical structure. Its unique architectural structure allows for simultaneous support of thousand of client and users while providing fault tolerance, speed, scalability and above all ease of management.

Since evaluating thin clients and thin client management requires having a complete SBC (Server Based Computing) environment, Chip PC offers you a complete evaluation environment.

With this DVD you can start evaluating Xcalibur Global management software version 1.2 in less then 15 minutes. This is done without the need to prepare and install a complex Server Based Computing environment by using the latest virtual server technologies. Our team has built a complete test environment and placed it on this DVD. It is highly tuned and ready for use during the specified evaluation period.

Note: During this manual it's assumed that you have an evaluation thin client device with image 6.5.0 or higher that you can use for the evaluation. If you don't have a device you can still use the evaluation DVD and understand the basic concepts and advantages of Xcalibur Global.

Note: The evaluation DVD is complete with both Xcalibur Global Server License and Domain Autenticator Server License. All operations described in this manual are coverd by the Xcalibur Global Basic license.

Note: In order to obtain your Device Licenses Please contact Chip PC support on https://www.chippc.com/support/request/

Warning: This system is intended for evaluation purpose only. It is not intended for commercial use.

Microsoft®, WINDOWS®, NT®, EXCEL®, Word®, PowerPoint® and SQL Server® are registered trademarks of Microsoft Corporation.

VMware is a registered trademark of VMware Inc.

Citrix is a registered trademark of Citrix Systems, Inc.

2 DVD Content

The enclosed DVD contains the following folders:

1. ***Xcalibur Image*** of Xcalibur Global 1.2 on windows 2003 R2 SP2.
   Folder Name: ***Xcalibur Global Evaluation Environment***
2. ***VMware Player*** Folder Name: ***VMware-player-1.0.2-29634***

3 Installation Prerequisites

- Computer, PC or Server with an Intel Pentium 4 CPU …or Higher.
- At least 512MB of memory, 1 GB preferable.
- At least 4GB of disk space.
- VMware Player v1.0.0 software (can be found on the DVD).

4 Xcalibur Virtual Environment Image Content

The Xcalibur Image supplied in the DVD contains the following:

- Windows 2003 (evaluation version)
- Active Directory Domain complete with predefined Users and Organizational Units
- Domain name: Xcalibur.com
- Host name: chippc-dc-xg
- IP: 192.168.15.131
- DNS
- WINS
- DHCP Server – ***The scope is disabled (to avoid network conflicts)***.
- Terminal Services – (Application Mode)
- IIS
- MSDE
- Xcalibur Global v1.2 complete with sample Xcalibur policies and Templates

What do you need:

Xcalibur Global Virtual Evaluation environment is designed to allow users to fully evaluate Xcalibur Global managment software, demonstrating Chip PC complete solution. Xcalibur Global can support any back-end solution selected by the customer with the same management and monitoring concepts. In order to fully simulate a scenario it may be required to use back-end solution which is not provided in the evaluation environment (e.g. Citrix, VMware VDI, etc.). Those external solutions are not part of this environment and we recommend end users to install the full Xcalibur Global management software in their own pilot environment to fully test and simulate their needs.

5 How to use this manual

This manual includes Step-By-Step scenarios that allow you to easily evaluate common thin client management scenarios. Each scenario includes server and client side instruction that will guide you through every step.

> **Note:**
>
> - In general, every action that can be done locally (on the thin client) can be done remotely from the management software.
> - It is highly recommended reading the whole scenario prior to beginning.

5.1 Starting-Point

This section describes the initial settings needed on both client and server.

In order to successfully complete the Step-By-Step scenarios initial settings are required on both the thin client side and the Xcalibur Global image (server side). These settings are referred to as Starting-Points.

Setting both client and server to their Starting-Points assures smooth scenario completion. In case you fail to complete a Step-By-Step scenario reverting both client and server to their Starting-Points is highly recommended.

See the Server Starting-Point and Client Starting-Point sections described further in this document.

> **Note:** once reverting to the Starting-Point, all previous settings will be erased!

6 Evaluation Environment Overview

6.1 Evaluation Environment Description

In order to start evaluating all you need to do is run the VMware image on your computer and connect an Xtreme PC thin client to it. The VMware image holds the complete evaluation environment including Active Directory, Terminal Services and the Xcalibur Global management software.

Evaluation environment components:

- Run the VMware image on your computer.
- Connect at least one Xtreme PC thin client to your computer via a crossed cable (Figure 1) or a network Hub / Switch (Figure 2).

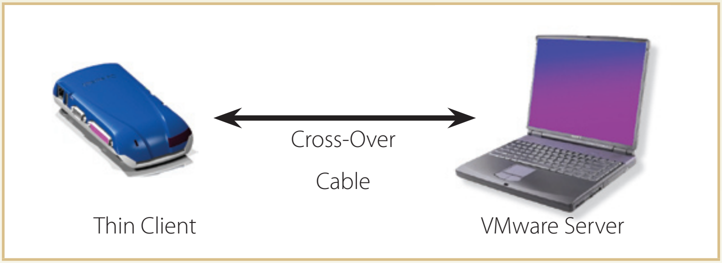


Figure 1: TC-VMware Server Communication - method 1

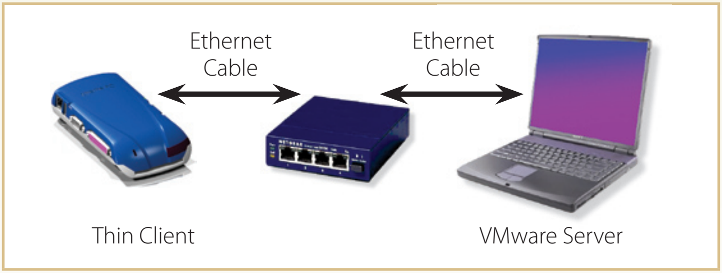


Figure 2: TC-VMware Server Communication - method 2

7 Initial Thin Client Configuration

Note: Scenarios can be practiced in a limited way without thin-clients if not available.

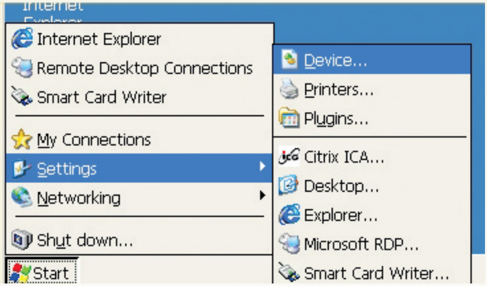
7.1 Client Starting-Point

Client-side settings described in this section are considered as the Client Starting-Point settings. Verify the following settings are applied on the Xtreme PC thin client prior to running any scenario.

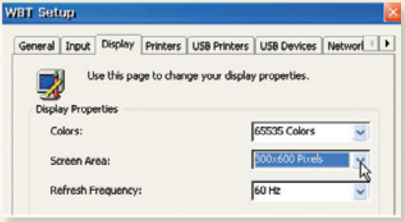
Note: If the thin client becomes inaccessible, resetting it to factory-defaults might be necessary. See appendix A for the "reset to factory-default" instructions.

7.2 Initial Device Display Configuration

1. Power ON the device by pressing the ***ON/STBY*** button.
2. Click the ***START* > *Settings* > *Device*** menu.



3. Browse to the ***Display*** Tab and select the following display settings:
   Colors = 65535
   Screen Area = 800x600
   Refresh Frequency = 60 Hz



Use this page to change your display properties.

Display Properties

Colors: 65535 Colors

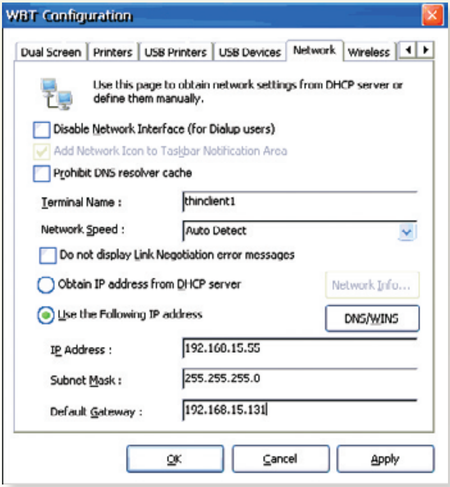
Screen Area: 800x600 Pixels

Refresh Frequency: 60 Hz

4. Click ***Apply***

7.3 Device TCP/IP Configuration

1. Browse to the ***Network*** Tab.
2. Configure the exact same settings as in the following figure:



Use this page to obtain network settings from DHCP server or define them manually.

□ Disable Network Interface (for Dialup users)

☑ Add Network Icon to Taskbar Notification Area

□ Prohibit DNS resolver cache

Terminal Name : thinclient1

Network Speed : Auto Detect

□ Do not display Link Negotiation error messages

○ Obtain IP address from DHCP server

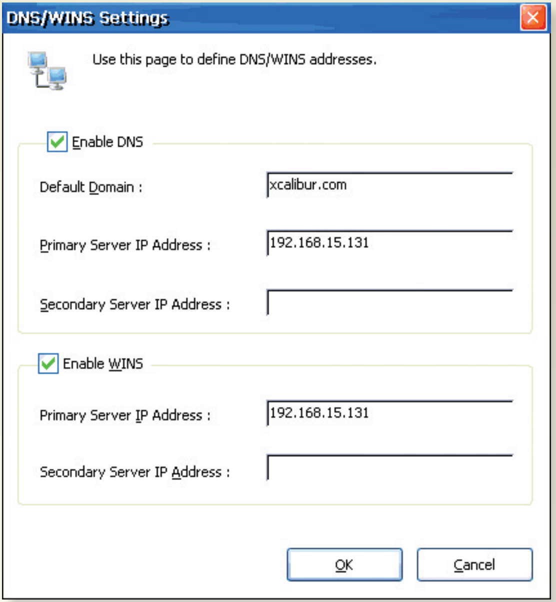
● Use the Following IP address

IP Address : 192.160.15.55

Subnet Mask : 255.255.255.0

Default Gateway : 192.168.15.131

3. Click the ***DNS/WINS*** button and configure the exact settings as in the following figure:



DNS/WINS Settings

Use this page to define DNS/WINS addresses.

☑ Enable DNS

Default Domain : xcalibur.com

Primary Server IP Address : 192.168.15.131

Secondary Server IP Address :

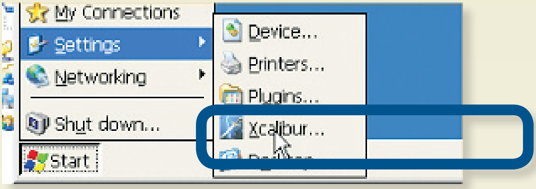
☑ Enable WINS

Primary Server IP Address : 192.168.15.131

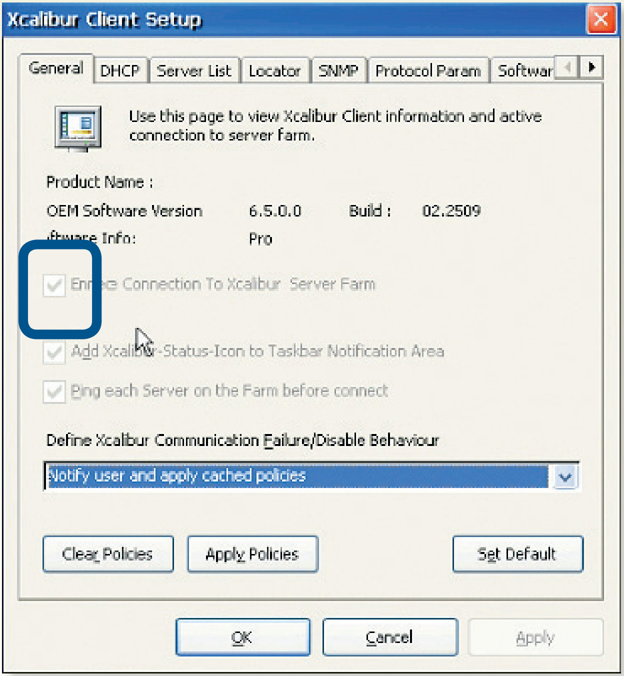
Secondary Server IP Address :

4. Click ***OK.***
5. Click ***Apply***
6. Close the ***WBT*** dialog

7. Go to ***Start \ Settings \ Xcalibur***



8. In the ***General*** Tab check ***Enable Connection to Xcalibur Farm***



Use this page to view Xcalibur Client information and active connection to server farm.

Product Name :

OEM Software Version 6.5.0.0 Build : 02.2509

ftware Info: Pro

☑ Enable Connection To Xcalibur Server Farm

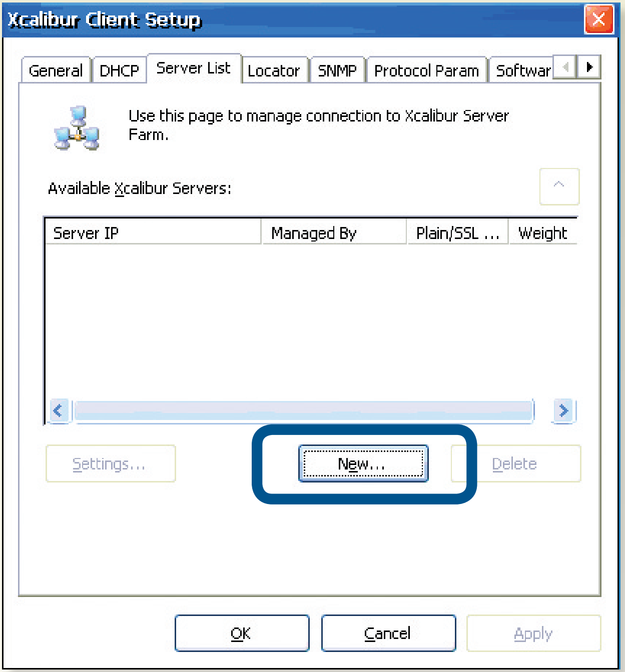
☑ Add Xcalibur-Status-Icon to Taskbar Notification Area

☑ Ping each Server on the Farm before connect

Define Xcalibur Communication Failure/Disable Behaviour

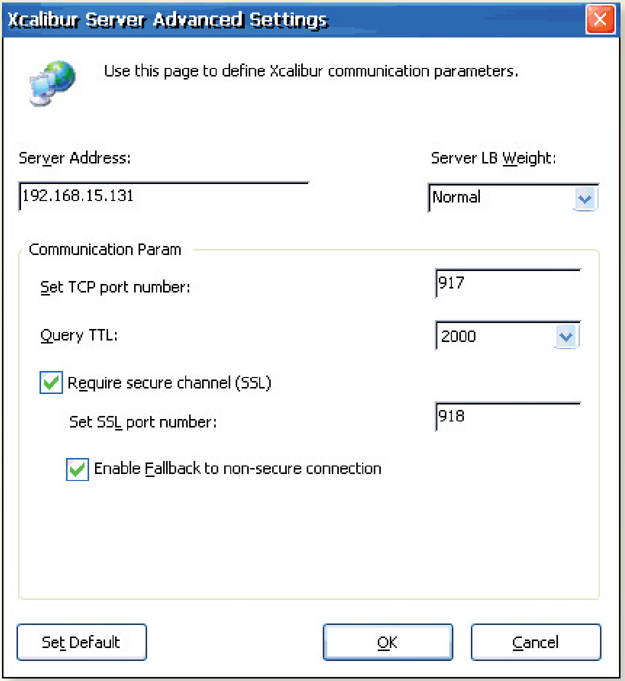
Notify user and apply cached policies

9. In the ***Server List*** tab click on ***New*** and insert the ***Server Address*** as ***192.168.15.131***



10. Click on ***Setting***

11. Configure as below


Xcalibur Server Advanced Settings

Use this page to define Xcalibur communication parameters.

Server Address: 192.168.15.131

Server LB Weight: Normal

Communication Param

Set TCP port number: 917

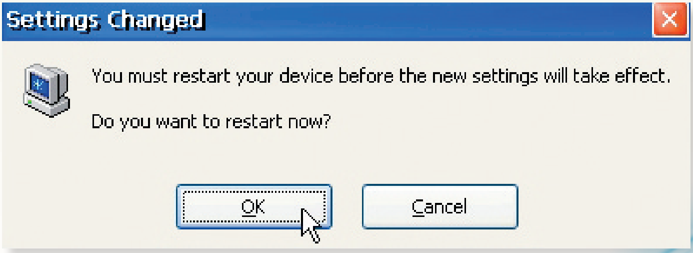
Query TTL: 2000

☑ Require secure channel (SSL)

Set SSL port number: 918

☑ Enable Fallback to non-secure connection

12. Click ***OK, Apply***
13. Click ***OK*** and ***Restart*** the device.


Settings Changed

You must restart your device before the new settings will take effect.

Do you want to restart now?

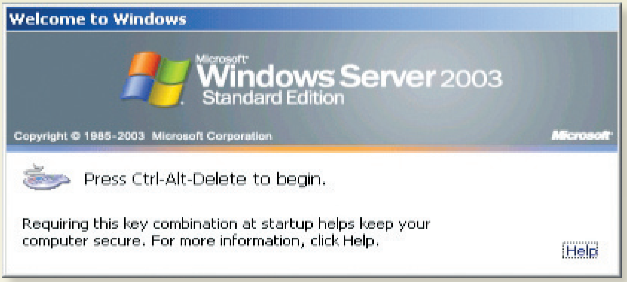
8 How to boot the Virtual Environment Xcalibur Image

1. Make sure the VMware Player 1.1 software is installed on your computer. A trial version is available on the DVD (***folder name: <u>VMware-player-1.0.2-29634</u>).***
2. Copy the Xcalibur Global Image directory (***folder name: Xcalibur Global Evaluation Environment***) from the DVD to your Hard Drive (make sure that you have at least 4 GB of free disk space).
3. Right click on the copied directory and make sure that the ***READ ONLY*** attribute is not checked (apply this setting also on subfolders if requested).
4. Open ***VMware Player***.
5. A Browser dialog will appear enabling you to browse to the copied folder select named ***<u>Xcalibur Global Evaluation Environment</u>***.

Note: Prior to booting the Xcalibur Image, make sure that your computer (Hosting the Xcalibur Image) is connected to the network. If it is connected to the Xtreme PC thin client via a crossed-cable the thin client must be turned ON before you boot the Xcalibur Image.

Note: The Xcalibur Image boot time might be relatively long depending on the host computer CPU strength and RAM memory size.

6. At the end of the boot process the windows logon window appears.



Welcome to Windows

Microsoft Windows Server 2003 Standard Edition

Copyright © 1985-2003 Microsoft Corporation

Press Ctrl-Alt-Delete to begin.

Requiring this key combination at startup helps keep your computer secure. For more information, click Help.

Press ***Ctrl* + *Alt* + *INSERT*** in order to logon.
User Name: ***Administrator***
Password: ***password***
Domain: ***xcalibur***

Note: Make sure you press ***Ctrl+Alt+INSERT* and NOT Ctrl+Alt+ Del.**

9 Start Evaluating…

General:

Once completing the "Initial Thin Client Configuration" and the "How to Boot the Xcalibur Image" sections, you are now ready to start evaluating.

Before you begin make sure that:

- The Xcalibur Image is started.
- The thin client is turned ON.

Note: You might encounter relatively long delays when performing various actions from within the Xcalibur Console. These might be due to the fact that the Xcalibur Image is running virtually on your computer thus requiring many resources. Please be patient.

10 Scenario 1: Find a new Device and Attach it to an OU

In this scenario you will launch the Xcalibur Console, identify your device and map it into an Organizational Unit in the Domain.

Successfully completing this scenario indicates that the client-server communication and initial settings are set correctly. If this scenario fails make sure that the server and client are set to their Starting-Points and start again.

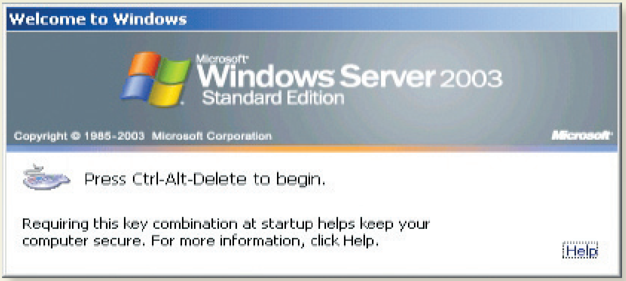
Note: Reading the whole scenario prior to beginning it, is highly recommended.

Note: Before starting this scenario, verify that the thin client is turned on and connected to the network.

10.1 Logon to the Virtual Server

Client-Side Action: None

Server-Side Actions:



Welcome to Windows

Microsoft Windows Server 2003
Standard Edition
Copyright © 1985-2003 Microsoft Corporation
Microsoft

Press Ctrl-Alt-Delete to begin.

Requiring this key combination at startup helps keep your computer secure. For more information, click Help.

1. Press ***CTRL + ALT + <u>INSERT</u>*** and type the following:
   User Name: ***administrator***
   Password: ***password***
   Domain: ***xcalibur***

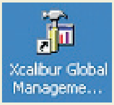
Note: Make sure you press ***Ctrl+Alt+<u>INSERT</u> and NOT Ctrl+Alt+Del.***

10.2 Launch the Xcalibur Console

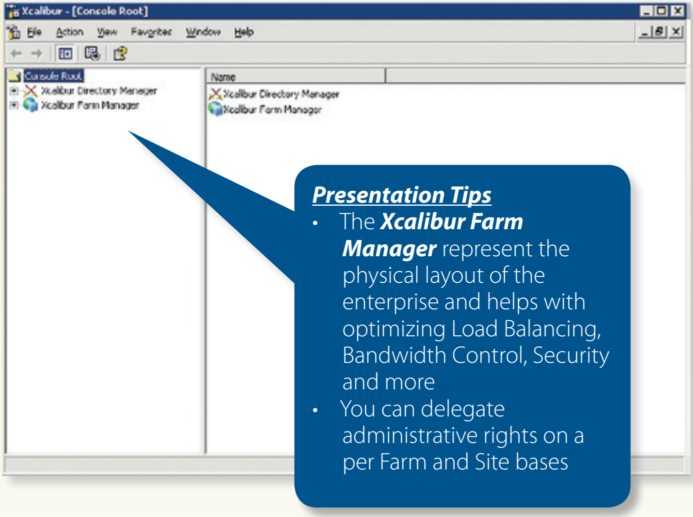
Client-Side Action: None

Server-Side Actions:

1. Double click the Xcalibur Global ICON on the desktop of the Xcalibur Server.



2. The ***Xcalibur Global MMC*** will appear:



Presentation Tips

- The ***Xcalibur Farm Manager*** represent the physical layout of the enterprise and helps with optimizing Load Balancing, Bandwidth Control, Security and more
- You can delegate administrative rights on a per Farm and Site bases

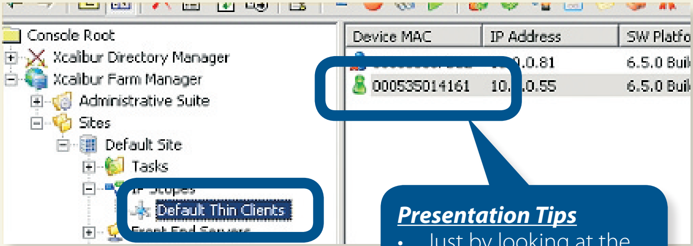
10.3 Find your new Device

Once a new device connects to ***Xcalibur***, it can be found under the ***Xcalibur Farm Manager***. In this exercise you will locate your device and learn about its status.

Client-Side Action: None

Server-Side Actions:

1. ***Select Scope*** - Select ***Xcalibur Farm Manager \ SItes\ Default Site \ IP Scope \ Default Thin Clients***



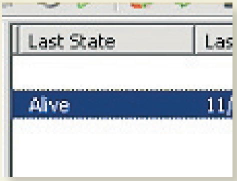
Device MAC	IP Address	SW Platfo
	.0.81	6.5.0 Buil
000535014161	10. .0.55	6.5.0 Buil

Presentation Tips

- Just by looking at the interface you can get detailed information about the device: IP address, name, MAC address and more

Your device appears on the right MMC pane in Green, indicating it has successfully been registered into the ***Xcalibur Global*** system.

Before moving on to the next step, please verify that the ***Last State*** column indicates the client's state as ***Alive***.



Last State	Las
Alive	11/

The status ***Alive*** means that the device is currently running and connected to Xcalibur

Note: The Xcalibur Farm Manager allows you to map the physical structure of the organization. You can create IP Scopes to represent the IP Address ranges in the company. One or more Scopes define a Site that represents a branch office.

10.4 Moving the Devices to a new OU

By moving a device between OUs it receives (by inheritance) all the policies linked to the current OU, the OUs above it and the Domain.

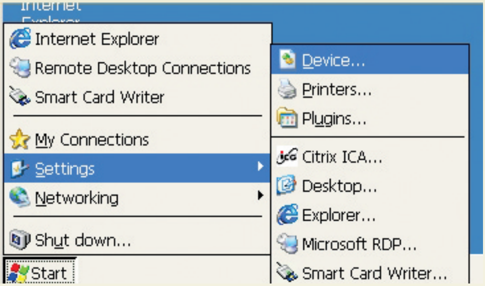
In this scenario the ***Lockdown Desktop policy*** assigned to the ***Lockdown Desktop*** OU, will prevent the user from accessing and changing the device settings locally unless he is authorized to do so. This policy sets a password to the WBT Configuration area.

Client-Side Actions:

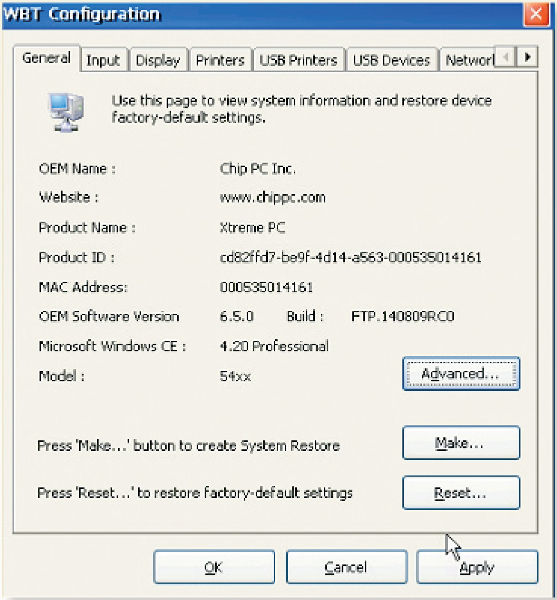
Verify that the WBT dialog is currently not password protected

At the moment any user can access the WBT dialog and change its settings.

1. ***Open the Device WBT*** - Go to ***Start \ Settings \ Device*** and verify that the WBT dialog opens (indicating anyone can access this area).



WBT Configuration dialog will appear



Use this page to view system information and restore device factory-default settings.

OEM Name : Chip PC Inc.

Website : www.chippc.com

Product Name : Xtreme PC

Product ID : cd82ffd7-be9f-4d14-a563-000535014161

MAC Address: 000535014161

OEM Software Version 6.5.0 Build : FTP.140809RC0

Microsoft Windows CE : 4.20 Professional

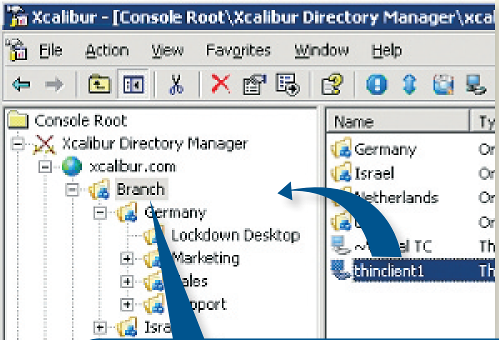
Model : 54xx

Press 'Make...' button to create System Restore

Press 'Reset...' to restore factory-default settings

Server-Side Actions:

2. ***Move the Device to the Lockdown Desktop OU*** - From the ***Xcalibur Directory Manager \ Xcalibur.com \ Branch*** select the "thinclient1" device (your device) and drag it to ***the Xcalibur Directory Manager \ Xcalibur.com \ Branch \ Germany \ Lockdown Desktop*** OU



Presentation Tips

- ***Xcalibur Directory Manager*** represents the logical structure of the organization.
- ***Xcalibur Directory Manage***r is derived from the organization's existing ***Active Directory*** tree making it easy to deploy new devices for the first time
- ***Xcalibur*** complies with the Active Directory permission scheme and therefore supports permission delegation at all levels

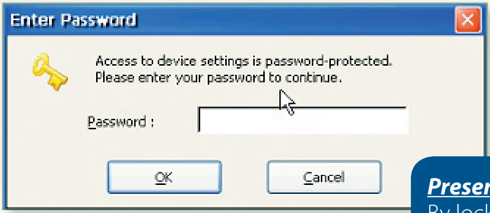
Note: Change of settings resulting from moving the device into the Lockdown Desktop OU will take affect after the device obtains the latest policy and reboots.

The process is expected to take 1 minute.

Client-Side Actions:

Verifying that the Device's WBT dialog is locked

3. ***Try to open the WBT dialog*** - Once completing Step #2 and after the device boots, go to ***Start \ Settings \ Device***. The password prompt indicates that the device settings have changed (and became more secure) as defined by the policy linked to the Lockdown Desktop OU.


Enter Password

Access to device settings is password-protected.
Please enter your password to continue.

Password :

Presentation Tips
By locking down the WBT dialog you can prevent unauthorized users from changing the device settings locally, making your network safer.

More about ***Xcalibur Policies*** in the next scenario

Congratulations!

You successfully completed Scenario 1. At the end of the thin client boot you can continue to Scenario 2.

11 Scenario 2 – Link a Policy that installs VNC on your device

General:

In this scenario you will learn about Xcalibur policies and their use during your daily work flow.

An ***Xcalibur Policy*** is a set of rules that can be linked to a Domain, OU, Device and User. All thin client management aspects, from software installations to user environment management, are controlled by Xcalibur policies.

Xcalibur Policy settings pass by inheritance from parent to child objects anywhere in the Active Directory tree

Before you begin:

It is assumed that you are already logged on to the Xcalibur Server, that the Xcalibur Console is opened and that you recognize your thin client.

11.1 View Current Policies

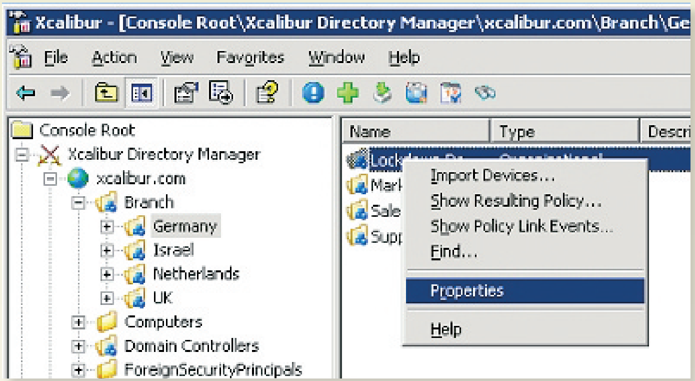
First let us look at the current policies linked to the ***Lockdown Desktop*** OU.

Client-Side Actions: None

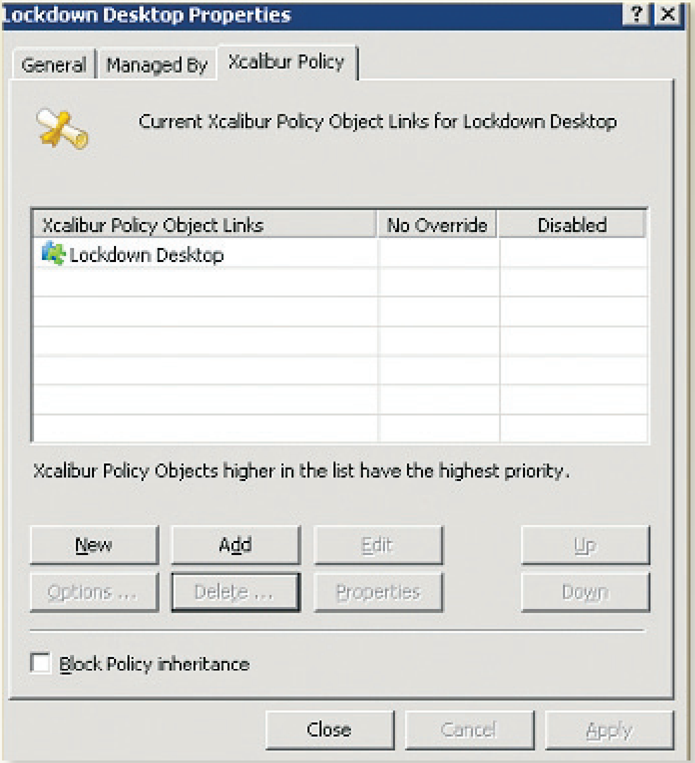
Server-Side Actions:

1. ***Select OU*** - Select ***Xcalibur Directory Manager \ Xcalibur.com \ Branch \ Germany \ Lockdown Desktop***

2. ***Open Properties*** - Right click on the ***Lockdown Desktop OU*** and then click ***Properties***.



3. Go to the ***Xcalibur Policy*** tab



Current Xcalibur Policy Object Links for Lockdown Desktop

Xcalibur Policy Object Links	No Override	Disabled
Lockdown Desktop		

Xcalibur Policy Objects higher in the list have the highest priority.

□ Block Policy inheritance

As you can see the ***Lockdown Desktop*** Policy (responsible of locking down the WBT dialog) is linked to this level

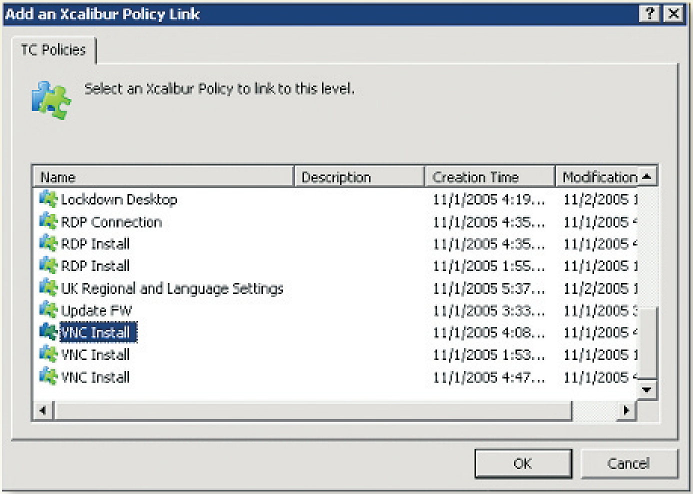
11.2 Link an existing policy to the OU

In this scenario we will link the ***VNC Install*** Policy to the ***Lockdown Desktop*** OU. This policy installs the VNC Plug-in on clients affected by it (in this exercise it is thinclient1 - your device).

Client-Side Actions: None

Server-Side Actions:

1. Click the ***Add***… button.
2. Select ***VNC Install*** from the policies list
3. Click ***OK***



Add an Xcalibur Policy Link

TC Policies

Select an Xcalibur Policy to link to this level.

Name	Description	Creation Time	Modification
Lockdown Desktop		11/1/2005 4:19…	11/2/2005 1
RDP Connection		11/1/2005 4:35…	11/1/2005 4
RDP Install		11/1/2005 4:35…	11/1/2005 4
RDP Install		11/1/2005 1:55…	11/1/2005 1
UK Regional and Language Settings		11/1/2005 5:37…	11/2/2005 1
Update FW		11/1/2005 3:33…	11/1/2005 3
VNC Install		11/1/2005 4:08…	11/1/2005 4
VNC Install		11/1/2005 1:53…	11/1/2005 1
VNC Install		11/1/2005 4:47…	11/1/2005 4

The newly added policy name is now displayed under the ***Xcalibur Policy Object Links*** column.

Note: Change of settings resulting from linking the VNC Install Policy to the Lockdown Desktop OU will take affect after the device obtains the latest policy and reboots.

The process is expected to take 1 minute.

Presentation Tips

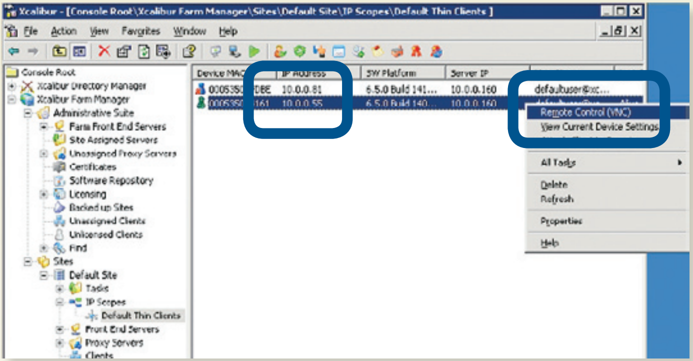
- Xcalibur policies can control all aspects of the device configuration, from connections to user environment and from software installations to security policies etc.
- Xcalibur Policies are inherited from parent OU to a child OU, the same way as Group Policies, making it easy to control and deploy large number of devices
- Although Xcalibur never modifies the Active Directory schema in any way, Xcalibur can be thought of as an Active Directory extension, providing a way to create thin client policies using the same guidelines and rules as those used to create and manage Group Policies in the Windows environment.

11.3 Shadow a device using VNC from the Xcalibur Farm Manger snap-in

Note: This exercise depends on the successful completion of the previous one. Please verify that VNC is installed on your thin client by entering the Start\Settings\Plug-ins menu on the local device and verifying that WinVNC Server appears under the Available Plug-ins column.

The ***Xcalibur Global*** comes complete with a VNC viewer. In order to use it:

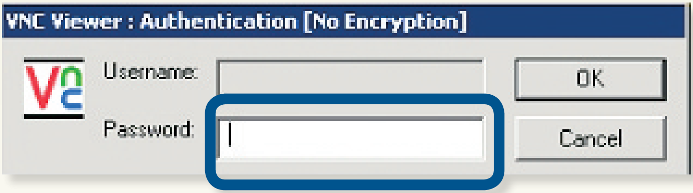
1. ***Shadow your device with VNC*** - Go to ***Xcalibur Farm Manager \ Sites \ Default Site \ IP Scope \ Default Thin Clients***
2. ***Select a device to shadow*** - On the right pane, select thinclient1 (your device), Right click it and select ***Remote Control (VNC)***.



Xcalibur - [Console Root\Xcalibur Farm Manager\Sites\Default Site\IP Scopes\Default Thin Clients]

Device MAC	IP Address	SW Platform	Server IP	
0005350 DBE	10.0.0.81	6.5.0 Build 141...	10.0.0.160	defaultuser@xc...
0005350 161	10.0.0.55	6.5.0 Build 140...	10.0.0.160	

3. ***Enter password*** - The password is: 1234



VNC Viewer : Authentication [No Encryption]

4. The remote session will appear and you are now able to shadow and control the thin client

From this point onward throughout this manual every time you will be referred to the client you can do that by using the VNC.

12 Scenario 3 – Software Installation and Distribution to Thin Client Devices using Xcalibur policy

In this scenario we will install the RDP Plug-in, create an RDP connection on the thin client and launch it automatically once the device restarts.

There are three parts to this scenario:

- Deploying the ***Client software*** to the device
- Creating the connection
- Configure the connection to auto start as the device boots

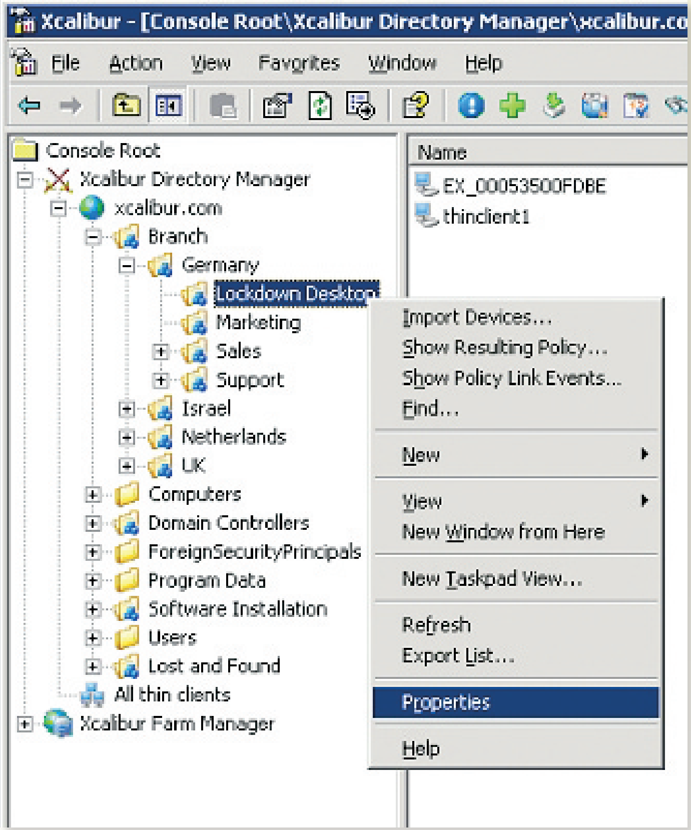
Client software is any software that is destined to be installed on Thin Client devices, such as software add-ons (e.g. Plug-ins) firmware and hotfix files. All installable and distributable software is first loaded to the ***Farm Software Repository*** and then it can be distributed to the Thin Clients.

The Xcalibur Global evaluation environment (on this DVD) comes with all the software files already installed. In a real-environment one would need to install software packages into the Xcalibur Software Repository prior to deploying those to thin clients.

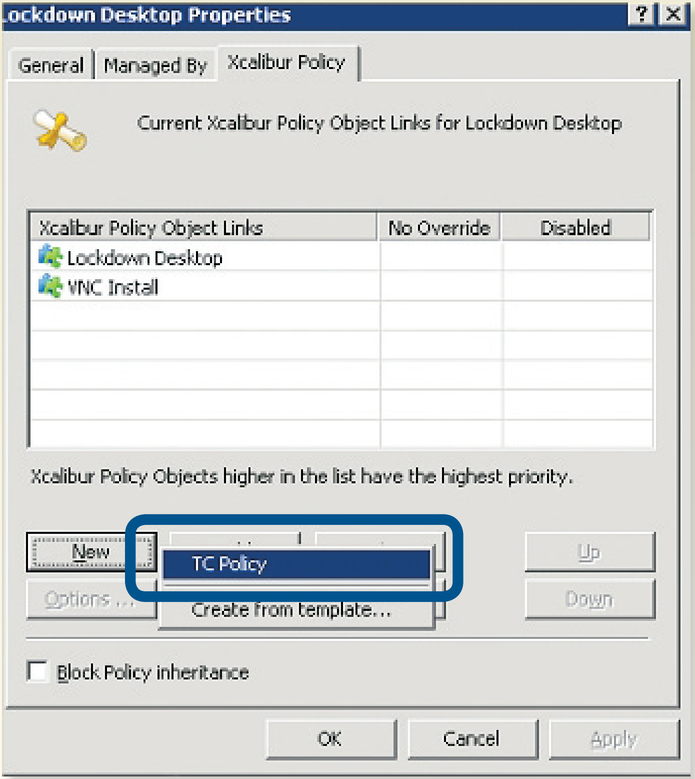
On how to load software packages to the ***Software Repository*** see ***Appendix B.***

12.1 Create a New Xcalibur Policy

1. ***Select Object*** - Go to ***Xcalibur Directory Manager \ Xcalibur.com \ Branch \ Germany \ Lockdown Desktop***
2. Select the ***Lockdown Desktop*** OU and right click
3. Click on ***Properties*** and go to ***Xcalibur Policy***



4. ***Create new Policy*** - Click on ***New \ TC Policy*** and create a new policy called RDP Connection Install and Launch



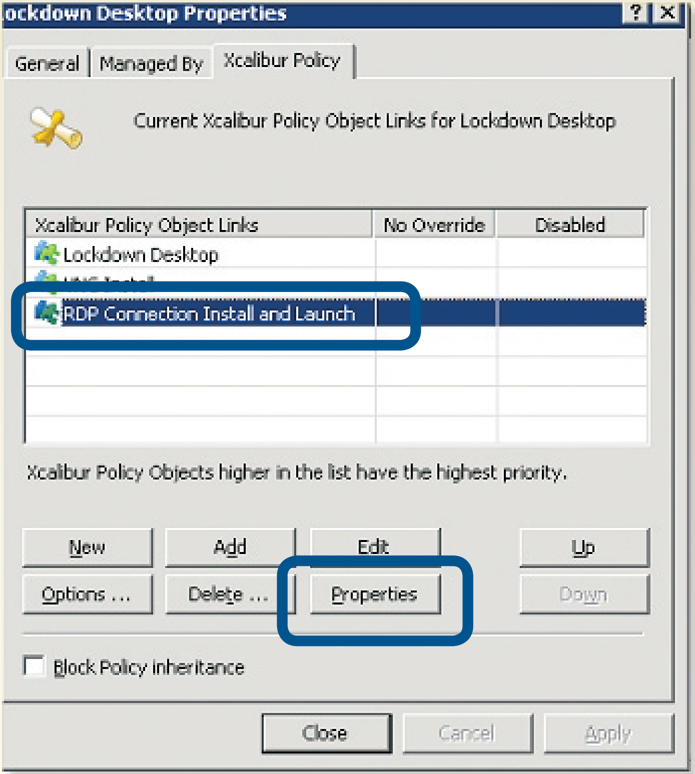
Current Xcalibur Policy Object Links for Lockdown Desktop

Xcalibur Policy Object Links	No Override	Disabled
Lockdown Desktop		
VNC Install		

Xcalibur Policy Objects higher in the list have the highest priority.

□ Block Policy inheritance

5. ***Edit the Policy*** - Select the new ***RDP Connection Install and Launch*** Policy from the ***Xcalibur Policy Object Links list and*** press ***Edit***, the ***Policy Editor*** will open



Current Xcalibur Policy Object Links for Lockdown Desktop

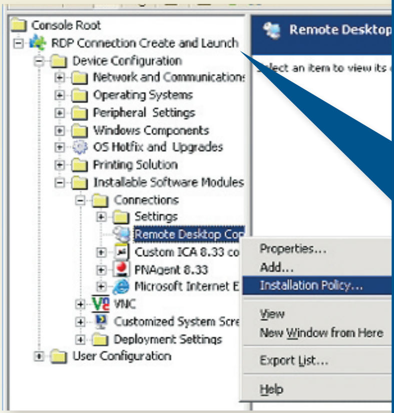
Xcalibur Policy Object Links	No Override	Disabled
Lockdown Desktop		
VNC Install		
RDP Connection Install and Launch		

Xcalibur Policy Objects higher in the list have the highest priority.

☐ Block Policy Inheritance

6. ***Configure the Policy to install RDP*** - Go to ***Device Configuration \ Installable Software Module \ Connections.***

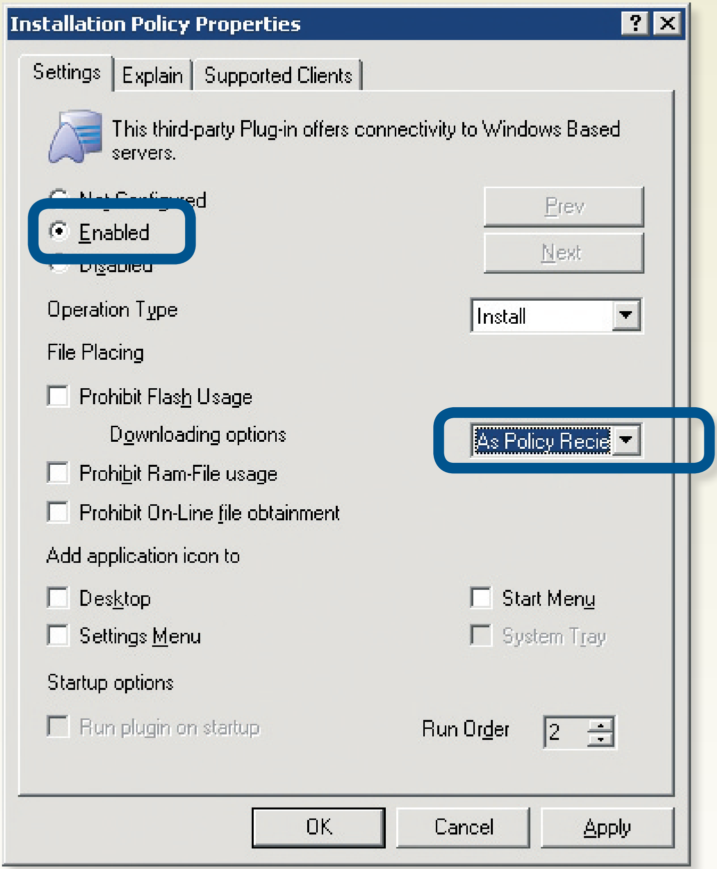
7. ***<u>Select Installation Policy</u>*** - Right click the ***Remote Desktop Connection*** and select the ***Installation Policy***…option



<u>Presentation Tips</u>

- ***Device configuration*** controls network and communication settings, operating system behavior, peripheral settings, Windows components, hotfix, upgrades and software deployment. These settings apply on thin client accounts according to their assignment in Active Directory tree and initiated as the thin client boot.
- ***User Configuration*** Controls Windows components, Software settings and communication options. These settings only apply once users logon to thin clients managed by Xcalibur Global

8. ***Enable the Installation Policy*** -Check the ***Enabled*** radio button
9. ***Specify Download Options*** - Set the ***Downloading Option*** to -> ***As Policy Received***



Installation Policy Properties

Settings | Explain | Supported Clients

This third-party Plug-in offers connectivity to Windows Based servers.

○ Not Configured
● Enabled
○ Disabled

Operation Type: Install

File Placing

□ Prohibit Flash Usage

Downloading options: As Policy Recie

□ Prohibit Ram-File usage
□ Prohibit On-Line file obtainment

Add application icon to

□ Desktop
□ Start Menu
□ Settings Menu
□ System Tray

Startup options

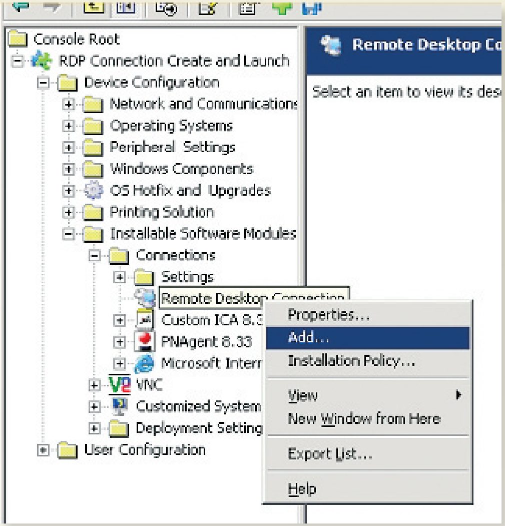
□ Run plugin on startup

Run Order: 2

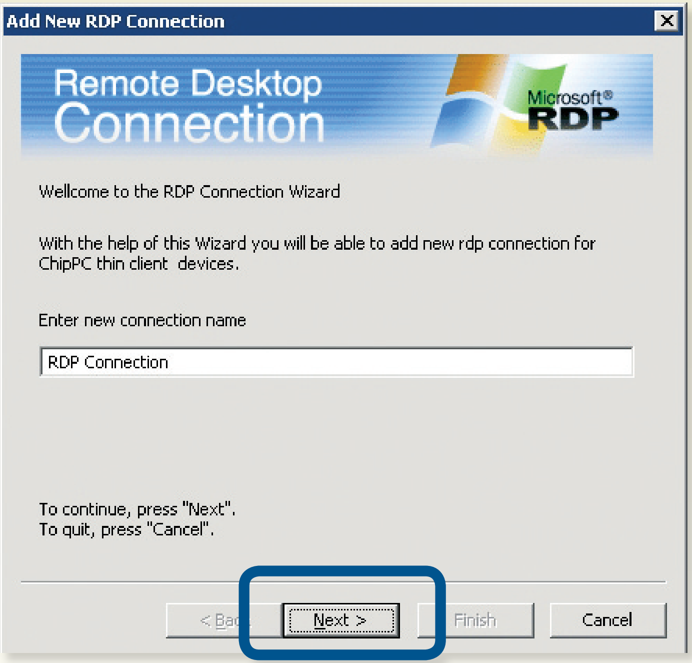
10. click ***Apply***
11. click ***OK***

12.2 Configure the policy to create a new RDP connection

1. ***Creating an RDP Connection*** - Right click the ***RDP Connection Create and Launch \ Device Configuration \ Installatllable Software Modules \ Connections \ Remote Desktop Connection*** and select the ***Add…*** option



2. ***Connection Name:*** Type RDP Connection as the Connection name and click ***Next***



Add New RDP Connection

Wellcome to the RDP Connection Wizard

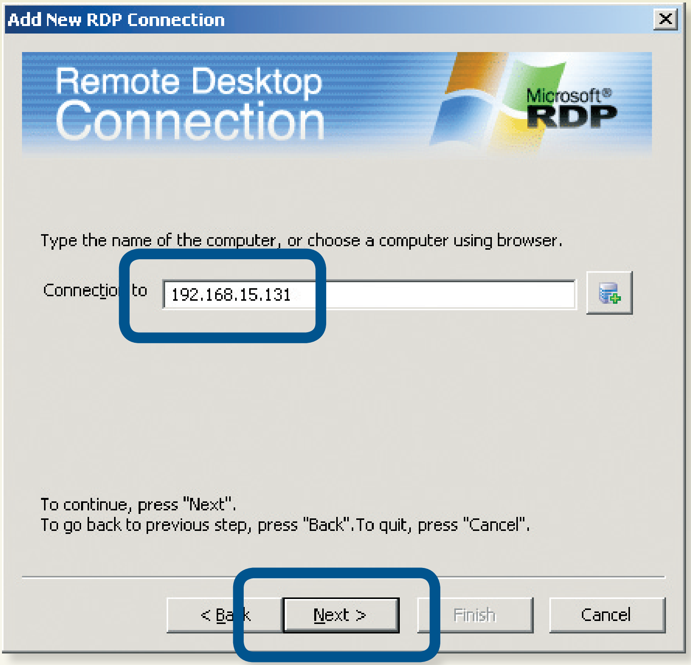
With the help of this Wizard you will be able to add new rdp connection for ChipPC thin client devices.

Enter new connection name

RDP Connection

To continue, press "Next".
To quit, press "Cancel".

3. ***Connect to:*** Type 192.168.15.131 as the target server and click ***Next***



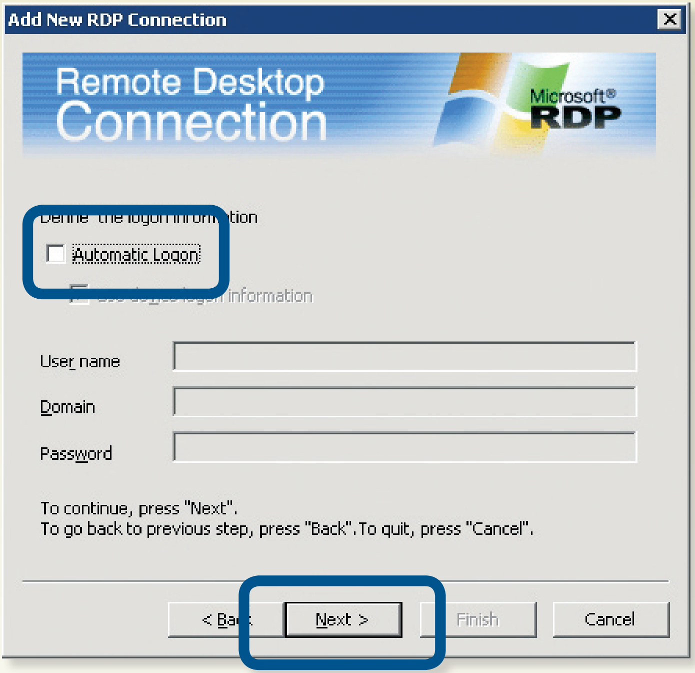
Add New RDP Connection

Type the name of the computer, or choose a computer using browser.

Connection to 192.168.15.131

To continue, press "Next".
To go back to previous step, press "Back". To quit, press "Cancel".

4. ***Logon Information*** - Uncheck the ***Automatic Log On*** and press Next



Add New RDP Connection

Define the logon information

□ Automatic Logon

□ Use default logon information

User name

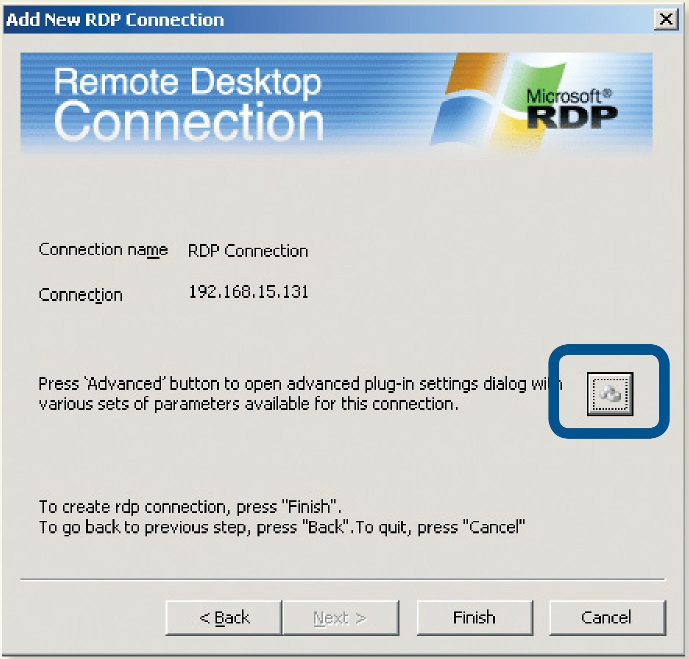
Domain

Password

To continue, press "Next".
To go back to previous step, press "Back". To quit, press "Cancel".

12.3 Enable the Auto Start Option (causes the thin client to launch the RDP connection on start up)

1. ***Go to the Advanced connection settings*** - Press ***Next*** twice and then click ***Advanced***.



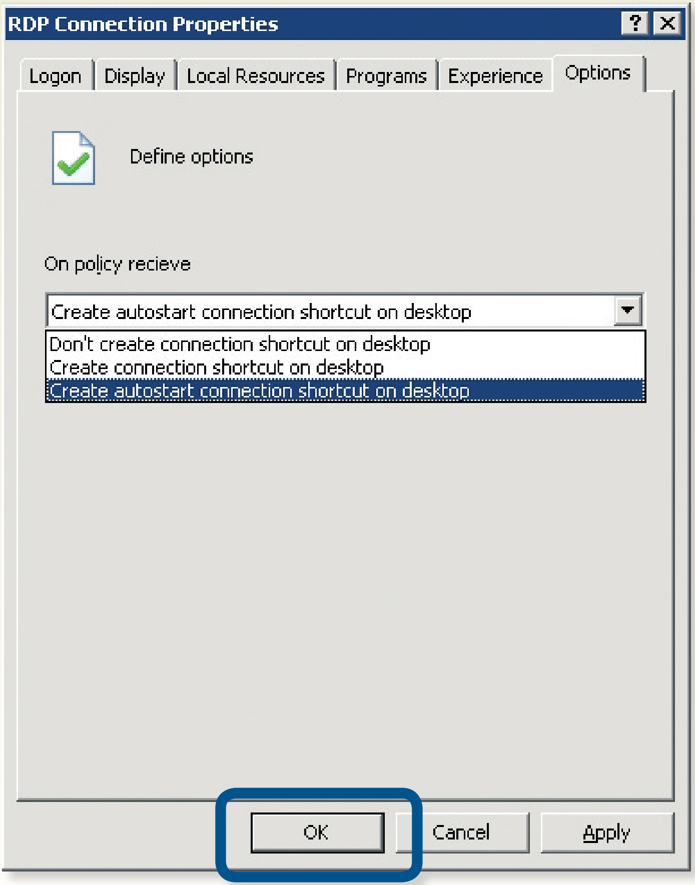
Connection name RDP Connection

Connection 192.168.15.131

Press 'Advanced' button to open advanced plug-in settings dialog wi h various sets of parameters available for this connection.

To create rdp connection, press "Finish".
To go back to previous step, press "Back".To quit, press "Cancel"

2. ***Set the connection to start-up automatically*** - From the scroll down menu, in the Options Tab, select the ***Create Auto Start Connection shortcut on the Desktop*** option
3. Click ***Apply*** and ***OK*** to close all property windows.



RDP Connection Properties
?
Logon
Display
Local Resources
Programs
Experience
Options
Define options
Don't create connection shortcut on desktop
Create connection shortcut on desktop
Create autostart connection shortcut on desktop
OK
Cancel
Apply

On policy recieve

Create autostart connection shortcut on desktop

Note: Change of settings resulting from linking the RDP Policy to the Lockdown Desktop OU will take affect once the device obtains the latest policy and reboots.

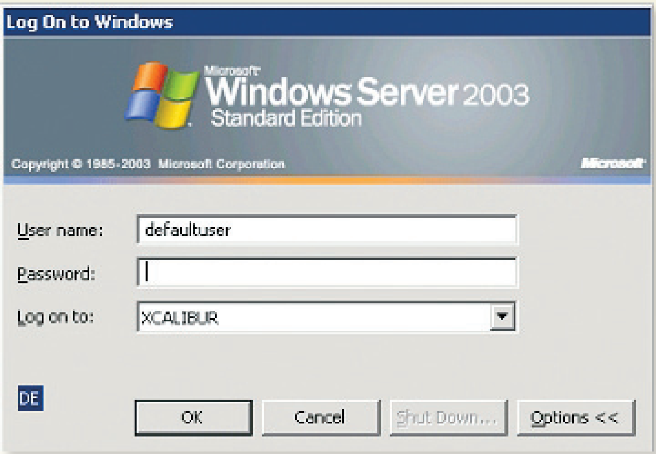
This process is expected to take about 1 minute.

Client-Side Actions:

Do nothing… until the device reboots.

After rebooting the RDP Connection pointing to 192.168.15.131 starts automatically.

4. ***Close the auto-started RDP Connection*** - In the Server Logon Window, press Cancel to close the RDP Connection.

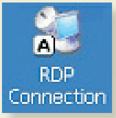


User name: defaultuser

Password:

Log on to: XCALIBUR

5. ***View the Connection Icon on Desktop*** - The RDP appears on the desktop. Note that the letter A on the connection icon indicates this connection is set to start-up automatical



13 Thin Client Device Authentication

The ***Xcalibur Global*** has a built-in Device and User authentication mechanisms. This ensures that only authorized (registered) thin clients and users can connect to the system.

A device is considered authenticated once its MAC address is registered in the Xcalibur Data Base and it is assigned to an OU. Authentication settings are specified from the Xcalibur Farm Manager snap-in and can be set at the Farm, Site or Scope levels. Child level authentication settings are inherited from the parent levels, therefore settings defined under the Farm will affect all Sites or Scopes below it.

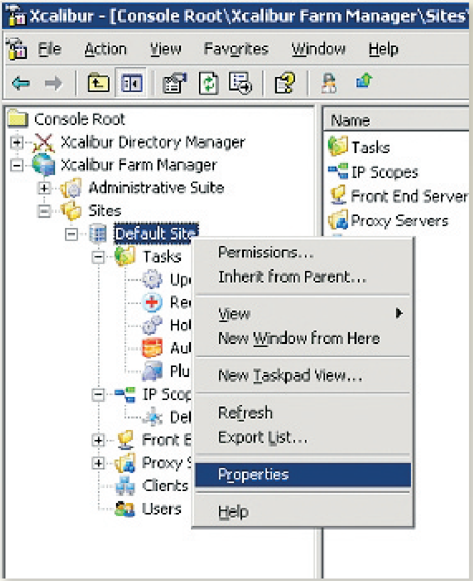
In this scenario we will set the thin client device authentication settings to block unrecognized thin clients until approved by the administrator.

13.1 Configure the site authentication to block new devices

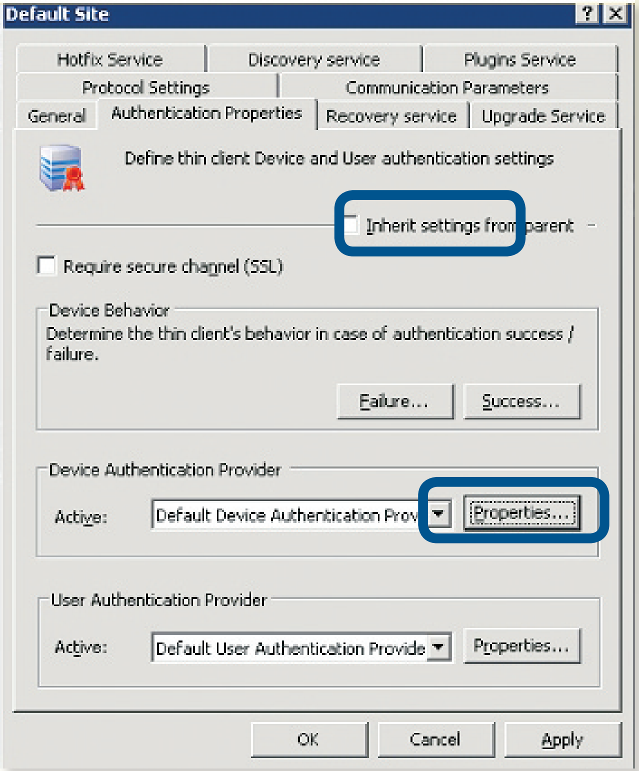
Client-Side Actions: None

Server-Side Actions:

1. ***Select Site*** - Go to ***Xcalibur Farm Manger \ Sites \ Default Site***
2. ***Select Properties*** - Right click on ***Default Site \ Properties***



3. ***Go to the Authentication Tab***- Select the ***Authentication Properties*** tab
4. ***Clear inheritance***- Uncheck the ***Inherit Settings from Parent*** checkbox
5. ***Enter the Device Authentication Provider Properties*** - Click on ***Properties*** in the ***Device Authentication Provider*** section



Default Site

Define thin client Device and User authentication settings

□ Inherit settings from parent

□ Require secure channel (SSL)

Device Behavior

Determine the thin client's behavior in case of authentication success / failure.

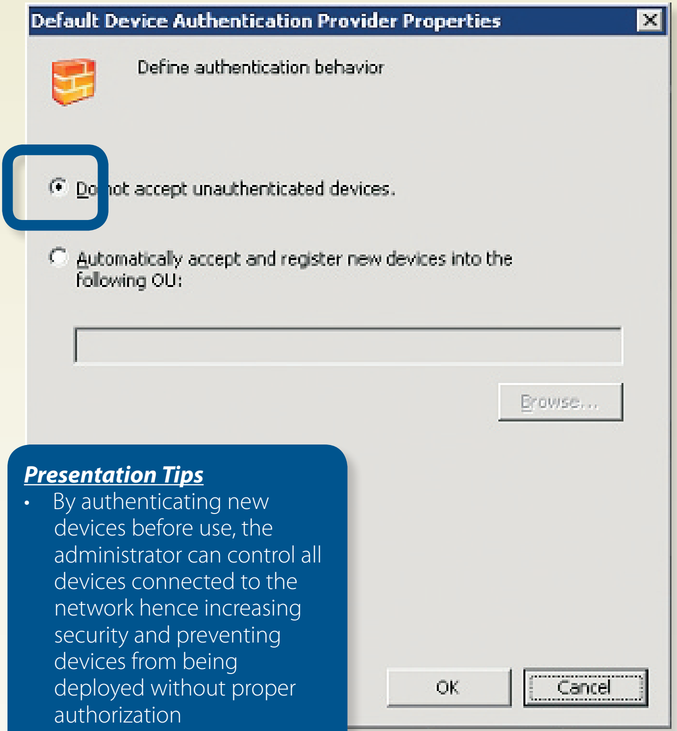
Device Authentication Provider

Active: Default Device Authentication Prov

User Authentication Provider

Active: Default User Authentication Provide

6. ***Change the Device Authentication Provider Properties*** - Check the ***Do not accept Unauthenticated Devices*** radio button.



Default Device Authentication Provider Properties

Define authentication behavior

● Do not accept unauthenticated devices.

○ Automatically accept and register new devices into the following OU:

Presentation Tips

- By authenticating new devices before use, the administrator can control all devices connected to the network hence increasing security and preventing devices from being deployed without proper authorization
- Administrators can define a default OU that will enable the device to be connected with lower security permissions

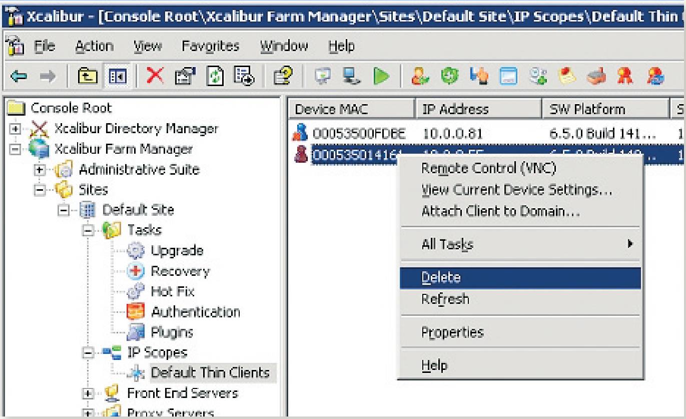
7. Click ***OK*** to close all dialogs.

By completing this step you have set the authentication configuration of the Default Site to automatically block new devices that connect to the Xcalibur from within the IP Address ranges that belong to this Site (e.g. 10.0.0.0 /24). Once an un-authenticated (new) device is recognized it will be blocked until manually approved by an Administrator.

13.2 Delete your device from the Xcalibur Database

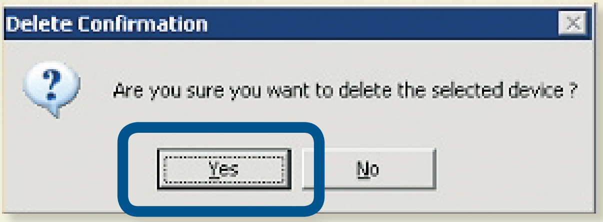
In order to view the changes made by the previous exercise you have to delete thinclient1 (your device) from the Default Thin Clients scope. This will simulate a new device being connected for the first time.

1. ***<u>Select the scope</u>*** - Select ***Xcalibur Farm Manger \ Sites \ Default Site \ IP Scopes \ Default thin cliens***
2. ***<u>Delete the device</u>*** - from the right view pane select thinclient1 (your device), Right click it and select the ***Delete*** option.



Device MAC	IP Address	SW Platform	S
00053500FDBE	10.0.0.81	6.5.0 Build 141...	1
00053501416		..	1

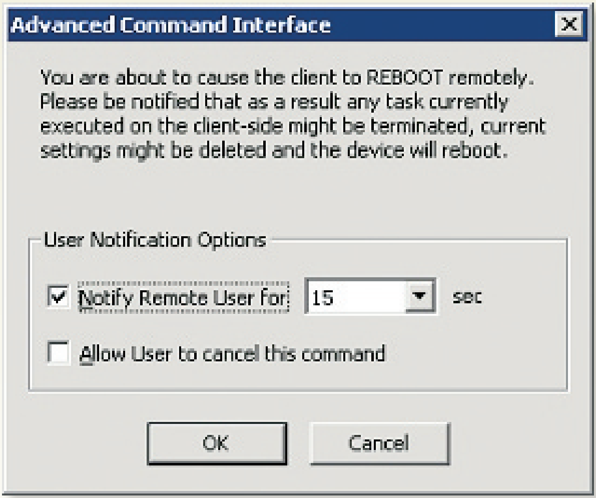
3. ***Confirm Deletion*** - Press ***YES*** at the ***Delete Confirmation pop-up.***



Delete Confirmation

Are you sure you want to delete the selected device ?

4. ***Notify user about the upcoming reboot*** - In the dialog asking whether to inform the user prior to rebooting, check the "Notify User for 15 Seconds" checkbox and press ***OK***.



Advanced Command Interface

You are about to cause the client to REBOOT remotely. Please be notified that as a result any task currently executed on the client-side might be terminated, current settings might be deleted and the device will reboot.

User Notification Options

☑ Notify Remote User for: 15 sec

□ Allow User to cancel this command

Expected Behavior:

The device will be deleted from the scope and restarted.

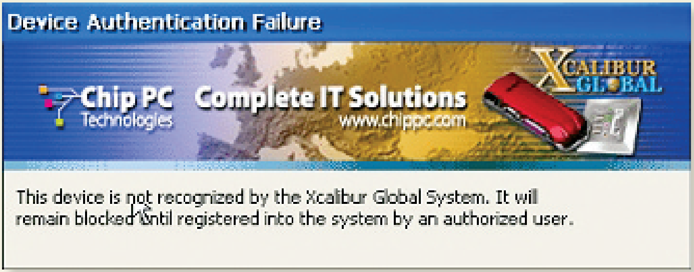
The user will receive a 15 seconds notice before shut down.

13.3 Verifying the Device is blocked by Xcalibur

After restarting, the device connects to Xcalibur and is automatically blocked since it is not registered into the Xcalibur Database.

Client Side Actions: None

1. ***See that the Device Interface is blocked*** - As you can see the device is unusable, thus no user can work on it until you unlock it from Xcalibur.



Device Authentication Failure

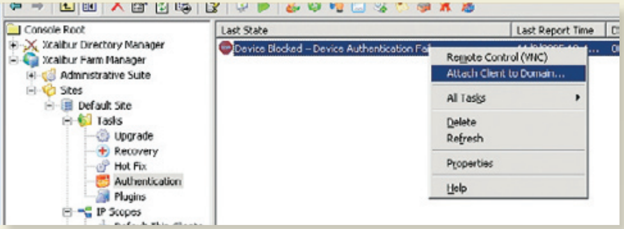
This device is not recognized by the Xcalibur Global System. It will remain blocked until registered into the system by an authorized user.

Server Side Action:

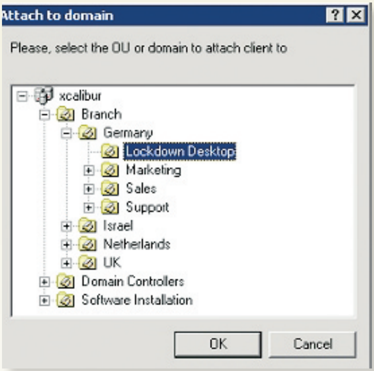
2. ***View the device status from Xcalibur*** **-** Go to ***Xcalibur Farm Manger \ Sites \ Default Site \ Tasks \ Authentication*** folder, there you'll see the device's status as Blocked.

13.4 Manually register the thin client into the Xcalibur

1. ***Attach Client to Domain…*** **-** In the Authentication Folder, right click your device and select the ***Attach Client to Domain…*** Option



2. ***Specify the destination OU*** **-** Expand the domain tree and select ***xcalibur \ Branch \ Germany \ Lockdown Desktop,*** then click ***OK***


Attach to domain

Please, select the OU or domain to attach client to

3. ***Refresh the Screen*** **-** Press ***F5*** to refresh MMC Interface and verify the device no longer appears under the ***Authentication*** folder.

Client Side Actions:

Once the Xcalibur registers the device, the Block-Message disappears from the client desktop and it becomes accessible. Device settings will be changed according to the Xcalibur Policies that apply on it based on its location in the Active Directory tree.

Note: The device may boot several times as result of the policies being applied on it.

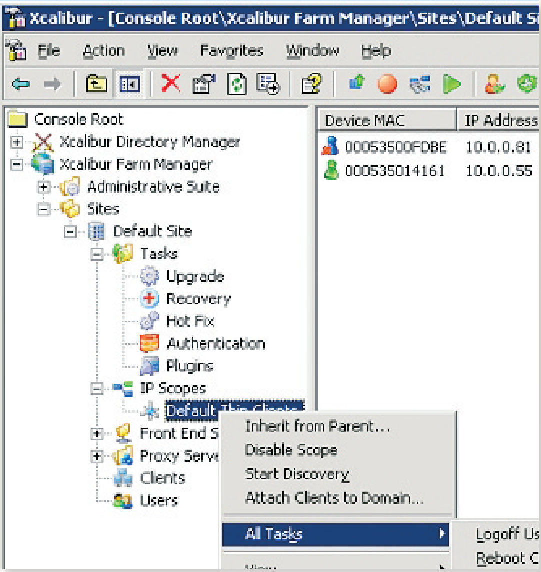
14 Appendix A – Reset to Factory Defaults

If in any time during the evaluation you receive results which are different from those described in this manual you need to reset the device to its factory defaults and start again.

> **Note:** The reset to factory defaults means that all licenses, Plug-ins, connection and settings will be erased returning to the OS initial state.

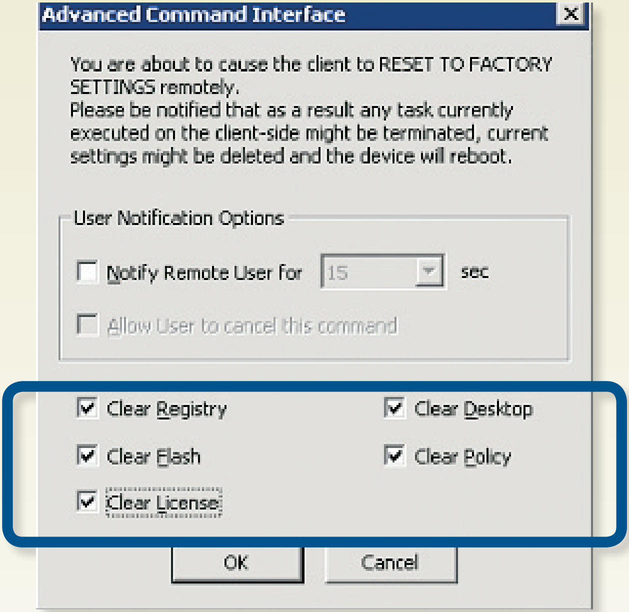
14.1 Reset using Xcalibur Global

1. ***Open default thin clients*** - Go to ***Xcalibur Farm Manger \ Sites \ Default Site \ IP Scopes \ Default Thin Clients***
2. ***Click Reset*** - Right click and select ***All Tasks \ Reset to Factory Defaults***



Device MAC	IP Address
00053500FDBE	10.0.0.81
000535014161	10.0.0.55

3. Check all the checkboxes on the lower part of the dialog as in the picture below and click ***OK***



Advanced Command Interface

You are about to cause the client to RESET TO FACTORY SETTINGS remotely.
Please be notified that as a result any task currently executed on the client-side might be terminated, current settings might be deleted and the device will reboot.

User Notification Options

□ Notify Remote User for 15 sec

□ Allow User to cancel this command

☑ Clear Registry ☑ Clear Desktop

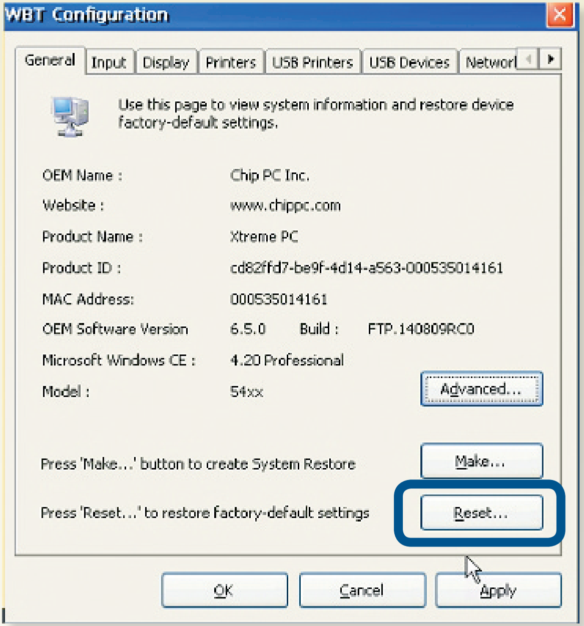
☑ Clear Flash ☑ Clear Policy

☑ Clear License

The device will be reset to the factory defaults and you will be able to start again.

14.2 Reset from the device software

Software reset can be initiated via the ***WBT \ General*** Tab once pressing the ***Reset*** button.



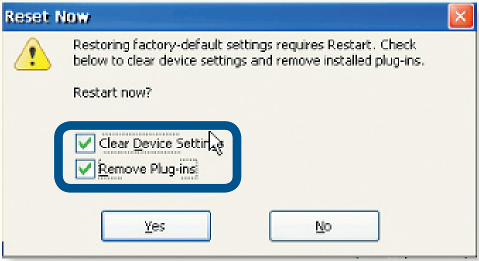
WBT Configuration

Use this page to view system information and restore device factory-default settings.

OEM Name :	Chip PC Inc.
Website :	www.chippc.com
Product Name :	Xtreme PC
Product ID :	cd82ffd7-be9f-4d14-a563-000535014161
MAC Address:	000535014161
OEM Software Version	6.5.0 Build : FTP.140809RC0
Microsoft Windows CE :	4.20 Professional
Model :	54xx

Press 'Make...' button to create System Restore

Press 'Reset...' to restore factory-default settings



Reset Now

Restoring factory-default settings requires Restart. Check below to clear device settings and remove installed plug-ins.

Restart now?

☑ Clear Device Settings

☑ Remove Plug-ins

14.3 Hardware Reset & Safe Mode Operation

A hardware reset can be initiated by running a certain action sequence by pressing the ON/STBY button. As result of this procedure, the device boots into a safe-mode state.

14.4 What is safe mode?

Safe mode is an intermediate state into which the device boots as a result to a hardware reset. This mode was designed to allow the device to complete its boot in any scenario. While in safe-mode only basic OS components are loaded therefore device settings are unchangeable. Administrators can only perform firmware or hotfix installation during this mode. To exit the safe mode, reboot the device.

As in software reset, all manually (and remotely) applied device settings and connections are cleared due to this operation. Additionally, ALL Plug-in settings are cleared.

14.5 Complete the following in order to perform hardware reset:

1. Take out (disconnect) the power cord connector from the device socket for one minute.
2. Plug in the power cord back into its device socket.
3. Once the ON/STBY lid turn red, press the ON/STBY button for one (1) second and than release it.
4. Once the ON/STBY lid turns green, press the ON/STBY constantly until the progress bar in the system-splash screen is filled, than release it. Please note that this procedure (deliberately) requires timing and accuracy in order to prevent user activation by mistake. Therefore several retries might be necessary before successfully entering the safe-mode.

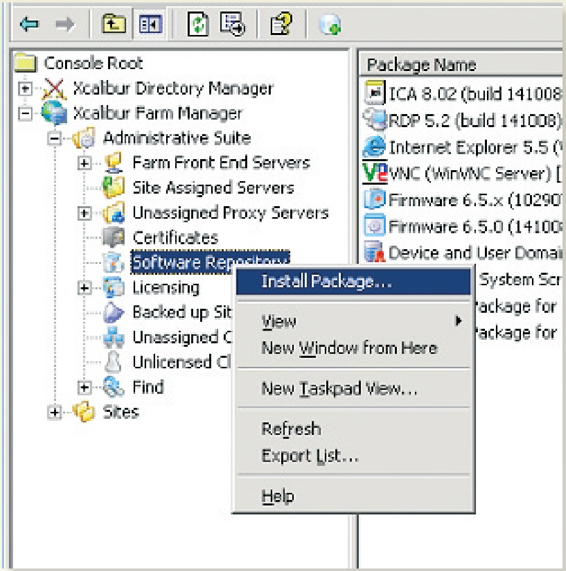
14.6 When to use hardware reset (examples)?

A hardware reset should be used whenever software reset isn't possible.

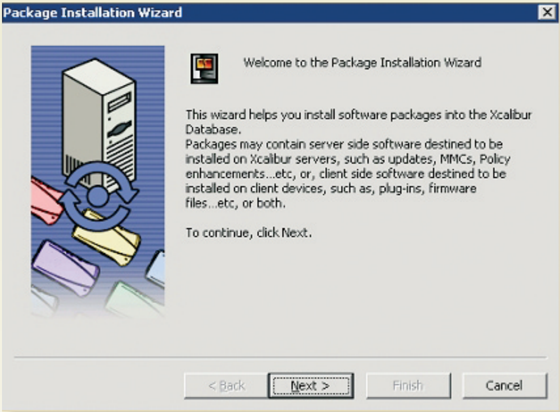
- ***Miss configured display:*** Miss-configured display settings (e.g. too high screen refresh frequency rate) may result in a clutter of colorful lines or a black screen display. This problem might appear when the monitor does not support the Xtreme PC's screen refresh rate / screen area size defined under the Display Tab. In this scenario, initiating a software reset becomes impossible therefore you can either connect the device to a different monitor or perform a hardware reset.
- Password Locked WBT: Incase the WBT Setup environment is inaccessible due to password protection, and the password set is forgotten. A hardware reset clears the password protection making device settings accessible again.

15 Appendix B - Loading the Software Package to the Repository

1. ***<u>Select the Install package wizard</u>*** - Go to ***Xcalibur Farm Server \ Software Repository*** right click ***Install Package***



2. Press ***Next***

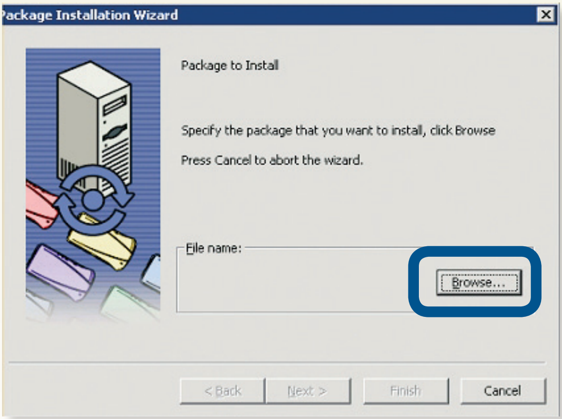


Welcome to the Package Installation Wizard

This wizard helps you install software packages into the Xcalibur Database.
Packages may contain server side software destined to be installed on Xcalibur servers, such as updates, MMCs, Policy enhancements...etc, or, client side software destined to be installed on client devices, such as, plug-ins, firmware files...etc, or both.

To continue, click Next.

3. You can now browse to the software package or file you need to load into the repository. ***Xcalibur Global*** evaluation comes with a complete set of upgrades and Add-ons already in the repository.



Package to Install

Specify the package that you want to install, click Browse

Press Cancel to abort the wizard.

File name:

The information contained in this document represents the current view of Chip PC on the issues discussed as of the date of publication. Because Chip PC must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Chip PC, and Chip PC cannot guarantee the accuracy of any information presented after the date of publication.

This Guide is for informational purposes only. CHIPPC MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Date of publication: December 2007

XCALIBUR GLOBAL

CPN03786

www.chippc.com

Chip PC
Technologies