

Xcalibur Global

Version 1.2

Quick Configuration Guide

Document Version 3.0



COPYRIGHT NOTICE

© 2010 Chip PC Inc., Chip PC (Israel) Ltd., Chip PC (UK) Ltd., Chip PC GmbH All rights reserved.

This product and/or associated software are protected by copyright, international treaties and various patents.

This manual and the software, firmware and/or hardware described in it are copyrighted. You may not reproduce, transmit, transcribe, store in a retrieval system, or translate into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual, or otherwise, any part of this publication without express written permission from Chip PC.

CHIP PC SHALL NOT BE LIABLE FOR TECHNICAL OR EDITORIAL ERRORS OR OMISSIONS CONTAINED HEREIN; NOR FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES RESULTING FROM THE FURNISHING, PERFORMANCE, OR USE OF THIS MATERIAL.

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. CHIP PC MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

TRADEMARKS

Chip PC, Xcalibur, Xtreme PC, Jack PC, Plug PC, ThinX, and the Chip PC logo are either trademarks or registered trademarks of Chip PC.

Products mentioned in this document may be registered trademarks or trademarks of their respective owners

The Energy Star emblem does not represent endorsement of any product or service.

U.S. GOVERNMENT RESTRICTED RIGHTS

The Software and documentation are provided with RESTRICTED RIGHTS.

You agree to comply with all applicable international and national laws that apply to the Software, including the U.S. Export Administration Regulations, as well as end-user, end-use and country destination restrictions issued by U.S. and other governments.

The information and specifications in this document are subject to change without prior notice.

Images are for demonstration purposes only.



Table of Contents

Chapter 1	Preface	5
-	Intended Audience	5
	Scope	5
	Objectives	5
	Reference Materials	5
	Prerequisites	5
	Document Features	6
	Conventions	6
	Notes	6
	Chapter Overview	6
Chapter 2	Getting Started	7
	Read the Setup Guide	7
Chapter 3	Xcalibur Farm Manager Tasks	9
-	Introduction	9
	Licensing	9
	Most Common Licenses	9
	Server Licenses	9
		9
	Installing Licenses	9
	Configuring the Farm Manager Discovery Service	
	Creating a New Site	18
	Configuring Authentication Settings	19
	Configuring Installation Services	23
	Upgrade Service	23
	Plugins Service	24
	Hotfix Service	25
	Creating a New IP Scope	26
	Starting the Xcalibur Front End Server	27
Chapter 4	Xcalibur Directory Manager Tasks	. 29
	Introduction	29
	Communication Policy	29
Chapter 5	Connecting Devices	. 35
	Prerequisites	35
	Connection Methods	35
	Initiate a Network Scan	36
	Viewing the Scan Results	37



	IP Scope View	
Chapter 6	Policy-Based Management	39
	General	
	Installing an RDP Plug-in via an Xcalibur Policy	
	Creating an RDP Connection via an Xcalibur Policy	41



Chapter 1 Preface

This chapter provides general information about the document.

Intended Audience

This document is targeted at the following professionals:

- Xtreme Certified Administrators
- Thin-client experts
- IT managers with adequate knowledge of Microsoft Active Directory architecture

Caution	Only professionals with MCSA 2003 or equivalent knowledge should attempt to implement the instructions in this document.
Important	It is recommended that this entire document be read prior to starting to configure Xcalibur Global .

Scope

This document applies to the following product:

Chip PC Xcalibur Global Management Software, version 1.2

Objectives

This document describes the fundamental configuration procedures that are required to activate an **Xcalibur Global** installation. Following the procedures described in this document will result with a basic configuration but fully operative and online **Xcalibur Global** environment.

Reference Materials

Xcalibur Global 1.2 - Installation Guide (ref: DG083U).

Prerequisites

Prior to implementing the procedures described in this document, all necessary installation procedures must be performed as described in the **Xcalibur Global 1.2 - Installation Guide**.



Document Features

Conventions

Bold formatting is used to indicate a product name, required selection or screen text entries.

Notes

Caution	Text marked Caution contains warnings about possible loss of data.
Important	Text marked Important contains information that is essential to
	completing a task.

Note Text marked Note contains supplemental information.

Chapter Overview

This document is divided into the following chapters:

- Chapter 1 Preface: provides general information about the document.
- Chapter 2 Getting Started: provides preliminary information before proceeding with **Xcalibur Global** configuration.
- Chapter 3 Xcalibur Farm Manager Tasks: provides step-by-step procedures for installing licenses, configuring the discovery service, creating a new site, configuring authentication settings, configuring installation services, creating a new IP scope, and starting the Xcalibur Global Front End Server service.
- Chapter 4 Xcalibur Directory Manager Tasks: provides step-by-step procedures to create a communication policy from an Xcalibur template.
- Chapter 5 Connecting Devices: Connecting Devices: provides a list of different methods for connecting thin client devices to Xcalibur Global with a special emphasis on the Network Scan method.
- Chapter 6 Policy-Based Management: provides step-by-step procedures for using an Xcalibur Policy to install an RDP plug-in and create an RDP connection on the client device.



Chapter 2 Getting Started

Read the Setup Guide

Xcalibur Global is designed to operate in a Windows 2000/3 Active Directory Environment. Before starting to configure **Xcalibur Global** ensure that you have performed all the required installation instructions as detailed in the **Xcalibur Global Installation Guide**.

This document assumes that:

- You have performed all necessary installation instructions described in the **Xcalibur Global Installation Guide**.
- All software packages (plug-ins) were installed during the database installation process (default option).
- All policy templates were installed during the database installation process (default option).
- You have obtained the required **Xcalibur Global** server and client licenses.
- **Note** For best results, you are recommended to work with a thin client device during the initial steps to observe real-time effects while configuring **Xcalibur Global**.

Important	The procedures described in the following sections allow the user
	to name objects according to his/her criteria. However, for
	improved support and documentation purposes, it is strongly
	recommended that the names used in this document are adopted
	and applied in the installed environment.



This page is left blank intentionally.



Chapter 3 Xcalibur Farm Manager Tasks

Introduction

This chapter provides step-by-step procedures to perform the following tasks:

- Install licenses
- Configure the Discovery Service at the Farm level
- Create a new site
- Configure authentication settings
- Configure installation services
- Create a new IP scope
- Start the Xcalibur Global Front End Server service

Licensing

In order to run **Xcalibur Global**, server and client licenses both need to be installed into the system. The following tables detail the most common licenses that are required for initial use.

Most Common Licenses

Server Licenses

Server License	License File Name	Notes
Xcalibur Global Server License	XGLicense	Required to start the Front End Server service
Domain Authentication	DALicense	Optional to enable the Domain Logon proxy

Client Licenses

Client License	License File Name	Notes
Xcalibur Global Client License	XCAL4	Required to manage thin clients
Domain Authentication Agent License	AUTHD	Optional to provide Domain Logon support on the client

Additional Licenses

Additional licenses may be required to achieve full functionality.



Installing Licenses

To complete this procedure you must have valid **Xcalibur Global** license files. Ensure that the license files are available on the **Xcalibur Global** server or through the network.

Proceed as follows to install licenses into the Xcalibur Global database:

- 1) Log on with an Xcalibur administrative account to the computer where **Xcalibur Global Management Console** is installed.
- From the Start button select Programs, Xcalibur Global (1.2), Management Console to launch Xcalibur Global Management Console, as illustrated.

Xcalibur - [Console Root]			- 0
🚡 Eile Action View Favorites V	jindow <u>H</u> elp		_181
Console Root	Name		
Bry Xcalibur Directory Manager	Kcalibur Directory Manager	Le .	

3) In the left pane, select and expand **Xcalibur Farm Manager**.



4) Select and expand **Administrative Suite** to display the full directory tree, as illustrated.

Help	<u>_8×</u>
Name Xcalibur Directory Manager Xcalibur Farm Manager	
	Help

5) In the Administrative Suite tree, select and highlight Licensing then from the right-click menu select Install License... to display the Welcome to the License Installation Wizard window, as illustrated.



6) The **Welcome to the License Installation Wizard** window enables you to install both server and client licenses. Click **Next** to continue and display the **License to Install** window.



7) In the License to Install window, as illustrated, click **Browse...** to display a standard Windows **Open** (file selection) window.

License Installation Wizard	License to Install
	Specify the license that you want to install, click Browse Press Cancel to abort the wizard. File name:
	Finish Cancel

8) In the Windows **Open** window, as illustrated, in the **Look in** dropdown box, click the dropdown arrow to browse to the directory where the required license file is located.

Look in	: 🔁 JackPC	-	🔄 🖻 💣 🅅 •	
My Recent Documents	MAUTHD.xd BMPS5.xd PERTE.xd VNCPI.xd XCAL4.xd			
My Documents				
hillel on MSDENET8	File <u>n</u> ame:			<u>O</u> pen
Places	F1 ()	D		Connol

9) Select the pertinent license file then click **Open** to complete the file selection process and return to the **License to Install** window.



10) The selected path and file name are displayed in the **License to Install** window, in the section **File name**, as illustrated.



Click Next to continue to the Ready to Install the Package window.

11) In the **Ready to Install the Package** window, as illustrated, click **Install** to install the selected license file.





12) After the license file is installed successfully, the **Completing the License Installation Wizard** window displays, as illustrated, informing you that the license is installed. Click **Finish** to exit the wizard and return to the **Xcalibur Global Management Console** window.



- 13) In the Xcalibur Global Management Console window, in the left pane, select and highlight Licensing then from the right-click menu select Refresh to verify that the newly-added license appears in the Licensing directory tree. (All added licenses can also be viewed in the right pane when Licensing is selected.)
- 14) Repeat this procedure for each license required to be installed.
- 15) After installing all required licenses, continue to the next procedure **Configuring the Farm Manager Discovery Service**.



Configuring the Farm Manager Discovery Service

Proceed as follows to configure the Farm Manager Discovery Service:

- 1) In the **Xcalibur Global Management Console** window, from the left pane select and highlight **Xcalibur Farm Manager**.
- From the right-click menu select Properties to display the Farm Properties window, then click the Discovery service tab to display the Discovery service settings tab page, as illustrated.

Notes	e Policvitic	tocol Setting Idater	js Ci Site Svr	ommunicati och	on Parameter RTI Interva
IP Scopes	Auth	entication Pr	operties	Rec	overv service
Upgrade Se	rvice	Hotfix Se	ervice	Disco	overy service
G Dis	covery servi	ce settings			
Server settir	ngs			- Inberi	t from Parent
Discovery s	erver:	one			• •
<u>W</u> orking on	: M	anual contro	bl		•
5grver table	to send to o	ilients:		Γ Igheri	from Parent
					+
					+
8					0

In the **Server settings** section, **Discovery server** dropdown box, click the dropdown arrow and select the server name from the displayed list; the selected server will execute the Discovery Service.

Note The selected server will be responsible for discovering thin client devices via network scans. Ensure that this server has access to all IP address ranges wherever thin clients may reside.



3) Click the **Advanced settings 1** button for the selected server to display, the **Advanced settings** window, as illustrated.



- 4) In the Advanced settings window, select the following options:
 - a) Use SNMP protocol for discovery
 - b) Enable Xcalibur Agent on discovered devices.
- 5) In the **Advanced settings** window click **OK** to save your changes and return to the **Discovery service settings** tab page.



6) In the Discovery service settings tab page, click the Add Server to
 Table button and select the server to add to the table in the section

Server table to send to clients, as illustrated.

m Properties		
Plugins Service Notes Polic IP Scopes A Upgrade Service	Protocol Settings Cc y Updater Site Syr Nuthentication Properties Hotfix Service service settings	mmunication Parameter ich RTI Interval Recovery service Discovery service
Server settings	DVSQLMATOS,xcalbur4.	C Inherit from Parent
Working on :	Manual control	•
- Server table to send	l to clients:	🗗 Igherit from Parent
		*
0		0
	OK	Cancel Apply

- **Note** The table lists details of Front End servers that the thin client device will attempt to connect to according to the displayed order (top to bottom).
- 7) Click **Apply** to save your settings then click **OK** to close the **Farm Properties** window.
- 8) Continue to the next procedure, Creating a New Site.



Creating a New Site

Proceed as follows to configure a new LAN site:

- 1) In the **Xcalibur Global Management Console** window, from the left pane select and highlight **Sites**.
- 2) From the right-click menu select **New, Site...**, as illustrated, to display the **New Site** window.



3) In the New Site window, as illustrated, complete the following fields:



- 4) Click **OK** to save your entries and add the new site to the **Sites** directory.
- 5) Continue to the next procedure, **Configuring Authentication Settings**.



Configuring Authentication Settings

Proceed as follows to configure site authentication settings for the new site defined in the previous procedure:

- 1) Select the newly-added site, LAN Site, in the Sites directory and from the right-click menu select **Properties** to display the LAN Site window.
- 2) In the LAN Site window, click the Authentication Properties tab to display the Authentication Properties tab page, as illustrated.

otfix Servic	e Discovery service Plugins Service Protocol Setting
Communicati	ion Parameters Notes Policy Updater Site Synch (thentication Properties Decouvery convice Upgrade Service
	Anerotación reportado in Recovery service opgrade dervic
ا <mark>ا</mark>	Define thin client Device and User authentication settings
-	
-	Inherit settings from parent
Require	secure chagnel (SSL)
-Deurice Pet	
Device Bel Determine	navior the thin client's behavior in case of authentication success /
Device Bel Determine failure.	navior the thin client's behavior in case of authentication success /
Device Beł Determine failure.	navior the thin client's behavior in case of authentication success / Failure Success
Device Beł Determine failure.	navior the thin client's behavior in case of authentication success /
Device Beh Determine failure.	havior the thin client's behavior in case of authentication success / Eailure Success
Device Beł Determine failure.	havior the thin client's behavior in case of authentication success / Eailure Success
Device Bef Determine failure. Device Aut Acti <u>v</u> e:	The thin client's behavior in case of authentication success / Eailure Success thentication Provider Default Device Authentication Provi
Device Beł Determine failure. Device Aut Acti <u>v</u> e:	The thin client's behavior in case of authentication success / Eailure Success thentication Provider Default Device Authentication Provi
Device Bet Determine Failure. Device Aut Acti <u>v</u> e:	The thin client's behavior in case of authentication success / Eailure Success thentication Provider Default Device Authentication Provider Entication Provider
Device Beł Determine Failure, Device Aul Acti <u>v</u> e:	The thin client's behavior in case of authentication success / Eailure Success thentication Provider Default Device Authentication Provider entication Provider
Device Bef Determine failure. Device Aul Acti <u>v</u> e: User Auth Act <u>i</u> ve:	The thin client's behavior in case of authentication success / Eailure Success thentication Provider Peroperties Default Device Authentication Provide Properties Default User Authentication Provide Properties



3) In the Authentication Properties tab page uncheck the option Inherit settings from parent, as illustrated.

Hothix Service	Discovery se	ervice	Plugins Se	rvice	Proto	col Setting
Communication	Parameters	Note	s Policy	Updat	er	Site Synch
General Authority	antication Prop	erties	Recovery s	ervice	Upgr	ade Servio
Def	ine thin client D	Device a	and User aut	hentica	tion set	tings
			- 🗖 Inher	t settin	gs from	parent
Require sec	ure channel (S	SL)				
Device Behav	ior					
Determine the	thin client's be	havior	in case of au	thentic	ation su	uccess /
failure.						
			Failure		Succ	ess
			Ealure		Succ	ess
C Device Author	otication Drovin	lar	Ealure		Succ	ess
Device Authe	ntication Provid	der	Ealure		Succ	ess
Device Authe	ntication Provid	der 9 Authe	Eailure	····	Succ	ess
Device Authe	ntication Provid	der 9 Authe	Eailure	 vi	Succ	ess
Device Authe	ntication Provid	ler e Authe	<u>E</u> alure	 vi. 💌	Succ	ess
Device Authe Acti <u>v</u> e:	ntication Provid	der 9 Authe r	Ealure	 vi⊧▼	Succ	ess
Device Authe Active:	ntication Provid Default Device ication Provide	der e Authe r	Ealure	v# •	<u>Succ</u>	rties
Device Auther Active: User Authent Active:	ntication Provide Default Device ication Provide Default User A	der 9 Authe 1 1 Authent	Eailure		<u>Succ</u> Prope	rties
Device Authe Acti <u>v</u> e: User Authent Active:	ntication Provid Default Device ication Provide Default User #	der e Authe r Authent	Eailure	vi T	<u>Succ</u> Prope	rties

- 4) In the **Device Authentication Provider** section, click **Properties** to display the **Default Device Authentication Provider Properties** window.
- 5) Select the option Automatically accept and register new devices into the following OU, then click Browse... to display the Browse for OU window, as illustrated.

Default Device Authen	tication Provider Properties
Define authe	ntication behavior
C Do not accept unaut	nenticated devices.
Automatically accept following OU:	and register new devices into the
	(Provee)
	Brouse for Oll 2
	Please, select the destination folder for default device authentication
	E ∰ net8 ⊕ ② Domain Controllers ⊨ ③ Xcalibur Global ⊕ ② <mark>Thin Clients Demo</mark>
	OK Cancel

Chapter 3 - Xcalibur Farm Manager Tasks



- 6) Select and highlight the OU that will be used to contain the authenticated device clients (e.g., Thin Clients Demo appearing in the previous illustration). Click OK to save the destination OU path in the Default Device Authentication Provider Properties window.
- 7) In the **Default Device Authentication Provider Properties** window click **OK** to save your changes and return to the **LAN Site** window.
- 8) In the LAN Site window click Apply to save your changes.
- 9) In the User Authentication Provider section, click Properties to display the Default User Authentication Provider Properties window, as illustrated, and then click Browse... to display the Select User window.

	ntication Provider Properties 🛛 🗙	
Define aut	thentication behavior	
utomatically use this	is account as the <u>d</u> efault user:	
	Browse	
	Colact Uron	
	Select Oser	
	Select this object type:	
	Select this object type: User	<u>Object Types.</u>
	Select this object type: User Erom this location:	Qbject Types.
	Select this object type: User Erom this location: xcalibur4.chippc	Qbject Types.
	Select bisc Select this object type: User From this location: [xcalibur4.chippc Enter the object name to select (<u>examples</u>);	
	Select bisc Select this object type: User From this location: [xcalibur4.chippc Enter the object name to select (<u>examples</u>):	
	Select bisc Select this object type: User From this location: [xcalibur4.chippc Enter the object name to select (<u>examples</u>)	Diject Types.
	Select bisc Select this object type: User Erom this location: [xcalibur4.chippc Enter the object name to select (<u>examples</u>):	Diject Types.

10) In the **Select User** window, in the text field **Enter the object name to select**, enter **defaultuser** then click **Check Names** to verify the user name; a valid name is underlined automatically.



11) Click **OK** to save your entry and return to the **Default User Authentication Provider Properties** window - the entered user name is displayed, as illustrated.

Default U	ser Authentication Provider Pro	perties	×
•••	Define authentication behavior		
Automatio	cally use this account as the <u>d</u> efault u user	iser:	
1			Browse
		ОК	Cancel

- 12) In the **Default User Authentication Provider Properties** window click **OK** to save your changes and return to the **LAN Site** window.
- 13) In the LAN Site window click OK to save your changes and close the window.
- 14) Continue to the next procedure, Configuring Installation Services.
- Note It is possible at any stage to revert to the default Authentication Properties settings by checking the option Inherit settings from parent.
- **Note** To reset all of the site settings to default, select the site name and then from the right-click menu select **Inherit from Parent...**

Chapter 3 - Xcalibur Farm Manager Tasks



nip P

Technologies

Upgrade Service

Proceed as follows to configure the upgrade service for the new site:

- 1) Select the newly-added site, LAN Site, in the Sites directory and from the right-click menu select **Properties** to display the LAN Site window.
- 2) In the LAN Site window click the Upgrade Service tab to display the Upgrade Service tab page.
- 3) In the **Upgrade Service** tab page, modify the following options, as illustrated:

Inherit from Parent

Uncheck this option

Working on:

From the dropdown list select Always

General Authentication Pro	operties Recovery service Up	grade Servi
Upgrade service	settings for scopes	
	Inherit From	n Parent
Maximum connections:	10	2
Bandwidth, kbps :	Use protocol settings	-
Working on:	Always	•

- 4) Click **Apply** to save your changes.
- 5) Continue to the next procedure, **Plugins Service**.



Plugins Service

Proceed as follows to configure the **Plugins Service** for the new site:

- 1) In the LAN Site window click the **Plugins Service** tab to display the **Plugins Service** tab page.
- 2) In the **Plugins Service** tab page modify the following options, as illustrated:

Inherit from Parent Uncheck this option

Working on:

From the dropdown list select Always

Plugins service s	ettings for scopes
Maximum connections:	10.
Bandwidth, kbps :	Use protocol settings
Working on:	Always

- 3) Click **Apply** to save your changes.
- 4) Continue to the next procedure, Hotfix Service.

Chapter 3 - Xcalibur Farm Manager Tasks



Hotfix Service

Proceed as follows to configure the Hotfix Service for the new site:

- 1) In the LAN Site window click the Hotifx Service tab to display the Hotfix Service tab page.
- 2) In the Hotfix Service tab page modify the following options, as illustrated:Inherit from Parent Uncheck this option

Inherit from Parent Working on:

From the dropdown list select Always

Easter	
I Inherit Fron	Parent –
10	
Use protocol settings	<i>v</i>
Always	•
	6
	10 Use protocol settings Alveays

- 3) Click **Apply** to save your changes then click **OK** to close the **LAN Site** window and return to the **Xcalibur Global Management Console** window.
- 4) Continue to the next procedure, Creating a New IP Scope.



Creating a New IP Scope

Proceed as follows to configure a new IP scope range:

- 1) In the Sites directory select and expand LAN Site.
- 2) Select and highlight **IP Scopes** then from the right-click menu select **New**, **Scope...** to display the **Define new IP scope** window.
- 3) In the **Define new IP scope** window complete the following fields defining the network where the thin clients reside, as illustrated:

Start Address	Enter the scope start IP address
End Address	Enter the scope end IP address
Net Mask	Enter the scope net mask
Display Name	Enter a suitable display name for the scope (e.g., Net 1 , as shown in the illustration)

Enabled

Check this option to activate the scope



- 4) Click **Add** to add the IP scope to the system; the selected scope is automatically listed in the upper columns.
- 5) Click **Close** to close the window and return to the **Xcalibur Global Management Console** window.
- 6) Continue to the next procedure, Starting the Xcalibur Front End Server.

Chapter 3 - Xcalibur Farm Manager Tasks



Starting the Xcalibur Front End Server

Proceed as follows to start the Xcalibur Front End Server service:

- 1) In the **Xcalibur Global Management Console** window, from the left pane select and expand the **Farm Front End Servers**.
- 2) Right-click on the Farm Front End Servers and select Refresh.
- 3) From the Farm Front End Servers tree select the pertinent server then from the right-click menu select **All Tasks, Start**, as illustrated.

TCalibur - Console Root Xca	libur Farm Manager\Administrative Suite\Licensi Is <u>Wi</u> ndow <u>H</u> elp	ng]		_ 5 ×
⇔ → 🗈 🖬 🗿 🗟 🗳	- -			
Console Root Xcalbur Directory Manager Xcalbur Farm Manager Administrative Suite Database Parm Front End Server Site Assign Server Software Software All Test	License Name Xcalibur Global 1.1 Server License Domain Authentication License Package Xcalibur Global Client License Stiffund History	License Type Server Licenses Server Licenses TC Licenses	Version Info 1 1 1 1	Installed By Administrator@xca Administrator@xca Administrator@xca
Consisting C	/indow from Here Pistart Restart Move To, the			
Sites S	rs			
1				

A window displays the server's initialization connection sequence and progress, as illustrated. (This process may continue for several minutes.)

DVSQLMATOS.xcalibur4.chippc	
Operation: Starting Server	⊆lose
Status: Initiating Service DataBase Cor	nnection Sequence

 In the left pane of the Xcalibur Global Management Console window select Xcalibur Farm Manager and from the right-click menu select Refresh to refresh the Xcalibur Global Management Console window.



5) From the **Farm Front End Servers** tree select the pertinent server then from the right-click menu select **Properties** to display the **Administrative Suite \ [Server Name]** window, as illustrated.

Name	Value
Server Id	1
Server GUID	{0A45F8AE-8ECA-CI
Server Name	DVSQLMATOS,xcalib
IP Address	192.168.7.25
Description	DVSQLMATOS.xcalib
Proprietary State	On-line
SCM Status Code	SERVICE_RUNNING
Last Synchronization Date & Time with Active Direct	
Last successful total rebuild operation	6/4/2006 4:14:26 PM
Last total rebuild operation attempt	6/4/2006 4:14:26 PM
Result of last total rebuild operation attempt	[0] The operation co
Last successful incremental update operation	Unknown
Last total incremental update attempt	Unknown
Result of last incremental update operation attempt	[0] The operation co
•	
	8

Verify that the server is running as indicated by the values for the following names:

Property State	On-line

SCM Status Code	SERVICE_RUNNING
-----------------	-----------------

- 6) After verifying the correct values click **OK** to close the window and return to the **Xcalibur Global Management Console** window.
- 7) Continue to the next procedure, Xcalibur Directory Manager Tasks.



Chapter 4 Xcalibur Directory Manager Tasks

Introduction

This section provides step-by-step procedures to perform the following task:

• Create a communication policy (from a template)

Communication Policy

This section takes you through the procedure to create a communication policy from a template.

- 1) In the **Xcalibur Global Management Console** window, in the left pane select and expand **Xcalibur Directory Manager** to display the full directory tree.
- Select and highlight the pertinent OU and from the right-click menu select **Properties** to display the OU window (e.g., **Thin Clients Properties** window as shown below).
- 3) In the **Thin Clients Properties** window click the **Xcalibur Policy** tab to display the **Xcalibur Policy** tab page, as illustrated.

		ity object take for This	Carenta
Xcalibur Pol	icy Object Links	No Override	Disabled
Kcalibur Polic	y Objects higher in	the list have the highest	priority.
New	Add	Edit	Up
		()()	()



 In the Xcalibur Policy tab page click New then select Create from template... from the popup menu to display the Create Policy from Template window, as illustrated.

E 🕹 T	C Policy Templa	tes		
-	TEMPLATE -	Device - Comn	nunication Policy	for l
-	TEMPLATE -	Device - Comn	nunication Polics	for I
	TEMPLATE -	Device - Conn	ection - ICA 9.0	4 (Cł
-	TEMPLATE -	Device - Conn	ection - ICA 9.0	4 Au
-	TEMPLATE -	Device - Conn	ection - ICA 9.0	14 wit
- 4	TEMPLATE -	Device - Conn	ection - Interne	t Exp
	TEMPLATE -	Device - Conn	ection - Interne	t Exp
-	TEMPLATE -	Device - Conn	ection - Interne	t Exp
- 3	TEMPLATE -	Device - Conn	ection - RDP 5.2	2 (Ch
- 4	TEMPLATE -	Device - Conn	ection - RDP 5.2	2 Aut
	TEMPLATE -	Device - Conn	ection - RDP 5.2	2 with
	TEMPLATE -	Device - Displa	ay Settings Polic	y 102
4				

- 5) In the Create Policy from Template window expand TC Policy Templates then select and highlight TEMPLATE - Device – Communication Policy for LAN Evaluation Environments.
- 6) Select **OK** to save your selection and display the OU properties window (e.g., **Thin Clients Properties** window as shown below).
- 7) The newly-created policy is now listed in the Xcalibur Policy tab. Select and highlight the policy and then from the right-click menu select Rename to edit the name of the selected policy, as illustrated. Rename the policy to Device – Communication Policy for LAN Evaluation Environments.

eneral Managed	i By Xcalibur nt Xcalibur Po	Policy Securi	ity s for Thin (Dãents
Xcalibur Policy 0	bject Links	Not	Override	Disabled
TEMPLATE	<u>N</u> o Override Disabled	e		
	Ne <u>w</u> Add Edit	,		
1.110.2016-770	Delete		1	- 10
Scalibur Policy 0	Rena e		highest p	monty
New	Properties Show Policy	History		(Jp.
Ontions	Delete	Properties	1	Diowin

- 8) In the **Xcalibur Policy** tab select and highlight the renamed policy and then click **Edit** to display the **Policy Editor** window.
- 9) In the **Policy Editor** window's left pane expand the policy name **Device Communication Policy for LAN Environments**.



10) Expand **Device Configuration**, **Network and Communication**, **Protocols** then select and highlight **Custom Protocol** to display its contents in the right pane, as illustrated.



11) In the right pane double-click **Custom protocol settings** to display the **Custom protocol settings** window, as illustrated.

stom protocol se	ttings			?
Settings Explain	Supported Clie	nts		
Custom pro	stocol settings			
 ○ Not Configured ○ Enabled ○ Digabled 	1		Prev Next	
Press 'Server List' database: IP Address:	button in order	to retrieve Xo	alibur server list fr	om the
IP Address	Port	SSL	Weight	
192 168 7.25	917	918	Normal	
)	6
	OK		Cancel	Apply

Chapter 4 - Xcalibur Directory Manager Tasks



12) In the Custom protocol settings window, Settings tab page, select and

highlight the existing server record then click the **Remove Server** button, as illustrated, to delete the server from the list.

tom protocol se	ttings		
ettings Explain	Supported I	Clients	
Custom pro	otocol setting	ge	
C Not Configured	ł		Brev
 Enabled Disabled 			Next
IP Address	Pod	122	Weight
	12	10 (A) 00	
IP Address	Port	SSL	Weight
192,168,7,25	917	918	Normal

13) Click the **Add Server** button and from the popup menu select your server's IP address to add the selected server to the server list, as illustrated.

tom protocol se	ttings			? X
ettings Explain	Supported Clier	nts		
Custom pro	tocol settings			
C Not Configured	ł		Brev	1
• Enabled			Next	
IP Address:			-	DVSQUMATOS.xcalibur4.chi
IP Address	Port	SSL	Weight	All IPs of all servers

14) In the **Custom protocol settings** window, click **Apply** to save your changes then click **OK** to close the window and return to the **Policy Editor** window.

Chapter 4 - Xcalibur Directory Manager Tasks



- 15) In the **Policy Editor** window from the main menu select **File**, **Close** to close the window and return to the **Thin Clients Properties** window.
- 16) In the **Thin Clients Properties** window click **Apply** to save your changes then click **Close** to close the window.
- 17) Continue to the next procedure, **Connecting Devices**.

Chapter 4 - Xcalibur Directory Manager Tasks



This page is left blank intentionally.



Chapter 5 Connecting Devices

The following chapter provides a list of different methods for connecting thin client devices to Xcalibur Global.

Although each of the listed methods can be used, this chapter will focus on the Network Scan method and will provide a detailed description of the procedure for implementing this method.

This procedure includes the following steps:

- Initiate a network scan using the Discovery Service
- View scan results
- View details about a connected device in real time via the IP Scope view

Prerequisites

The procedures described in this chapter are dependent on having completed the following:

- All the procedures described in the previous chapters.
- At least one Chip PC thin client is running.
- The thin client is turned ON, connected to the network and its IP address is within the range defined for Net 1 in Chapter 3, IP Scope Settings.

Connection Methods

Use one of the following methods to connect devices to Xcalibur Global::

- DNS A Record In your DNS server, create a new Address (A) record named XCglobal11 that points to your Xcalibur Global Front End server IP address.
- Local Device Settings
 On Windows CE thin clients, click Start > Settings > Xcalibur
 - In the General tab, select Enable Connection to Xcalibur Server Farm.
 - In the **Server List** tab, click **New**, type your server's IP address and then click **OK**. Click **OK** to close the window and save your settings.

On ThinX thin clients, click Start > Settings > Device > Xcalibur Settings > General.

- In the General tab, select Enable Connection to Xcalibur Server Farm.
- In the **Server List** tab, click **Add**, type your server's IP address and then click **OK**. Click **OK** to close the window and save your settings.
- Network Scan follow the procedure described below¹.
- For additional connection methods (such as DHCP), please refer to the Xcalibur Global Administrator's Guide.

¹ Applicable only to Windows CE thin clients



Initiate a Network Scan

The network scan is performed using the Discovery Service process which scans a selected IP address range in search of connected thin client devices.

Note For best results, you are recommended to view a thin client device during these initial steps in order to observe real-time effects while performing this procedure.

Proceed as follows to initiate a network scan:

- In the Xcalibur Global Management Console window, in the left pane, select and expand Xcalibur Farm Manager \ Sites \ LAN Site \ IP Scopes.
- 2) From **IP Scopes** select and highlight **Net 1** then from the right-click menu select **Start Discovery...** to display the **Start Discovery** window.
- 3) In the Start Discovery window, as illustrated, select the following options:
 - Full Range
 - Force reconnect discovered devices

Discovery S	erver: [) VSQLM	ATO5.x	calibur	4.chippo
🖲 Eull Ran	je				
⊂ <u>⊆</u> ustom i	Range -				
≦tart IP :	192	168	1) 7	+[40
End IP :	192	168	: 7	91	50
Clear all	Xcalibur #	\aent se	ttings		
(use with	n caution	discont	iects de	vices	from

Verify that the IP address range covers the network where your thin clients reside.

4) Click OK to save your changes, close the window and start the Discovery process. The Xcalibur Farm Manager information window displays, as illustrated, informing you that Discovery started successfully and that you can now view the scan results.







Note Discovered devices reboot after they have been scanned, then the device connects to **Xcalibur Global** automatically.

Additional reboots may occur due to policy applications.

5) In the **Xcalibur Farm Manager** Information window click **OK** to close the window and continue to the next procedure, **Viewing the Scanned Results**.

Viewing the Scan Results

Proceed as follows to view the Discovery Service scan results:

- 1) In the Xcalibur Global Management Console window, in the left pane, select and expand Xcalibur Farm Manager \ Sites \ LAN Site \ IP Scopes.
- 2) From **IP Scopes** select and highlight **Net 1** then from the right-click menu select **Properties** to display the **LAN Site\Net 1** properties window.
- 3) In the LAN Site\Net 1 properties window click the Client Discovery tab to display the Client Discovery tab page, as illustrated.

2000	Protocol Settings	Notes Policy Updater
Sene H	ral Authentication Pro lotfix Service	perties Recovery service Upgrade Servic Plugins Service Client Discovery
N	Date and Time	Extended Task Status
1	6/4/2006 4:41:53 PM	Replying client IP 192 168 7 49. Ok
2	6/4/2006 4:41-53 PM	Reniving client IP 192 168 7 50. Ok
3	6/4/2006 4:41:53 PM	Replying client IP 192,168,7,45, Ok.
4	6/4/2006 4:41:53 PM	Replying client IP 192,168,7,46, Ok.
5	6/4/2006 4:41:53 PM	Replying client IP 192,168,7,47, Ok.
6	6/4/2006 4:41:53 PM	Replying client IP 192,168,7,44, Ok.
7	6/4/2006 4:41:53 PM	Replying client IP 192.168.7.43. Ok.
8	6/4/2006 4:41:53 PM	Replying client IP 192.168.7.42, Ok.
9	6/4/2006 4:41:53 PM	Replying client IP 192.168.7.41. Ok.
10	6/4/2006 4:41:53 PM	Discovery procedure completed.
11	6/4/2006 4:41:53 PM	Discovery procedure progress: 100%.
12	6/4/2006 4:41:53 PM	Discovery procedure progress: 90%.
13	6/4/2006 4:41:53 PM	Discovery procedure progress: 80%.
14	6/4/2006 4:41:53 PM	Discovery procedure progress: 70%.
15	6/4/2006 4:41:53 PM	Discovery procedure progress: 60%.
16	6/4/2006 4:41:53 PM	Discovery procedure progress: 50%.
17	6/4/2006 4:41:53 PM	Discovery procedure progress: 40%.
18	6/4/2006 4:41:53 PM	Discovery procedure progress: 30%.
19	6/4/2006 4:41:53 PM	Discovery procedure progress: 20%.
20	6/4/2006 4:41:53 PM	Discovery procedure progress: 10%.
		N
how	20 • events fr	om: 33 💿 🏩 👩 🚽
1044	1 co levens n	

The **Client Discovery** tab in the **LAN Site\Net 1** properties window provides information regarding the progress and results of the **Discovery** procedure.

Review the scan results that include information of the discovery progress and a report of replying clients. After reviewing the scan results click **OK** to close the window.

4) Continue to the next procedure, **IP Scope View**.





IP Scope View

This procedure enables you to view details about a connected device in real time.

In the Xcalibur Global Management Console window, click the Refresh
 button in the toolbar to refresh the screen and display all connected devices in the right pane, as illustrated.

Xcalibur - [Console Root\Xcalibur Far	m Manager\Sites\LAN Site\IP Sco	ppes\Net 1]			E 6 2
j Eile Action View Favgrites Wind	low Help				_151>
• → 🗈 🖬 🗙 🗗 🕅 🗗	2 🖉 😵 🖉 🐨 🖉	o 🖣 🖉 🐔 🧔	8.8		
Console Root	Device MAC IP Address T	SW Platform	Server IP	User Name	Last State
🖂 Xcalibur Directory Manager	8 000535018A21 192.168.7.50	6.5.3 Build 120	192.168.7.25	DefaultUser@x	Alive
🖓 Xcalibur Farm Manager	8 000535018A36 192.168.7.49	6.5.3 Build 120	192.168.7.25	DefaultUser@x	Alive
🕀 🅡 Administrative Suite	8 000535018911 192.168.7.46	6.5.3 Build 120	192.168.7.25	DefaultUser@x	Alive
E 😲 Sites	& 00053501890F 192.168.7.45	6.5.3 Build 120	192.168.7.25	DefaultUser@x	Alive
Default Site	8 000535018A65 192.168.7.44	6.5.3 Build 120	192.168.7.25	DefaultUser@x	Alive
E III LAN Site	8 000535018903 192.168.7.43	6.5.3 Build 120	192.168.7.25	DefaultUser@x	Alive
🛨 💕 Tasks	8 000535013164 192.168.7.42	6.5.3 Build 120	192.168.7.25	DefaultUser@x	Alive
E P Scopes	8 0005350186F1 192,168,7,41	6.5.3 Build 120	192,168,7,25	DefaultUser@x	Alive
2.168.7.40 - 192.168.7.50	4		Net 1	ī	otal: 8 TC

- Select and highlight a device in the right pane and from the right-click menu select **Properties** to browse and view information in the various tab pages.
- **Note** Clients that fall into the scan range will connect to **Xcalibur Global**, obtain policies then reboot.

It may take several minutes until new clients appear in the **Xcalibur Global Management Console** window.

Important	Clients that do not have an Xcalibur Global Client License will not
	appear in the IP Scope view. These clients can be found in
	Xcalibur Farm Manager, Administrative Suite, Unlicensed
	Clients.



Chapter 6 Policy-Based Management

This chapter describes how use an Xcalibur policy to perform the following tasks:

- Install an RDP plug-in
- Create an RDP connection

General

Xcalibur Policy is used to fully administer thin client devices in the organization. All thin client management aspects, from software installation to user environment management are dealt with by Xcalibur Policies.

An Xcalibur policy is a set of rules defining client device settings based on the device's location in the Active Directory tree and the location of the account of the user logged on at the device. By using Xcalibur Policies you can define client and user settings once and then rely on **Xcalibur Global** to constantly enforce your policy settings throughout the network.

When linking policies to an OU that contains thin clients, the policies apply on the thin clients approximately two minutes after being assigned. Therefore, after linking a policy to an OU you can expect the device to reboot after two minutes or less (indicating that policy changes have been applied).

To simplify software distribution, preinstalled Xcalibur Policy Templates can be used for installing software plug-ins such as RDP/ICA/Internet Explorer/Other on the thin client devices.

Installing an RDP Plug-in via an Xcalibur Policy

This procedure shows how to install an RDP plug-in by using a policy template.

- **Note** For best results, you are recommended to view a thin client device during these initial steps in order to observe real-time effects while performing this procedure.
- 1) In the Xcalibur Global Management Console window, in the left pane, select and expand Xcalibur Directory Manager.
- Select and expand the domain name to display the full directory tree, select and highlight the pertinent OU then from the right-click menu select **Properties** to display the OU window (e.g., **Thin Clients Properties** window as shown below).

Chapter 6 - Policy-Based Management



3) In the **Thin Clients Properties** window click the **Xcalibur Policy** tab to display the **Xcalibur Policy** tab page, as illustrated.

4.0		ancy ubject	Links for Thin L	aents
Xcalibur Policy	y Object Links		No Override	Disabled
Device - C	ommunication Po	blicy for		
ALL DATE	Obligate black as to	the list here		
Acaibur Holicy	ubjects nigher in	i the list na	ve the nighest p	nonty.
New	Agd	EK	iit.	Úp
Options	Déleté	Ecope	uties	Down
		and the second s		-

- 4) In the Xcalibur Policy tab page click New then select Create from template... from the popup menu to display the Create Policy from Template window.
- In the Create Policy from Template window expand TC Policy Templates, scroll down the list then select TEMPLATE - Device - RDP -Install, as illustrated.

🗄 쵫 TC Policy Templates	
	Policy for L4
- 😣 Template - Device - Communication (Policy for L4
	A 10.09 wit
- 🛞 Template - Device - Connection - RD	P with Desł
- 🛞 Template - Device - Display Settings	Policy 1024
	all
- 🛞 Template - Device - Input Local Engli	ish US
	nch - Frenc
	man - Germ
- 🌏 Template - Device - Security - Limiter	d Desktop a
🔜 🔤 😣 Template - Device - Security - Passw	ord protect
0	•

- 6) Select **OK** to save your selection and display the OU window (e.g., **Thin Clients Properties** window).
- 7) The selected policy is now listed in the Thin Clients Properties window. Select and highlight the selected policy then from the right-click menu select Rename to modify the policy name. Rename the policy to Device -RDP - Install.
- **Note** After policy updates occur, RDP will be installed automatically on the thin clients, after which the clients will reboot.
- 8) Continue to the next procedure, Creating an RDP Connection by Policy.

Chapter 6 - Policy-Based Management



Creating an RDP Connection via an Xcalibur Policy

This procedure enables you to create an RDP connection via an Xcalibur policy.

- In the Xcalibur Policy tab page click New then select Create from template... from the popup menu to display the Create Policy from Template window.
- In the Create Policy from Template window expand TC Policy Templates. Scroll down the list and select TEMPLATE - Device -Connection - RDP with Desktop Shortcut, as illustrated, then select OK to save your selection and display the Thin Clients Properties window.

1 39	I C Policy Templates
1	- 🎭 Template - Device - Communication Policy for L/
4	- 🎭 Template - Device - Communication Policy for L
-	- 🎭 Template - Device - Connection - ICA 10.09 wit
	- 💫 Template - Device - Connection - RDP with Des
	- 🌛 Template - Device - Display Settings Policy 1024
1	
4	🗏 💩 Template - Device - Input Local English US
	- 🌛 Template - Device - Input Local. French - Frenc
4	- 🌏 Template - Device - Input Local. German - Gern
	- 💩 Template - Device - RDP - Install
	🛞 Template - Device - Security - Limited Desktop -
4	Template - Device - Security - Password protect

3) The selected policy is now listed in the Xcalibur Policy tab page. Select and highlight the selected policy from the Xcalibur Policy Object Links column then from the right-click menu select Rename to modify the name of the selected policy, as illustrated. Rename the policy to Device – Connection - RDP with Desktop Shortcut.

	Current X	calibur Polic	y Objec	t Links for Thin (lient	\$
Xcalibu	r Policy Objec	t Links		No Override	D	isabled
💐 Dev	ice - Commun	ication Polic	y for		0.03	
Dev 💏	ice - RDP - In	stall	D			
l em	plate - Device	: - Lonneo	<u>N</u> o O [.] Disab	override bled		
Xcalibur Policy Objects higher in		Ne <u>w</u> ▶ Add Edit		۲		
		(c)	Delet	в		
<u>N</u> ev	v	Add 📗	<u>R</u> ename			Up
<u>O</u> ption	s] De	elete	Properties Show Policy History			Do <u>w</u> n
Elock	Policy inherit	ance				



- 4) In the **Xcalibur Policy** tab page select and highlight the renamed policy then click **Edit** to display the **Policy Editor** window.
- 5) In the **Policy Editor** window's left pane expand the policy name **Device -Connection - RDP with Desktop Shortcut**.
- Expand Device Configuration, Installable Software Modules, Connections then select and highlight Remote Desktop Connection to display its contents in the right pane, as illustrated.



7) In the right pane double-click **RDP Desktop** to display the **Remote Desktop Connection** window.

Chapter 6 - Policy-Based Management





8) In the **Remote Desktop Connection** window, **Settings** tab page, enter the name or IP address of your RDP terminal server, as illustrated.

mote Desktop Connection	1
Settings Explain Supported Clients	
This third party plug-in offers connec	tivity to servers.
	Prev
	Next
Connection Name RDP Desktop	
Connection to [192.168.7.21]	-
Description	
This third part/Silug-in offers connectivity to	servers.
DK I	Capcel Applu

- In the Remote Desktop Connection window click Apply to save your changes then click OK to close the window and return to the Policy Editor window.
- 10) In the **Policy Editor** window from the main menu select **File**, **Close** to close the window and return to the **Thin Clients Properties** window.
- 11) In the **Thin Clients Properties** window click **Apply** to save your changes then click **OK** to close the window.
- **Note** After policy updates occur, an RDP Connection will be created and a shortcut will be placed on the thin client's Desktop.



This page is left blank intentionally.

Chapter 6 - Policy-Based Management