Xcalibur Global

Version 1.2

Quick Configuration Guide

Document Version 3.0

COPYRIGHT NOTICE

TRADEMARKS

U.S. GOVERNMENT RESTRICTED RIGHTS

Table of Contents

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

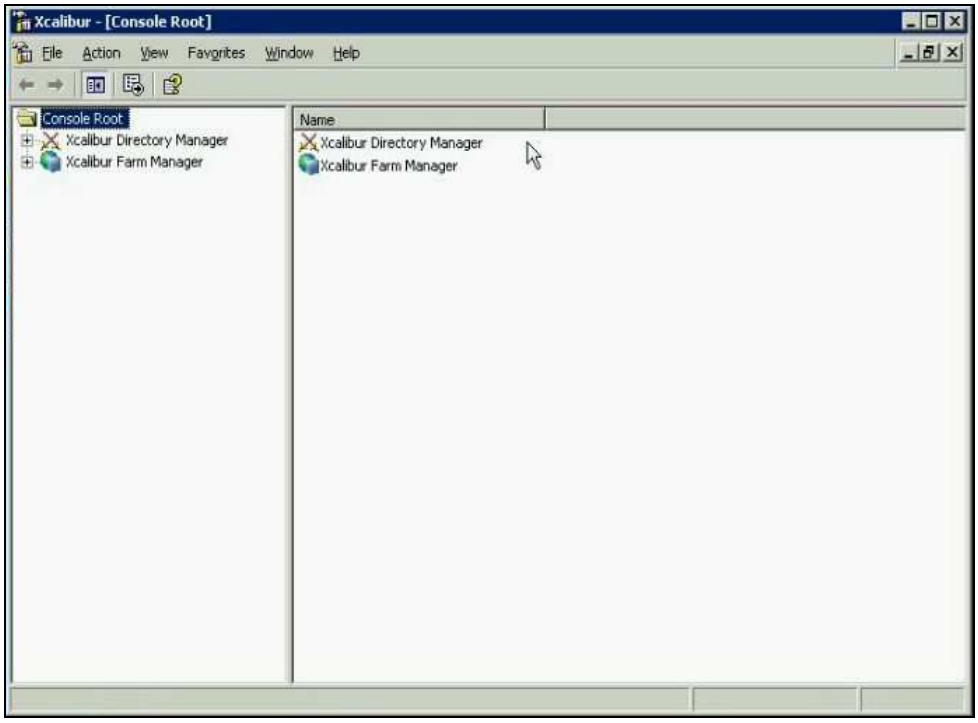
Additional licenses may be required to achieve full functionality.

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.
2) From the **Start** button select **Programs, Xcalibur Global (1.2), Management Console** to launch **Xcalibur Global Management Console**, as illustrated.



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

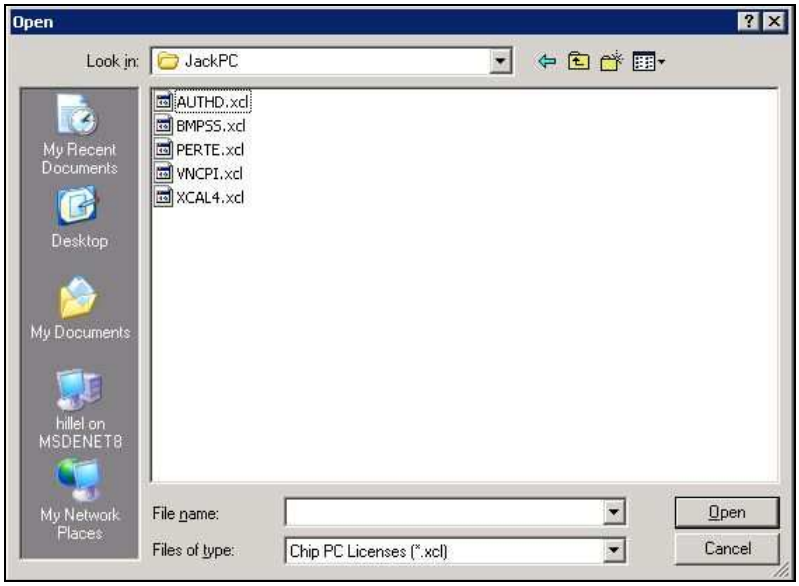
4) Select and expand **Administrative Suite** to display the full directory tree, as illustrated.

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.

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.



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.)

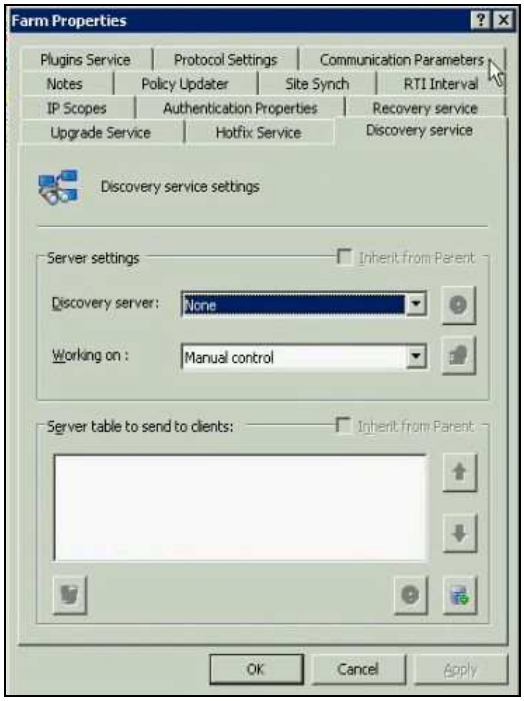
14) Repeat this procedure for each license required to be installed.

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**:

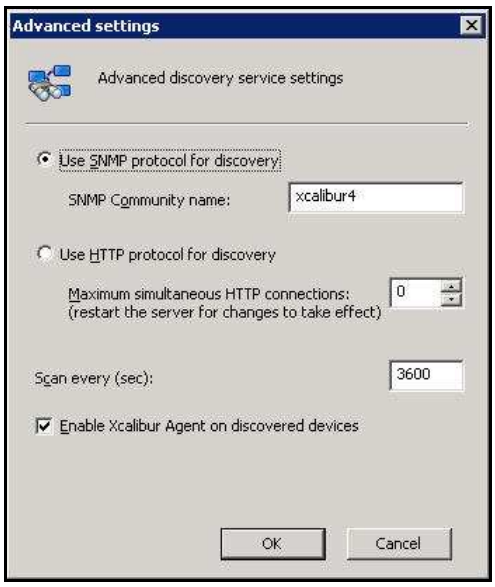
1) In the **Xcalibur Global Management Console** window, from the left pane select and highlight **Xcalibur Farm Manager**.
2) From the right-click menu select **Properties** to display the **Farm Properties** window, then click the **Discovery service** tab to display the **Discovery service settings**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



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.

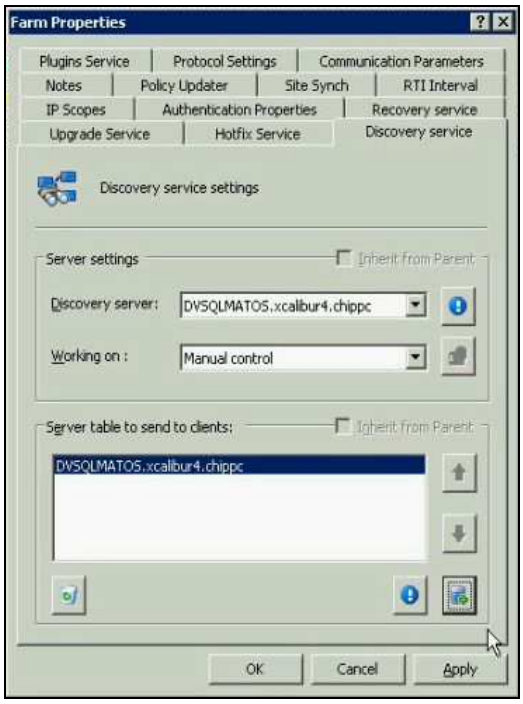
Note The selected server will be responsible for discovering thin client devices via network scans. Ensure that this server has access to all IP address ranges wherever thin clients may reside.

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



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.



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).

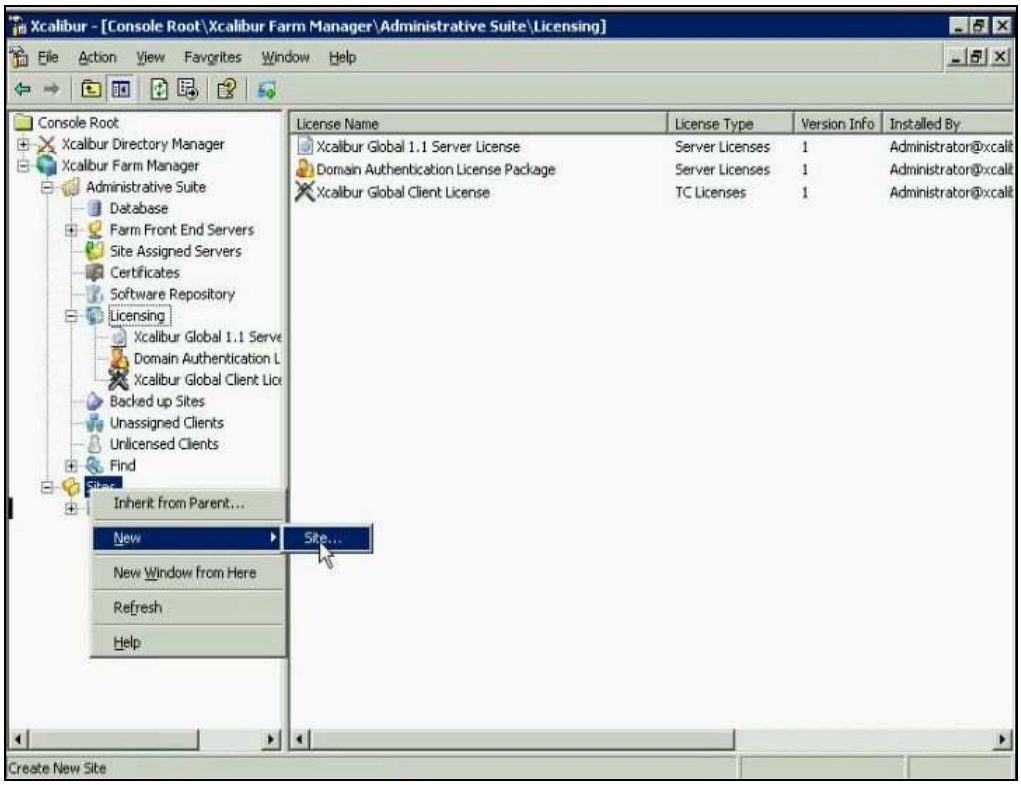
7) Click **Apply** to save your settings then click **OK** to close the **Farm Properties** window.

8) Continue to the next procedure, **Creating a New Site**.

Creating a New Site

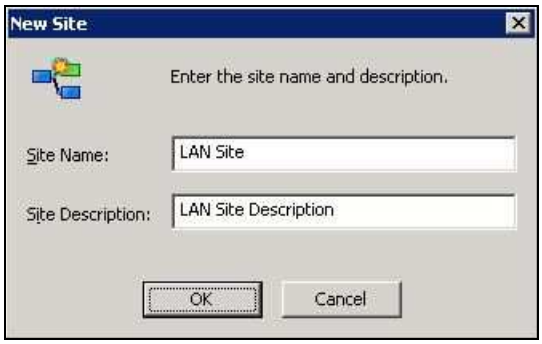
Proceed as follows to configure a new LAN site:

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:

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



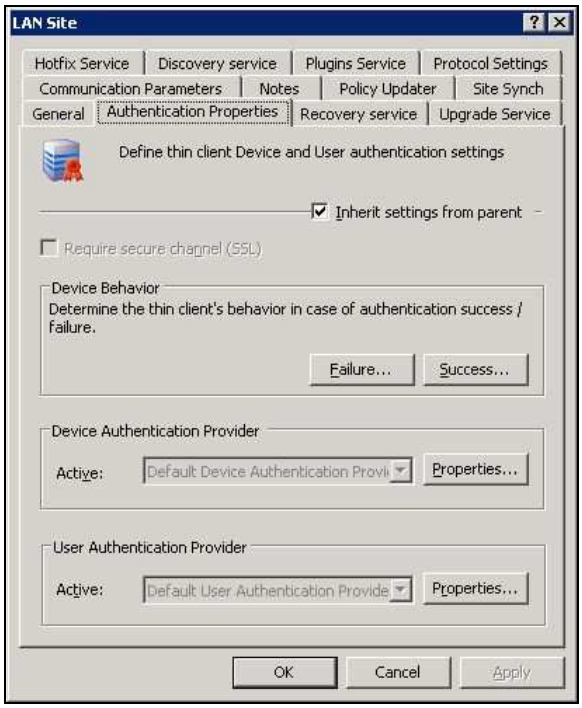
4) Click **OK** to save your entries and add the new site to the **Sites** directory.
5) Continue to the next procedure, **Configuring Authentication Settings**.

Configuring Authentication Settings

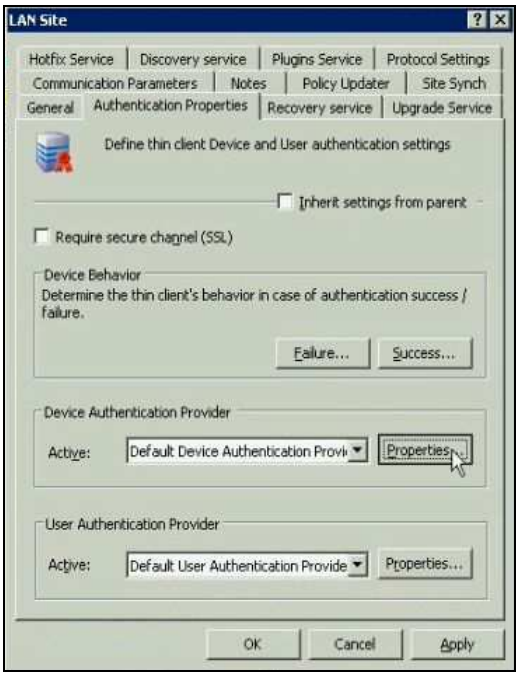
Proceed as follows to configure site authentication settings for the new site defined in the previous procedure:

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.



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



4) In the **Device Authentication Provider** section, click **Properties** to display the **Default Device Authentication Provider Properties** window.

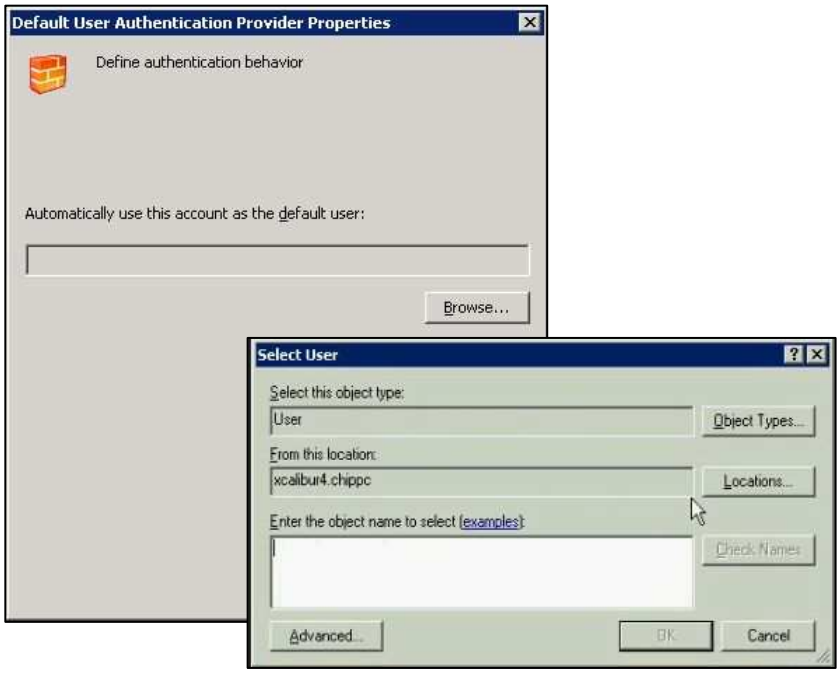
5) Select the option **Automatically accept and register new devices into the following OU**, then click **Browse…** to display the **Browse for OU** window, as illustrated.

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.

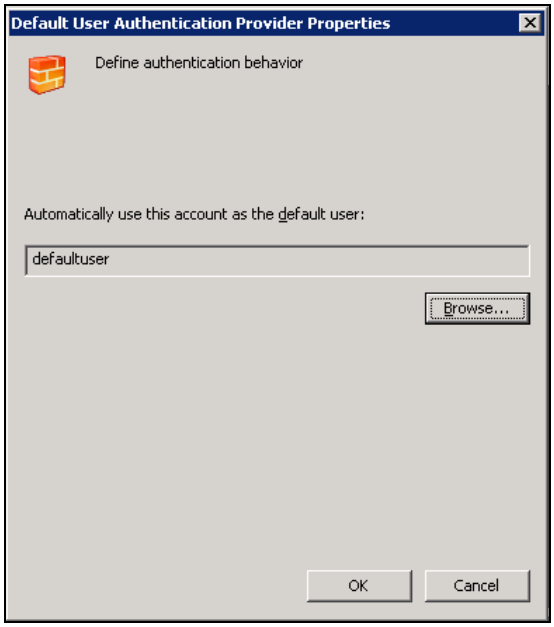
8) In the **LAN Site** window click **Apply** to save your changes.

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.



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.



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

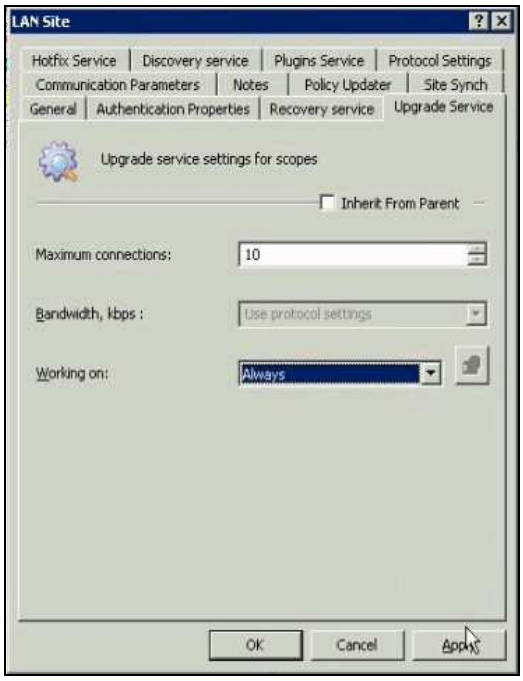
Upgrade Service

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**



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

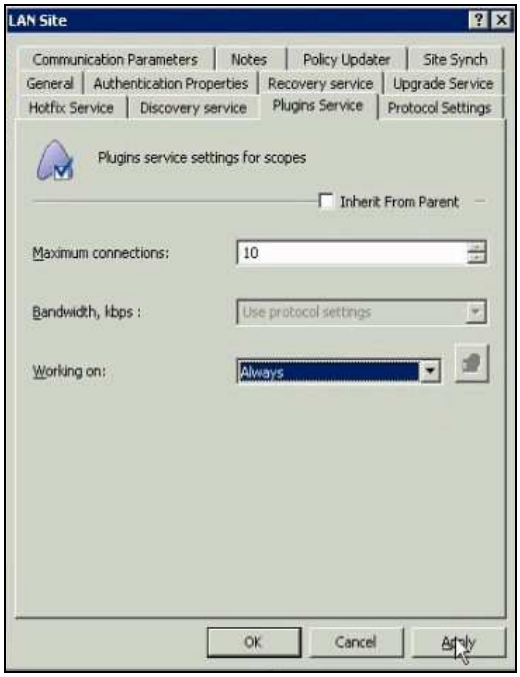
Plugins Service

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**



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

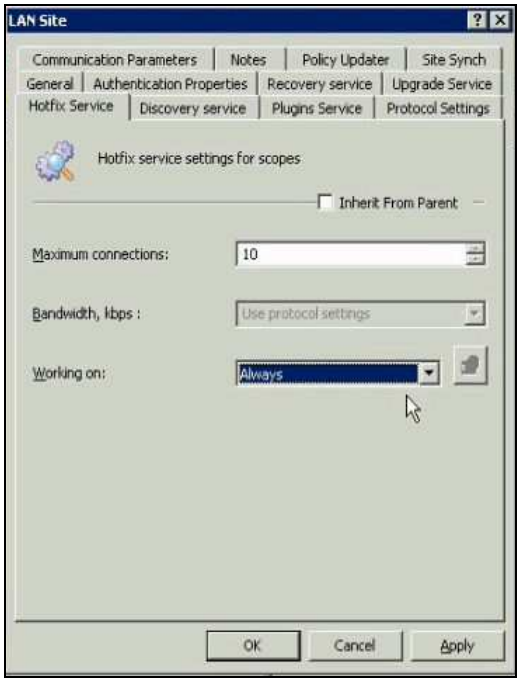
Hotfix Service

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

   Working on: From the dropdown list select **Always**



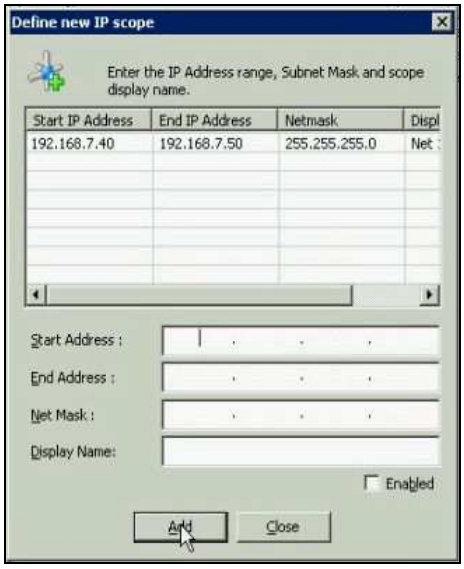
3) Click **Apply** to save your changes then click **OK** to close the **LAN Site** window and return to the **Xcalibur Global Management Console** window.
4) Continue to the next procedure, **Creating a New IP Scope**.

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

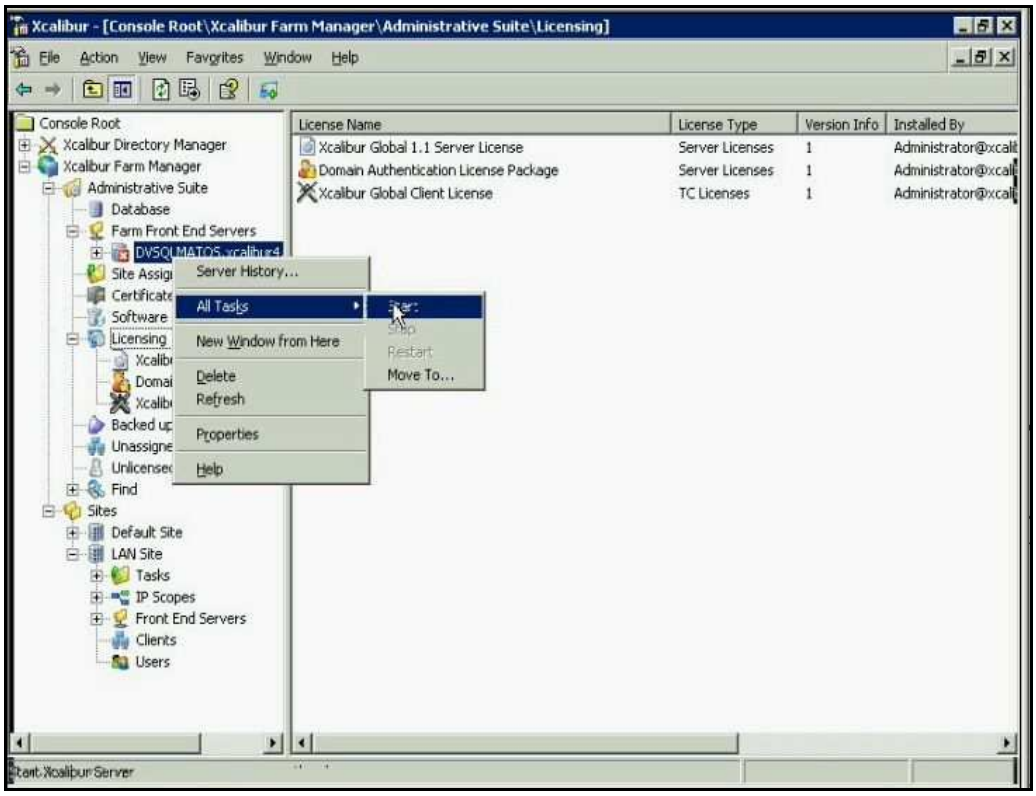


4) Click **Add** to add the IP scope to the system; the selected scope is automatically listed in the upper columns.
5) Click **Close** to close the window and return to the **Xcalibur Global Management Console** window.
6) Continue to the next procedure, **Starting the Xcalibur Front End Server**.

Starting the Xcalibur Front End Server

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

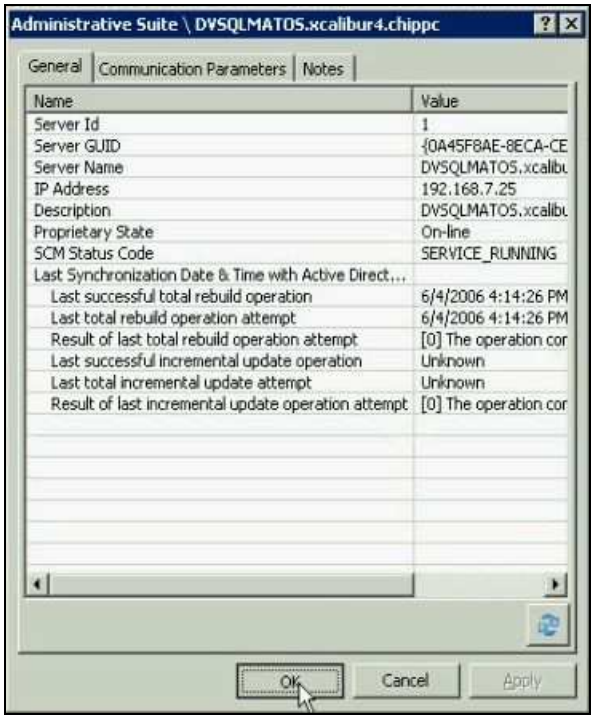
1) In the **Xcalibur Global Management Console** window, from the left pane select and expand the **Farm Front End Servers**.
2) Right-click on the Farm Front End Servers and select **Refresh**.
3) From the Farm Front End Servers tree select the pertinent server then from the right-click menu select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



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

4) 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.



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

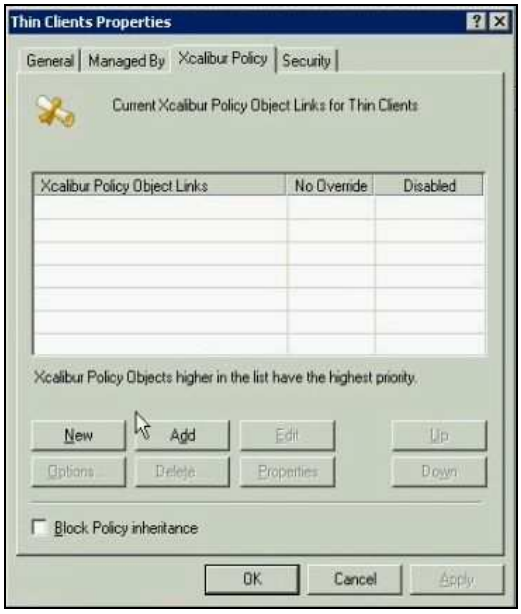
This section provides step-by-step procedures to perform the following task:

- Create a communication policy (from a template)

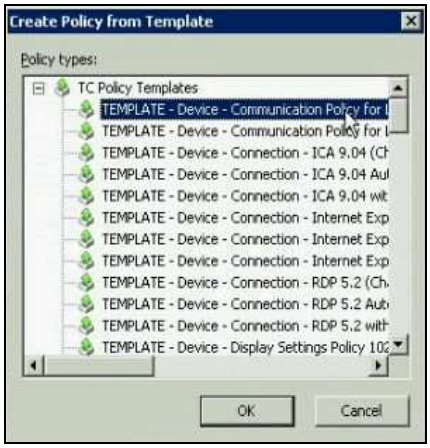
Communication Policy

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.
2) 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.



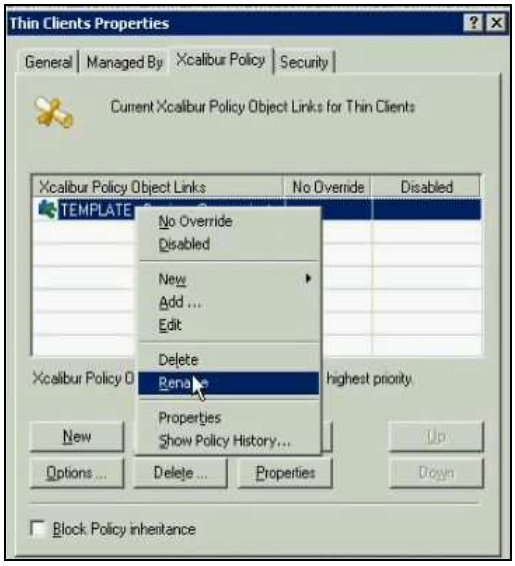
4) In the **Xcalibur Policy** tab page click **New** then select **Create from template…** from the popup menu to display the **Create Policy from Template** window, as illustrated.



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).

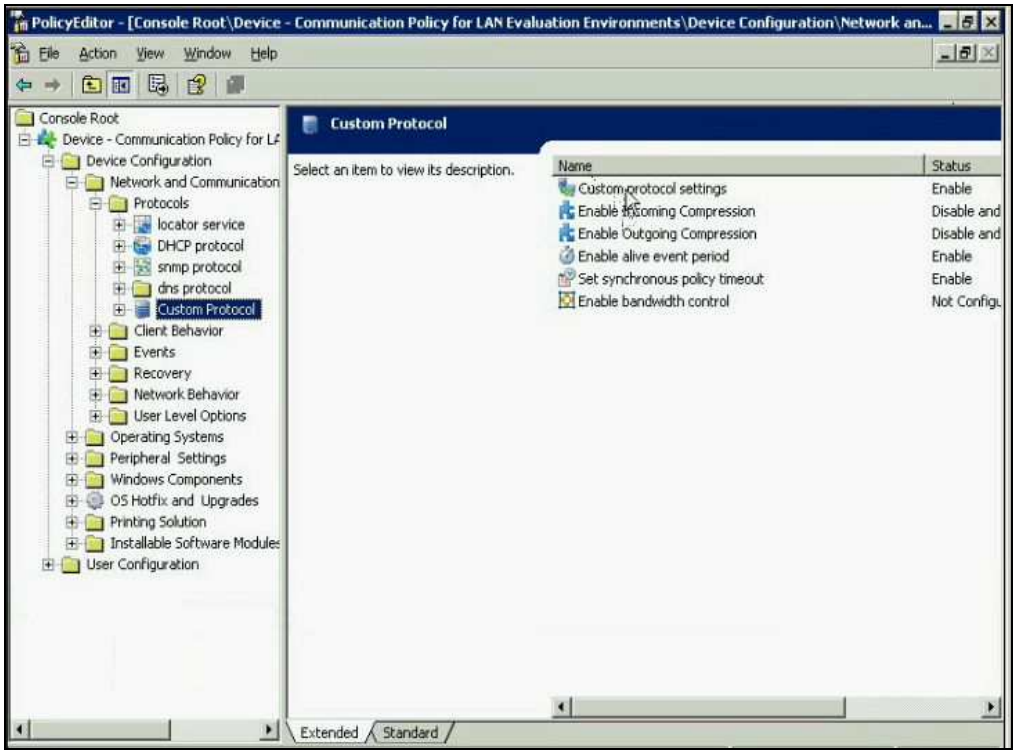
7) The newly-created policy is now listed in the **Xcalibur Policy** tab. Select and highlight the policy and then from the right-click menu select **Rename** to edit the name of the selected policy, as illustrated. Rename the policy to **Device – Communication Policy for LAN Evaluation Environments**.



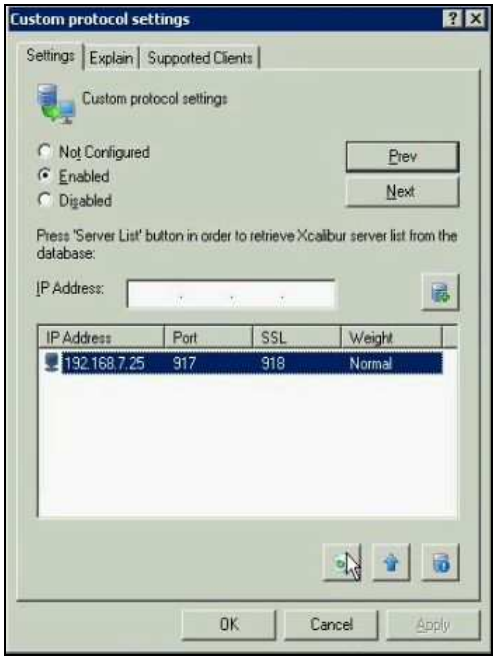
8) In the **Xcalibur Policy** tab select and highlight the renamed policy and then click **Edit** to display the **Policy Editor** window.

9) In the **Policy Editor** window's left pane expand the policy name **Device – Communication Policy for LAN Environments**.

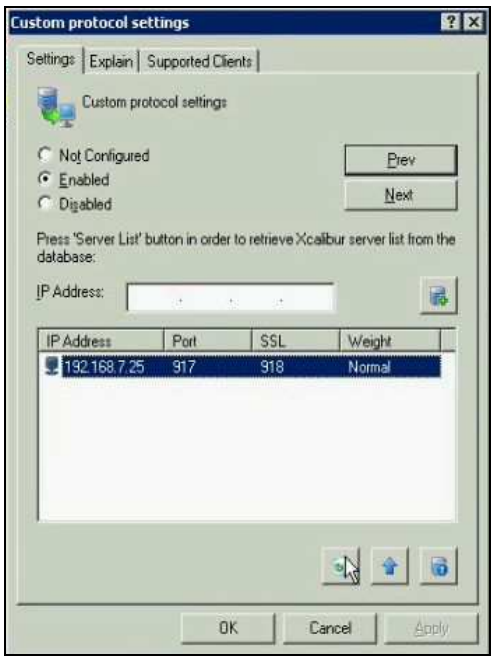
10) Expand **Device Configuration**, **Network and Communication**, **Protocols** then select and highlight **Custom Protocol** to display its contents in the right pane, as illustrated.



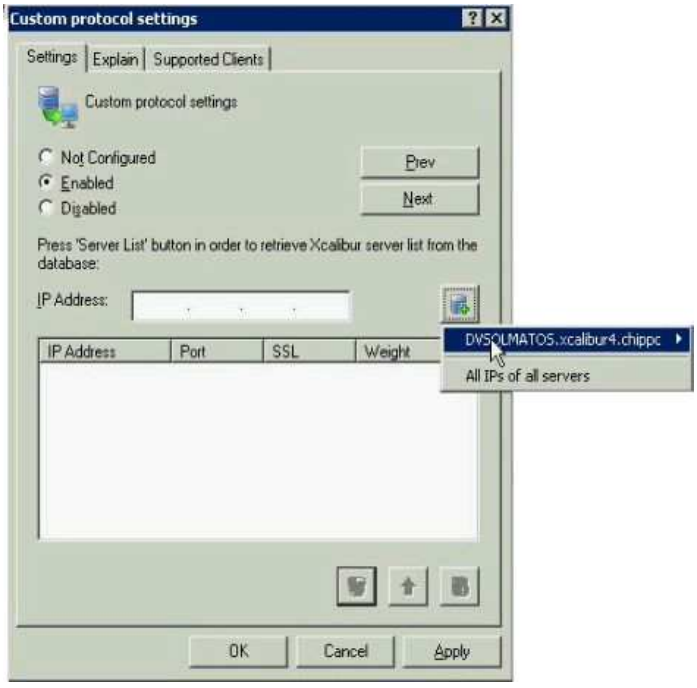
11) In the right pane double-click **Custom protocol settings** to display the **Custom protocol settings** window, as illustrated.



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.



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.



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.

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**.

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 below[1].
- For additional connection methods (such as DHCP), please refer to the Xcalibur Global Administrator's Guide.

[1] Applicable only to Windows CE thin clients

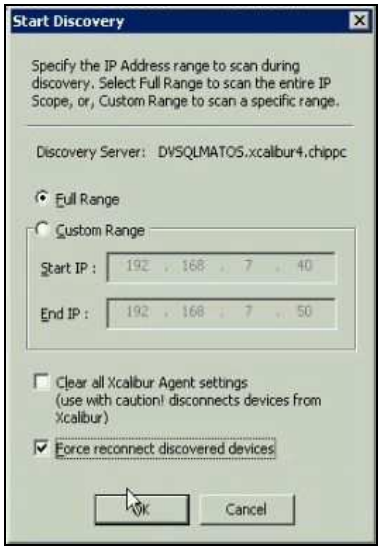
Initiate a Network Scan

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:

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



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.

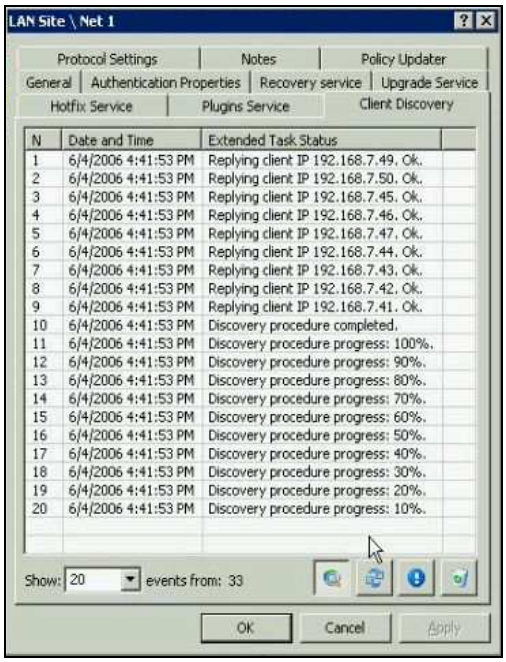
Additional reboots may occur due to policy applications.

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.



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

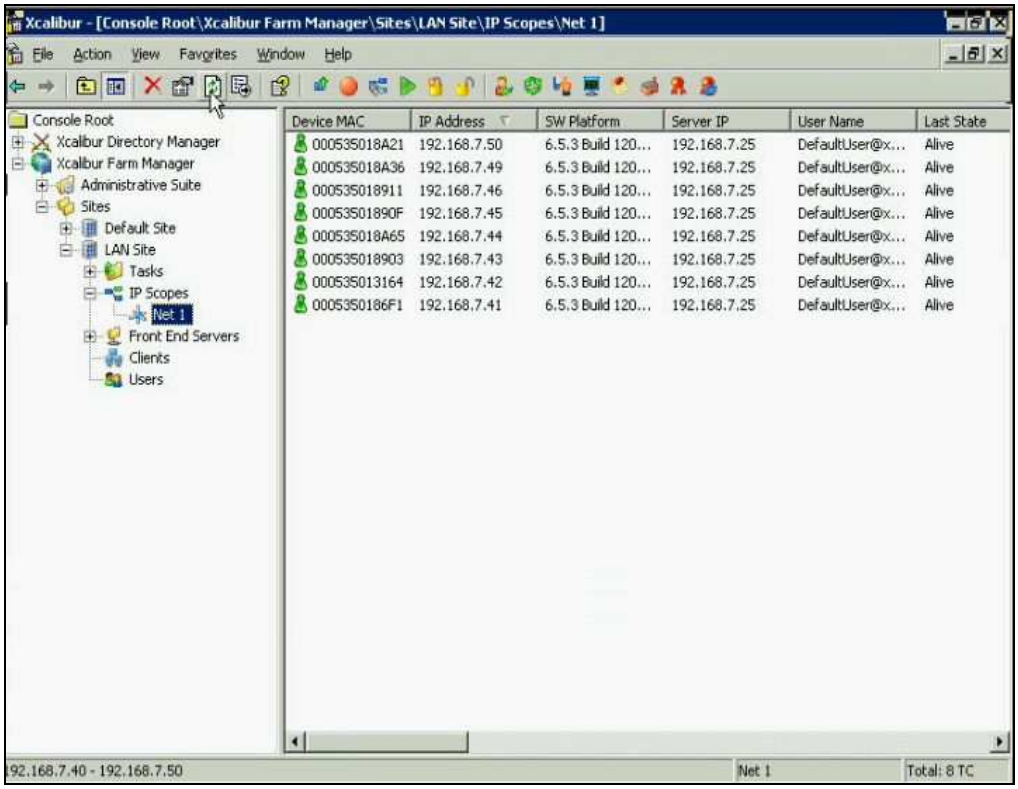
Review the scan results that include information of the discovery progress and a report of replying clients. After reviewing the scan results click **OK** to close the window.

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.

1) 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.



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 X**calibur 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.

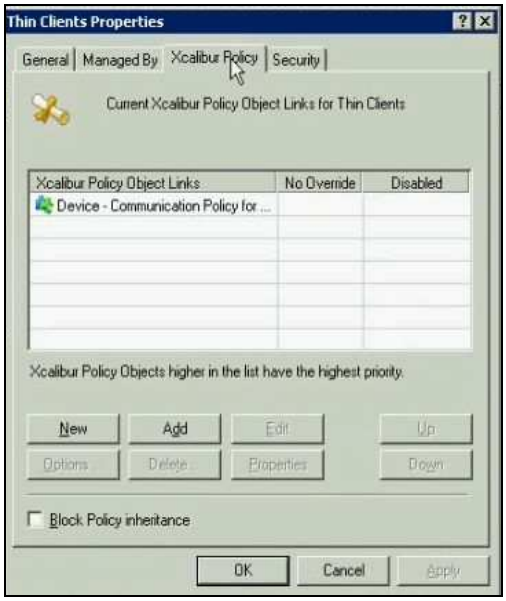
Installing an RDP Plug-in via an Xcalibur Policy

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.

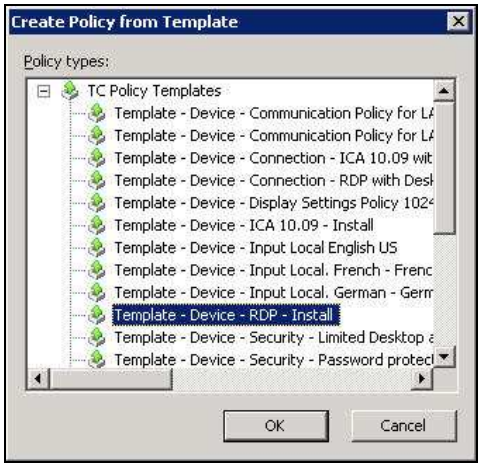
1) In the **Xcalibur Global Management Console** window, in the left pane, select and expand **Xcalibur Directory Manager**.
2) Select and expand the domain name to display the full directory tree, select and highlight the pertinent OU then from the right-click menu select **Properties** to display the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

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



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.

5) In the **Create Policy from Template** window expand **TC Policy Templates**, scroll down the list then select **TEMPLATE - Device - RDP - 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 - Install**.

Note After policy updates occur, RDP will be installed automatically on the thin clients, after which the clients will reboot.

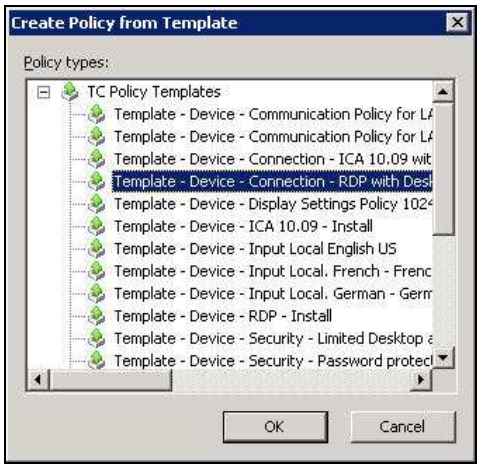
8) Continue to the next procedure, **Creating an RDP Connection by Policy**.

Creating an RDP Connection via an Xcalibur Policy

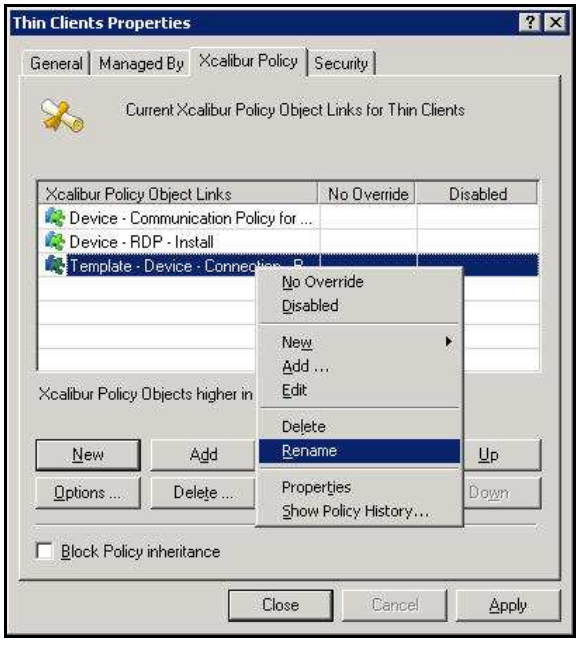
This procedure enables you to create an RDP connection via an Xcalibur policy.

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 with Desktop Shortcut**, as illustrated, then select **OK** to save your selection and display the **Thin Clients Properties** window.



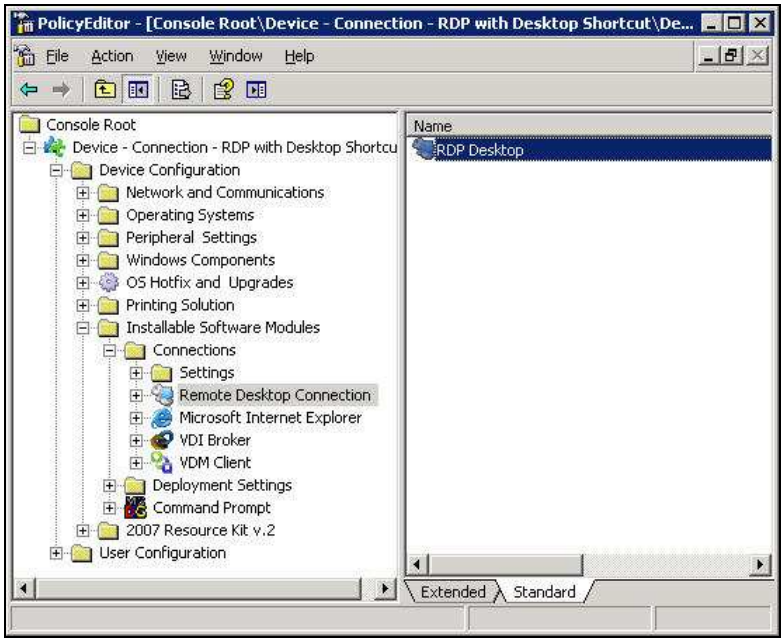
3) The selected policy is now listed in the **Xcalibur Policy** tab page. Select and highlight the selected policy from the **Xcalibur Policy Object Links** column then from the right-click menu select **Rename** to modify the name of the selected policy, as illustrated. Rename the policy to **Device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



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**.

6) 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.

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

9) 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.