

# **Xcalibur Global**

Version 1.1 - Rev. 2

# **Quick Configuration Guide**

**Document Version 1.0** 



#### **COPYRIGHT NOTICE**

© 2006 Chip PC Inc., Chip PC (Israel) Ltd., Chip PC (UK) Ltd. 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, 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	
	, Objectives	
	Reference Materials	
	Prerequisites	5
	Document Features	
	Conventions	
	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	
	Additional Licenses Installing Licenses	
	Configuring the Farm Manager Discovery Service	
	Creating a New Site	
	Configuring Authentication Settings	
	Configuring Installation Services	
	Upgrade Service	
	Plugins Service	
	Hotfix Service	24
	Creating a New IP Scope	25
	Starting the Xcalibur Front End Server	26
Chapter 4	Xcalibur Directory Manager Tasks	29
	Introduction	29
	Communication Policy	29
Chapter 5	Connecting Devices	35
-	Prerequisites	
	Initiate a Network Scan	
	Viewing the Scan Results	
	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 Policy41



# 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:

Xcalibur Global version 1.1 rev. 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 Installation Guide, version 1.0 (Ref. G001U-1.0)

#### **Prerequisites**

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



#### **Document Features**

#### Conventions

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

#### Notes

Caution	Text marked <b>Caution</b> contains warnings about possible loss of data.
Important	Text marked <b>Important</b> contains information that is essential to completing a task.
Note Tex	t marked <b>Note</b> 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 provides step-by-step procedures for performing a network scan, viewing scan results, and viewing details about connected devices.
- 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	<b>Required</b> to start the Front End Server service
Domain Authentication	DALicense	<b>Optional</b> 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	<b>Optional</b> 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 (1.1), Management Console to launch Xcalibur Global Management Console, as illustrated.

🚡 Xcalibur - [Console Root]				- 🗆 ×
🚡 Eile Action View Favorites V	⊻indow <u>H</u> elp		4	_ & ×
← → 🖪 🖪 😫				
Console Root	Name			
<ul> <li>★ Xcalibur Directory Manager</li> <li>★ Acalibur Farm Manager</li> </ul>	Xcalibur Directory Manager	2		

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.

🚡 Xcalibur - [Console Root]	
🚡 Eile <u>A</u> ction <u>V</u> iew Fav <u>o</u> rites <u>W</u> indo	w Help
⇔ →    🖪   🗟   😫	
Console Root Xcalibur Directory Manager Xcalibur Farm Manager Administrative Suite Database Farm Front End Servers Site Assigned Servers Certificates Software Repository Licensing Backed up Sites Unassigned Clients Site Assigned Clients Find	Name Xcalibur Directory Manager
⊞ 🤣 Sites	

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:
	< <u>Back</u> <u>N</u> ext > Finish <b>Cancel</b>

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.

)pen	- 14 - 25 - 24 - 24 - 24 - 24 - 24 - 24 - 2				?
Look jr	n: 🔀 JackPC		•	🗢 🗈 💣 📰	•
My Recent Documents Docktop	AUTHD.xd BMPSS.xd PERTE.xd VNCPI.xd XCAL4.xd				
My Documents					
hillel on MSDENET8					
My Network Places	File <u>n</u> ame: Files of <u>type</u> :	Chip PC Licenses (*.xcl)		<u> </u>	<u>O</u> pen Cancel

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.

and the second	Protocol Settings   y Updater   Site S	Communication Parameter Synch RTI Interva
and the second s	Authentication Properties Hotfix Service	Recovery service
Upgrade Service	Hodrix service	Discortery service
Discovery s	ervice settings	
00		
Server settings		🕂 Inherit from Parent
Discovery server:		
Discovery server:	None	<u> </u>
Working on :	Manual control	- 1
Server table to send	to clients:	🕂 Igherit from Parent
-		
		+
-		
		0 8

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** button for the selected server to display, the **Advanced settings** window, as illustrated, and check the option **Enable Xcalibur Agent on discovered devices**.

Advanced disc	overy service settings
SNMP Community name:	xcalibur4
Scan every (sec):	3600
☑ Enable Xcalibur Agent	on discovered devices

- 4) In the **Advanced settings** window click **OK** to save your changes and return to the **Discovery service settings** tab page.
- 5) In the **Discovery service settings** tab page, click the **Add Server to**

TableImage: Server to add to the table in the sectionServer table to send to clients, as illustrated.

Plugins Service	Protocol Settings C	ommunication Parameter
Notes Pol	cy Updater Site Sy	nch RTI Interval
IP Scopes	Authentication Properties	Recovery service
Upgrade Service	Hotfix Service	Discovery service
004	service settings	
Server settings		Inherit from Parent
Discovery server:	DVSQLMATOS.xcalibur4	.chippc 💌 🙂
Working on :	Manual control	• <b>1</b>
Server table to sen	d to clients;	- Inherit from Parent
	alibur4 chinne	*
DVSQLMATOS.xc	and a stampps	and the second se
DV5QLMATO5.xc	and a stamppe	-
DVSQLMATOS.xc	andra a na na pa	+
DVSQLMATOS.xc	ander Freihige.	•
DVSQUMATOS.xc		•

**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).



- 6) Click **Apply** to save your settings then click **OK** to close the **Farm Properties** window.
- 7) 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.

	rm Manager\Administrative Suite\Licensing]			_ 8 ×
Elle Action Yiew Favgrites Wind	dow Help			_ 5 ×
Console Root	License Name	License Type	Version Info	
Xcalibur Directory Manager	Xcalibur Global 1.1 Server License	Server Licenses	1	Administrator@xcalit
🖻 🌍 Xcalibur Farm Manager	Domain Authentication License Package	Server Licenses	1	Administrator@xcalit
Administrative Suite  Administrative Suite  Farm Front End Servers  Certificates  Certificates  Continue Repository  Certificates  Comain Authentication L  Comain Authent	Xcalbur Global Client License	TC Licenses	1	Administrator@xcalit
B - 🎸 Siler B -   Inherit from Parent				
<u>N</u> ew ►	Site			
New <u>Window</u> from Here	-16			
Refresh				
Help				
4 N	4			F
Create New Site				

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

Enter a suitable name (e.g. **LAN Site**, as illustrated)

**Site Description** 

Site Name

Enter a suitable description

<b>.</b>	Enter the site name and description.
e Name:	LAN Site
e Description:	LAN Site Description
e Description:	LAN Site Description



- 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.

lotfix Servic	e Discovery	service	Plugins :	Service	Protocol Se	ttino
Communicat	on Parameters	Note	s Pol	icy Updat	er   Site S	ynd
eneral Au	ithentication Pr	operties	Recovery	/ service	Upgrade S	ervi
	Define thin clier	nt Device a	and User a	uthentica	tion settings	
9. 			- Inh	erit settin	igs from parei	nt ·
Require	secure cha <u>n</u> nel	(SSL)				
Device Bel	navior					
	the thin client's	behavior	in case of	authentic	ation success	1
failure.						
			<u>E</u> ailu	re	Success	1
			Eailu	re	Success	
failure.	hentication Pro	ovider	Eailu	re	Success	
failure. -Device Aul	hentication Pro					
failure.					Success	
failure. -Device Aul	hentication Pro					
failure. -Device Aul Acti <u>v</u> e:	hentication Pro	vice Authe				
failure. −Device Aul Acti <u>v</u> e: −User Auth	hentication Pro	vice Authe	ntication P	rovi 💌	Properties,	
failure. -Device Aul Acti <u>v</u> e:	hentication Pro	vice Authe	ntication P	rovi 💌		
failure. −Device Aul Acti <u>v</u> e: −User Auth	hentication Pro	vice Authe	ntication P	rovi 💌	Properties,	





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

The first per free	Discovery se	ervice	Plugins S	ervice	Proto	col Settings
Communication	Parameters	Notes	Poli	cy Updat	er	Site Synch
General Authority	entication Prope	erties	Recovery	service	Upgr	ade Servio
Def	ine thin client D	Device an	nd User au	ithentical	tion set	tings
			- Inhe	rit settin	gs from	parent -
	use channel /S	(17)				
I Require sec	ure channel (5)	SL)				
T Device Behav	ior					
Determine the	thin client's be	havior in	n case of a	authentic	ation su	iccess /
failure.						
			The manager			CONTRACTOR OF STREET,
			Eailur	e	Succe	ess
			<u>E</u> ailur	e	Succe	ess
Device Authe	ntication Provid	ler	Ealur	e	Succe	ess
Device Authe	ntication Provid	Jer	<u>E</u> alur	e	Succe	ess
	ntication Provid					
Acti <u>v</u> e:		Authen				
Acti <u>v</u> e:	Default Device	Authen				
Acti <u>v</u> e:	Default Device	e Authen		ovi		rties
Acti <u>v</u> e:	Default Device	e Authen		ovi	Prope	rties
Acti <u>v</u> e:	Default Device	e Authen		ovi	Prope	rties
Acti <u>v</u> e:	Default Device	e Authen		ovi	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 Authentic	ation Provider Properties
Define authenti	ication behavior
C Do not accept unauthe	nticated devices.
Automatically accept ar following OU:	nd register new devices into the
	Browse
	Browse for OU ? 🗙
	Please, select the destination folder for default device authentication
	OK Cancel



- 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, then click Browse... to display the Select User window.

Default User Authentica	tion Provider Properties	
Define authentio	ation behavior	
Automatically use this acco	ount as the <u>d</u> efault user: Browse	
	Select User	? ×
	Select this object type: User	Object Types
	From this location:	
	xcalibur4.chippc	Locations
	Enter the object name to select (examples):	A
	1	Check Names
-	Advanced	0K Cancel

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.



 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 Prop	erties	×
<b>9</b>	Define authentication behavior		
Automat	ically use this account as the default u	ser:	
Taciada		Browse	e II.
			. 1
		OK Cance	el

- 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...**



### **Configuring Installation Services**

#### **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

for scopes	
Inherit From Parent	
)	100
se protocol settings	¥
ways	8

- 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:

/orking on:	From t	he dropdov	vn list select	Always
AN Site		? ×		
Communication Parameters General   Authentication Pro Hotfix Service   Discovery	operties Recovery service Up	Site Synch   grade Service   rocol Settings		
Plugins service se	ttings for scopes	Parent —		
Maximum connections:	<b>1</b> 0			
Bandwidth, kbps :	Use protocol settings	*		
Working on:	Always			
	OK Cancel			

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



## 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

Hotfix service sett	ings for scopes	
	Inherit Fro	m Parent —
Maximum connections:	10	-
<u>B</u> andwidth, kbps :	Use protocol settings	¥
Working on:	Always	•
		2

- 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**

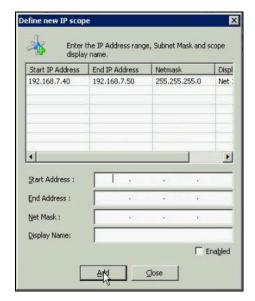
Proceed as follows to configure a new IP scope range:

- 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., <b>Net 1</b> , as shown in the illustration)

#### Enabled

Check this option to activate the scope



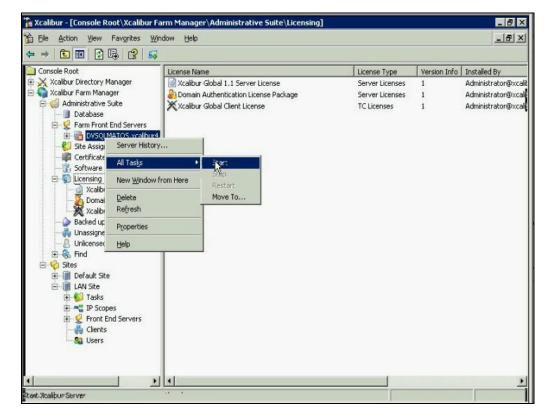
- 4) Click **Add** to add the IP scope to the system; the selected scope is automatically listed in the upper columns.
- 5) Click **Close** to close the window and return to the **Xcalibur Global Management Console** window.
- 6) Continue to the next procedure, Starting the Xcalibur Front End Server.



#### 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) From the **Farm Front End Servers** tree select the pertinent server then from the right-click menu select **All Tasks, Start**, as illustrated.



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	Close
Status: Initiating Service DataBase Con	nnection Sequence
1111111111111	

 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.





 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		¥alue
Server I	d	1
Server G	JUID	{0A45F8AE-8ECA-CE
Server N	lame	DVSQLMATOS.xcalib
IP Addre	55	192.168.7.25
Descripti	ion	DVSQLMATOS.xcalib
Proprieta	ary State	On-line
SCM Sta	tus Code	SERVICE_RUNNING
Last Syn	chronization Date & Time with Active Direct	
	uccessful total rebuild operation	6/4/2006 4:14:26 PM
	otal rebuild operation attempt	6/4/2006 4:14:26 PM
	of last total rebuild operation attempt	[0] The operation co
	uccessful incremental update operation	Unknown
	otal incremental update attempt	Unknown
Result	of last incremental update operation attempt	[0] The operation co
1		
		20

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

Property State	On-line

SCM Status Code SERVICE\_RUNNING

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



This page is left blank intentionally.



# 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.

3/0	Juneni Acaibur Folicy	Object Links for Thin C	lients
Xcalibur Poli	cy Object Links	No Override	Disabled
Xcalibur Polic	y Objects higher in the	list have the highest p	riority.
New	Agd	Edit	<u>U</u> p
Options	Deleje	Eroperties	Diawn



 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 🍭	TC Policy Templates	
- de	- 😣 TEMPLATE - Device - Communication Po	icy for l
1	TEMPLATE - Device - Communication Po	toy for L
-	- 😣 TEMPLATE - Device - Connection - ICA !	9.04 (Ch
-	B TEMPLATE - Device - Connection - ICA !	9.04 Aul
1		9.04 wit
-	B TEMPLATE - Device - Connection - Inter	net Exp
	B TEMPLATE - Device - Connection - Inter	net Exp
-	B TEMPLATE - Device - Connection - Inter	net Exp
4	- 😣 TEMPLATE - Device - Connection - RDP	5.2 (Ch
Jun	- B TEMPLATE - Device - Connection - RDP	5.2 Auto
	TEMPLATE - Device - Connection - RDP	5.2 with
-	• Revised and the second se	olicy 102
•		•

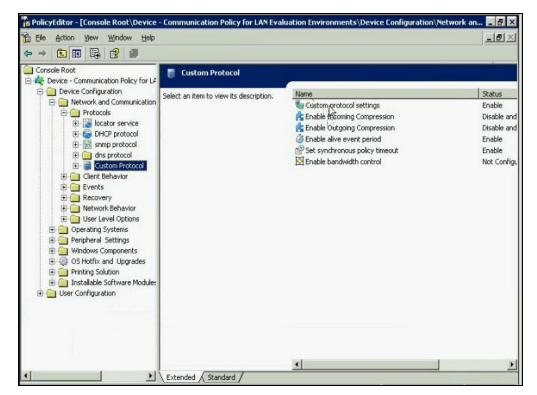
- 5) In the Create Policy from Template window expand TC Policy Templates then select and highlight TEMPLATE - Device – Communication Policy for LAN Evaluation Environments.
- 6) Select **OK** to save your selection and display the OU properties window (e.g., **Thin Clients Properties** window as shown 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   Manageo	f By Xcalibur nt Xcalibur Pol	540		Dients
Xcalibur Policy 0	bject Links	No	Override	Disabled
TEMPLATE	No Override Disabled	•		
	Ne <u>w</u> <u>A</u> dd <u>E</u> dit	,		
<calibur 0<="" policy="" td=""><td colspan="2">Delete Rena e</td><td>highest p</td><td>oriority.</td></calibur>	Delete Rena e		highest p	oriority.
New	Properties Show Policy History		1	Ųр
Options	Delete	Properties	1	Dow

- 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.

tom protocol set	tings		
ettings Explain S	Supported Clien	ts	
Custom prot	ocol settings		
<ul> <li>Not Configured</li> <li>Enabled</li> </ul>			Prev
C Disabled			Next
P Address:	l Dest		
IP Address	Port	SSL	Weight
192.168.7.25	917	918	Normal
			•
			a de la companya de la

Chapter 4 - Xcalibur Directory Manager Tasks



12) In the **Custom protocol settings** window, **Settings** tab page, select and highlight the server record with IP address 192.168.7.25 then click the

**Remove Server** button, as illustrated, to delete the server from the list.

tings Explain Support Custom protocol set Enabled Digabled ress "Server List" button in abase: Address: IP Address Port 192168.7.25 917	ttings order to		Weight
Not Configured Enabled Digabled ress 'Server List' button in atabase: Address:	order to	SSL	Next
Enabled Digabled ress 'Server List' button in atabase: Address:		SSL	Next
Digabled ress 'Server List' button in atabase: Address: IP Address: P ort		SSL	
ress 'Server List' button in atabase: <sup>9</sup> Address: IP Address Port		SSL	Weight
			and the second se
			and the second se
192.168.7.25 917		010	Manager
		310	Normal
		510	Normal
	ОК	1	Cancel

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.

-	Supported Cli otocol settings		1
Not Configure		Prev	1
Enabled		Next	
database: P Address:	Port	 Weight	DVSQLMATOS.xcalibur4.ct
			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

This chapter describes how to perform the following procedures:

- 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 firmware version 6.5.3 or higher.
- 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.

#### 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:

- 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 **Start Discovery...** to display the **Start Discovery** window.

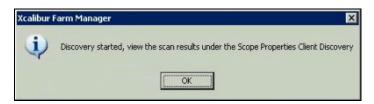


- 3) In the **Start Discovery** window, as illustrated, select the following options:
  - Full Range
  - Force reconnect discovered devices

7 , 4	0
7 , 5	0

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.
- In the LAN Site\Net 1 properties window click the Client Discovery tab to display the Client Discovery tab page, as illustrated.

	Protocol Settings	Notes Policy Updater
ene	ral Authentication Pro	operties   Recovery service   Upgrade Serv
H	iotfix Service	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	Replying 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%.
how	20 vevents fr	
1099		

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 Fa	rm Manager\Sites	\LAN Site\IP Sc	opes\Net 1]			- 8
j Eile Action ⊻iew Favgrites Win	dow <u>H</u> elp					_ 5
• → 🖻 🖪 🗙 🗗 🕅 🗟 🖆	2   🖉 🥚 🤫 🎙	> 🔁 🕑 🕹	Ø 🧤 🛒 🥌 🥩	8.8		
Console Root	Device MAC	IP Address 💎	SW Platform	Server IP	User Name	Last State
Xcalibur Directory Manager	& 000535018A21	192.168.7.50	6.5.3 Build 120	192.168.7.25	DefaultUser@x	Alive
Calibur Farm Manager	& 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
🖻 🍄 Sites	& 00053501890F	192.168.7.45	6.5.3 Build 120	192.168.7.25	DefaultUser@x	Alive
😟 🏢 Default Site	& 000535018A65	192.168.7.44	6.5.3 Build 120	192.168.7.25	DefaultUser@x	Alive
E 🗑 LAN Site	\$ 000535018903	192.168.7.43	6.5.3 Build 120	192.168.7.25	DefaultUser@x	Alive
E Tasks	8 000535013164	192.168.7.42	6.5.3 Build 120	192.168.7.25	DefaultUser@x	Alive
e P Scopes	& 0005350186F1	192.168.7.41	6.5.3 Build 120	192.168.7.25	DefaultUser@x	Alive
.168.7.40 - 192.168.7.50	•			Net 1	6	otal: 8 TC

- 2) 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).

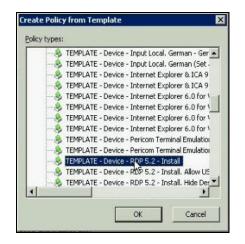
Chapter 6 - Policy-Based Management



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

		ity objec	t Links for Thin (	atenta
Xcalibur Policy	Object Links		No Override	Disabled
Device - Co	ommunication Po	licy for		
calibur Policy	Objects higher in	the list ha	ve the highest p	riority.
New	Add	E	dit	<u>Up</u>
Options	Delete	Prop	erties	Down

- 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 5.2
   Install, as illustrated.



- 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 5.2 - 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.

- 1) 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.
- 2) In the Create Policy from Template window expand TC Policy Templates. Scroll down the list and select TEMPLATE - Device -Connection RDP 5.2 with Desktop Shortcut, as illustrated, then select OK to save your selection and display the Thin Clients Properties window.

TEMPL	ATE - Device - Communication Policy for L
- 🤌 TEMPI	ATE - Device - Communication Policy for L
- 😣 TEMPI	ATE - Device - Connection - ICA 9.04 (Ch
😣 TEMPL	ATE - Device - Connection - ICA 9.04 Au
- 🤌 TEMPI	ATE - Device - Connection - ICA 9.04 wit
- 😣 TEMPI	ATE - Device - Connection - Internet Exp
- 😣 TEMPI	ATE - Device - Connection - Internet Exp
- 😣 TEMPI	ATE - Device - Connection - Internet Exp
🛛 😣 TEMPL	ATE - Device - Connection - RDP 5.2 (Ch.
- & TEMPL	ATE - Device - Connection - RDP 5.2 Auto
	ATE - Device - Connection - RDP 5.2 with
TEMPI	ATE - Device - Display Settings Policy 102

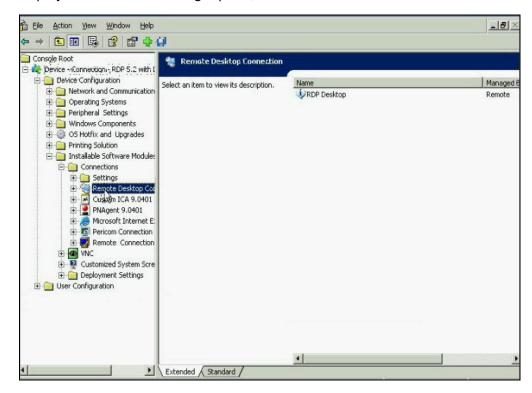
3) The selected policy is now listed in the Xcalibur Policy tab page. Select and highlight the selected policy from the Xcalibur Policy Object Links column then from the right-click menu select Rename to modify the name of the selected policy, as illustrated. Rename the policy to Device -Connection RDP 5.2 with Desktop Shortcut.

🔏 Cu	rent Xcalibur P	olicy Objec	t Links for Thin (	Clients
Xcalibur Policy	Object Links		No Override	Disabled
💐 Device - Co		Contract The second states of the		
TEMPLATE		and the state of t		
	-Device C	No Over Disabled	ride	
		Ne <u>w</u> <u>A</u> dd		•
Kcalibur Policy Objects highe		Edit		nity.
		Delete		
New	Add	Rename		Up
Options	Delete	Propertie Show Po	es licy History	Dayyn
Block Policy	inharitanca –			





- 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 5.2 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	?
ettings Explain Supported Clients	
This third party plug-in offers conne	ctivity to servers.
	Prev
	Next
Connection Name RDP Desktop	
Connection to [192.168.7.21]	×
Description	
This third partifilug-in offers connectivity t	o servers.

- 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