



Xcalibur Global

Version 1.2

Administrator's Guide

Document Version 3.1



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	7
	Intended Audience.....	7
	Scope.....	7
	Objectives	7
	Prerequisites.....	7
	Document Features	8
	Conventions	8
	Notes.....	8
Chapter 2	Introduction	9
	Objectives	9
	Xcalibur Concepts	9
	Working Environment	9
	General:.....	9
	Windows Domain.....	10
	Network Infrastructure	10
	Xcalibur Architectural Structure.....	11
	Xcalibur Farm Database Server.....	11
	Front End Servers	11
	Management Stations.....	12
	Management Model	12
	The Logical Management Model.....	12
	The Physical Management Model.....	12
Chapter 3	Directory Manager.....	13
	Objectives	13
	Xcalibur Directory Manager and Active Directory Rights	13
	General.....	13
	Active Directory Integration.....	13
	Active Directory Permissions	14
	Xcalibur Folders	16
	All Thin-Clients Folder	16
	System Container	17
	Xcalibur Policies.....	18
	Policy Application Levels	18



Xcalibur Policy Application Rules.....	19
Policy Settings.....	20
Policy Sections.....	20
Policy Settings.....	21
Associating Policies.....	22
Administering Xcalibur Thin-Client Policies.....	23
Creating New Xcalibur Policies.....	23
Linking an Existing Xcalibur Policy.....	24
Block Policy Inheritance.....	25
No Override.....	26
Disable Policy Links.....	27
Disable Policy Objects.....	28
Delete Policy Links.....	29
Delete Policy Objects.....	30
Advanced Policy Administration.....	30
Manage Deleted Policies.....	30
Create a Policy Template.....	32
Export a Policy.....	33
Import Policy.....	33
Policy Monitoring Tools.....	34
Resulting Policy Viewer.....	35
Resulting Policy Viewer - Domain / Organizational Unit Level.....	35
Resulting Policy Viewer - Devices.....	36
View Current Device Settings.....	37
Enable Current Device Settings View.....	38
Find which policy takes affect.....	39
Policy History Viewer.....	41
Show Changes.....	42
Undo Changes.....	42
Policy Link Status Viewer.....	43
View Current Policy Links.....	44
Policy Application.....	45
Chapter 4 Farm Manager.....	47
Objectives.....	47
Physical Management Module.....	47
General:.....	47
The Xcalibur Farm Features.....	48
Xcalibur Farm Management Permissions.....	48
Inheritance Options.....	48
Xcalibur Farm Manager Snap-in Description.....	49
Xcalibur Farm Manager.....	49
Administrative Suite.....	50
Sites.....	51
Chapter 5 Thin-Client Deployment and Discovery.....	53



Objectives	53
Thin-Client Deployment.....	53
Thin-Client Discovery	53
Locator Service and Xcalibur Server List	53
Ways to Discover Client Devices.....	54
DHCP Configuration for Vendor Class Options.....	54
What to configure under the DHCP	54
Map Xcalibur Server Name to DNS	55
Discovery Service Settings (SNMP)	56
Using Xcalibur Policy to Configure the Locator Service	60
Chapter 6 Device and User Authentication	63
Device Authentication Advantages	64
Thin-Clients Authentication	65
Domain Based Device Authentication	70
Thin-Client User Level Authentication	72
Domain Based User Authentication	72
Default User Authentication Provider	77
Monitoring Authentication	79
Chapter 7 Software Deployment	81
Objectives	81
Software Installation and Distribution to Thin-Client Device.....	81
Software Deployment Concepts	81
Trigger Software Deployment process.....	81
Software Deployment Flowchart	83
Software Deployment Mechanism	83
Installation Service Providers.....	84
Software Deployment Guidelines.....	84
Software Deployment Procedure.....	86
Adding Packages into the Software Repository	86
Installation Service Configuration.....	88
Use Xcalibur Policy for Software Deployment.....	90
Plug-in Installation Policy Properties	91
Hotfix Installation Policy Properties.....	93
Firmware Upgrade Installation Policy Properties.....	95
Create a Task for Software Deployment	96
Recovery	100
Recovery Installation Service Configuration.....	102



System Restore	103
Install Package to Repository	103
Monitoring Software Deployment.....	105
Appendix A Advanced Features	107

Chapter 1 Preface

Xcalibur Global 1.2 Manual is intended on providing Administrators with the knowledge and understanding of Xcalibur Global.

After reading this article users should be able to navigate and configure Xcalibur Global to best suit their company's needs.

This manual covers the main subjects needed in order to configure the system:

- Xcalibur Directory Manager
- Xcalibur farm
- Software deployment

On completion users should be able to perform management tasks such as: Add/Remove Thin-Clients, create device and user level policies and monitor them, manage software deployment etc'.

Intended Audience

This article is intended for Administrative users who are looking to improve their knowledge and understanding of Xcalibur Global.

System Administrators, Thin-Client experts and IT managers who have adequate knowledge of Microsoft Active Directory architecture as well as students in Chip PC technical course, may use this guide to advance their understanding and skills within the Xcalibur Global Software.

Scope

Xcalibur Global Version 1.2.

Objectives

Provide knowledge and understanding of Xcalibur Global. After completing this article Users should be able to navigate and use the "Xcalibur Directory Manager" as well as the "Xcalibur Farm Manager", and be able to perform management tasks such as: Add/Remove Thin-Clients into the system, create device and user level policies, monitor all policies, manage software deployment etc'.

Prerequisites

Good level of knowledge and understanding of Microsoft Active Directory.



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 2 Introduction

Objectives

Understand the general structure of **Xcalibur Global 1.2**.

Xcalibur Concepts

Chip PC **Xcalibur Global 1.2** is a policy based enterprise management software, designed for Thin-Client management in large scale environments.

Xcalibur Global 1.2 is based on the structure of the Microsoft Windows 2003/2008 Active Directory infrastructure.

Xcalibur has the following features:

- Standard MMC snap-in administration tool
- A combination of logical (Active Directory based) and physical (Xcalibur Farm based) management models
- Active Directory Based structure for management tasks.
 - Assign management policies to devices in any Active Directory level.
 - Uses existing Active Directory permission delegation and inheritance model to assign management permissions.
- Centralized remote deployment of software to devices
- Centralized configuration, upgrade and troubleshooting of devices
- Optimized for enterprise network-infrastructure by using Xcalibur Sites for bandwidth optimization
- Scalable by adding Xcalibur Front End-Servers to the Xcalibur Farm as needed.
- Fault tolerant through Redundancy & Load Balancing
- Uses an Independent Management Protocol that has built-in support for: SSL Encryption, Compression, Port Number Control, Bandwidth Control and more.

Working Environment

General:

Xcalibur Global 1.2 is designed to operate in a **Windows 2003/2008** Active Directory environment. This section covers Xcalibur system components and explains what environment prerequisites must be fulfilled for **Xcalibur Global 1.2** operations.



Windows Domain

Active Directory structure is used as the groundwork of the Xcalibur logical structure. By mapping the Active Directory Tree, the management structure of Xcalibur is identical to the already existing Active Directory. This prevents building different management structures and allows applying management settings based on the same logical structure used for managing the Windows environment.

Network Infrastructure

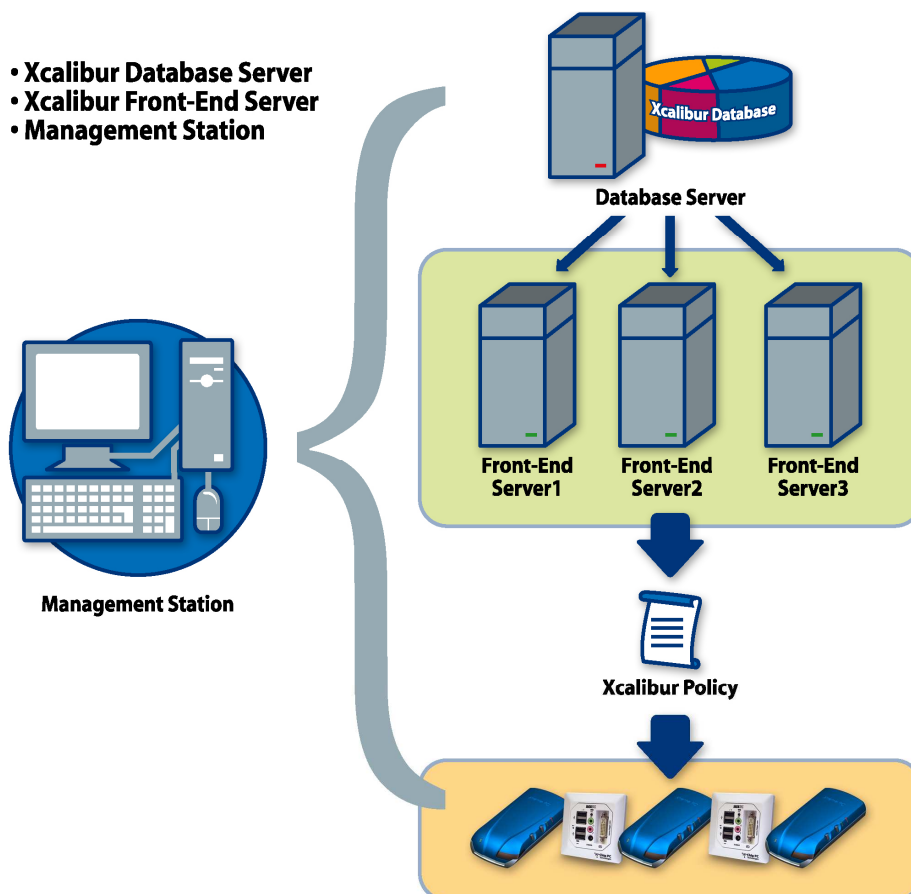
- TCP/IP Protocol: used as the communication protocol for client-to-server, server-to-server and management-to-server components.
- DHCP: in addition to its role in any TCP/IP network, DHCP can be used for Standard / Vendor-Class option assignment to client devices. These options may include the Xcalibur Front End Server addresses and more.
- DNS: in addition to its role in any TCP/IP network, DNS can be used for mapping Xcalibur Front End Server IPs-to-Name in the network.
- SNMP: used by Xcalibur Front End Servers to discover thin clients (optional).

Xcalibur Architectural Structure

Xcalibur Global 1.2 architectural structure is designed to simultaneously support thousands of clients and users while providing fault tolerance, speed, scalability and ease of management.

The following system components are comprised in the Xcalibur solution.

- **Xcalibur Database Server**
- **Xcalibur Front-End Server**
- **Management Station**



Xcalibur Farm Database Server

This is an SQL Server database instance, hosting all Xcalibur data including Front End server settings, software modules, MMC snap-ins, Xcalibur Policies and client configuration information. An Xcalibur Farm will always work with a single Xcalibur Farm Database Server.

Front End Servers

Each Front End Server (FES) holds a locally cached copy of the information held in the Xcalibur database it is linked to, and is responsible for communicating with client devices and applying the configuration and policies to them. In addition to this, Front End Servers are responsible for forwarding client management information to the database. An Xcalibur Farm can support several Front End Servers.



Management Stations

A Management station is any desktop or server computer installed with Xcalibur Directory Manager, Xcalibur Farm Manager, Xcalibur Log Viewer and Xcalibur Policy Editor MMC snap-ins.

A user who has been granted the necessary permissions can use a Management Station to control the Xcalibur management environment.

Permissions for the Management Station should be allocated as required for each of the company's branches. This way each of the company's branches or Organizational Units can be managed by a dedicated person rather than have a single manager for an entire system which could be distributed around the world.

Management Model

Xcalibur Global 1.2 is capable of mapping both the logical organizational structure represented by the Active Directory, as well as the physical company infrastructure layout represented by the Xcalibur Farm.

This combination allows for applying company wide management rules while considering network infrastructure limitations.

The Logical Management Model

Xcalibur Global management is based on a policy model. An Xcalibur policy is a set of rules defining User and/or Client device settings based on the device's location in the Active Directory tree and the location of the account of the user who is logged on at the device.

Although **Xcalibur Global** never modifies the Active Directory schema in any way, Xcalibur can be thought of as an Active Directory extension, providing a way to create Thin-Client policies using the same guidelines and rules as those used to create and manage Group Policies in the Windows environment.

Anyone who is familiar with Active Directory, Group Policy and the Microsoft applications that manage it, will very quickly become familiar with the Xcalibur management snap-ins. Xcalibur Policies for Thin-Client management can be linked to any Active Directory level.

The Physical Management Model

Through the Xcalibur Farm Manager snap-in, administrators can control the physical aspects of Thin-Client management in the organization.

The Xcalibur Farm enables a mapping of the organization's physical network layout by creating Sites that stand for branches and IP Scopes that stand for the IP Address ranges that is used in each branch. Based on the farm structure administrators can configure software deployment rules while considering network limitations, such as bandwidth.

Chapter 3 Directory Manager

Objectives

This chapter will review the Active Directory permissions required in order to start working with the Xcalibur Administration Station.

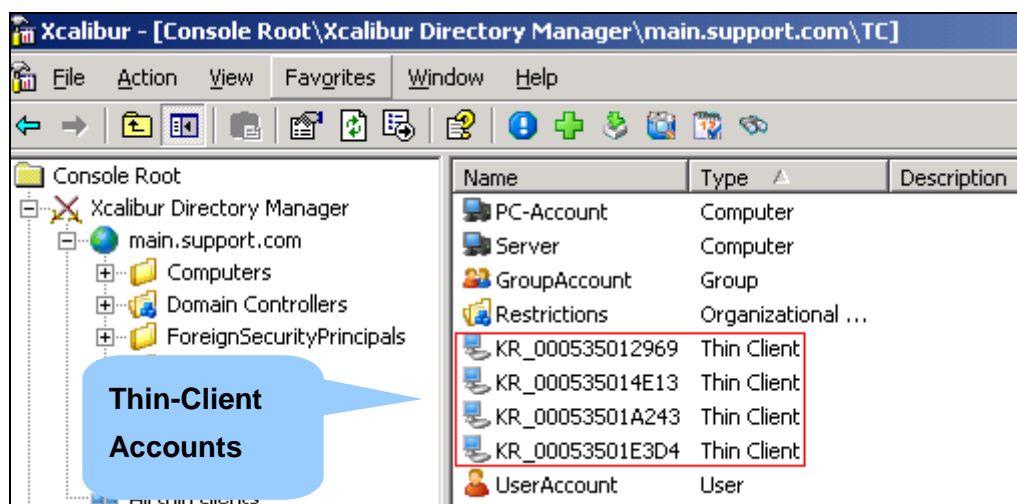
It also aims to provide users with better understanding of the Xcalibur Policy concepts, tools and administration options.

Xcalibur Directory Manager and Active Directory Rights

General

The Xcalibur Directory Manager snap-in is an enhanced Active Directory Users & Computers view, capable of displaying both Xcalibur oriented objects and original Active Directory objects under the same interface.

In addition to standard Active Directory objects, Xcalibur oriented objects such as Thin-Client device accounts and Xcalibur policies (which are held in the Xcalibur database) are presented to administrators within the Xcalibur Directory Manager MMC Snap-in.



Active Directory Integration

Although the Xcalibur Directory Manager Snap-in integrates Xcalibur and Active Directory objects together under the same view, Xcalibur objects are not part of the Active Directory schema.

In fact Xcalibur installation does not modify the Active Directory schema in any way.

The Xcalibur database is set to constantly synchronize with the domain controllers hosting the Active Directory database. Directory service updates sent out during the standard Active Directory synchronization process are intercepted by the Xcalibur service allowing constant real-time synchronization between the Xcalibur database and the Active Directory database.

Database and Active Directory Synchronization:

- Xcalibur links to the Active Directory using LDAP.
- Active Directory objects are viewable using the Xcalibur Directory Manager MMC snap-in.
- Thin-Client objects and policies are added to the Xcalibur database through the Xcalibur Directory Manager MMC snap-in.
- Xcalibur complies with the Active Directory permission scheme and therefore supports permission delegation at all levels.

Active Directory Permissions

Xcalibur Global 1.2 takes advantage of the Active Directory in such a way that rights and delegation settings specified within the Active Directory are also used by Xcalibur. The following table describes the minimum permissions required for performing administrative tasks within the Xcalibur Directory Manager snap-in.

Task Description	Required Active Directory Permissions
■ View Active Directory and Xcalibur Objects	■ Read
■ Resulting Policy Generation	■ Generate Resultant Set of Policy (Planning)
■ View current device Settings	■ Generate Resultant Set of Policy (Logging)
■ Create Thin-Client device account	■ Create Computer account
■ Delete Thin-Client device account	■ Delete Computer account
■ Move Thin-Client account between Organizational Units	■ Full Control on source and target Organizational Unit
■ Create Xcalibur Policy	<ul style="list-style-type: none"> ■ Have Read + Write gPLink permission on the target object ■ Have Read + Write gPOptions permission on the target object

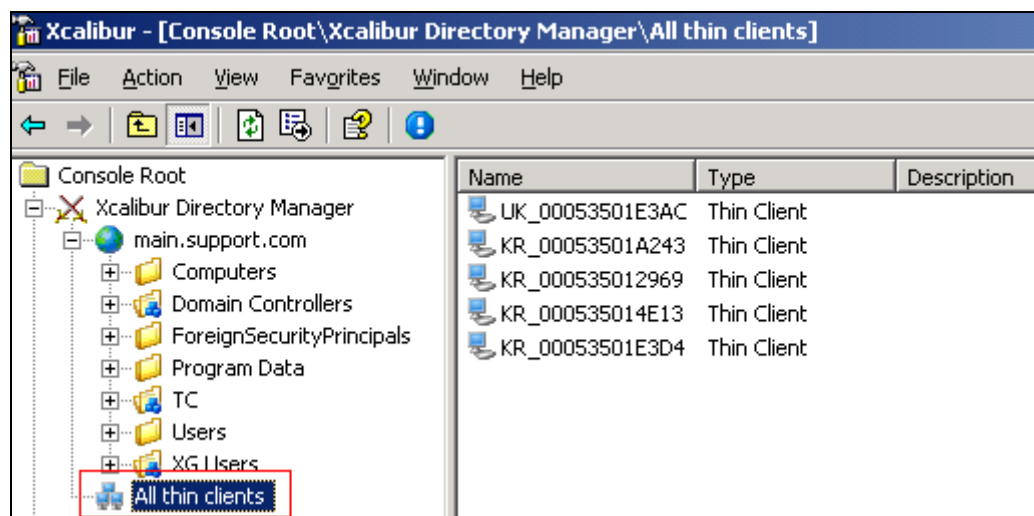
Task Description	Required Active Directory Permissions
<ul style="list-style-type: none"> Edit Xcalibur Policy 	<ul style="list-style-type: none"> Have Read + Write gPLink permission on the target object Have Read + Write gPOptions permission on the target object Have Write permissions on the policy object
<ul style="list-style-type: none"> Disable Device / User Policy Sections 	<ul style="list-style-type: none"> Have Read + Write gPLink permission on the target object Have Read + Write gPOptions permission on the target object Have Write permissions on the policy object
<ul style="list-style-type: none"> Link / Unlink Xcalibur Policy Block Inheritance No Override Disable Policy Link Sort Policy Order (Up/Down) Show Per Date Policy Links 	<ul style="list-style-type: none"> Have Read + Write gPLink permission on the target object Have Read + Write gPOptions permissions on the target object
<ul style="list-style-type: none"> Delete an Xcalibur Policy Object 	<ul style="list-style-type: none"> Have Read + Write gPLink permissions on the target object Have Read + Write gPOptions permissions on the Target object Have Full Control permissions on the policy object

Xcalibur Folders

Xcalibur Folders are Thin-Client management related folders that are created in the Xcalibur database during the Xcalibur installation. These are displayed in the Xcalibur Directory Manager snap-in in addition to the Active Directory Tree.

All Thin-Clients Folder

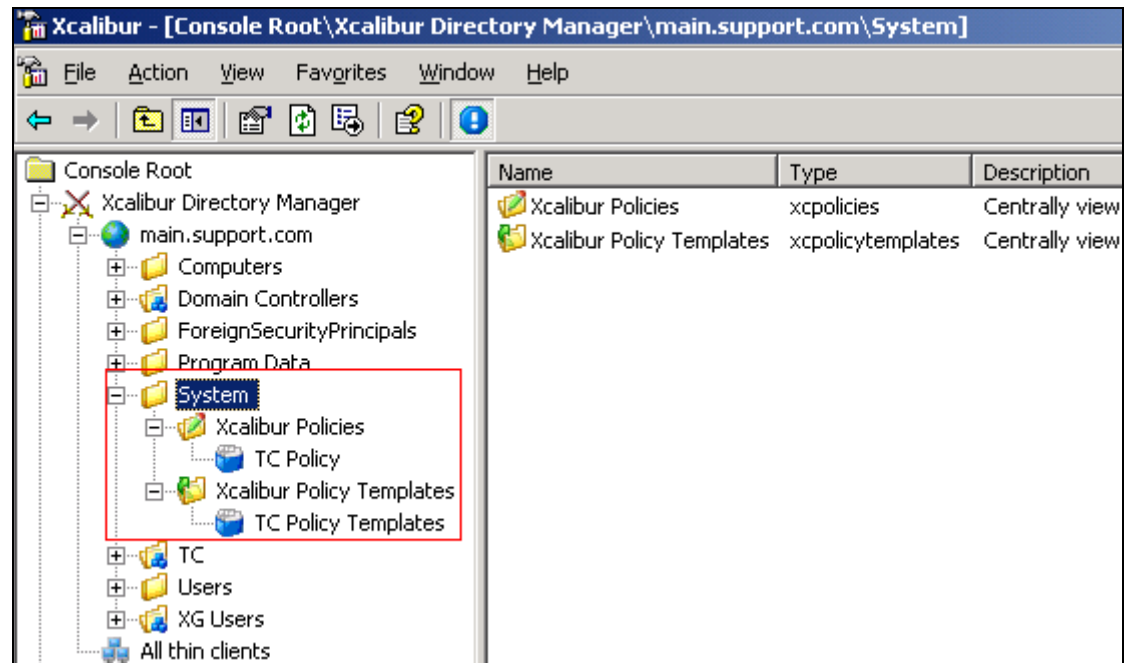
The *All Thin-Clients* folder groups all the Thin-Client accounts residing in the Xcalibur Database into a centralized view. This folder, which is viewable only to the members of the Administrators group, allows searching the database for a specific client as well as taking administrative actions on per device bases.



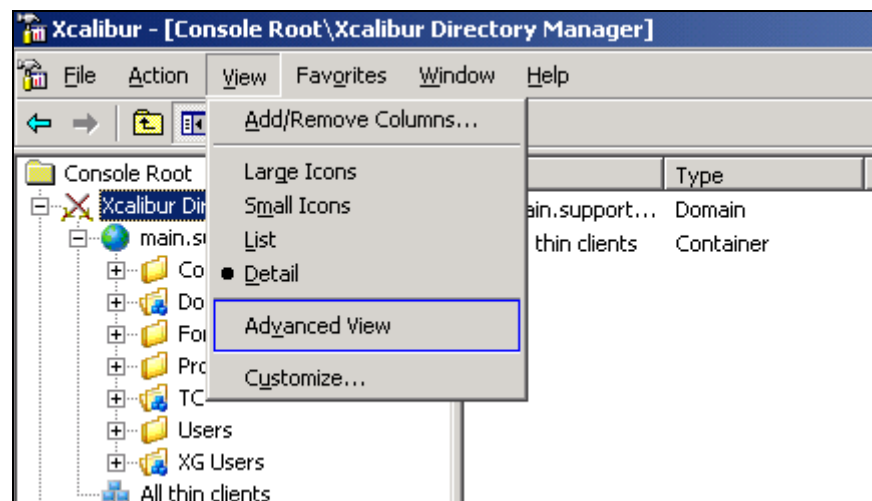
System Container

The *System* container provides a centralized view of the Xcalibur Policy and policy templates list for members of the Administrators group.

The *system* container also allows to perform several management tasks such as: save as template, delete policy, import policy etc'.



In order to add the System Container to the Xcalibur Directory Manager display, select the Advanced View option from the MMC View Menu.



Xcalibur Policies

Xcalibur Global 1.2 management software is based on a policy allocation module. An Xcalibur policy is a set of rules defining user and/or client device settings, based on the device's location in the Active Directory tree and the location of the account of the user who is logged on at the device. By using Xcalibur Policies you can define client and user settings once and then rely on Xcalibur to continually enforce your policy settings throughout the network.

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. The extent of policy usage is determined by the level of service required by different areas of the organization. Some areas might require strict and comprehensive settings while others might content with minimal settings.

Although Xcalibur never modifies the Active Directory schema in any way, Xcalibur can be thought of as an Active Directory extension providing a way to create Thin-Client policies using the same guidelines and rules as those used to create and manage Group Policies in the Windows environment. Anyone who is familiar with Active Directory, Group Policy and the Microsoft applications that manage it will very quickly become familiar with the Xcalibur management snap-ins.

Policy Application Levels

Xcalibur Policies for Thin-Client management can be linked to the following levels:

- Domain
- Organizational Unit
- Device
- User

Applying Xcalibur Policies at any of these levels has advantages and disadvantages. How an organization will use Xcalibur Policies depends on the level of Thin-Client and Thin-Client users management desired.

What to consider when applying Xcalibur Policies at the domain level:

Xcalibur Policies that are assigned to the domain are applied to all Thin-Clients and Thin-Client users within the domain. If you consider creating only domain level policies, you can prevent policy conflicts from occurring, this can occur when (conflicting) policies exist at multiple levels. However, applying Xcalibur Policies at the domain level only prevents benefiting from control delegation options, meaning that all policies will need to be administered at the domain level.



What to consider when applying Xcalibur Policies at the Organizational Unit level:

Applying Xcalibur Policies at the Organizational Unit level allows you to tightly control the application of Xcalibur Policy to specific users and Thin-Clients. Creating Xcalibur Policies for Organizational Units gives you precise control over applying Xcalibur Policies because it eliminates the need to filter policy settings. However, it also means that there are more policies to manage. Additionally, conflicts between policies can occur because Organizational Units can be nested and because Xcalibur Policy is inherited from parent Organizational Unit to child Organizational Unit. Careful planning of Organizational Units and Xcalibur Policies can reduce conflicts caused by inheritance.

What to consider when applying Xcalibur Policies at the Device and User levels:

Linking an Xcalibur Policy directly to a Thin-Client or user object allows enforcing policy settings on that object. This should be mainly done for troubleshooting or help desk scenarios where a specific device or user requires specific settings.

Xcalibur Policy Application Rules

Understanding the Xcalibur Policy application rules will help you plan your policy strategy. Xcalibur Policy application rules ultimately determine which settings will affect users and Thin-Clients.

The order in which Xcalibur applies Xcalibur Policies is based on the object to which the Xcalibur Policies are linked. Xcalibur Policies are applied first to the Domain, which is the furthest away from the User or Thin-Client, and then applied to Organizational Units and then to Thin-Clients and then to users.

Within a domain, Xcalibur Policies are inherited from one Active Directory object to another, so that in the Active Directory structure, any Xcalibur Policy applied to a parent object will also be applied to child objects.

Any policy created at the domain level will be passed down through inheritance to all objects within the domain. Any policy applied to a parent Organizational Unit will be applied to all of its child Organizational Units.

Policy Conflicts:

Xcalibur Policies are cumulative, that is, all Xcalibur Policy settings from all policies affect target users and / or Thin-Clients, unless two or more settings conflict. The rules for determining which Xcalibur Policy settings apply when they conflict are as follows:

- Parent object policy settings conflict with child object policy settings: when settings from a parent object policy conflict with settings from a child object policy, policies of parent objects are processed before child object's own policies. Therefore, by default, policies which are closest to the object apply last and take effect.
- Settings from different policies linked to the same object, conflict: when multiple policies are linked to the same object, the settings of the policy placed at the top of the policy list are applied last and take effect.

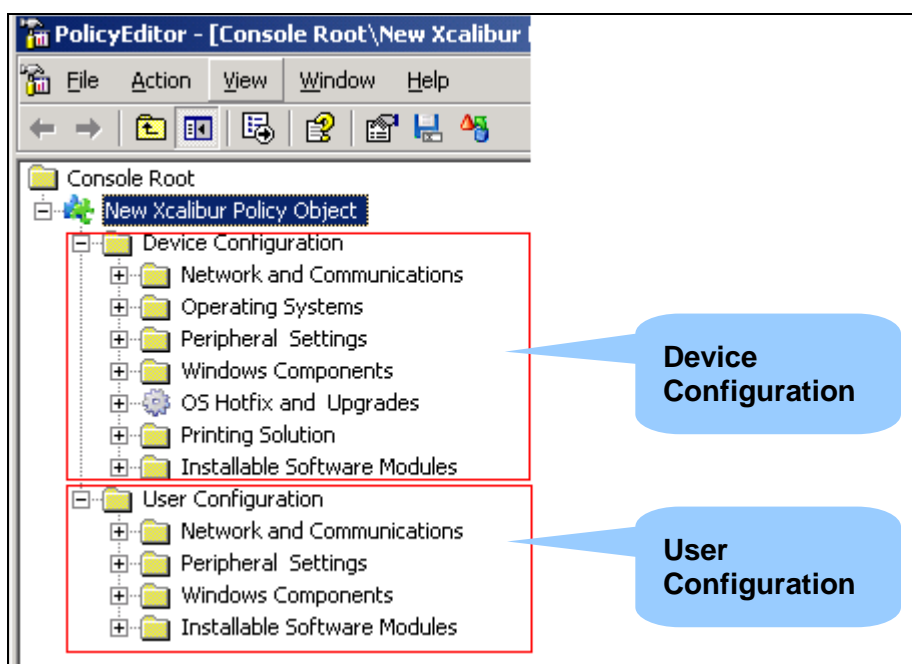
Policy Settings

The following can be set by an Xcalibur Policy:

- **Network and Communication:** configure the client-management communication settings. These settings include communication protocol settings, server discovery methods, monitoring events behavior, network authentication and PXE recovery parameters.
- **Operating System:** Add / Remove optional registry based settings.
- **Peripheral Settings:** Configure input / output device settings such as Keyboard, Mouse, Display, USB, COM and LPT ports, Printer setup etc'.
- **Windows Components:** Settings for configuring Start Menu, Desktop, Control Panel and Internet Explorer appearance and security. These settings include controlling the access rights to specific operating system parts and menus. For example you can hide specific Internet Explorer menus and prevent access to the Control Panel.
- **OS Hotfix and Upgrades:** Specify an upgrade and hotfix installation policy.
- **Installable Software Modules:** Settings for centralizing the management of software deployment, updates and removals. You can set applications to be automatically installed, upgraded or removed from the target Thin-Clients.
- **Connection Configuration:** Configure client connections including RDP, ICA and Internet Explorer. Connection settings include load balancing and published applications settings.

Policy Sections

Policies have two sections, Device and User. Therefore a policy assigned to the Domain or Organizational Unit can affect both users and devices.



Device Configuration:

Xcalibur Policy settings for Devices specify network and communication settings, operating system behavior, peripheral settings, Windows components, hotfix, upgrades and software deployment.

These settings apply on Thin-Client accounts according to their assignment in the Active Directory tree. Device Configuration settings initially apply during the Thin-Client boot and then refreshed according to specified refresh interval.

Computer accounts residing in the Active Directory are not affected by Xcalibur Policies.

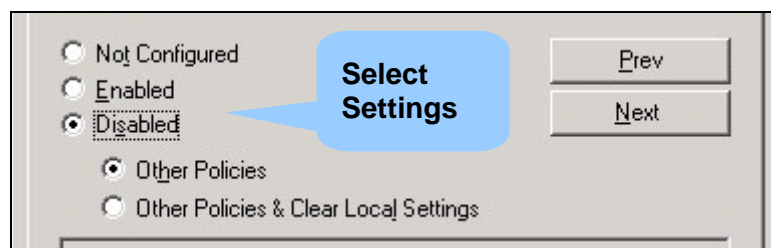
User Configuration:

Xcalibur Policy settings for Users specify Windows components, Terminal Server Connections and Xcalibur communication options. These settings apply only once users logon to Thin-Clients managed by the Xcalibur. User Configuration settings initially apply during user's logon to the Thin-Client. Users logging on to computers or servers that reside in the Active Directory are not affected by Xcalibur Policies.

Policy Settings

Policy Settings definition is where you determine whether a policy item is sent to the target object (Domain, Organizational Unit, Device or User) to which the policy is linked to.

The status of the policy will determine whether it will be applied on the target object or not.



Policy settings can be set to the following status:

- **Not Configured:** This is the default status of all policy settings. Not Configured means that no changes will be made by this policy to target Domain, Organizational Unit, Device or User object settings. Therefore, the local client settings are not altered by this policy.
- **Enabled:** A policy which is set as Enabled will be applied on target objects. Enabled policy parameters are sent to target objects during policy application. Since policy settings override local settings, Enabled policy settings modify the local device settings.
- **Disabled / Other Policies:** A policy which is set to Disable-Other-Policies prevents other policies from applying on target objects. This means that in case there is another policy(s) which "Enables" the same settings that are disabled by this policy, no settings are sent to the target objects. Therefore the local settings of the client device are not altered by any policy.



- **Disabled / Other Policies & Clear Local Settings:** A policy which is set to Disable-Other-Policies-&-Clear-Local-Settings prevents other policies from applying on target objects while also clearing the target device settings accordingly. This means that this policy not only prevents other policies from applying, but also sends the target devices a command to disable (clear) the local parameters for this policy.

Associating Policies

An Xcalibur Policy is saved in the Xcalibur Database as an object. A single policy object can be linked to one or many objects (Domain, Organizational Unit, Device or User). A policy link associates a policy item to a target object, thus making the policy item settings apply on the target object.

The linking of a policy to the Domain or Organizational Unit causes the policy settings to affect user and Thin-Client accounts in that Domain or Organizational Unit.

Policies can be linked in the following ways:

- **One to Many:** Link one Xcalibur Policy to multiple objects (Domain, Organizational Units, Devices and Users). This allows applying the same policy settings onto different targets (e.g. Domain, Organizational Units, Devices and users). For example, you can create an Xcalibur Policy that prevents users from accessing the Control Panel, and then link it to the Organizational Units where you have users from whom you want to prevent the access.
- **Many to One:** Link multiple Xcalibur Policies to one Domain, Organizational Unit, Device or User. Instead of having one policy with multiple settings in it, you can create several policies, each policy for specific purpose and then link them to the appropriate Domain, Organizational Units, Devices or Users. For example, you can link a policy that sets Display Resolution, and another policy that specifies software deployment settings to the same Organizational Unit.

Note Xcalibur Policies can be created, managed and linked only from the Xcalibur Directory Manager snap-in.

Xcalibur Policies, like other Xcalibur objects, are stored in the Xcalibur Database and not in the Active Directory or Schema.

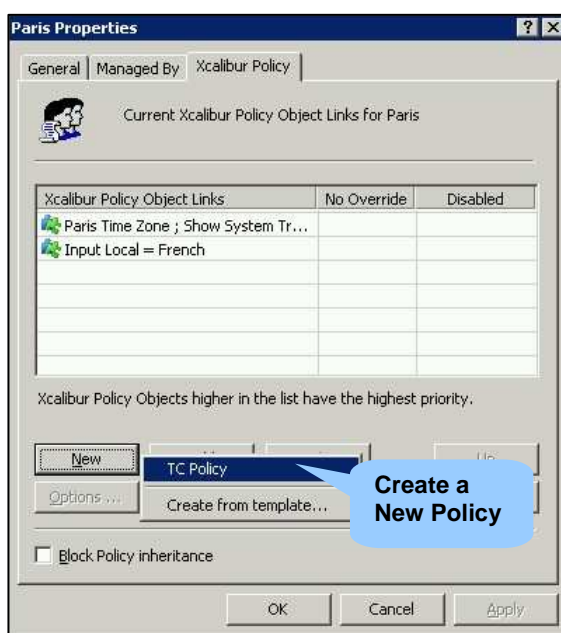
Device Level Policies settings affect only Thin-Client devices. Computer objects stored in the Active Directory are not affected by Xcalibur TC Policies.

User Level Policies settings affect Users only when they logon to a Thin-Client.

Administering Xcalibur Thin-Client Policies

Creating New Xcalibur Policies

Xcalibur Policies are stored in the Xcalibur Database. You can create a new empty Xcalibur Policy or a new template-based Xcalibur Policy and link it to the object that you wish to manage.



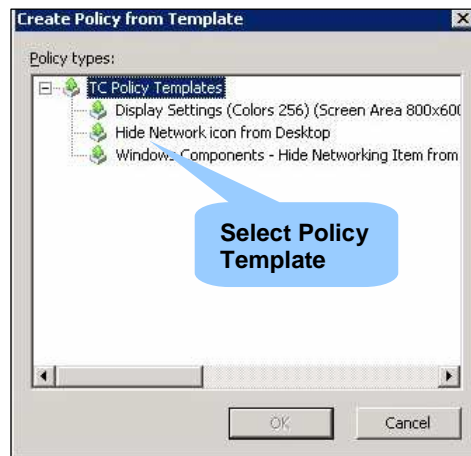
Creating New Xcalibur Policy

- Open the Xcalibur Directory Manager.
- Right click the Domain / Organizational Unit / Device or User for which you want to create an Xcalibur Policy, and then click Properties.
- On the Xcalibur Policy Tab click New, select the TC Policy option, type a name for the new Xcalibur Policy, and then press Enter. The Xcalibur Policy that you created appears in the list of Xcalibur Policies associated with the Domain / Organizational Unit / Device or User you selected.

Creating new Template-Based Xcalibur Policy

- Open the Xcalibur Directory Manager.
- Right click the Domain / Organizational Unit / Device or User for which you want to create an Xcalibur Policy, and then click Properties.
- On the Xcalibur Policy Tab click "New", select the "Create from template..." option.

- From the TC Policy Templates list select your preferred template and press OK.



- Type a name for the new Template-Based Xcalibur Policy, and then press Enter. The Xcalibur Policy that you created appears in the list of Xcalibur Policies associated with the Domain, Organizational Unit, Device or User you selected.

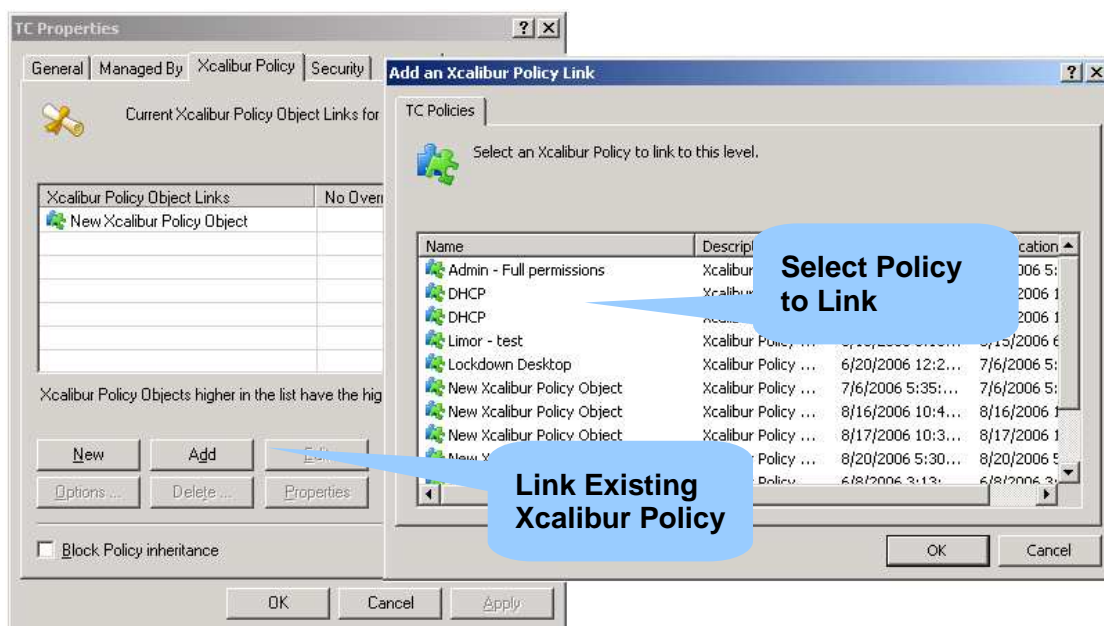
Linking an Existing Xcalibur Policy

You can apply existing Xcalibur Policy settings to additional target objects (Organizational Units, Devices and Users) by linking the Xcalibur Policy that contains the requested settings to those objects. To link an Xcalibur Policy, you must have read and write permissions on the gPLink and gPOptions attributes of the target object.

Linking an Existing Xcalibur Policy:

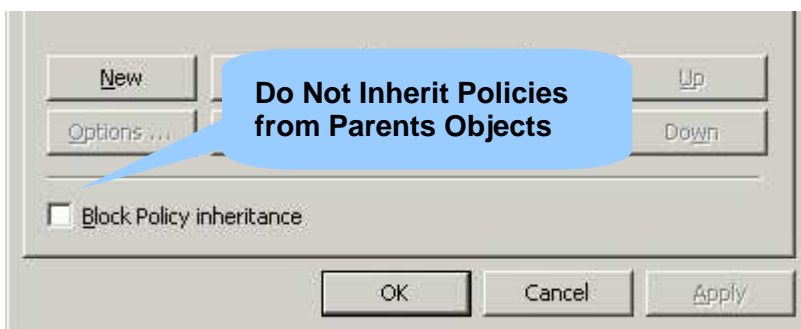
- To link an existing Xcalibur Policy to a Domain, Organizational Unit, Device or User, open the Xcalibur Directory Manager.
- Right click the Domain / Organizational Unit / Device or User that you want an existing policy to be linked to, and then click Properties.
- On the Xcalibur Policy Tab click Add.

- In the All Xcalibur Policy Objects list, click the Xcalibur Policy you wish to link to, and then click OK.



Block Policy Inheritance

Block Policy Inheritance prevents a child object from inheriting all Xcalibur Policy settings from all parent objects. This is useful when an object requires unique policy settings and you want to ensure that settings are not inherited.



To Block Policy Inheritance from effecting an object:

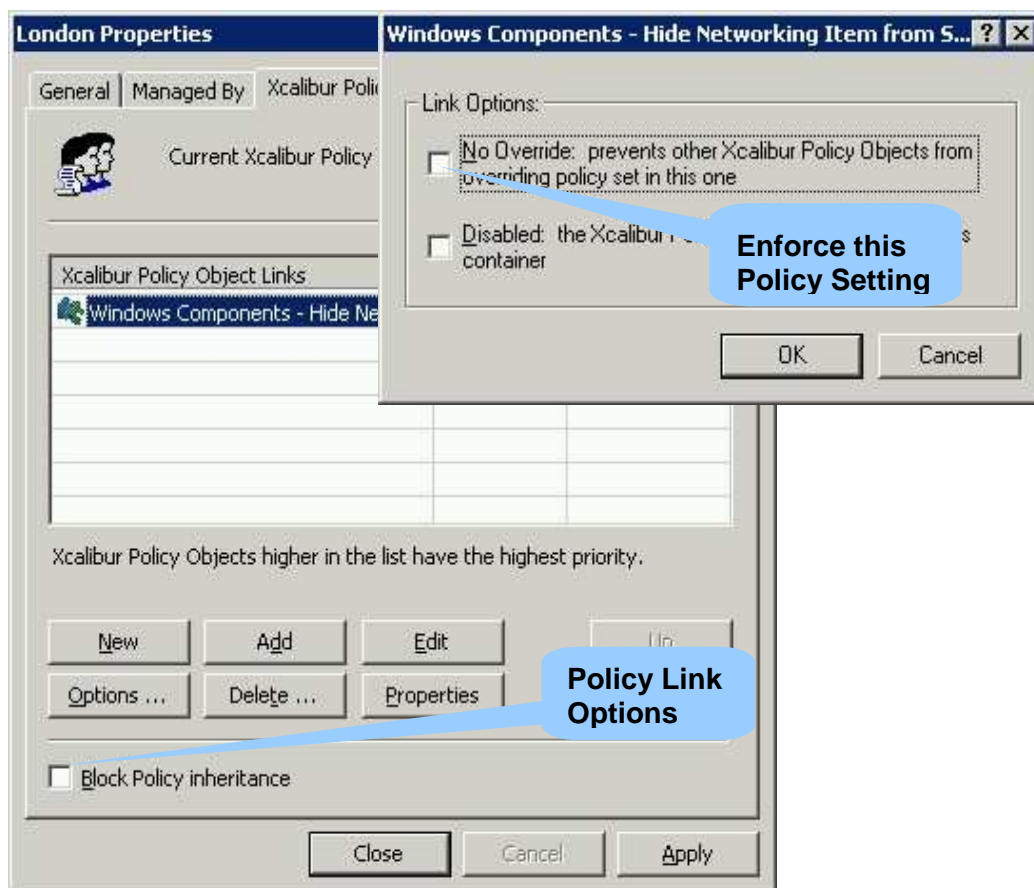
- Open its Properties dialog box.
- On the Xcalibur Policy Tab, select the Block Policy Inheritance checkbox.

Block Policy Inheritance Limitations:

- Once enabled, all parent level policies are blocked.
- Block Inheritance cannot prevent parent level policies that are configured as No Override from applying.

No Override

No Override allows enforcing a policy onto all child objects with no exception. Setting a policy link with the No Override option, ensures that even if this policy conflicts with other policies, or if Block Inheritance is enabled lower in the policy's route, policy settings will be applied.



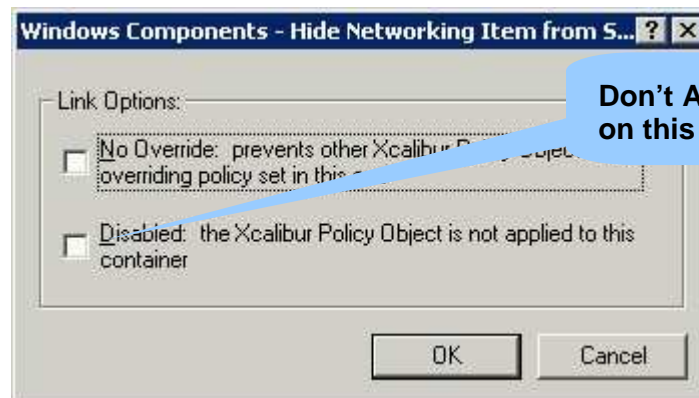
Only critical, corporate-wide, rules should be applied with No Override policies. Remember that No Override policy links take effect regardless of how other policies are set up.

To enable the No Override Option:

- Open the Properties dialog box for the object to which the policy is linked.
- On the Xcalibur Policy Tab, select the policy you wish to set as No Override and then click the Options button.
- In the Options dialog box, select the No Override checkbox and click OK.

Disable Policy Links

Disabling a policy link prevents the selected policy settings from applying on target objects (Domain, Organizational Unit, Device and User). Disabled policy links are displayed under the object's Xcalibur Policy tab but do not take effect. Disabling a policy link prior to editing it is highly recommended. This ensures that target objects will not obtain partial policy settings due to the edit operation.

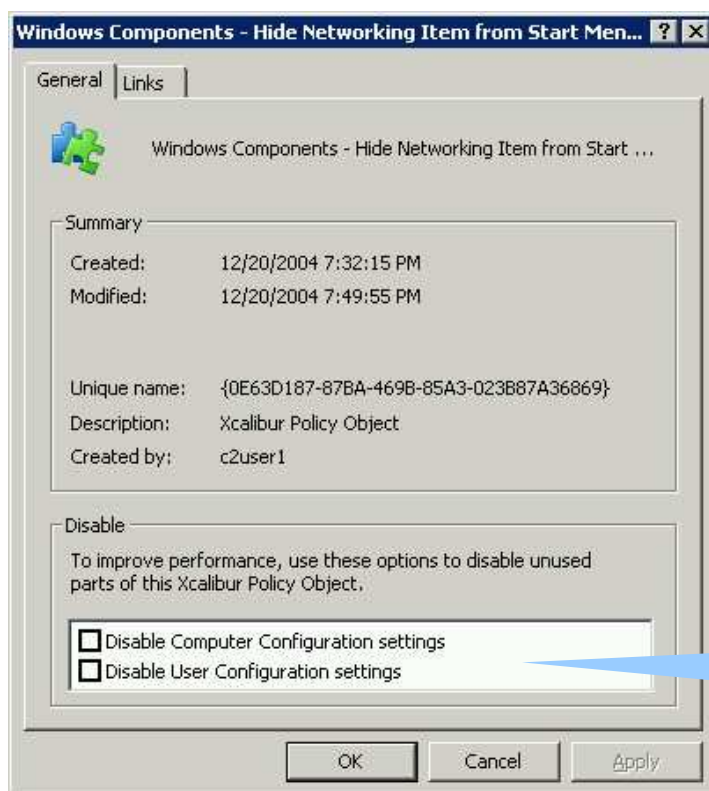


Disable Policy Link:

- Open the Properties dialog box for the object to which the policy is linked.
- On the Xcalibur Policy Tab, select the policy link you wish to disable and then click the Options button.
- In the Options dialog box, select the Disabled check box, click OK and confirm the Disable prompt.

Disable Policy Objects

Disabling an Xcalibur Policy Object prevents this policy from affecting all target objects it is linked to. Therefore in case you disable an Xcalibur Policy Object which is linked to multiple target objects (Domain, Organizational Units, Devices, Users) these will no longer apply the disabled policy settings. For performance improvement, disabling unused policy sections is suggested.



**Disable Policy
Section**

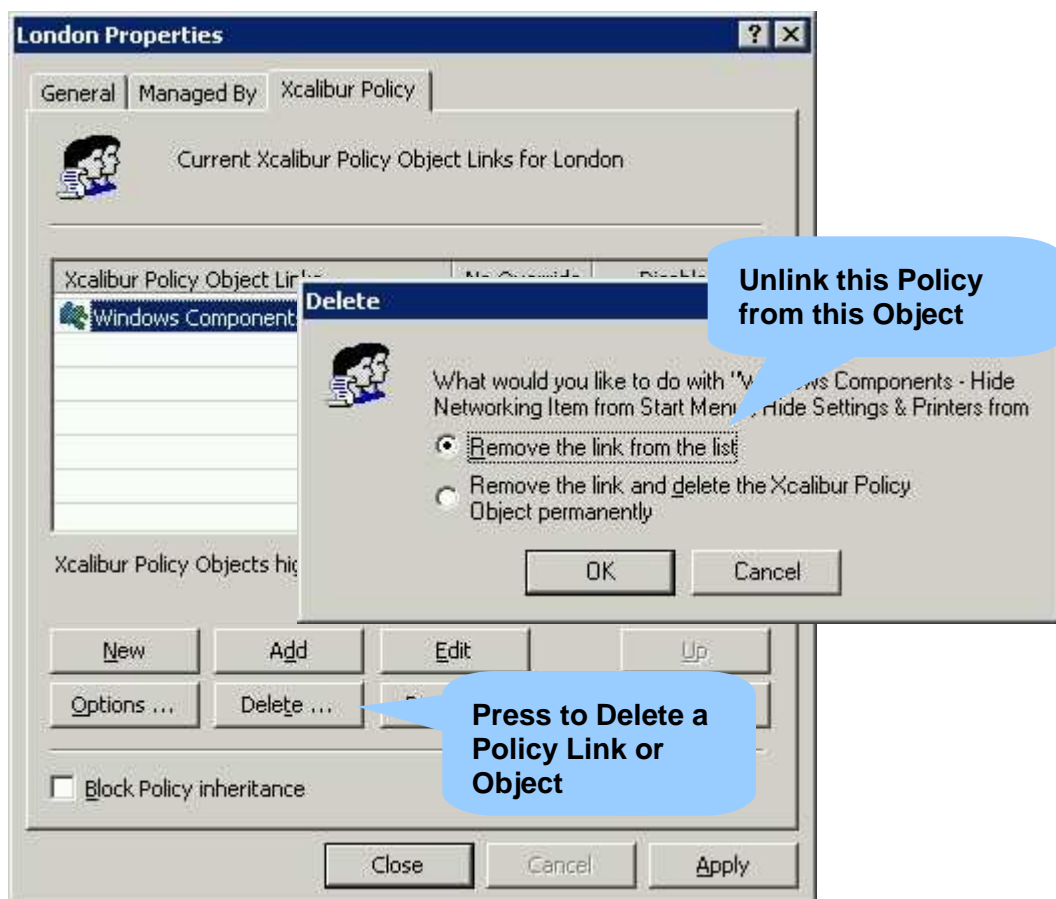
Disable Policy Object:

- Open the Properties dialog box for one of the objects to which the policy is linked.
- On the Xcalibur Policy Tab, select the policy you wish to disable and then click the Properties button.
- In the General Tab, select the Disable Device Configuration and/or User Configuration, click OK and confirm the Disable prompt.

Note Disabling a policy object prevents it from applying wherever linked.

Delete Policy Links

Deleting a policy link from the object it is linked to (Domain, Organizational Unit, Device and User) stops the policy settings from affecting that object. When you no longer want a policy to affect the Domain, Organizational Unit, Device or User, remove the policy link from the Xcalibur Policy Object Links list under that object's properties.



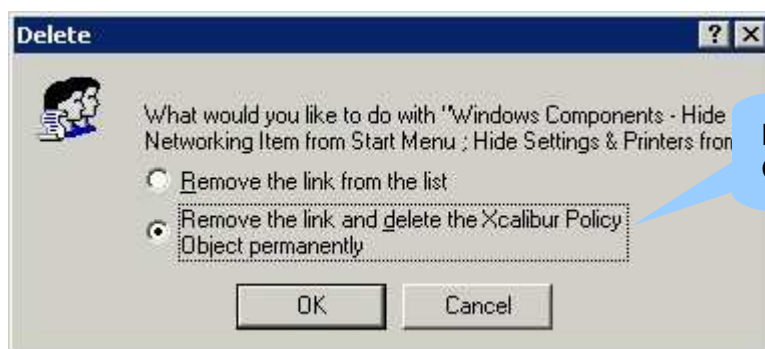
Delete Policy Links:

- Open the Properties dialog box for the object to which the policy is linked.
- On the Xcalibur Policy Tab, select the policy link that you want to delete and then click the Delete button.
- In the Delete dialog box select the Remove the link from the list option and then click OK.

Note Deleting a policy link does not delete the Policy Object from the Xcalibur Database.

Delete Policy Objects

Deleting a policy object removes it from the Xcalibur Database. Once deleted, a policy is moved to the Deleted Policies container which is only viewable to members of the Administrators group. All policy links associated with this policy are removed from the Domain, Organizational Unit, Device or User objects it was linked to.



Delete this Policy Object

Delete Policy Objects:

- Open the Properties dialog box for the object to which the policy is linked.
- On the Xcalibur Policy Tab, select the policy that you want to delete and then click the Delete button.
- In the Delete dialog box select the Remove the link and delete the Xcalibur Policy Object permanently option and then click OK.

Note Deleted policy objects are kept in the database for a limited time period until fully purged.

Only members of the Administrators group can administer deleted policy objects.

Advanced Policy Administration

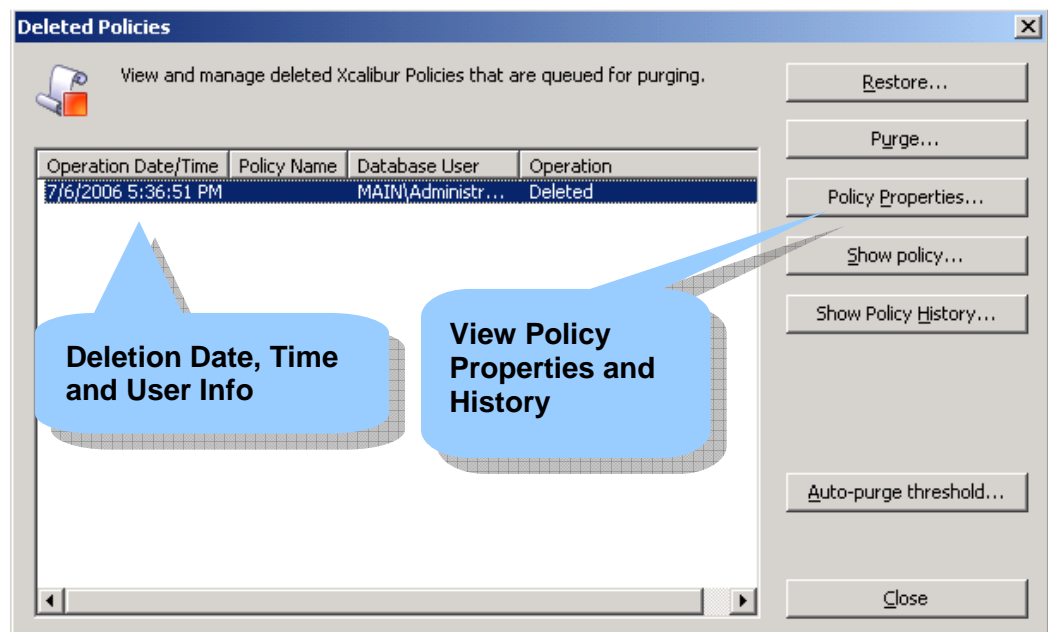
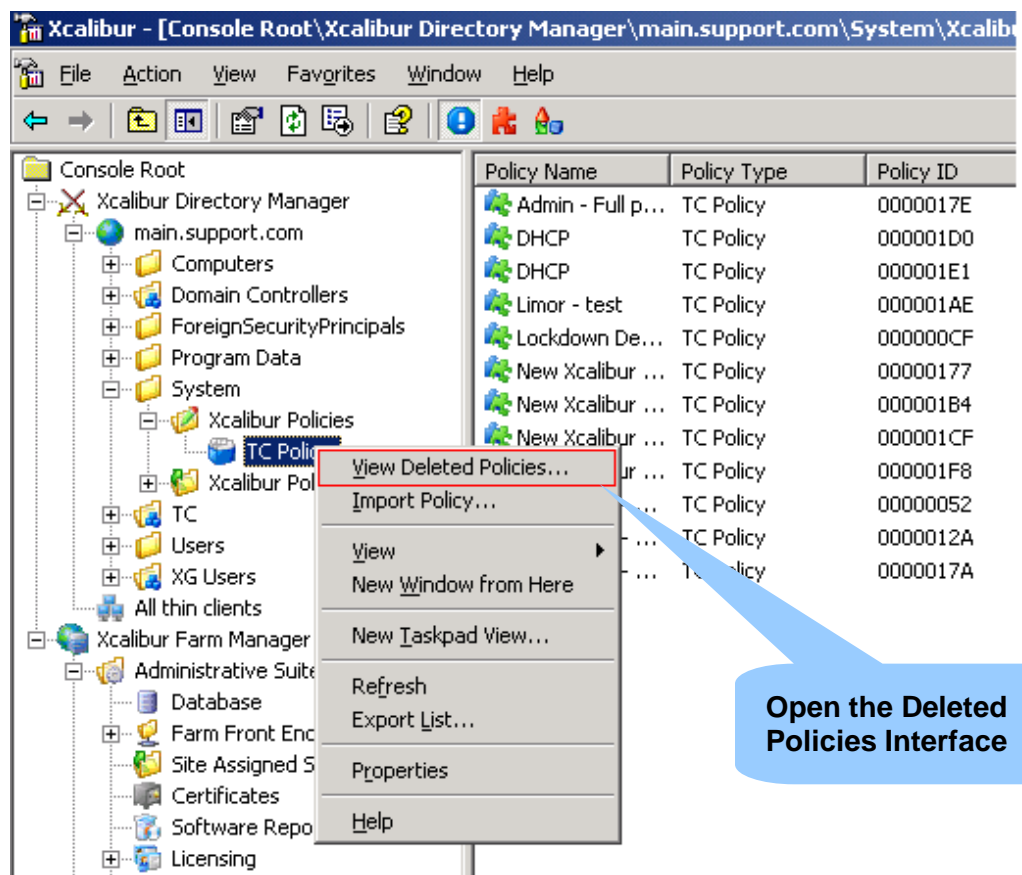
Xcalibur Global provides a number of advanced administration options for optimizing policy administration tasks.

Manage Deleted Policies

Deleted Policies

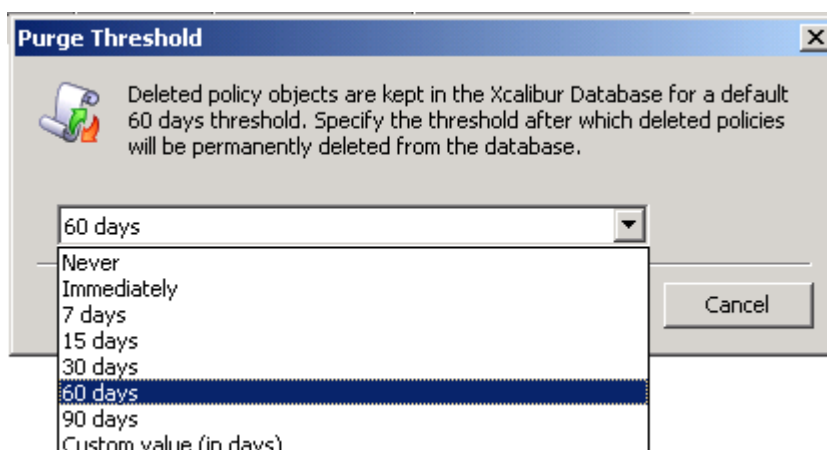
Deleted policy objects are kept in the Xcalibur Database for a default 60 days threshold. During this period members of the Administrators group can view each policy properties and history including the deletion date, time and the deleted user information.

Once the threshold limit is reached, the policy object is permanently deleted from the Xcalibur Database.



To Change the default Auto-purge Threshold:

- Right click the System \ Xcalibur Policies \ TC Policies container and then click View Deleted Policies.
- Press the Auto-purge Threshold button, select your desired threshold period and press OK.



Restore Policy Object

As long as a deleted policy object remains in the Database, it can be restored and then re-linked to any desirable Active Directory level. After completing the Restore operation, the policy object can be linked by following the 'Linking an Existing Xcalibur Policy' guidelines (see page 26).

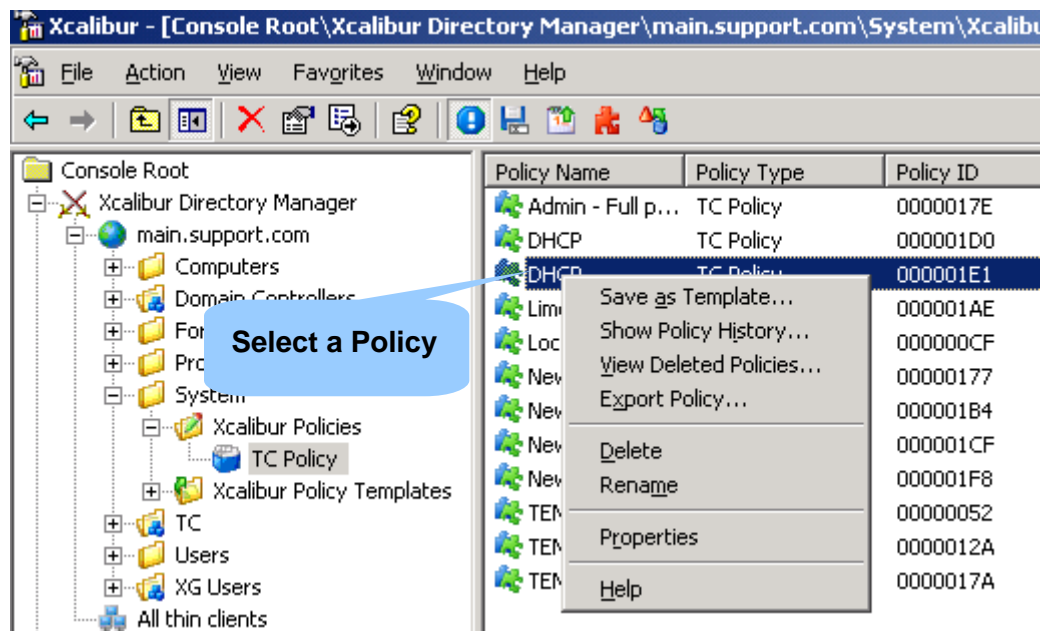
To restore a policy object:

- Right click the System \ Xcalibur Policies \ TC Policy container and then click View Deleted Policies.
- Select the Xcalibur Policy that you want to restore and then click the Restore button.

Create a Policy Template

Policy Templates allow you to save an existing Xcalibur Policy as a starting point for future policies. You can instruct your delegates to use policy templates as their initial framework when creating new policies.

Policy Templates are based on existing policies therefore you need to have at least one Xcalibur Policy in order to create a policy template. Saving an existing policy as a template can be carried out from multiple interfaces including the Policy Editor and the Thin-Client Policy container.



To Create a Policy Template:

- Browse to the System \ Xcalibur Policies \ TC Policy container.
- Select a policy, right click it, and then select the Save as template option.
- On the Save as template dialog box, type a template name and description and press OK.

Export a Policy

Xcalibur Policies can be exported to a *PLS* file (*.pls). In this way policy backups can be created. The export option may be useful when wanting to copy existing Xcalibur Policies between two separated Xcalibur environments. Thus, for example, you can export Xcalibur Polices from your test-environment to your production-environment.

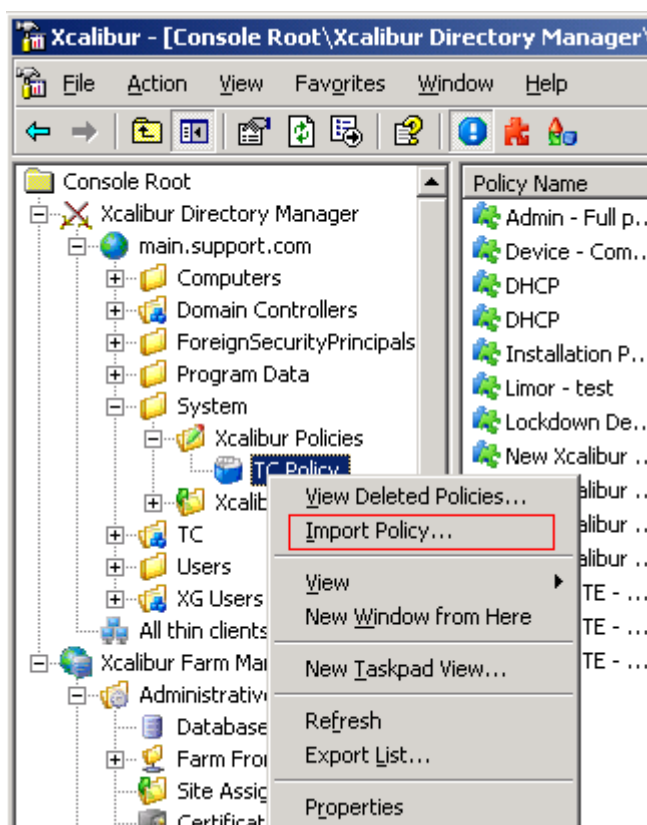
The *Export Policy* option can be carried out from multiple interfaces including the *Policy Editor* and the *Thin-Client Policy container*.

Export a Policy:

- Browse to the System \ Xcalibur Policies \ TC Policy container.
- Select a policy, right click it, and then select the Export policy option.
- On the "Save as: dialog box, type A for the policy file and press OK.

Import Policy

Imported policies are saved into the Xcalibur Database. A new policy object is created for each newly imported policy. Policy links are not importable; therefore an imported policy needs to be linked to destination objects in order to take effect.



Import a Policy:

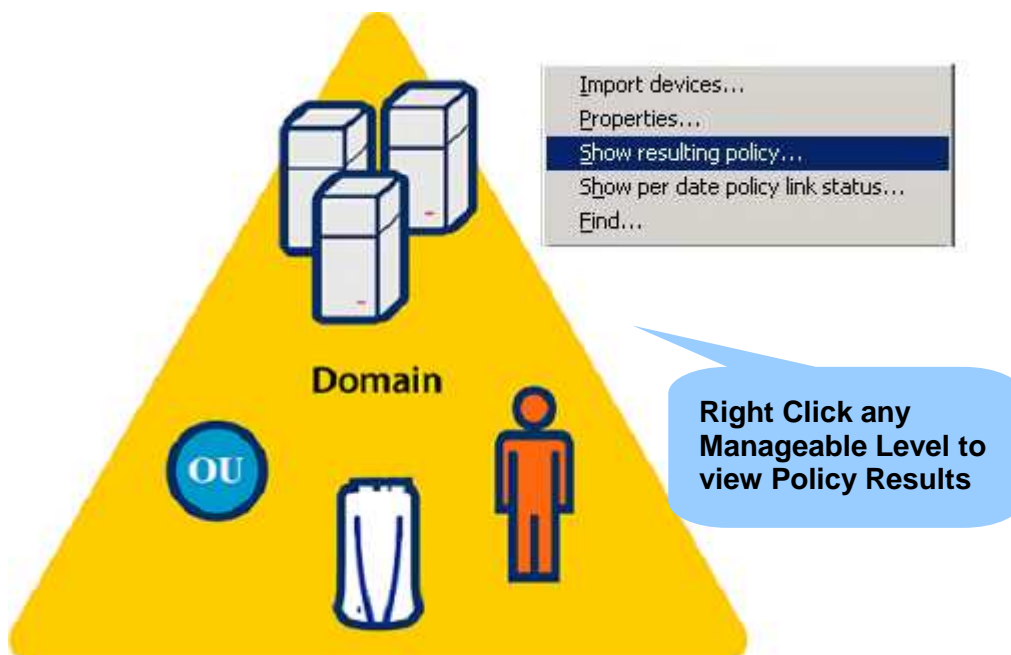
- Browse to the System \ Xcalibur Policies container.
- Right click it and then select the *Import policy* option.
- In the Open dialog box, browse to the folder where you place the *.pls file/s, and press *Open*.

Policy Monitoring Tools

When implementing Xcalibur Policy, in either small or enterprise scale environments, policy monitoring tools are essential for maintenance, troubleshooting and logging.

Proper use of these tools can save time and help you accurately plan your Xcalibur Policy strategy.

Resulting Policy Viewer



The Resulting Policy Viewer tool assists planning and testing Xcalibur Policies.

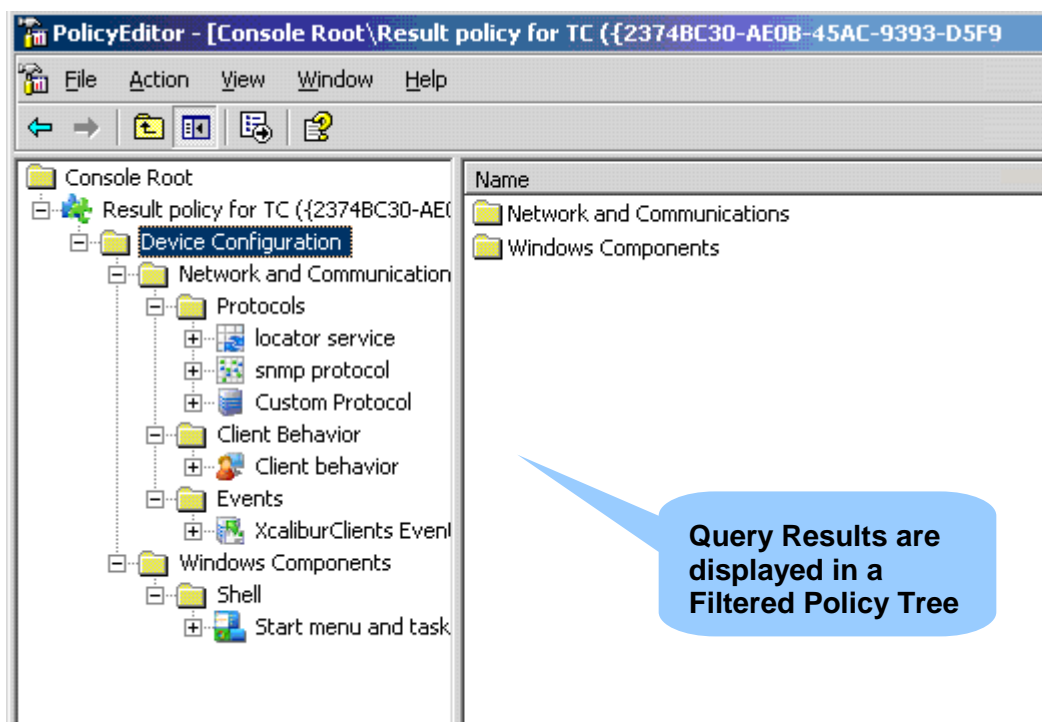
By running it on the Domain, Organizational Unit, Device or User, you can query the Xcalibur Database and find out how Xcalibur Policy settings will apply on an object. It calculates all policy settings while considering policy inheritance and order rules, thus anticipating the final policy results that will affect the target object. The query results are displayed in a filtered Policy Editor interface, so that, only Enabled or Disabled policy settings are displayed within the Policy Tree.

Since *resulting policy* queries are calculated based on policy settings, you can plan and test how Xcalibur Policy affects the Domain, Organizational Unit, Device or User, prior to deploying users and devices in a production environment.

Note In order to run the Show resulting policy viewer tool specific permissions must be in place (to the Active Directory Permissions table).

Resulting Policy Viewer - Domain / Organizational Unit Level

Running the *Resulting Policy Viewer* at the Domain or Organizational Unit level provides a complete picture of how Xcalibur Policy settings apply to this object, allowing you to troubleshoot problems, or plan ahead before applying a new policy on the object, thus avoiding conflicts.

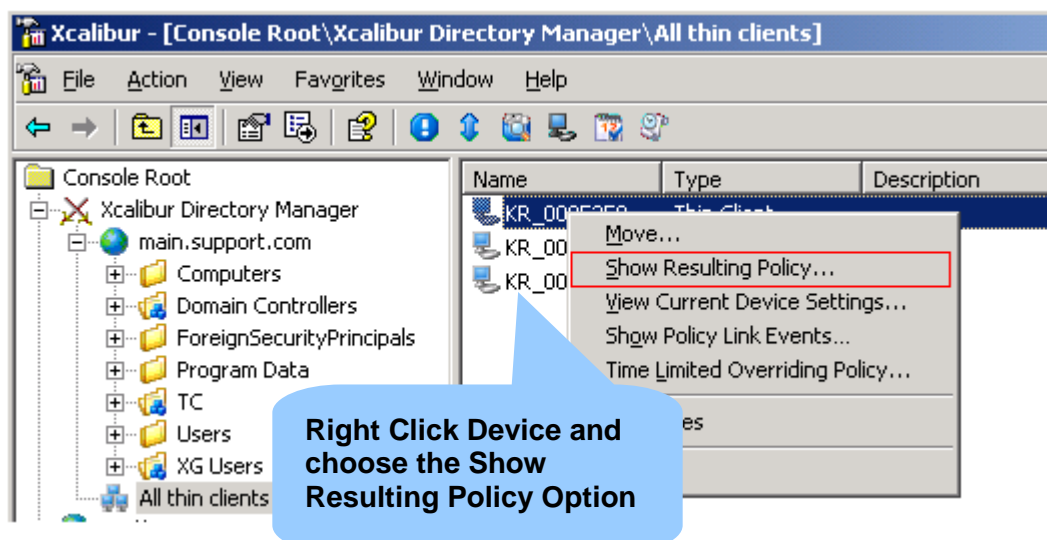


Run resulting Policy Viewer on Domain / Organizational Unit:

- Right click the Domain or Organizational Unit and select the *Show Resulting Policy* option
- The *Policy Editor* displays the policy settings that are applied on the Active Directory level where Resulting Policy was run.

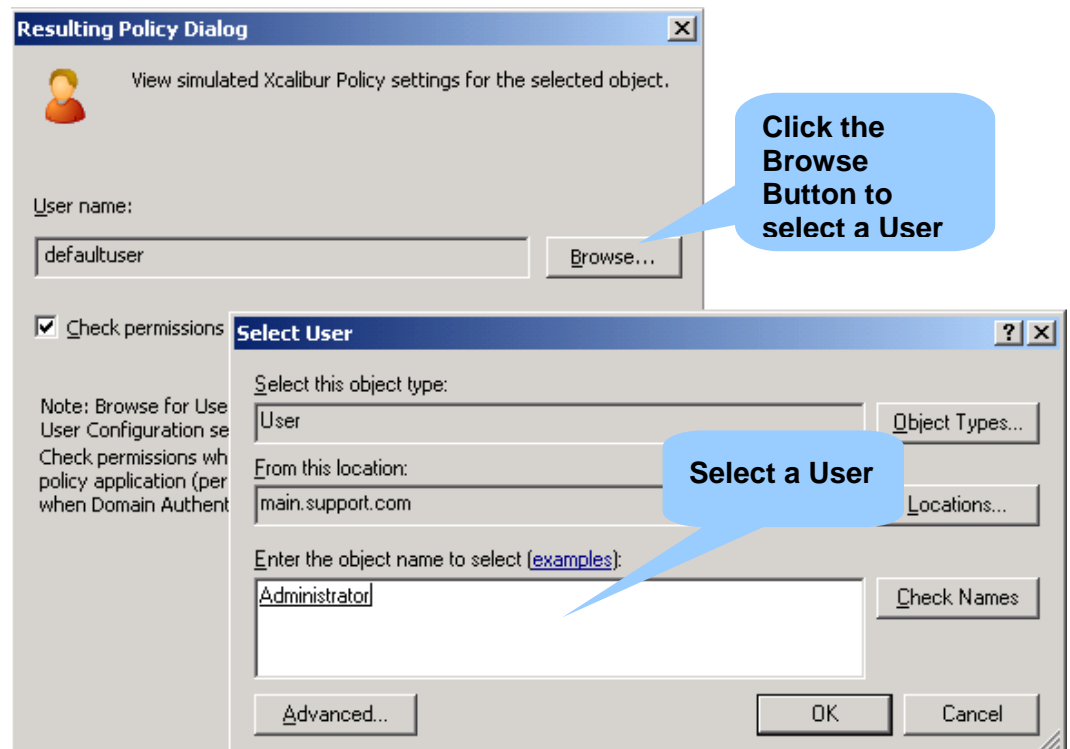
Resulting Policy Viewer - Devices

Running the *Resulting Policy Viewer* at the device level displays both Device and User policy settings that affect the selected device.



Resulting Policy Dialog

When run at the device level, a *Resulting Policy Dialog* prompts you to specify a user name. This way you can simulate how User Level policies (associated with the selected user) affect the target device in addition to Device Level policies.

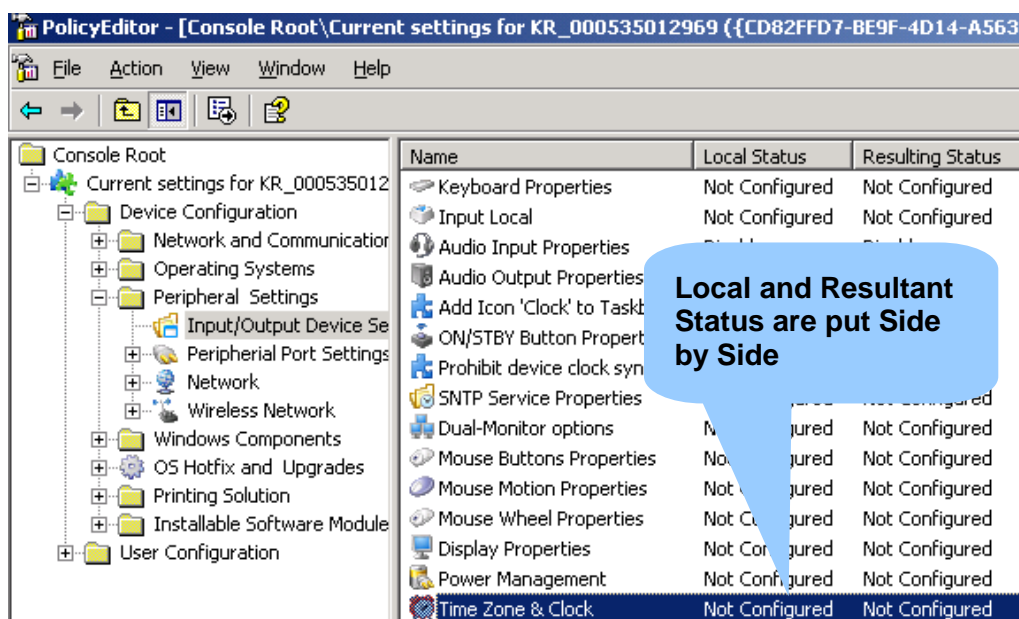


View Current Device Settings

The *Current Device Settings Viewer*, helps troubleshooting and simulating how Xcalibur Policy setting merges with local Thin-Client settings.

View Current Device Settings displays local device information, obtained from the Thin-Client and resultant policy information, obtained from the database, under the same interface thus providing administrators a complete picture of the Thin-Client status in a single view. Knowing the local Thin-Client settings before and after Xcalibur Policy application helps better understanding and troubleshooting Thin-Client management and Xcalibur Policy.

The query results are displayed in a Policy Editor interface showing all Policy Tree sections. Local device status is displayed under the Local Settings column while under the Resulting Status column, resultant settings are displayed. This way you can see whether local settings were affected by an Xcalibur Policy



To View Current Device Settings

- Right click the Thin-Client that you want to query, choose *Current Device Settings*.
- When the *Policy Editor* appears, right click the Policy Settings you wish to display.

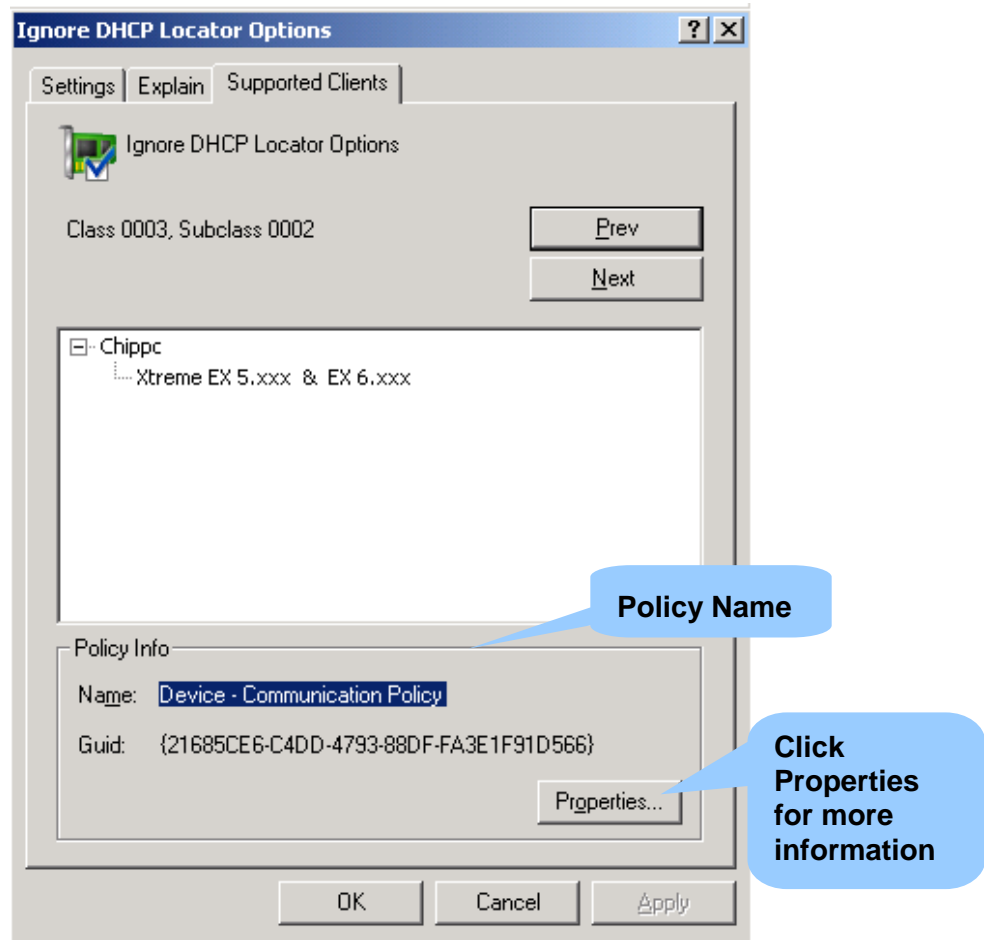
Enable Current Device Settings View

By default, Current Device Settings information is sent from the client device to Xcalibur. Once connected to Xcalibur, every device reports its local settings by sending a "Device Settings Event" to Xcalibur. This information, stored in the Xcalibur database, is used to enumerate the "Local Policy" when running the View Current Device Settings utility.

In order for the *Current Device Settings* to be viewed make sure that the *Disable Device Setting Event* policy option is **not Enabled**.

Find which policy takes affect

Knowing which policy takes affect helps planning future policies and troubleshooting.



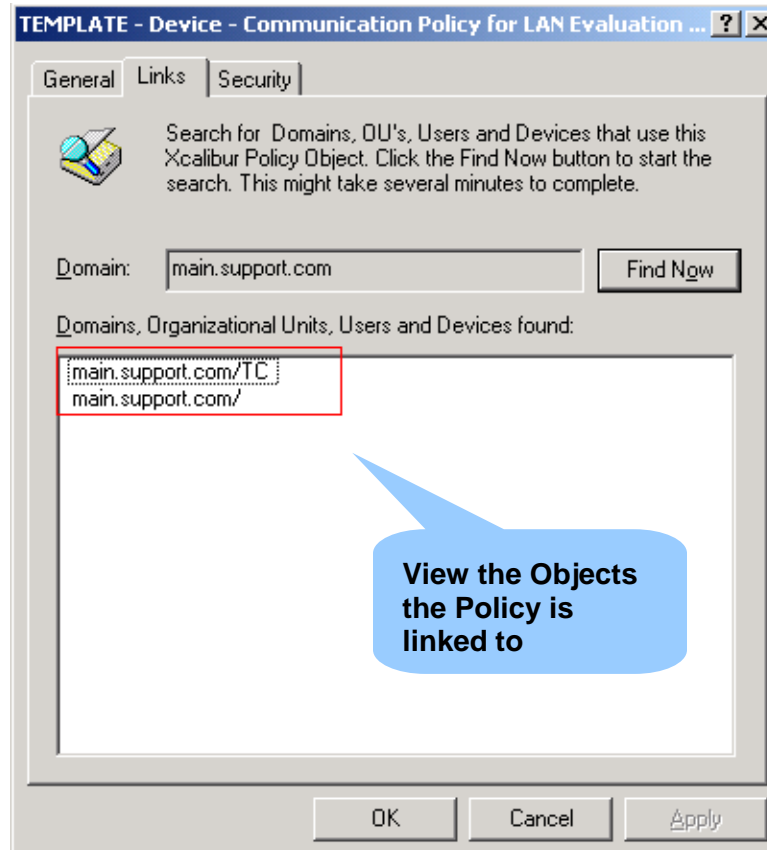
When running the View Resulting Policy /or/ View Current Device Settings tool, you can find the policy name that changed a specific setting.

- In the *Policy Editor* on the right-hand panel choose a policy item to review, right click it and select the *Settings* option.
- Go to the *Supported Clients* tab, in the *policy Info* rubric view the name of the policy.

Once finding the policy name you can find where it is linked to by entering the policy properties.

View Policy Links

Knowing to which objects a policy is linked to allow understanding from where a device / user get their settings.

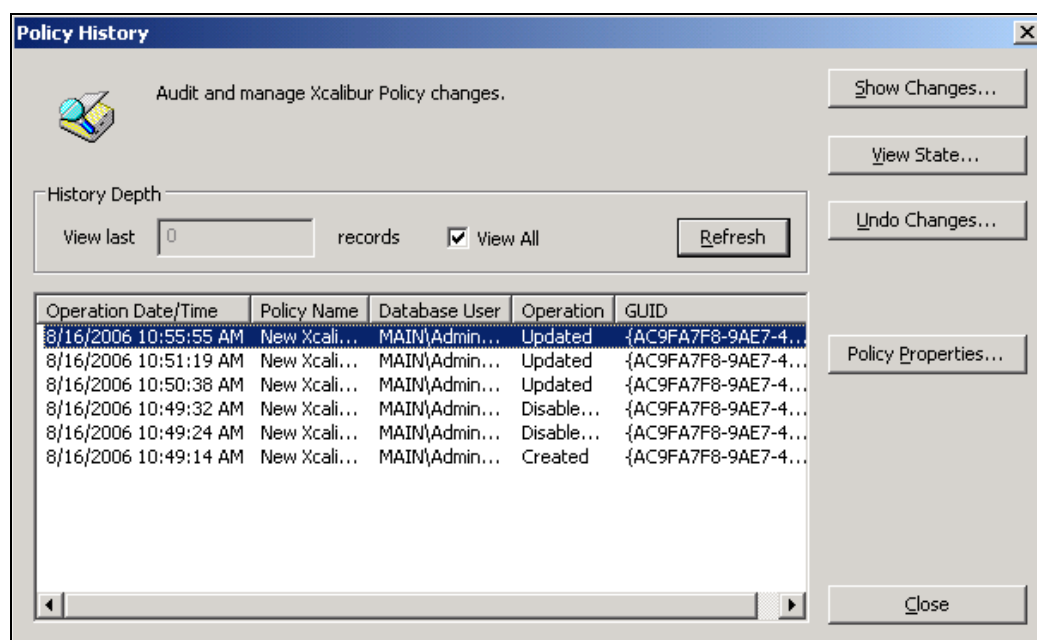


- From the policy item's *Settings* choose the *Supported Clients* tab and click on *Properties*.
- Choose the *Link* tab to view the objects his policy is connected to.

Policy History Viewer

The Policy History Viewer allows monitoring, auditing and managing Xcalibur Policy Objects.

Once creating an Xcalibur Policy Object, all operations that are related to that policy are logged into the Xcalibur Database. Each operation's date & time, type, and originating user information is displayed by the main interface. Additionally you can view the policy settings before and after every change, as well as, undo the changes.



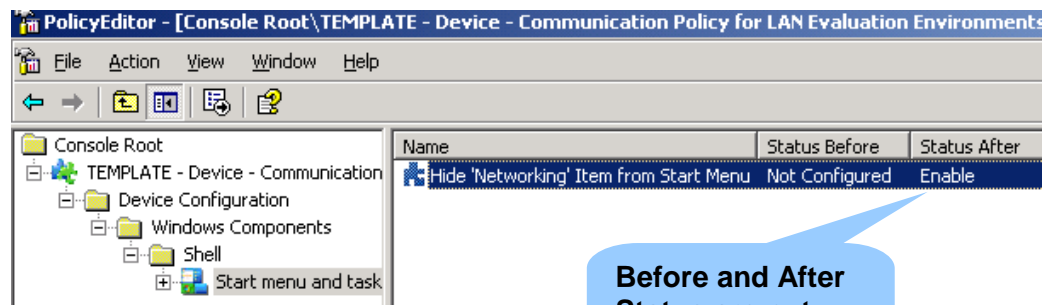
Initializing the Policy History Viewer can be carried out from multiple interfaces including the Policy Link properties-menu and the TC Policy container.

Policy History Viewer:

- Browse to the System \ Xcalibur Policies \ TC Policy container.
- Select the Xcalibur Policy that you want to monitor, right click it and then select the Show policy history option.

Show Changes

Changes to the Policy Object are displayed in a filtered Policy Editor interface. This means that only changed policy settings are displayed within the Policy Tree. An Update operation for example, can contain multiple actions therefore sorting the search by date & time is the (default) preferred sort option.



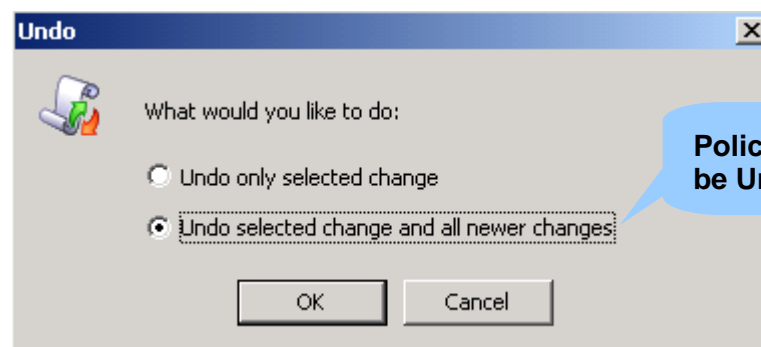
**Before and After
Status are put
Side by Side**

Track Policy Changes:

- Open the Policy History Viewer.
- Sort the display according to your desired search criteria (Date & Time / action type / originating user).
- Select the operation from the list and then press the Show Changes button.

Undo Changes

Changes made to a policy can be reversed, if needed a policy can be either changed back to "original" settings prior to the new changes made to it, or have only specific changes "undone"



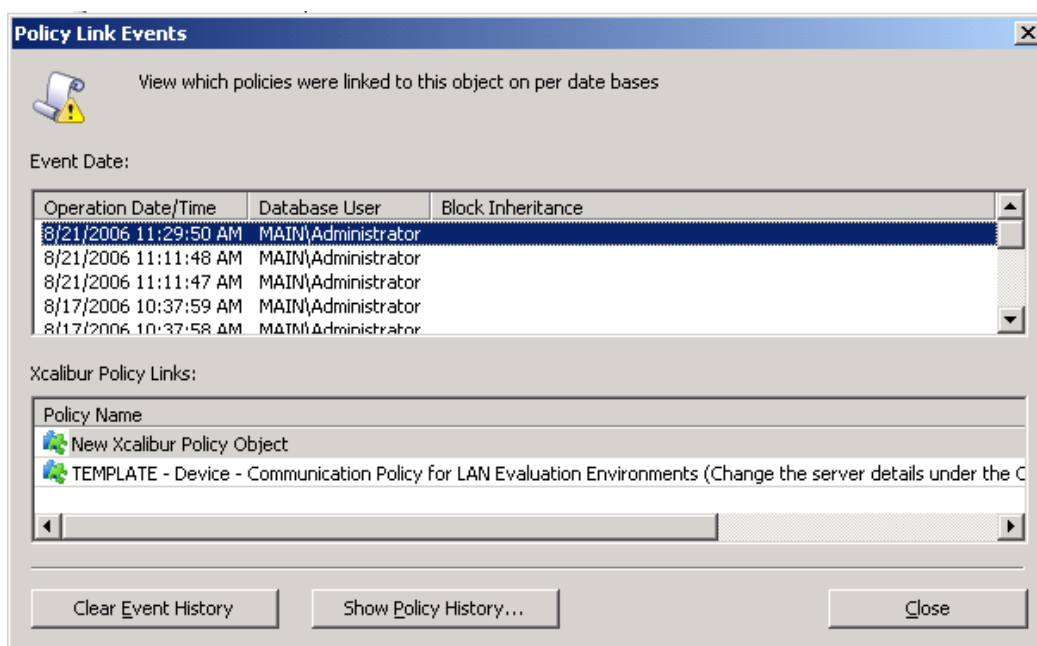
**Policy Changes can
be Undone**

Undo Changes to a Policy:

- Select the operation that you want to undo from the list and then press the Undo Changes button.
- Undo selected change and all newer changes: Reverts the policy to its state before the selected change. All changes done after this operation will be undone.
- Undo only selected change: Clears only the selected change while not modifying newer changes.

Policy Link Status Viewer

The Policy Link Status Viewer shows which policies were linked to an object on per date bases. By running it on the Domain, Organizational Unit, Device or User you can query the Xcalibur Database and find out which Xcalibur Policies were linked to an object at specific dates. This auditing tool can help resolve and understand policy conflicts. It also indicates which user linked each policy to the selected object.



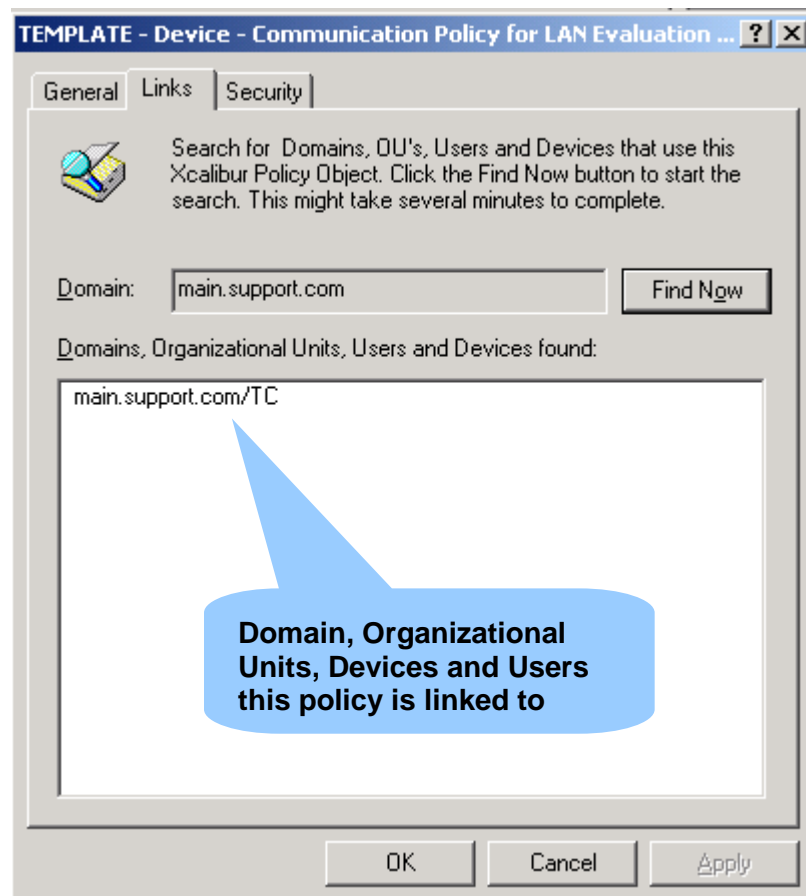
- View Policy Links
- All Policies & Templates (Advanced view\System)
- Monitoring Policy History, Changes etc'.
- Resulting Policy
- Real Time Policy

Open Policy Link Status Viewer:

- Right click the Domain / Organizational Unit / Device or User object.
- Select the Show per date policy link status option from the menu.
- Once selecting a date from the upper window frame, all policy links that were linked to the selected object at that date are displayed in the lower window frame.

View Current Policy Links

In order to know to which Domain, Organizational Unit, Device or User a Policy is currently linked to, use the Links Tab. A single Xcalibur Policy can be linked to multiple objects. Therefore prior to modifying a policy, you should check where it is linked to. The Links Tab can be found under each Policy Properties. The policy Properties can be accessed from multiple interfaces including the TC Policy container and the Xcalibur Policy Tab.



View Current Policy Links for Policy:

- Open the Properties dialog box for that Policy.
- Select the Links Tab.
- Press the Find Now button to refresh the links display.

Policy Application

Policy Updater

Through the Farm / Site / IP Scope properties -> Policy Updater Tab, you can control when Device and User Policies apply on client devices.

When set to Always (this is the default option) Device and User policies apply according to the rules below. Changing the default Policy Updater options lets you specify on which time and day policies should apply. This is useful when you do not want policy changes (which in most cases trigger a device reboot) to interfere with users work.

Device Policy:

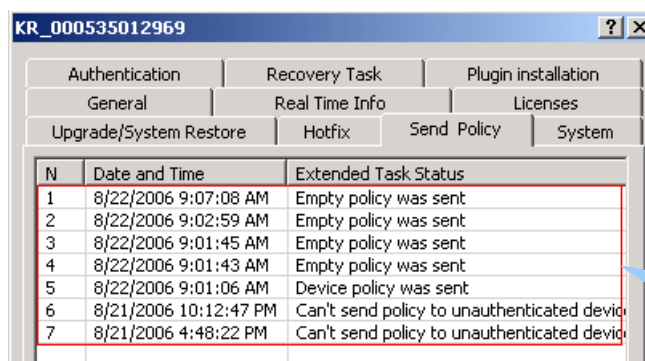
Xcalibur Policy settings for Devices apply on Thin-Client accounts according to their assignment in the Active Directory tree. Device Configuration settings initially apply during the Thin-Client boot and then refreshed according to a specified refresh interval (Alive Event Period).

User Policy:

Xcalibur Policy settings for Users apply once users logon to Thin-Clients managed by the Xcalibur. User Configuration settings are applied during the user's logon.

Monitoring Policy Application

On the Xcalibur Farm manager from within each client's properties, you can monitor application of policies for device and user through the Send Policy Tab.



N	Date and Time	Extended Task Status
1	8/22/2006 9:07:08 AM	Empty policy was sent
2	8/22/2006 9:02:59 AM	Empty policy was sent
3	8/22/2006 9:01:45 AM	Empty policy was sent
4	8/22/2006 9:01:43 AM	Empty policy was sent
5	8/22/2006 9:01:06 AM	Device policy was sent
6	8/21/2006 10:12:47 PM	Can't send policy to unauthenticated device
7	8/21/2006 4:48:22 PM	Can't send policy to unauthenticated device

**View Policy
Application
Status**

Client Side Policy Caching

To reduce bandwidth taken by policy application, the last policies applied on the Xtreme PC device are automatically cached. At specific intervals, the device queries Front End servers for policy updates. When policies have changed or when new policies have been created, the changed policy settings are sent to the device. If there has been no change to the policy since the last check, no additional traffic is generated since no policy changes are sent to the client. Policy caching also assures that administrative restrictions take effect even when a device temporarily loses communication with the Front End Server.



This page is left blank intentionally.

Chapter 4 Farm Manager

Objectives

Get familiar with the Xcalibur Farm Manager MMC snap-in. Understand the Farm, Site and Scope Structure and permissions. Understand Thin-Client deployment and shadowing.

Physical Management Module

General:

Through the Xcalibur Farm Manager snap-in administrators can control the physical aspects of Thin-Client management in the organization.

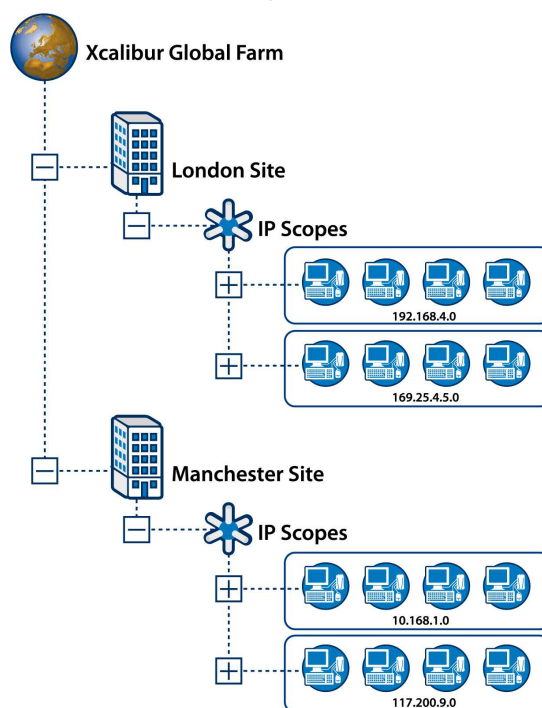
One of the Farm's main roles is to allow settings defined under the logical Xcalibur Directory Manager interface apply on target devices and users while considering network limitations, such as bandwidth.

Second level Xcalibur Sites can be created under the Farm to represent company branches. Sites allow grouping together Front End servers according to their physical location and/or the physical location of their clients, in order to reflect the physical layout of the company's infrastructure.

This allows the group to share common configuration and settings that can be administered centrally.

IP Scopes define the site boundaries. Thin-Clients are dynamically assigned to a site once their IP Address falls within an IP Scope.

IP Scopes allow further customizing sites by specifying unique settings at an IP Scope level. This allows different settings to be applied to groups of devices based on which scope their IP address belongs to.



The Xcalibur Farm Features

The Xcalibur Farm allows:

- Mapping the organization's physical network layout by creating Sites that stand for branches and IP Scopes that stand for the IP Address ranges, used in every branch.
- Delegating administrative rights on per Farm and Site bases.
- Manage Front End Servers, Thin-Clients and Users.
- Control device maintenance and security services.

Xcalibur Farm Management Permissions

In order to view the Xcalibur Farm contents and perform administrative tasks you must have adequate permissions. As default, members of the Authenticated Users group are assigned with Read permission while Domain Admin members have Full Control.

The following table describes the minimum permissions required for performing administrative tasks within the Xcalibur Farm Manager snap-in.

Farm Task Description	Required Permission
■ View Xcalibur Farm Objects and Settings	■ Read All Farm Data
<ul style="list-style-type: none"> ■ Add / Remove Software ■ Add / Remove Sites ■ Update Farm Information 	<ul style="list-style-type: none"> ■ Read All Farm Data ■ Write all Farm Data
■ Site Task Description	■ Required Permission
■ View Site Objects and Settings	■ Read Site Data
<ul style="list-style-type: none"> ■ Add / Remove IP Scope ■ Add / Remove Server 	■ Write Site Data
■ Advanced Force Deletion	■ Delete Devices when Parent OU is missing

Inheritance Options

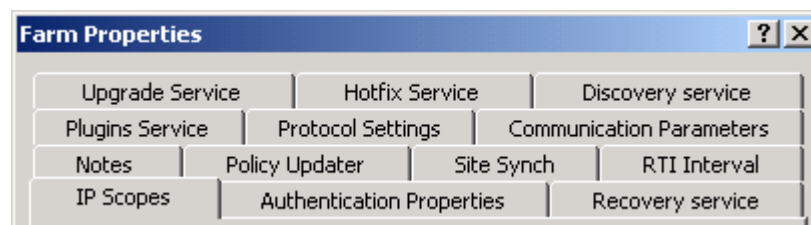
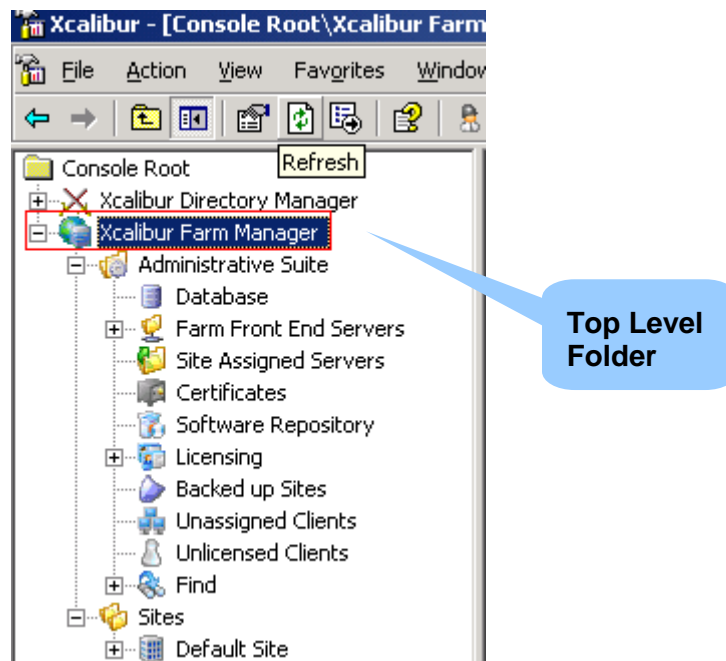
The Farm, Site and IP Scope are the three main management levels of the Xcalibur Farm. As default, top level settings are inherited by lower levels. Therefore, settings specified under the Farm automatically apply on the Site and IP Scope. Inheritance options can be disabled under the child object properties.

Xcalibur Farm Manager Snap-in Description

General:

This section shortly describes each container's role under the Xcalibur Farm Manager MMC snap-in.

Xcalibur Farm Manager

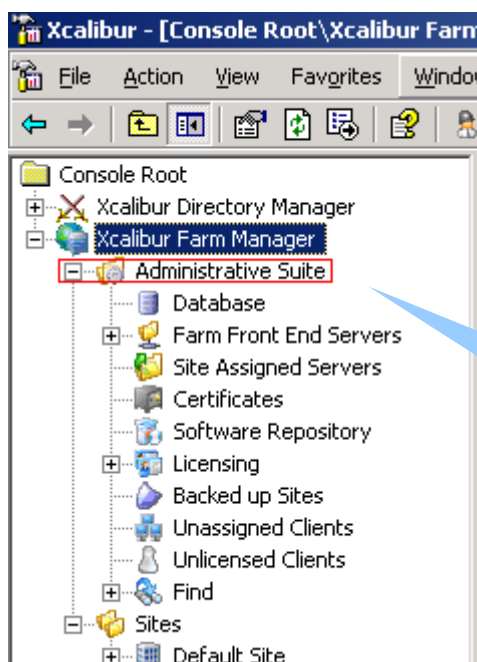


The Xcalibur Farm object is the root of the Xcalibur Farm structure.

Under its properties you can manage the following:

- Installation, maintenance, discovery and authentication services.
- Set client communication parameters such as the maximum number of clients that can connect to the farm.
- Set farm administration permissions.
- Initiate the Network Topology Import utility.

Administrative Suite



**Groups Common
Management Interfaces**

The Administrative Suite group's common management interfaces. It is used as a central point of administration for the following:

Database:

The Database container provides information regarding the database, such as Type, Size, connections etc'.

Farm Front End Servers:

This container holds all Front End servers that belong to the farm.

Site Assigned Servers:

This container displays all Front End Servers allocated to a specific site.

Certificates:

Centrally view and manage certificates for Xcalibur use.

Software Repository:

Centrally view and manage software packages

Licensing:

Centrally view and manage Client, Server and software licenses

Backed up sites:

Collects sites where front end servers fail to service clients

Unassigned Clients:

Collects thin clients who does not fall into any IP Scope address range.

Unlicensed Clients:

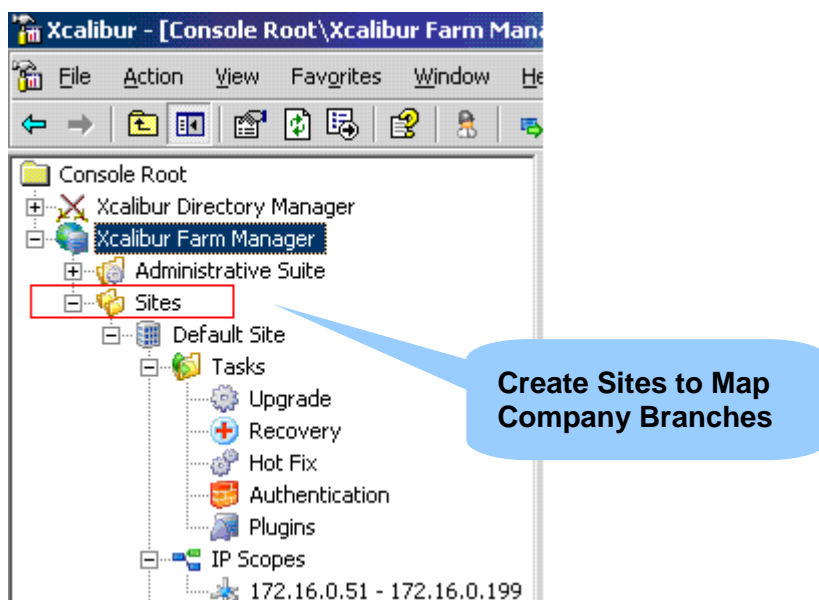
Collects thin clients that does not have Xcalibur client license

Find:

The Find container displays a Central view of defined search results.

Sites

This container provides a centralized view of all the sites belonging to the organization. A site is a logical object representing a branch office or a remote location. Under each site you will find the following containers:



- **Tasks:**
Allows site administrators to monitor different activities such as, Firmware Upgrade, Plug-in Installation, Client Recovery and more.
- **IP Scopes:**
Specify rang of IP addresses to create a scope within the Site.
- **Front End Servers:**
This container groups Front End Servers belonging to this site.
- **Clients:**
This is a centralized view of all clients from all scopes belonging to this site.
- **Users:**
Displays the list of users who are logged on to Thin-Clients in this site.



This page is left blank intentionally.

Chapter 5 Thin-Client Deployment and Discovery

Objectives

Understand how to Deploy and Manage Thin-Clients through Xcalibur Global.

Thin-Client Deployment

Deploying Thin-Clients involves planning of the following elements:

- Thin-Client Discovery
- Xcalibur Independent Management Protocol (XIMP) settings
- Thin-Client Device Authentication
- Policy Application

Thin-Client Discovery

Thin-Client Discovery is the process of establishing an initial connection between the Thin-Client and the management server.

In any communication scenario, client devices must be configured with communication parameters in order to successfully connect to their destined management servers. These parameters can be obtained in various ways including DHCP and SNMP. Initially these include the management server's IP Address, Plain port number, SSL Port Number and SNMP Community name.

Locator Service and Xcalibur Server List

Once configured with the initial communication parameters, the client attempts to connect to a management server as defined by its Locator Service settings. The Locator Service is a client side interface that consolidates and combines the communication parameter information obtained from all available sources, such as SNMP, DHCP, DNS and Xcalibur Policy, into a single list called the Xcalibur Server List.

The client device follows the list order from top to bottom in other words, it tries to connect to the first server in the list and if that fails it tries the second server, and so on until connection is established.

As a starting point, the Xcalibur Server List should reflect the link costs and connection priorities by placing the lowest cost connection at the top of the list. In most cases the Site Front End Server will be approached first then the Farm Front End Server address.

Note Although client devices can obtain the Xcalibur Server List from multiple sources (e.g. DHCP / SNMP / Xcalibur Policy / DNS) you do not have to use them all. Having more than a single source for the Xcalibur Server List provides redundancy while increases the management overhead

Ways to Discover Client Devices

Clients can obtain the Xcalibur Server List in the following ways:

- DHCP: During boot (if configured to use DHCP) the device is capable of obtaining the Xcalibur Server List from a DHCP Server that is set with the corresponding Standard / Vendor class options.
- DNS: During boot the device queries the DNS server (specified under its TCP/IP Properties) for the following name: XCGLOBAL11
- SNMP: Initiate a network scan using SNMP protocol from Xcalibur Front End Server.
- Manual: Locally configure the Xcalibur Agent on the client device with one or more Xcalibur Server addresses.
- Xcalibur Policy: once initially discovered, by the methods mentioned above, a device can be configured with a list of servers using Xcalibur Policy

DHCP Configuration for Vendor Class Options

Scope Options		
Option Name	Vendor	Value
163 Xcalibur Server List	ChipPCv70	192.168.7.20, 192.168.7.30
164 SNMP Community	ChipPCv70	xcalibur4
166 Plain Port Number	ChipPCv70	917
167 SSL Port Number	ChipPCv70	918

**Settings for
ChipPCv70 Vendor
Class**

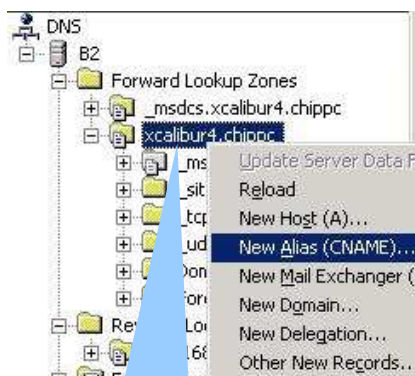
What to configure under the DHCP

Configure the following under your DHCP to provide Thin-Clients with the communication parameters:

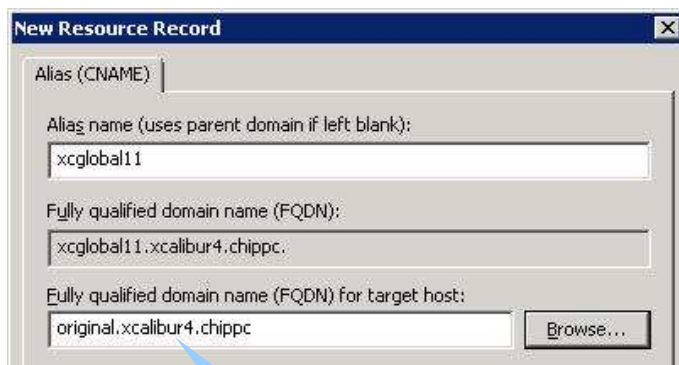
- Create a new Vendor Class named: ChipPCv70
- Set the following predefined options under the 'ChipPCv70' Vendor Class:
 - Option ID 163: Xcalibur Server List (IP Address Array)(Type the IP Addresses of your Front End Servers)
 - Option ID 164: SNMP Community Name (String)(The default value is: xcalibur4)
 - Option ID 166: Plain Port Number (String)(The default value is: 917)
 - Option ID 167: SSL Port Number (String) (The default value is: 918)

Map Xcalibur Server Name to DNS

Use a CNAME (Alias) record to map your Front End Server to the name XCGLOBAL11.



Right click your
DNS Domain and
Select "New Alias"



Map the Alias name
(xcglobal11) to the
FQDN name of your
Front End Server

What to configure under the DNS*

On a Windows Server 2003/8 DNS Server complete the following:

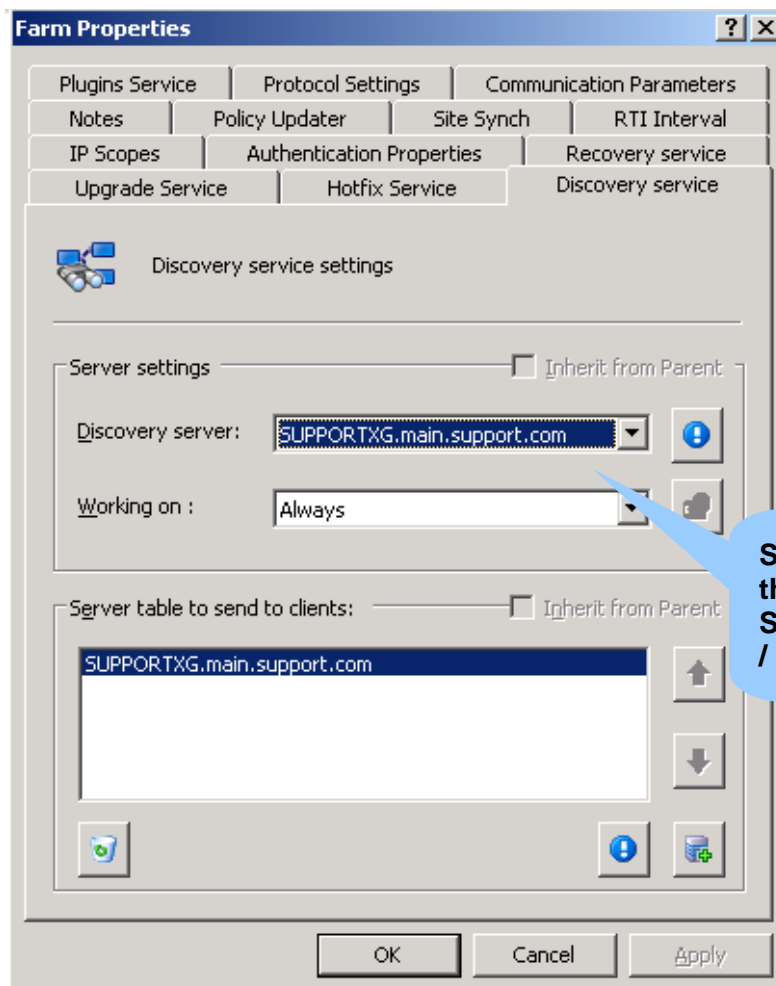
- Open the DNS Management Console
- Right click your Forward Lookup DNS Domain Name (in the example: xcalibur4.chippc).
- Select the New Alias (CNAME)...option from the context menu.
- In the New Resource Record window \ Alias name box, type: xcglobal11
- In the Fully qualified domain name (FQDN) box, type (or Browse) the server name that is running the Xcalibur Global Front End Server component. (in the example: original.xcalibur4.chippc).
- Repeat this process, if necessary, to map all your Front End servers to this name.
 - In case multiple servers are mapped to the same name, the DNS (as default) will perform round robin to balance between them.

Note For a non-Microsoft DNS configuration refer to your DNS vendor specifications.

Discovery Service Settings (SNMP)

The Discovery Service scans the IP Address ranges defined by IP Scopes, discovers Thin-Clients and configures them with an IP Address List of management servers (Xcalibur Server List).

This service configurable under the Farm and Site levels can simultaneously run only on one Front End server at a certain time to prevent setting mismatch.



Farm Properties

Plugins Service | Protocol Settings | Communication Parameters

Notes | Policy Updater | Site Synch | RTI Interval

IP Scopes | Authentication Properties | Recovery service

Upgrade Service | Hotfix Service | **Discovery service**

Discovery service settings

Server settings ☐ Inherit from Parent

Discovery server: **SUPPORTXG.main.support.com**

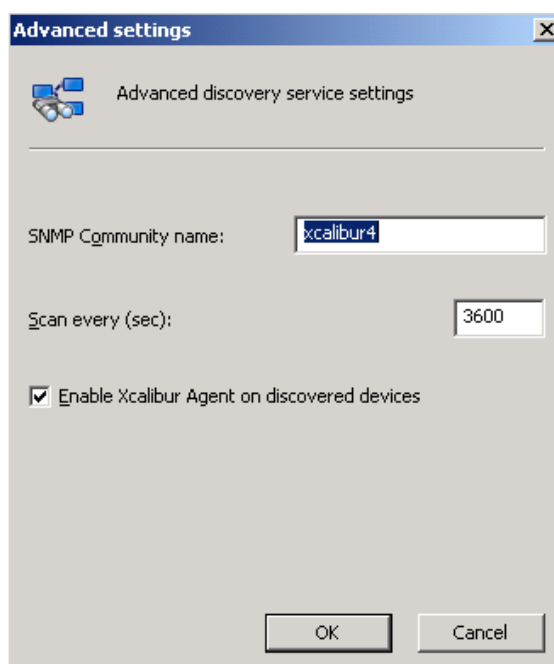
Working on : **Always**

Server table to send to clients: ☐ Inherit from Parent

SUPPORTXG.main.support.com

OK Cancel Apply

Set Conditions for the Discovery Service at the Farm / Site Level

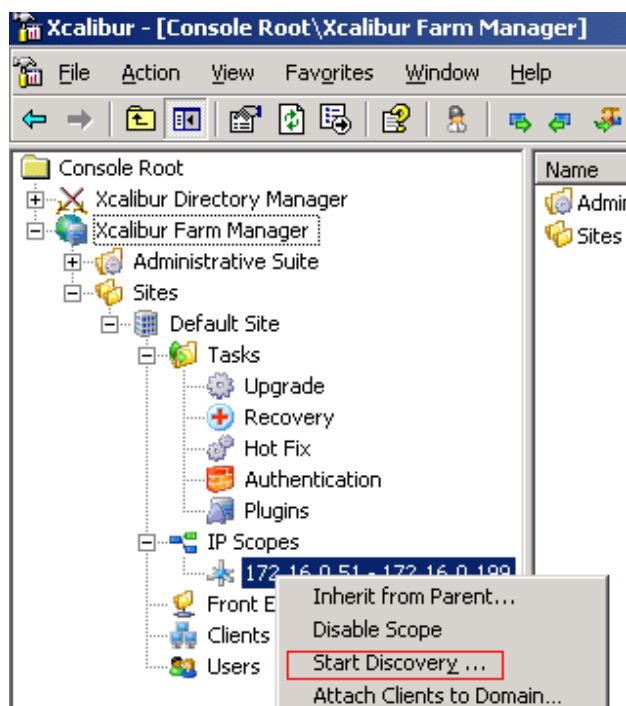


Discovery Service Configuration:

- From the Xcalibur Farm Manager, right click the Farm / Site and then click Properties.
- From the Discovery Service Tab specify the following:
 - Server Running the Service: From the dropdown menu select the Front End server that will be running the Discovery Service.
 - Working on: specify whether the service is constantly active or set to work during specific schedules.
 - Working Hours: Specify when the service becomes operational (e.g. Off-Work hours / Midnight...etc)
 - Always: The service constantly scans the network.
 - Manual Permission: The service runs only once manually triggered.
- Advanced Settings: Press the Advanced button to set:
 - Community Name: Specify SNMP community name, the default is: xcalibur4 (Lower case - case sensitive).
 - Timeout between Discovery Cycles: Specify the delay between one scan to another, the default is: 3600 seconds (1 Hour).
 - Enable Xcalibur Agent on discovered Devices: Sends a command that enables the service responsible for Xcalibur communication on the scanned devices.
- Server Table to send to Clients: Press the Add Server button to create a list of servers that will be sent to the scanned clients. Set server priority by using the Up / Down arrows. High priority servers should be placed at the top of the list.

Manually Trigger a Discovery:

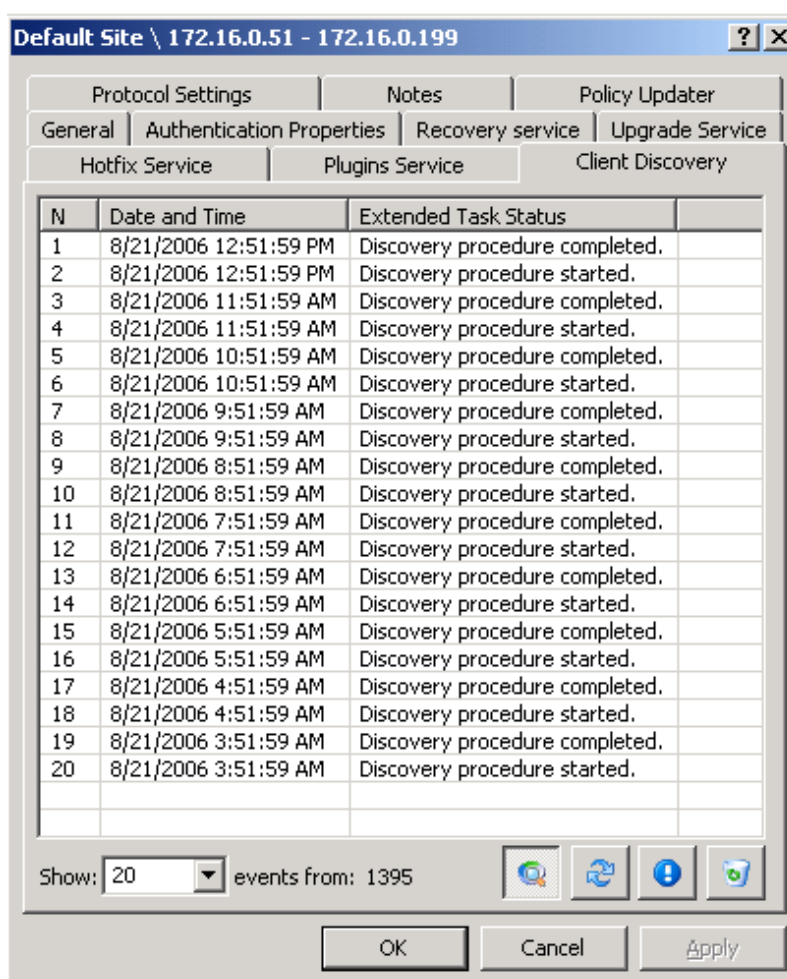
- Right click the IP Scope that covers the IP Address range that you want to scan.
- Click the Start Discovery option.





Viewing Discovery Results:

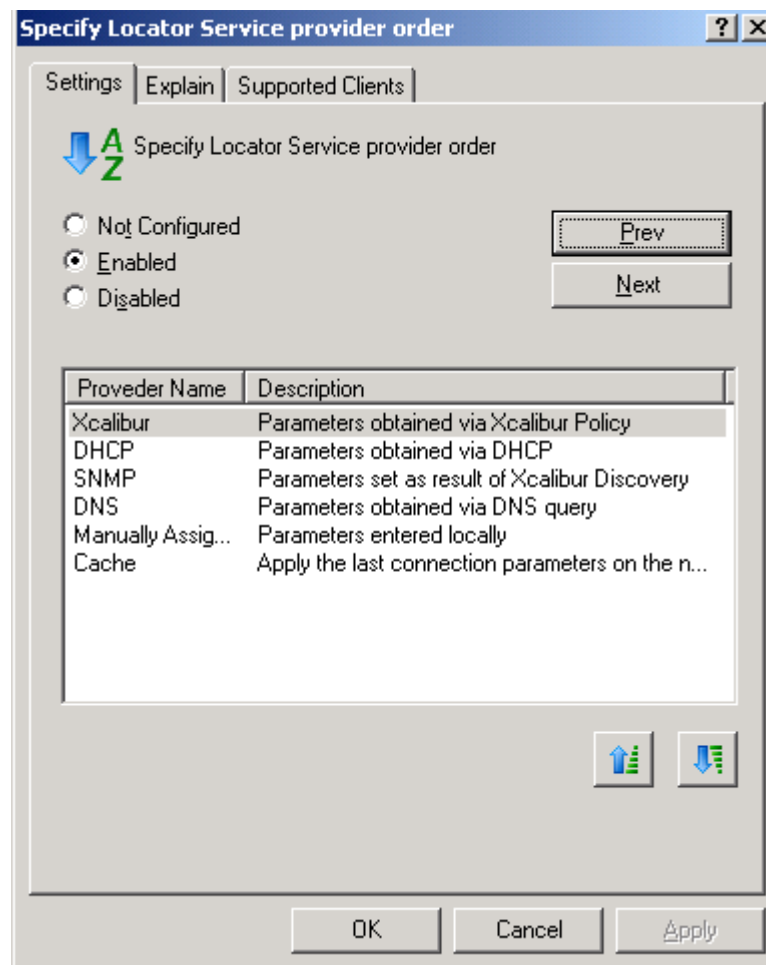
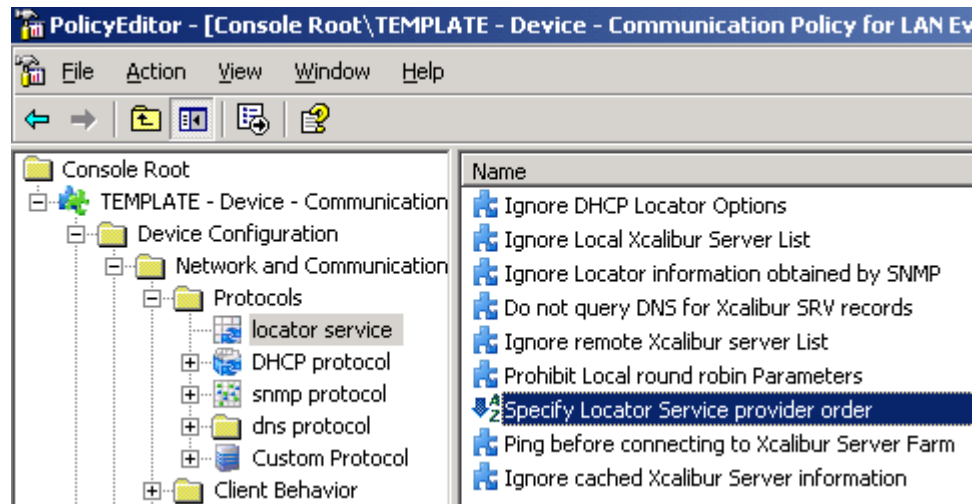
- From the Xcalibur Farm Manager, expand the Sites container, right click an IP Scope and then click Properties.
- Select the Client Discovery tab to view a list of all the clients that responded to the Discovery process.



Using Xcalibur Policy to Configure the Locator Service

An Xcalibur Policy can be created in order to filter the Xcalibur Server List sources which affect Thin-Clients.

Additionally sources can be prioritized according to “weight” through the Locator Service Provider Order settings.





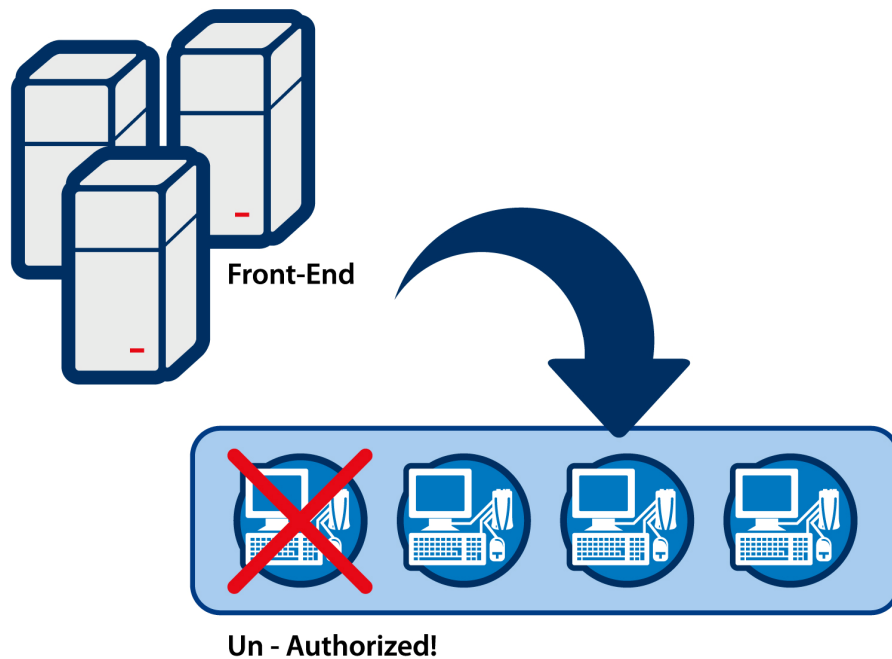
How to configure the Locator Service through Xcalibur Policy:

- From the Xcalibur Directory Manager, Create a new Xcalibur Policy
- In the Policy Tree expand the Device Configuration \ Network and Communications \ Protocols \ Locator Service container.
- In the right view pane, select the option that you want to configure and then double click it to enter its properties.
- Enable this policy to apply the selected settings.



This page is left blank intentionally.

Chapter 6 Device and User Authentication



The Xcalibur management system has built-in device and user authentication mechanisms. This ensures that only authorized (registered) Thin-Clients and users can be connected to the system.

Various rules and settings can be applied on both unauthenticated and authenticated devices and users, allowing administrators to strictly distinguish between them while managing both.

A device is considered to be authenticated once its MAC Address is registered in the Xcalibur database and it is assigned to one of the Active Directory Organizational Units.

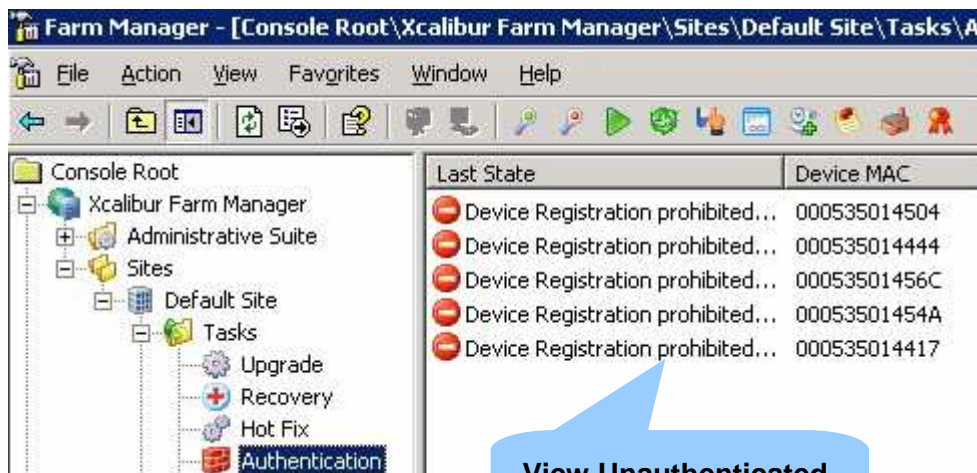
Once authenticated, device settings are changed as defined by the Xcalibur Policies that are linked to its location in the Active Directory tree.

A user is considered to be authenticated once his/her credentials are validated in front of the domain. Once authenticated, User Level policies which are linked to the user's account location in the Active Directory tree, affect the logged on device.

Authentication settings are specified from the Xcalibur Farm Manager snap-in and can be set at the Farm, Site and IP Scope levels. As default, child object settings are inherited from parent levels. Therefore settings defined under the Farm affect all Sites and settings defined under the Site affect all IP Scopes that belong to that Site.

Once inheritance is disabled, settings from the level which is closer to the device override higher levels.

Device Authentication Advantages



View Unauthenticated Device Queue



Unauthenticated Thin-Clients are blocked until Authenticated

Block new devices until authorized:

As default, Xcalibur is set to block unauthenticated devices. Once an unknown (unauthenticated) device has been recognized, the Xcalibur management system will lock it. It will remain locked until it has been unlocked by an authorized user. Unauthenticated devices are queued under the Farm \ Site \ IP Scope \ Tasks \ Authentication container.

Increased Security:

Device authentication allows you to have full control over your Thin-Client devices making sure that only authorized devices are used and preventing unrecognized / foreign device usage.

Asset Management:

- Device Mapping: Device authentication maps all the Thin-Clients in the Xcalibur system. You can know exactly which devices are being used and what is their physical whereabouts.
- Control spare device usage: By isolating and blocking spare-devices from other devices, you get better control over you assets assuring that spare merchandise is not used without permission.

Thin-Clients Authentication

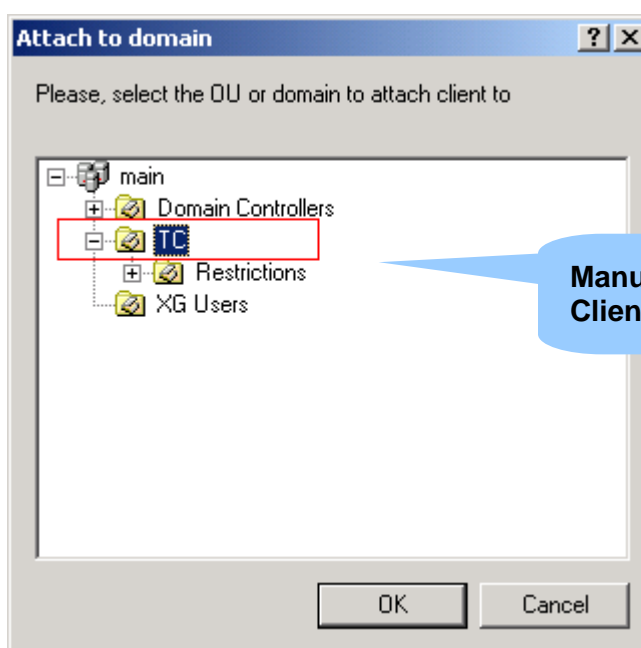
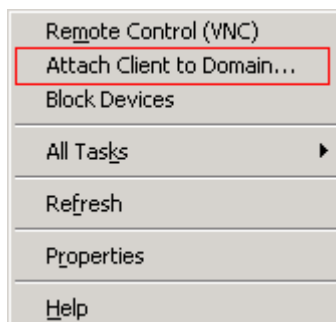
There is a variety of authentication mechanisms that can be used for Thin-Client device authentication. This section covers the Pending Device Accounts, Preconfigured Device Accounts, Default Device Authentication Provider and the Domain Based Device Authentication mechanisms.

Pending Device Accounts

In this method, new unauthenticated devices which are grouped under the Farm \ Site \ Tasks \ Authentication container can be manually authenticated by an authorized user.

Once an Xcalibur Administrator adds a device to the domain, it is authenticated and therefore becomes ready for use.

Last State	Device MAC	Last Report Time	IP Address
Device Registration prohibited...	000535014504	3/9/2005 11:33...	192.168.7.130
Device Registration prohibited...	000535014444	3/9/2005 11:33...	192.168.7.146
Device Registration prohibited...	00053501456C	3/9/2005 11:33...	192.168.7.147
Device Registration prohibited...	00053501454A	3/9/2005 11:33...	192.168.7.148
Device Registration prohibited...	000535014417	3/9/2005 11:33...	192.168.7.149

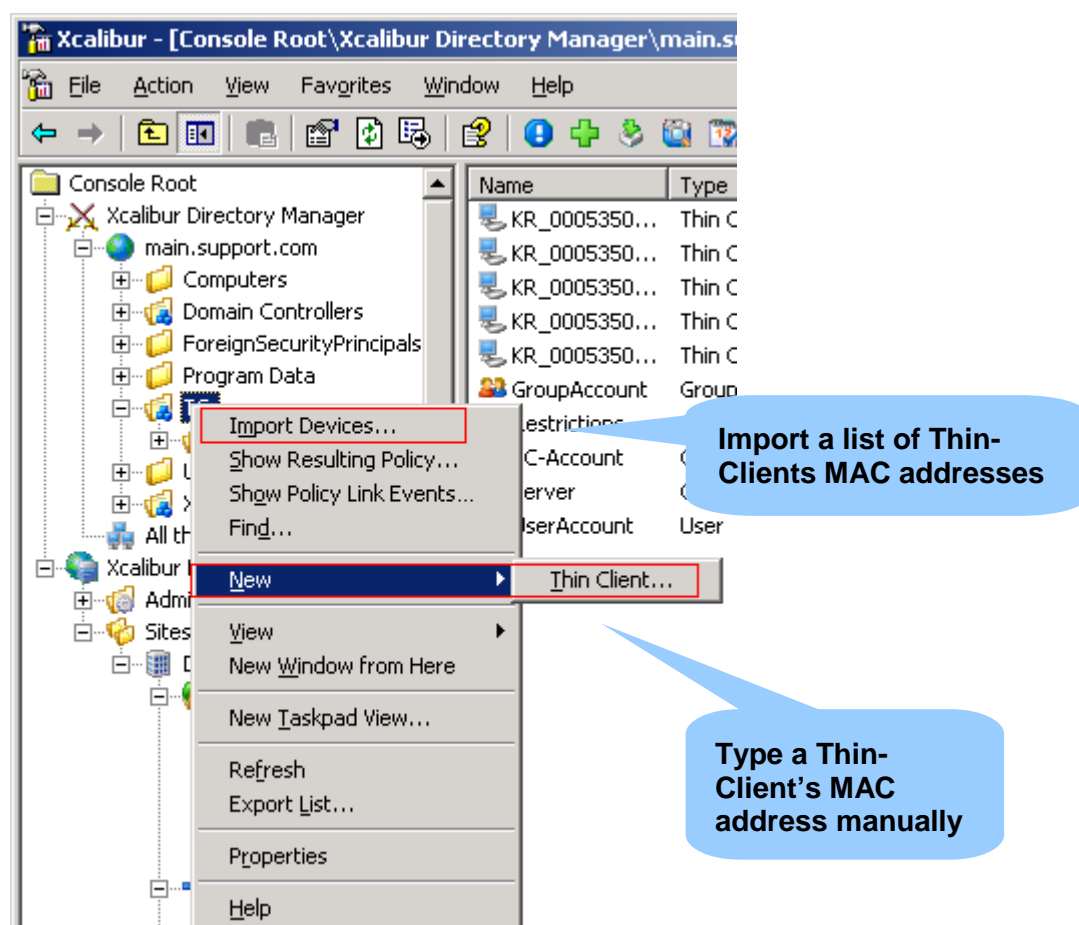


Manually attach pending devices to the domain:

- From the list of unauthenticated devices viewable under the Farm \ %Site name% \ Tasks \ Authentication container, select the Thin-Clients that you want to authenticate.
- Right click the selected clients and then press the Attach Client to Domain...option.
- In the Attach to domain...window, browse for the Organizational Unit where you want the client accounts to reside, and then press OK.
- Once authenticated, the selected devices reboot and are then ready for use.

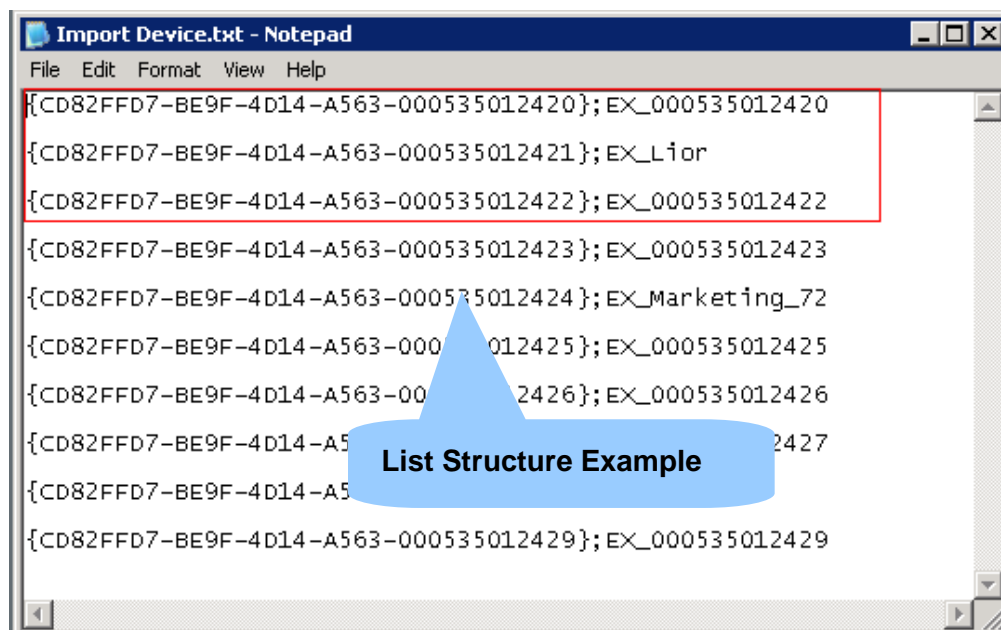
Preconfigured Device Accounts

In this method Thin-Client MAC Addresses are entered into the Xcalibur database manually. This is usually done before connecting the Thin-Clients to the network. You can enter one address at a time, or import a list of Thin-Client MAC Addresses. When buying new devices, a MAC Address list can be obtained from Chip PC. After importing it into the Xcalibur Database, you can allocate the devices into their destined Organizational Units according to their shipping destinations. Once these devices connect to the network, they will be recognized as authorized and therefore will become ready for use. No local user intervention is needed when using this method of authentication.



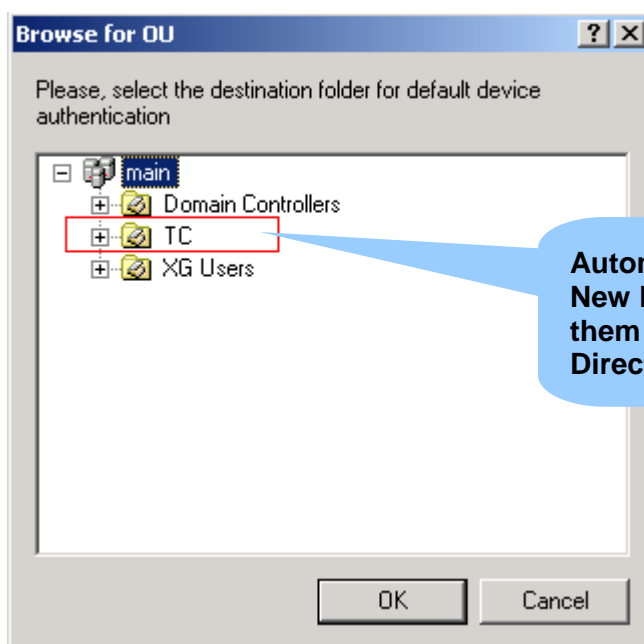
Manually add Preconfigured devices into the database:

- From the Xcalibur Directory Manager snap-in right click the Organizational Unit where you want to create new device accounts.
- To add a single device, select the New → Device...option and type it's MAC Address in the Add Device dialog box, then press OK.
- To add multiple devices, select the Import Devices...option and browse for the MAC Address list that you want to import, then press OK.



Default Device Authentication Provider

In this method, when Xcalibur recognizes a new device it automatically creates a new device account for it and assigns it to a predefined Organizational Unit. The predefined Organizational Unit can be a temporary location for grouping newly detected devices together until an Xcalibur administrator manually moves them to an operational Organizational Unit, or it can be the operational Organizational Unit where the client's account will eventually reside. In either case, no local user intervention is needed.

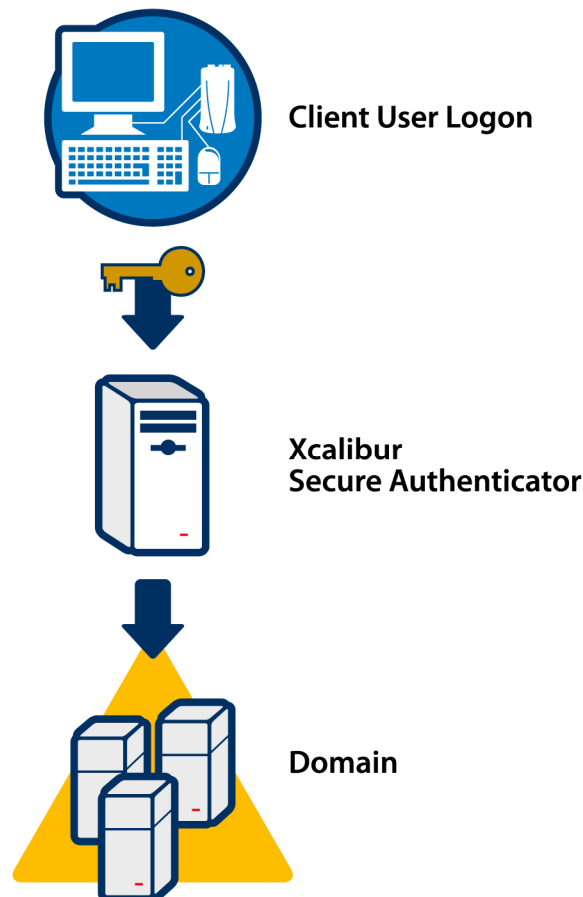


Configuring the Farm / Site / IP Scope Default Device Authentication Provider:

- From the Xcalibur Farm Manager snap-in right click the Farm / Site or IP Scope.
- Under the Authentication Tab \ Device Authentication Provider, select the Default Device Authentication Provider option and press the "Configuration" button.
- In the Device Authentication Provider Configuration window select the automatically accept devices...option.
- To specify the Organization Unit where client accounts should be created press the Browser...button.
- Press OK to close all property windows.

Xcalibur Secure Authenticator

The Xcalibur Secure Authenticator is an advanced authentication service that is used as a mediator between the Thin-Client and the authentication service, such as, Active Directory. Front End servers running this service relay logon information (e.g. user credentials) between the client and the authentication service. This allows Thin-Clients to become part of a security realm regardless of their O.S limits.



How does it work?

User information used for device or user authentication is passed in a secured manner from the client to the Secure Authenticator service running on the Front End server, the server then connects to the authentication service via standard APIs (e.g. Kerberos / LDAP) on behalf of the client and authenticates the user.



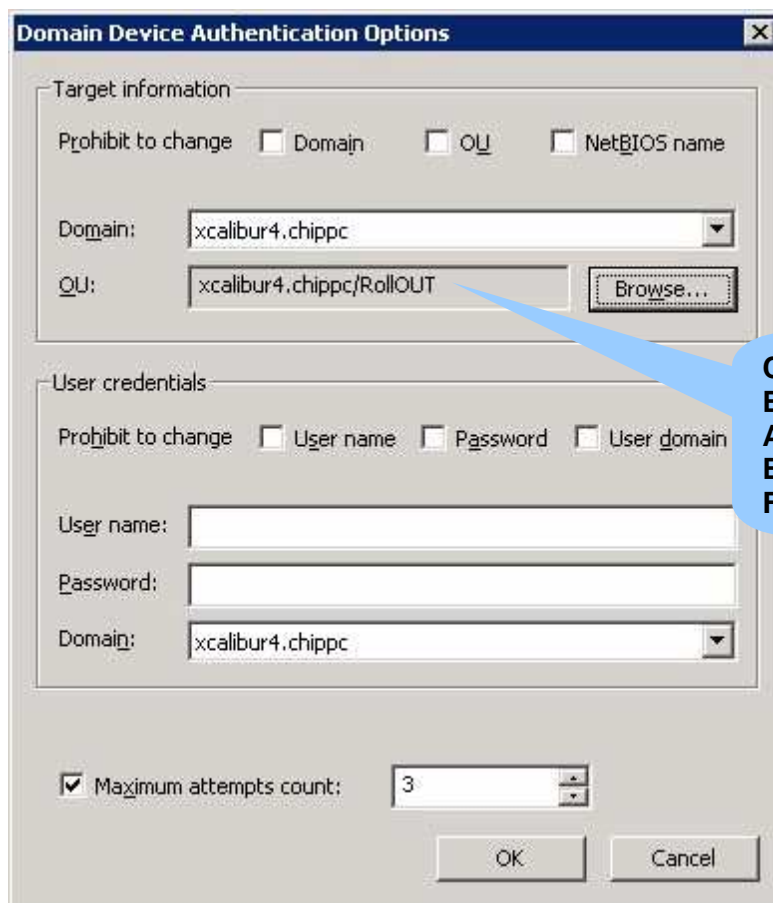
Benefits

- Secure Communication: Providing security over standard SSL communication.
- Leverage the Server's O.S Power: By relying on the Front End server to authenticate the user on behalf of the client, customers are no longer limited by the client's O.S for performing authentication related tasks. For example, Windows CE based clients that do not support changing a user's password in the Active Directory domain can rely on the server for doing it in a transparent way.
- Third Party Authentication Support: The Secure Authenticator can support multiple authentication services. Customers can install the Secure Authentication package that fits their needs.
- Minimum Client Configuration: Client side support can be set to install automatically on Thin-Clients requiring little effort from the IT staff.

Domain Based Device Authentication

This authentication method is similar to the process of joining a new computer to the domain. Valid domain credentials are required whenever connecting a new Thin-Client device to the network. The user connecting the device must be granted permissions to create computer accounts within the Active Directory level he wishes the device to be assigned to.

When connecting a brand new device to the network, during its initial communication with Xcalibur it is recognized by Xcalibur as unauthorized. As a result, Xcalibur triggers a pop-up prompt that appears on the client's screen requiring the user to provide valid domain credentials that have the appropriate permissions. Once these have been provided, the new Thin-Client can be either assigned into a predefined target Organizational Unit, which was set by the Xcalibur Administrator beforehand, or the local user is allowed to browse (subject to AD permissions) for the Organizational Unit into which the Thin-Client should be registered.



Domain Device Authentication Options

Target information

Prohibit to change ☐ Domain ☐ OU ☐ NetBIOS name

Domain: xcalibur4.chippc

OU: xcalibur4.chippc/RollOUT Browse...

User credentials

Prohibit to change ☐ User name ☐ Password ☐ User domain

User name:

Password:

Domain: xcalibur4.chippc

☒ Maximum attempts count: 3

OK Cancel

Configure Domain Based Device Authentication Behavior under the Farm/Site/Scope



Client's Pop-Up for Domain Based Device Authentication

Configuring the Farm / Site / IP Scope with Domain Device Authentication Provider:

- From the Xcalibur Farm Manager snap-in right click the Farm / Site or IP Scope.
- Under the Authentication Tab \ Device Authentication Provider, select the Domain Device Authentication Provider option and press the "Config..." button.



- Under the Target Information section set the following:
 - Domain: Choose the domain that will be used for authentication.
 - Organizational Unit: Browse to the Organizational Unit where new client accounts should be created.
 - Prohibit to Change: Specify whether local users can change the authentication settings.
- Under the User Credentials section set the following:
 - User Name: Type a user name that will be used to authenticate new client accounts.
 - Password: Type the password for the User account. This allows automatically registering new devices.
 - Domain: Choose the domain that will be used for authentication.
 - Prohibit to Change: Specify whether local users can change the authentication settings.
 - Maximum Attempts Count: Set a number of logon failures that will lock the device.
- Press OK to close all property windows.

Thin-Client User Level Authentication

While Thin-Client device authentication is mandatory, user authentication at the Thin-Client level is optional. Assuming that Thin-Clients are network access devices used for connecting to terminal service environments which are secured anyway, customers might not want to enforce user authentication at the Thin-Client level. Therefore, as default, once the Thin-Client device is authorized for use (authenticated) by Xcalibur it does not require user's to logon to it and can be used by any one.

For organizations where high security is an issue of importance, and where you want to benefit from user level authentication advantages, such as, single sign-on and User Level Xcalibur Policies, there is a variety of authentication mechanisms that can be used for user authentication at the Thin-Client level.

This section covers the Domain Based User Authentication and the Default User Authentication Provider.

Domain Based User Authentication

This authentication method extends the domain user logon process to operate on Thin-Clients. Once implemented, valid domain credentials are required whenever logging on to a Thin-Client device. User credentials are sent from the client to the Xcalibur Secure Authenticator service that validates the user in front of the Domain.

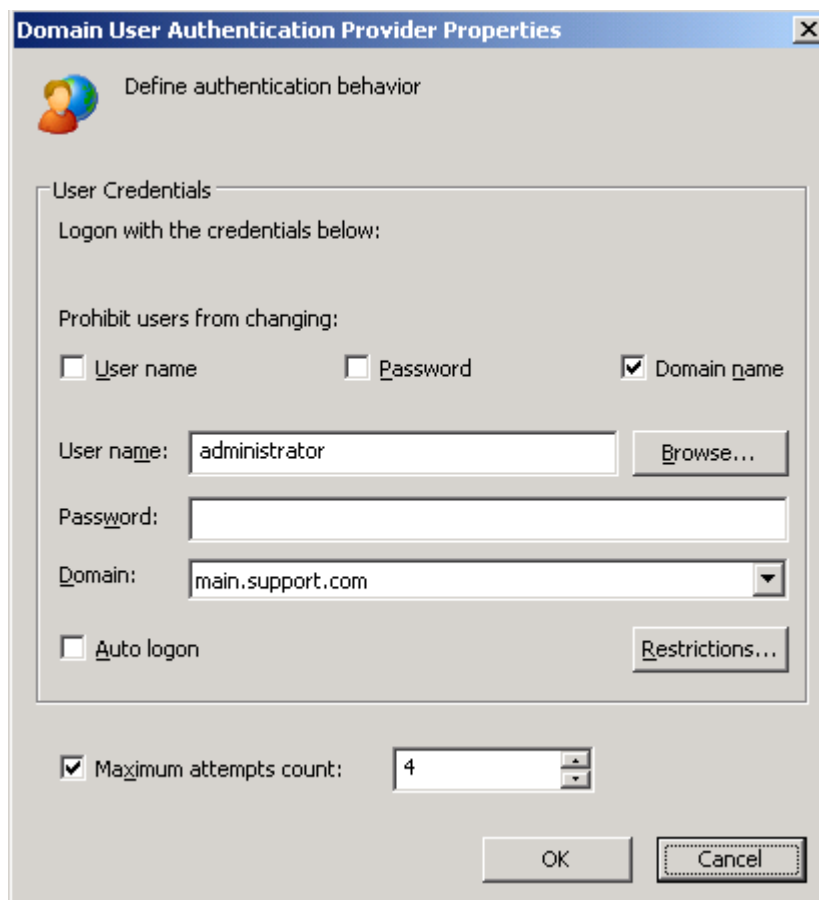


Domain Based User Authentication Advantages:

- Secure device access is achieved once prompting users for credentials or smart cards. This way, device access is limited only to users who can be successfully validated in front of Microsoft Active Directory.
- Dynamic, user-based, settings deployment: Connections and other User Level policy settings are applied on the device based on the user who's logging on at it. Different device settings and access rights can be set on a single device according to its logged on user.
- Single sign-on: Credentials used during the logon process can be cached for pass through authentication. The single sign on support, maps user credentials into any process that requires authentication thus requiring users to provide credentials only once, during device logon.
- Restrict users to logon only to specific Organizational Unit s or Devices: Device and network security can be tightened further by restricting user's logon privilege to devices that belong to a certain Organizational Unit or to a specific device.

Note While device authentication is mandatory thus preventing unauthorized device usage, User Authentication is optional.

Configure Domain Based User Authentication

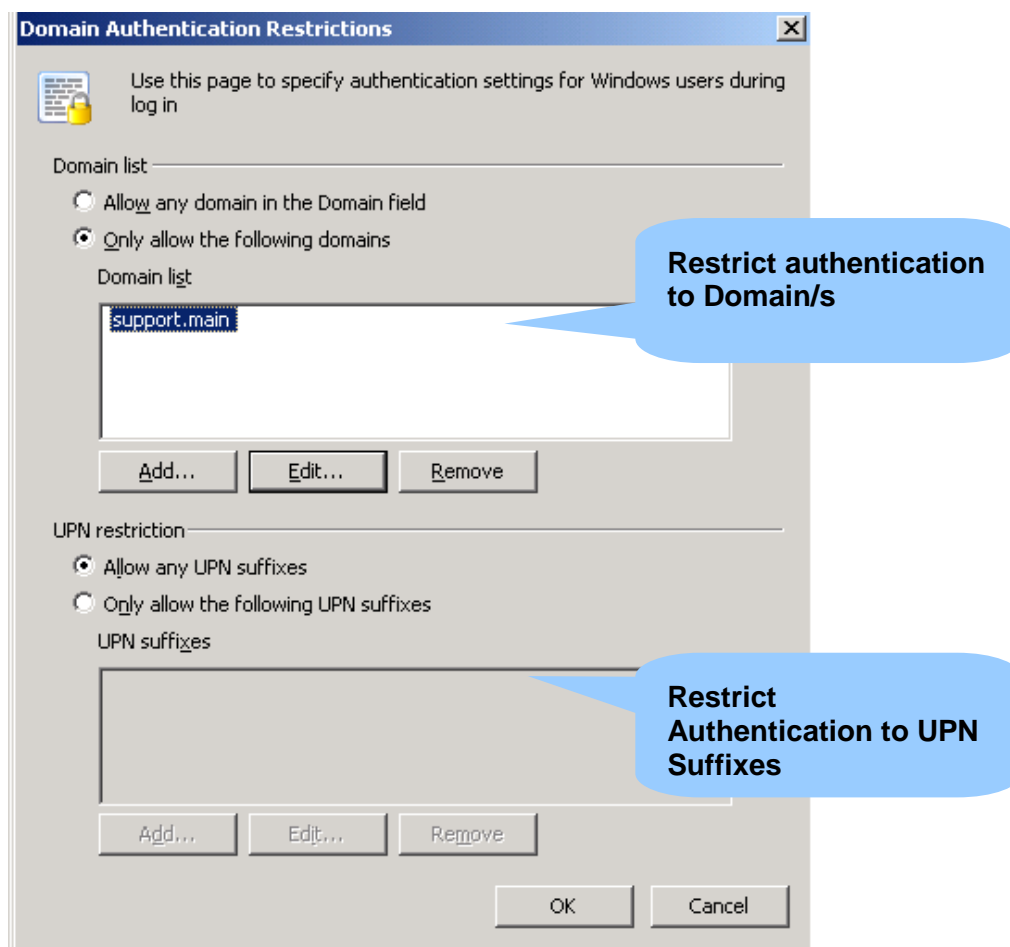


Configuring the Farm / Site / IP Scope with Domain User Authentication Provider:

- From the Xcalibur Farm Manager snap-in right click the Farm / Site or IP Scope.
- Under the Authentication Tab \ User Authentication Provider select the Domain User Authentication Provider option and press the Config... button.
- Under the User Credentials section set the following:
 - User Name: Type a user name that will be set as default user name for user authentication. Blank field requires the user to type his user name.
 - Password: Type the password for the User account. This allows automatically logging on the default user. Blank field requires the user to type his password.
 - Domain: Choose the domain that will be used for authentication.
 - Prohibit to Change: Specify whether local users can change the authentication settings.
 - Maximum Attempts Count: Set a number of logon failures that will lock the device.
- Press OK to close all property windows.

Restrictions on Users Logon

During logon to the thin client, users may have a list of domains to which they can login to; Through the Domain Authentication Restrictions window, as illustrated, you can choose whether to allow users to logon to any domain or you can limit them to specific domain name lists. In the UPN Restriction section, you can choose whether to allow any UPN suffix or restrict the allowed UPNs to a specific list.



Restrict User Authentication

- From the Xcalibur Farm Manager snap-in right click the Farm / Site or IP Scope.
- Under the *Authentication Tab* click the *Restrictions* button.
- In the *Domain* rubric define domain restrictions.
- In the *UPN* rubric define UPN suffixes restrictions.
- Click the *OK* button to finish.

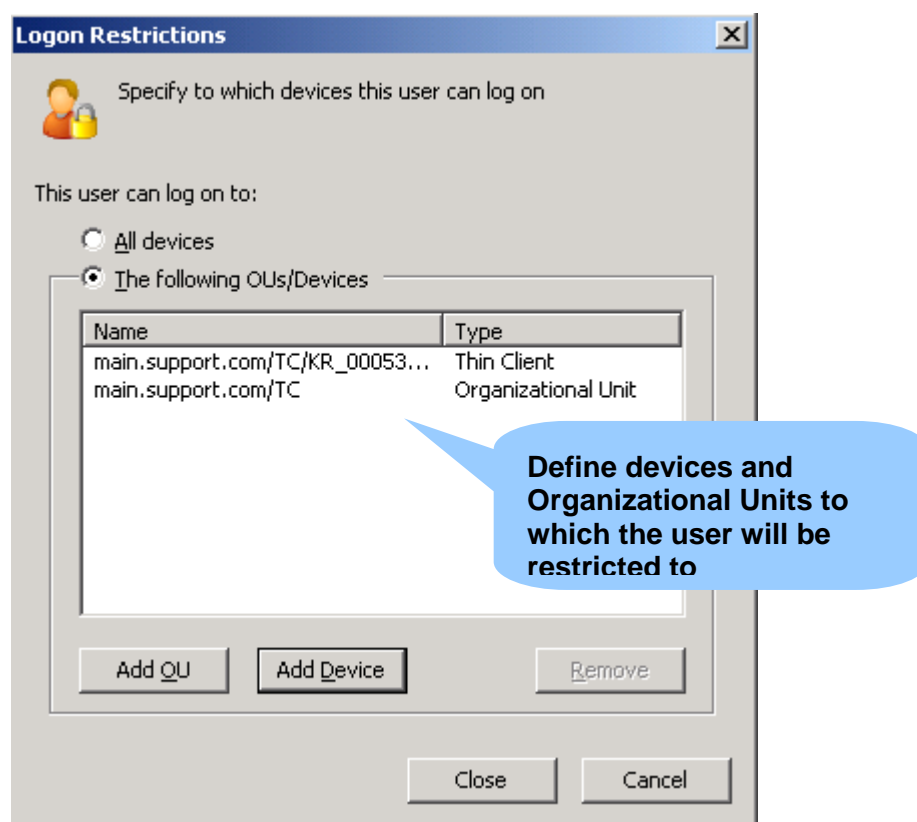
Restrict Users to Logon only to Specific Devices

Through Xcalibur, user's logon can be restricted to specific devices.

You can restrict a user to logon to a specific device, or, to devices that reside in specific Organizational Unit (OU).

- By selecting a specific device, the user will be allowed to logon to that device only.
- By selecting an Organizational Unit (OU), the user will be allowed to logon to any device that is mapped to the selected OU.

This option provides a way to restrict users to logon only to devices that belong to their working area / department / building etc.



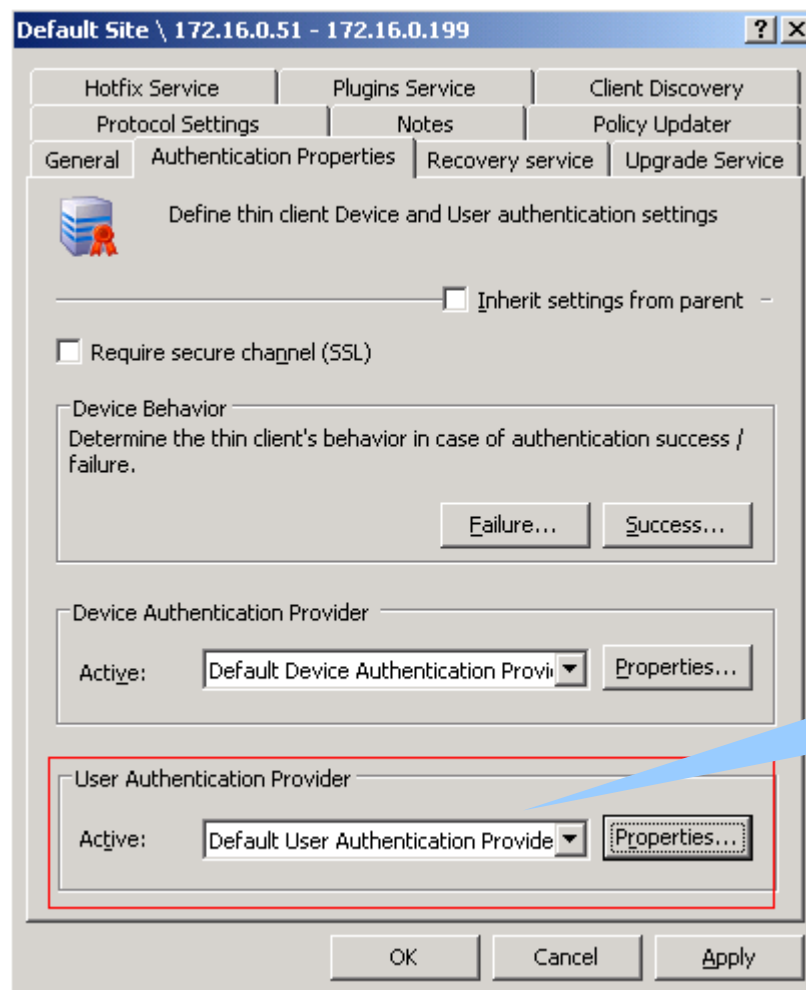
Restrict Users to Logon only to Specific Organizational Units or Devices:

- From the Xcalibur Directory Manager snap-in right click the user whose logon you want to restrict, and then click *Properties*.
- In the *Account tab* press the "Logon To..." button.
- As default users are allowed to logon to all Thin-Client devices, to change this, select The following Organizational Units/Devices radio button.
- Press the Add OU button and select the Organizational Units this user is allowed to logon to from the Active Directory tree. This allows the user to logon to all the Thin-Client devices that belong to the selected Organizational Unit.

- Press the Add Device button and select the devices that this user is allowed to logon to from the device list.
- Press Close and OK to close all property windows.

Default User Authentication Provider

In this method, you can set a default user account that will be used by all Thin-Client devices for user level authentication purposes. This allows applying user level policy settings on multiple devices by assigning them to the same account.



Default Site \ 172.16.0.51 - 172.16.0.199

Hotfix Service | Plugins Service | Client Discovery

Protocol Settings | Notes | Policy Updater

General | **Authentication Properties** | Recovery service | Upgrade Service

Define thin client Device and User authentication settings

☐ Inherit settings from parent

☐ Require secure channel (SSL)

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

Failure... Success...

Device Authentication Provider

Active: Default Device Authentication Provi... Properties...

User Authentication Provider

Active: Default User Authentication Provide Properties...

OK Cancel Apply

**Define User
Authentication
Method**

Users working on the Thin-Clients are not prompt for identification while user level policies, assigned to the default user, affect their devices in a transparent way.



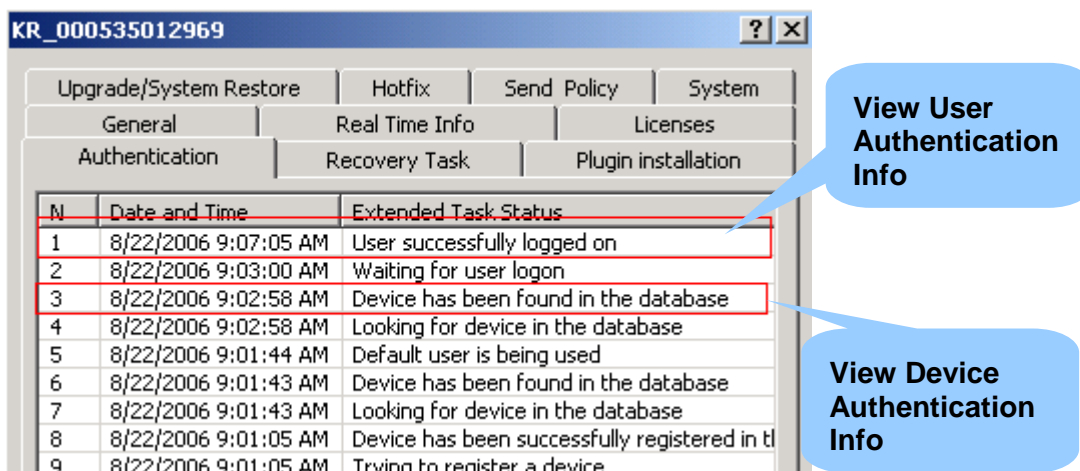
When you want to have user-level management in a somewhat stealth way, use the Default User Authentication Provider. Once selected, the user name predefined under the Default User Authentication Provider is used for authentication during device boot. In this mode, the device operates in user-level without prompting for user credentials or the user being aware of that.

Configuring the Farm / Site / IP Scope Default User Authentication Provider:

- From the Xcalibur Farm Manager snap-in right click the Farm / Site or IP Scope.
- Under the Authentication Tab \ User Authentication Provider, select the Default Device Authentication Provider option and press the Config... button.
- In the Default Device Authentication Provider Configuration window select the automatically accept devices...option.
- To specify the Organizational Unit where client accounts should be created press the Browser...button.
- Press OK to close all property windows.

Monitoring Authentication

From within the Xcalibur Farm Manager you can monitor both device and user authentication process.



The screenshot shows the 'Authentication' tab in the Xcalibur Farm Manager. The window title is 'KR_000535012969'. The 'Authentication' tab is selected, showing a list of events. Two callouts are present: 'View User Authentication Info' pointing to row 1, and 'View Device Authentication Info' pointing to row 3.

N	Date and Time	Extended Task Status
1	8/22/2006 9:07:05 AM	User successfully logged on
2	8/22/2006 9:03:00 AM	Waiting for user logon
3	8/22/2006 9:02:58 AM	Device has been found in the database
4	8/22/2006 9:02:58 AM	Looking for device in the database
5	8/22/2006 9:01:44 AM	Default user is being used
6	8/22/2006 9:01:43 AM	Device has been found in the database
7	8/22/2006 9:01:43 AM	Looking for device in the database
8	8/22/2006 9:01:05 AM	Device has been successfully registered in tl
9	8/22/2006 9:01:05 AM	Trying to register a device

Viewing Authentication Service Queue:

Under the Farm \ Site \ Tasks \ Authentication container you can view the Authentication service queue and manually authenticate client devices.

Monitoring Authentication in Real Time:

Real time information including policy application, software deployment and Authentication progress can be viewed under the client's properties \ Real Time Info tab.



This page is left blank intentionally.

Chapter 7 Software Deployment

Objectives

Understand Software Deployment Guidelines, concepts and services.

Software Installation and Distribution to Thin-Client Device

Software installation needs to be considered for both client and server software.

- Client software is any software that is destined to be installed on Thin-Client devices, such as software add-ons (plug-ins) and firmware files.
- Server software is any software that is destined to be installed on the Xcalibur servers, such as Xcalibur software updates, MMC snap-ins and Xcalibur Policy enhancements.

All installable and distributable software is first loaded into the Xcalibur database using the Farm Software Repository interface and then distributed from there to the Front End Servers from where it becomes available for Thin-Client Devices.

Software deployment files can be obtained from any Xcalibur Front End but ideally, clients will connect to servers residing on their own local area network rather than connecting to remote servers. This is accomplished by placing the local servers at the top of the Xcalibur Server List sent to clients via DHCP SNMP or DNS during the discovery phase.

The software deployment files are transferred using the Independent Management Protocol used for client-server communication. This allows the distribution to benefit from built-in protocol features such as compression and bandwidth control.

Software Deployment Concepts

Software Deployment refers to the deployment of:

- Plug-ins
- Hotfixes
- Firmware files
- Recovery files

Trigger Software Deployment process

Software deployment is performed by using a three step mechanism that can be initiated as a result of logical or physical management requirements.



Policy based Software Deployment:

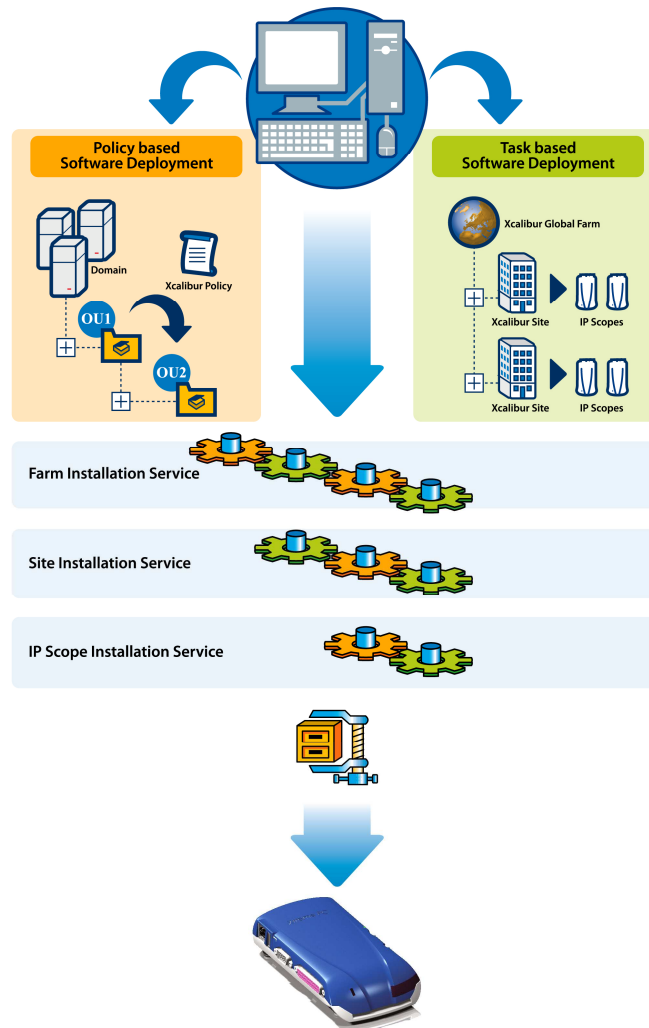
Software deployment is initiated based on logical management requirements. Xcalibur Administrators can initiate software deployment based on the logical structure of the organization as represented by the Active Directory, by creating an Xcalibur Policy. The policy specifies what software to install and it can be assigned to any Active Directory level from the Xcalibur Directory Manager MMC snap-in. All target devices affected by this policy will connect to their local Installation Service providers to retrieve the software files.

Task based Software Deployment:

Software deployment is initiated based on management requirements using physical location of the Thin-Client Device. Xcalibur Administrators can initiate software installation based on the physical structure of the organization as represented by the Xcalibur Farm, by creating a Management Task. This task specifies what software to install and is assigned to devices residing under the Farm, Site or IP Scope levels from the Xcalibur Farm Manager MMC snap-in. All target devices affected by this task will connect to their local Installation Service providers and retrieve the software files.

Note Defining a software standard which specifies what firmware and plug-in file versions will be used is highly recommended. This standard should be applied to all client devices throughout the organization. When a change to this standard is required for a particular reason, a new standard should be developed and applied in addition to the original one.

Software Deployment Flowchart



Software Deployment Mechanism

The following explains the steps taken during software deployment whenever plug-in; hotfix, upgrade or recovery files are deployed:

- **Installation Request Generation:** In order to initiate software deployment an installation request must be sent from the Thin-Client to the server running the Installation Services. The client will send such a request when triggered to do so by either an Xcalibur Policy or by a Management Task. An installation request includes the name of the software to be installed and additional installation options.
- **Installation Request Initiation:** When a client is triggered to initiate an installation request, it first verifies that the requested software is not already installed and then initiates the request to the server running the Installation Services.
- **Installation Services:** The Installation Services are responsible for plug-in, hotfix, upgrade and recovery installations on Thin-Client devices. See the next section for further details.

Installation Service Providers

Installation service providers are Front End Servers running the following services:

- Plug-in Installation Service
- Hotfix Installation Service
- Upgrade Installation Service
- Recovery Installation Service

All Installation Services share common options. Therefore the descriptions specified here are suitable for all services.

An Installation Service is responsible for the installation of software on client devices. This service is available on all Front End Servers and is configured through the Farm, Site and IP Scope levels. The service has configurable properties including service operation hours (schedule), bandwidth limits and maximum simultaneous connections. Once a Software Installation Request is received by the Installation Service it is added to the service queue for processing.

Note Installation Request Generation for firmware recovery is automatically initialized by the client in case of a firmware crash.

Software Deployment Guidelines

Network Topology Perfection:

In either policy or task based software deployment scenarios the actual installation process is always applied according to the Installation Service settings defined under the Farm, Site and IP Scope levels. This gives high level administrators the freedom to manage software deployment from any logical or physical level while knowing that the actual process will consider the network utilization settings as uniquely defined for every branch or physical site.

Software standard:

A software standard should be based on the aim of achieving the fewest client-side software updates to generate the lowest bandwidth while still achieving low software maintenance overhead.

**Update policy:**

All software is liable to become outdated. Version updates should be carefully considered as in many events updates might not be worthwhile. An update policy including plug-in, hotfix and firmware subchapters should be established. This policy should determine a minimum target period of at least 8 months for a software version to be live before it needs to be updated. During this period, with the exception of emergencies, no software updates should be allowed. This will provide system stability and reduce the software maintenance overhead as much as possible. Whenever a new software version is to be released a careful study must be made prior to replacing the current version. This study should provide a benefit / cost table summarizing the advantages of the newer version and the relevance / impacts to the project. Please note that in some cases, server side software updates including Citrix and Windows, might be required in order to support new client side features.

Plug-in Updates:

Plug-ins are compact client-side applications that can be installed on Chip PC Thin-Client devices. The Plug-in technology makes keeping client-side software up to date possible without the need to fully upgrade the client's firmware. This way, for example, the ICA client application can be updated once a newer version is released, tested and found essential for the project needs. Due to the small file size factor, the plug-in installation process is fast, less bandwidth consuming and considered highly reliable in terms of the client's operating system stability. In some cases, plug-in updates require the latest hotfix installation.

Hotfix Updates:

A hotfix is a small software package usually containing operating system update files. The Hotfix technology makes keeping the client's operating system up to date possible without the need to fully upgrade its firmware each time. This way, for example, driver updates or bug fixes can be applied to clients in a low bandwidth consuming, highly reliable way. In general, hotfixes relating to system stability should be given higher priority than others. New hotfix releases should be checked for compatibility and thoroughly tested with earlier plug-in versions as necessary before deployment.

Firmware Updates:

The client's Windows CE based firmware should be infrequently updated. New firmware releases mainly occur when a new Windows CE operating system is released by Microsoft.

Software Deployment Procedure

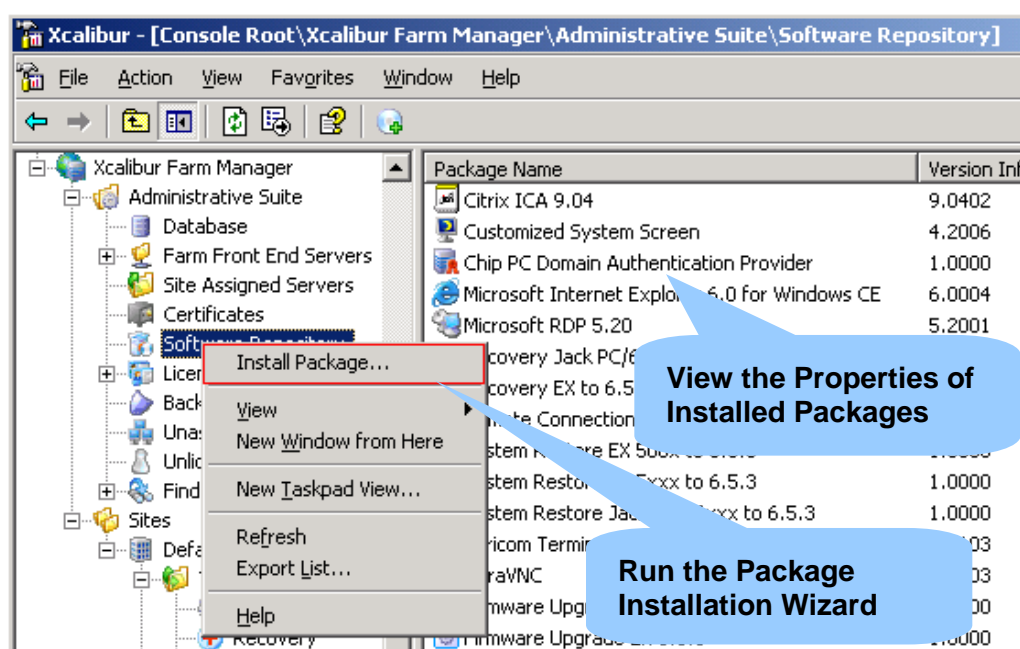
The following settings are needed to setup the software deployment mechanism:

- Add software packages into the Software Repository.
- Configure the Installation Services under the Farm / Site / IP Scope.
- Use Xcalibur Policy for Software Deployment.

And / or

- Create a Task for Software Deployment.
- Monitoring Software Deployment

Adding Packages into the Software Repository

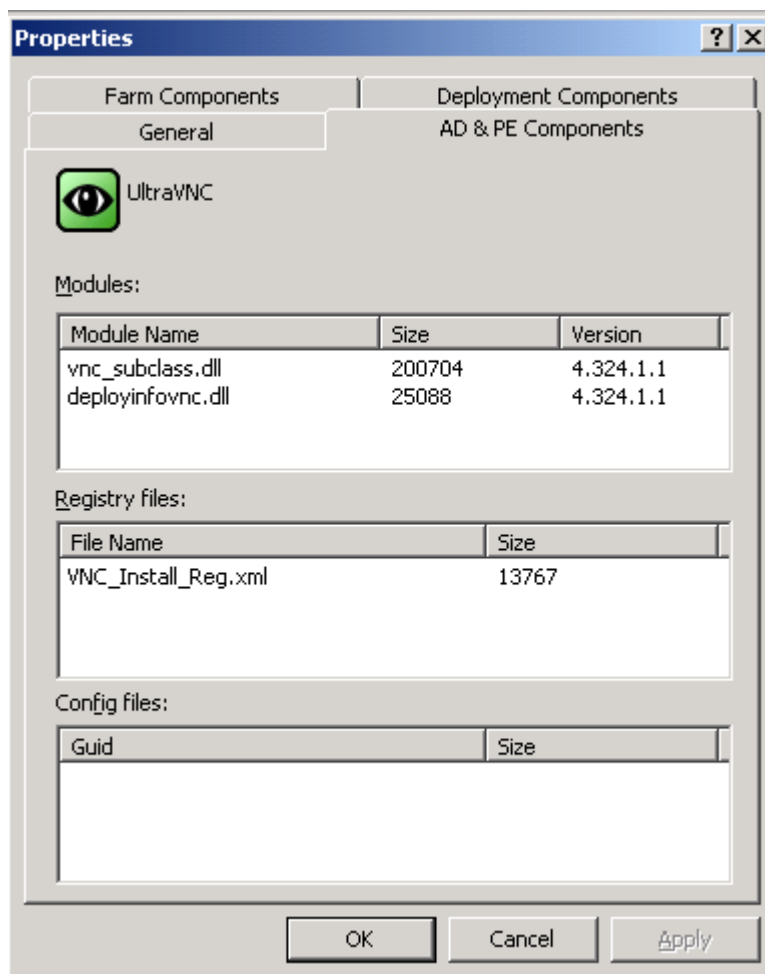


The Package Installation Wizard guides you through the process of adding software packages into the Software Repository.

Run the Package Installing Wizard:

- Expand the Administrative Suite container located under the Xcalibur Farm Manager snap-in.
- Right click the Software Repository container and select the Install Package...option.
- Press *Next* at the Welcome screen and then browse to the folder where the package files reside.
- Select the package that you wish to install, for example: vncinstallpack.xcp for the VNC Package, press Open and then Next.
- Make sure that the package name, version and description match your desire and press the Install button to begin the installation.
- Press Finish to complete the installation wizard.

Package Properties



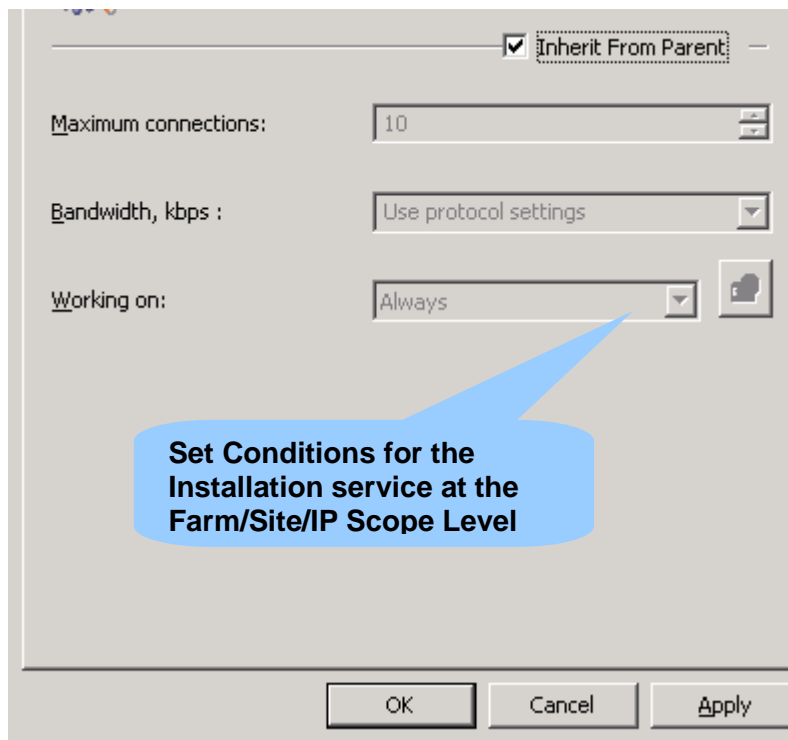
Typically a software package contains 3 content categories:

- Policy Editor Components: These files enhance the Xcalibur Policy Tree to support the configuration of the installed software.
- Server Farm Components: These files enhance the Farm Manager snap-in to support the configuration of the installed software.
- Software Deployment Components: These files are installed on client devices during the software deployment process.

Viewing package properties:

- Expand the Administrative Suite container located under the Xcalibur Farm Manager snap-in and select the Software Repository container.
- In the right view pane select a package, right click it and then click Properties.

Installation Service Configuration



The dialog box for 'Installation Service Configuration' contains the following elements:

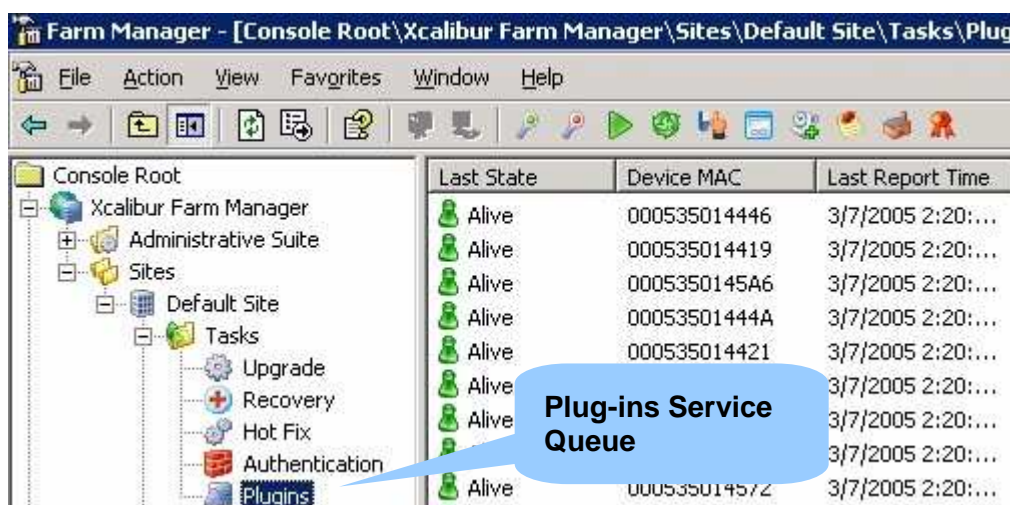
- Inherit From Parent:** A checkbox that is checked.
- Maximum connections:** A text box containing the value '10'.
- Bandwidth, kbps :** A dropdown menu currently showing 'Use protocol settings'.
- Working on:** A dropdown menu currently showing 'Always'.
- Buttons:** 'OK', 'Cancel', and 'Apply' buttons at the bottom.

A blue callout bubble points to the 'Working on:' dropdown menu with the text: **Set Conditions for the Installation service at the Farm/Site/IP Scope Level**

The Plug-ins, Upgrade and Hotfix Installation Services share common options. Therefore the descriptions specified here are suitable for all services (for recovery, see the Recovery Service Configuration section described further in this document).

Installation Service settings are specified from the Xcalibur Farm Manager snap-in and can be set at the Farm, Site and IP Scope levels. As default, child object settings are inherited from parent levels. Therefore settings defined under the Farm affect all Sites and settings defined under the Site affect all IP Scopes that belong to that Site.

Once inheritance is disabled, settings from the level which is closer to the device override higher levels.



Installation Service Configuration:

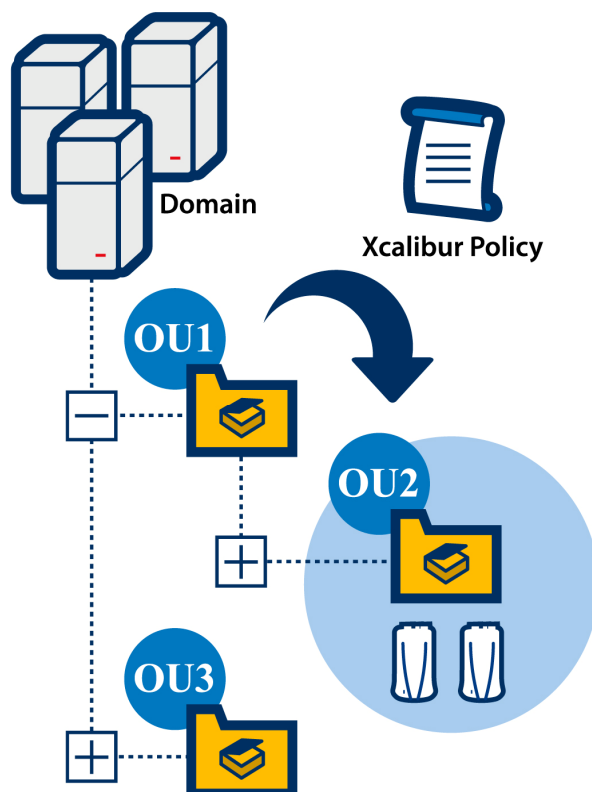
- From the Xcalibur Farm Manager snap-in right click the Farm / Site or IP Scope, and then click Properties.
- Select the Installation Service Tab for the service that you want to configure (e.g. Plug-ins Service / Upgrade Service / Hotfix Service).
- Clear the Inherit from Parent checkbox to disable inheritance.
- Maximum Connections: Set the maximum number of simultaneous client connections that can be connected to this service at the same time.
- Bandwidth, Kbps: Set the maximum bandwidth to be utilized by each client connection during the installation process.
- Working on: The installation service constantly listens for client requests. Once a request arrives, it is added to the service queue and will be handled during the service Working Hours.
 - Working Hours: Specify when the service becomes operational (e.g. Off-Work hours / Midnight...etc)
 - Always: The service immediately answers client requests.
 - Manual Permission: Client requests are queued until an administrator manually approves them from the Tasks container.
- Press OK to close the Properties window.

Note Client requests pooled by the Installation Services can be viewed under the Farm \ Site \ IP Scope \ Tasks \ %Installation Service Name% container.

Note To manually approve a client's request, right click the client name and select the Accept Client's Request...option.

Use Xcalibur Policy for Software Deployment

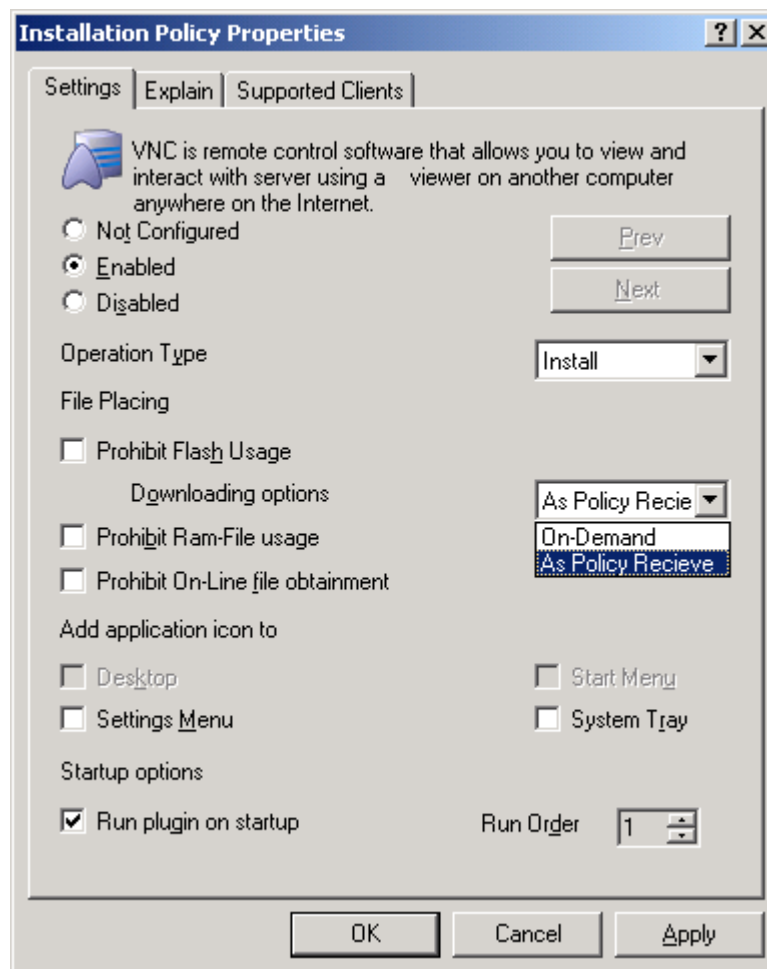
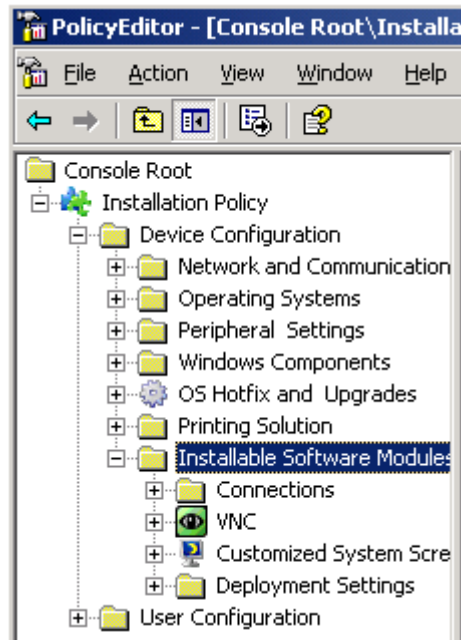
Xcalibur Policy can be used for software deployment. Once creating a policy that contains software installation settings and linking it to an Active Directory object, Xcalibur will install this software on all the Thin-Clients that are affected by this policy.



For example, linking a policy which is configured to install the RDP 5.2 plug-in to OU1 will result in this plug-in being installed on all the Thin-Client devices that are assigned to this Organizational Unit and to all child Organizational Units. Any device that is moved into this Organizational Unit will automatically retrieve the installation settings during Xcalibur Policy application. The device then triggers an installation request and is added to the installation service queue. The software will be installed on the device according to the installation service Working Hours settings.

By using Xcalibur Policy for software deployment, you can make sure that all the Thin-Clients that belong to a specific Domain or Organizational Unit will have the same software installed.

Plug-in Installation Policy Properties

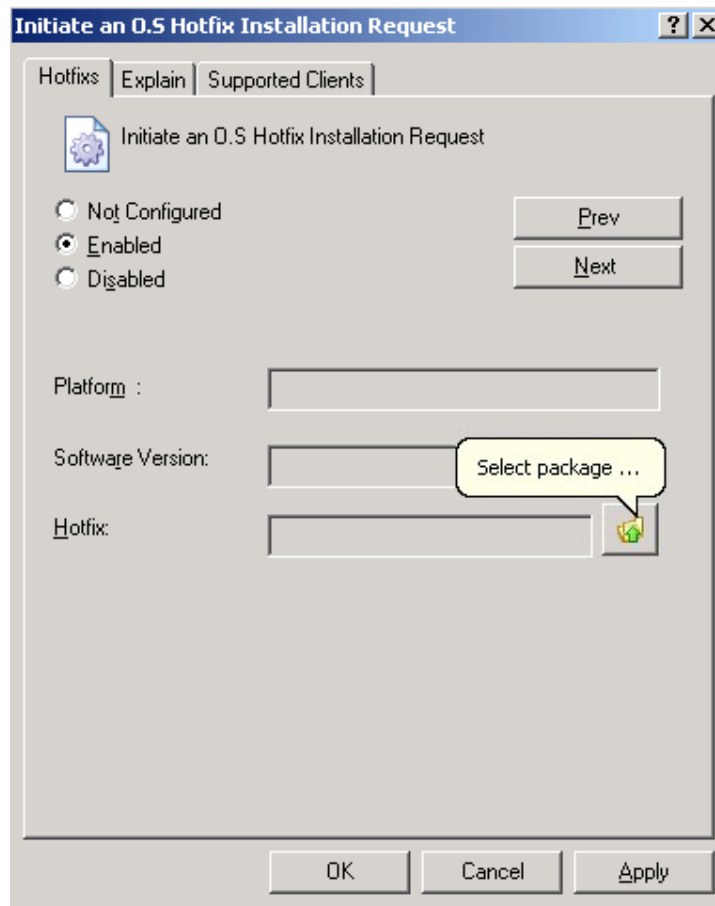


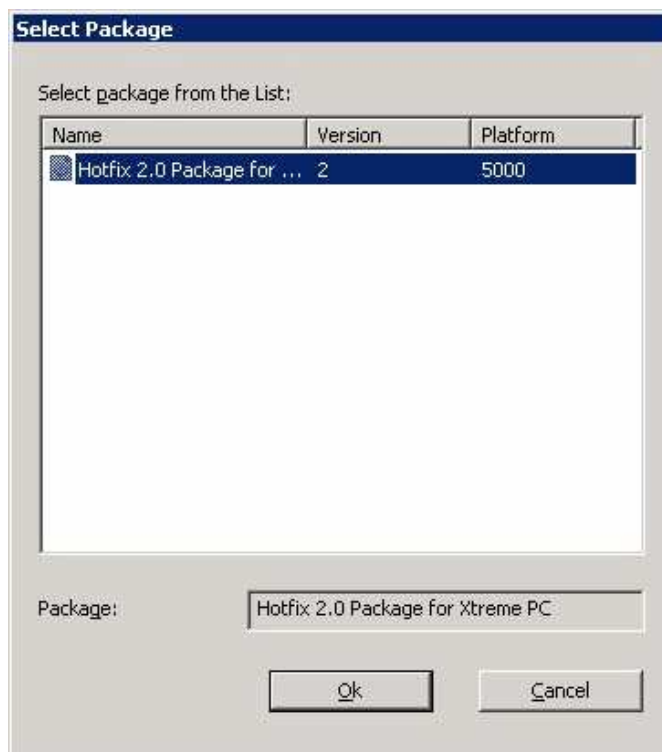


Configure Xcalibur Policy for Plug-in Software Deployment:

- Create a new Xcalibur Policy
- In the Policy Tree expand the Device Configuration \ Installable Software Modules container.
- Right click the name of the software that you want to install and then click Installation Policy...
- Enable this policy to install the selected software.
- File Placing: as default, plug-ins are installed into the device flash (Disk on chip). File placing settings allow specifying alternate locations.
 - **Prohibit Flash Usage**: Prevents plug-in files from being installed on the flash. Once selected plug-ins will be installed into a RAM-File. A RAM-File specifies that the RAM Memory can be used for Plug-in files storage. Plug-ins installed into RAM-File are retrieved once (during installation) from the network and then run from the RAM-File until the next device boot. Use the RAM-File option when you run out of flash storage space.
 - **Prohibit RAM-File usage**: Prevents plug-in files from being installed into the RAM.
- Downloading Options: as default plug-in installation is triggered during Xcalibur Policy application. The Downloading Options allows further customizing the installation options.
 - **As Policy Received**: this is the default settings. Once the Xcalibur Policy is applied, the Thin-Client triggers an installation request and waits for the Plug-ins Installation Service Working Hours.
 - **On-Demand**: Installs plug-ins in a dynamic way. Plug-ins are only installed if required. The installation process is initialized once the plug-in is required.
- Add Application Icons To: Specify whether to place an icon on the Desktop / Start Menu / Settings Menu / System Tray.
- Allow Local Operator To: Specify the access rights local users will have on this Plug-in.
 - **Uninstall**: Allows the local user to uninstall the Plug-in.
 - **Configure**: Allows the local user to configure the Plug-in.
- Start-up Options: Specify whether the Plug-in will be activated during the boot process.
- Press OK to close the Installation Policy Properties window and then close the Policy window.

Hotfix Installation Policy Properties

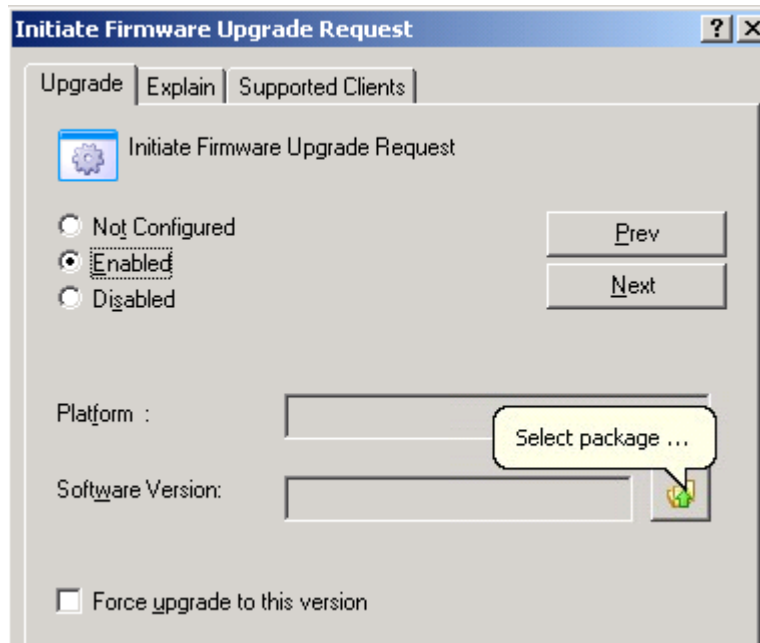




Configure Xcalibur Policy for Hotfix Software Deployment:


- Create a new Xcalibur Policy
- In the Policy Tree expand the Device Configuration \ OS Hotfix and Upgrades container.
- In the right view pane, double click the Initiate an O.S Hotfix Installation Request item.
- Enable this Policy to install the selected software.
- Installation Options: Select the Hotfix version to install. Once the Xcalibur Policy is applied, the Thin-Client triggers an installation request and waits for the Hotfix Installation Service Working Hours.
 - Try to install the latest software hotfix: This will automatically install the Hotfix with the highest version number.
 - Select the Hotfix version from the list: Press the Select Package button to browse through the Hotfix package list (obtained from the Software Repository) and manually select which Hotfix version to install.
- Press OK to close all property windows and then close the Policy window.

Firmware Upgrade Installation Policy Properties



Initiate Firmware Upgrade Request

Upgrade | Explain | Supported Clients

 Initiate Firmware Upgrade Request

☐ Not Configured
☒ Enabled
☐ Disabled

Prev

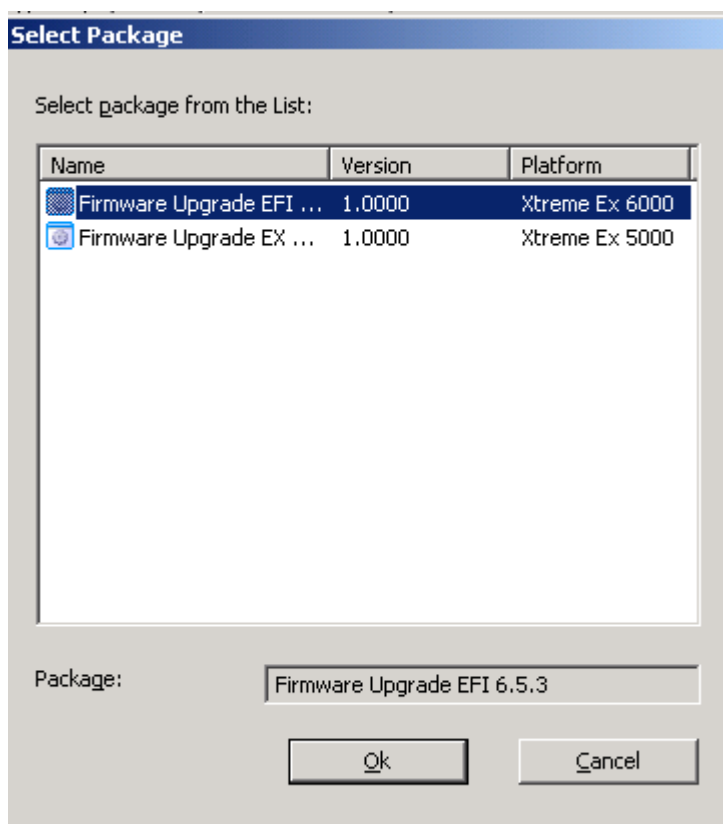
Next

Platform :

Software Version:

☐ Force upgrade to this version

Select package ...



Select Package

Select package from the List:

Name	Version	Platform
Firmware Upgrade EFI ...	1.0000	Xtreme Ex 6000
Firmware Upgrade EX ...	1.0000	Xtreme Ex 5000

Package:

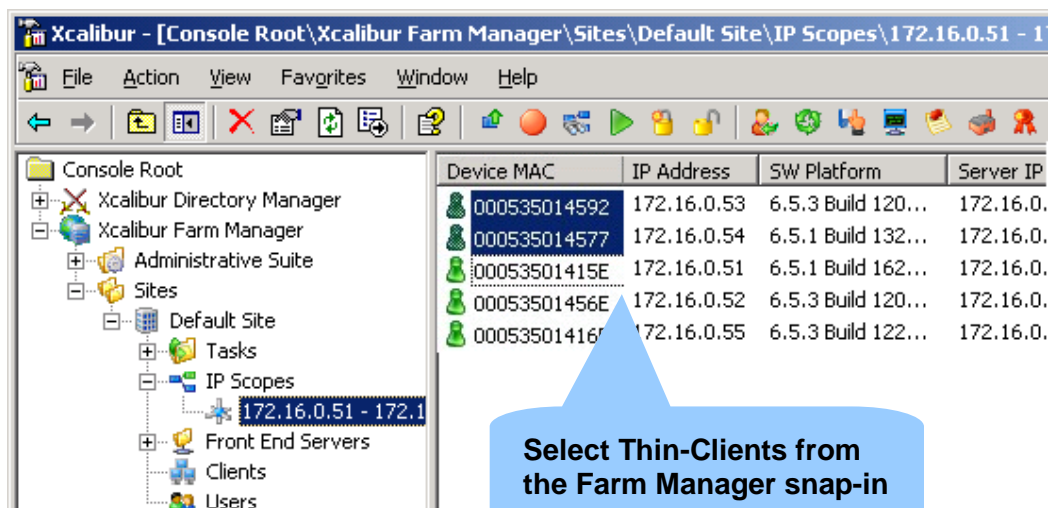
Ok Cancel

Configure Xcalibur Policy for Firmware Upgrade Deployment:

- Create a new Xcalibur Policy
- In the Policy Tree expand the Device Configuration \ OS Hotfix and Upgrades container.
- In the right view pane, double click the Initiate Firmware Upgrade Request item.
- Enable this Policy to install the selected software.
- Press the Select Package button to browse through the Firmware Upgrade package list (obtained from the Software Repository) and manually select which Firmware version to install.
- Press OK to close all property windows and then close the Policy window.

Once the Xcalibur Policy is applied, the Thin-Client triggers an installation request and waits for the Upgrade Installation Service Working Hours.

Create a Task for Software Deployment



The screenshot shows the Xcalibur Farm Manager console. The left pane displays a tree view with the following structure:

- Console Root
 - Xcalibur Directory Manager
 - Xcalibur Farm Manager
 - Administrative Suite
 - Sites
 - Default Site
 - Tasks
 - IP Scopes (selected)
 - 172.16.0.51 - 172.16.0.55
 - Front End Servers
 - Clients
 - Users

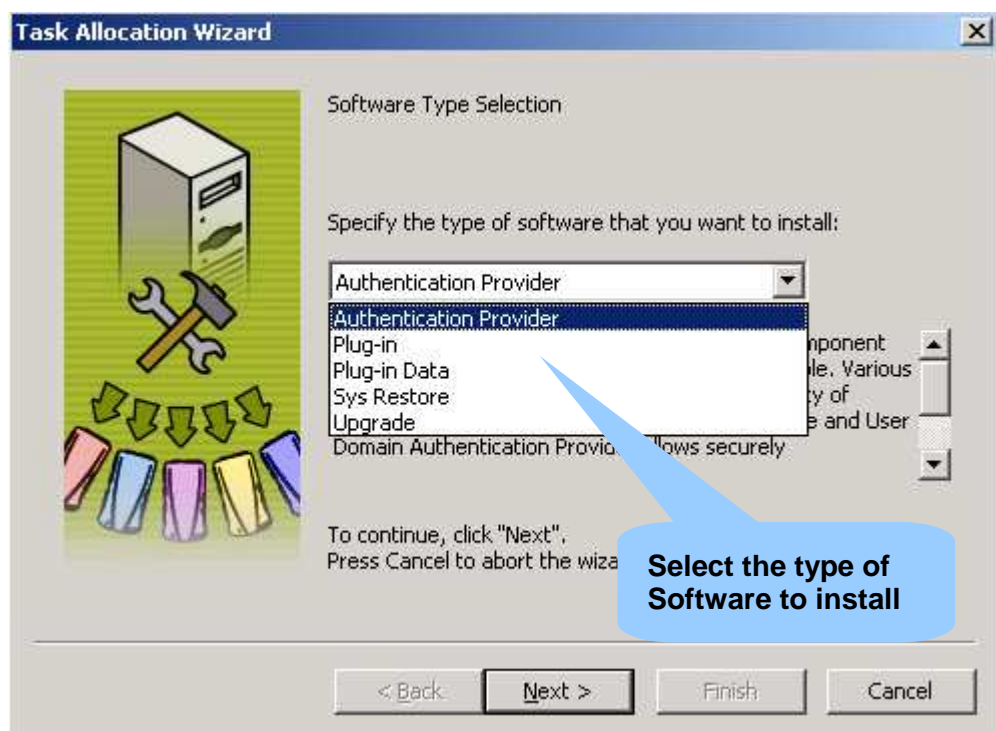
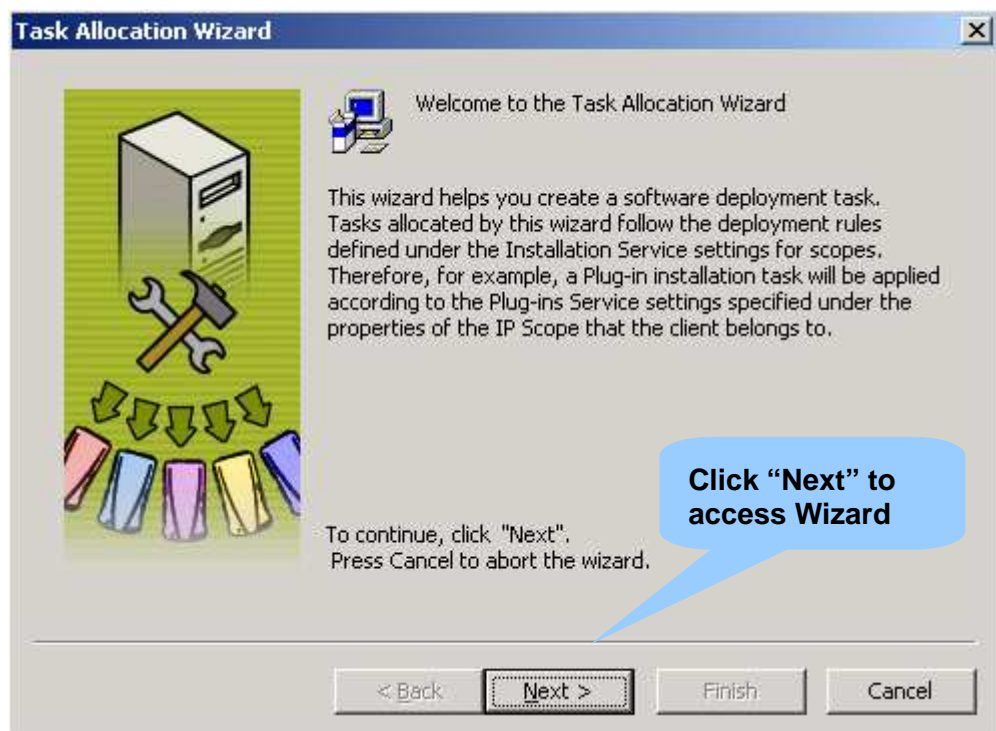
The right pane displays a table of thin-clients:

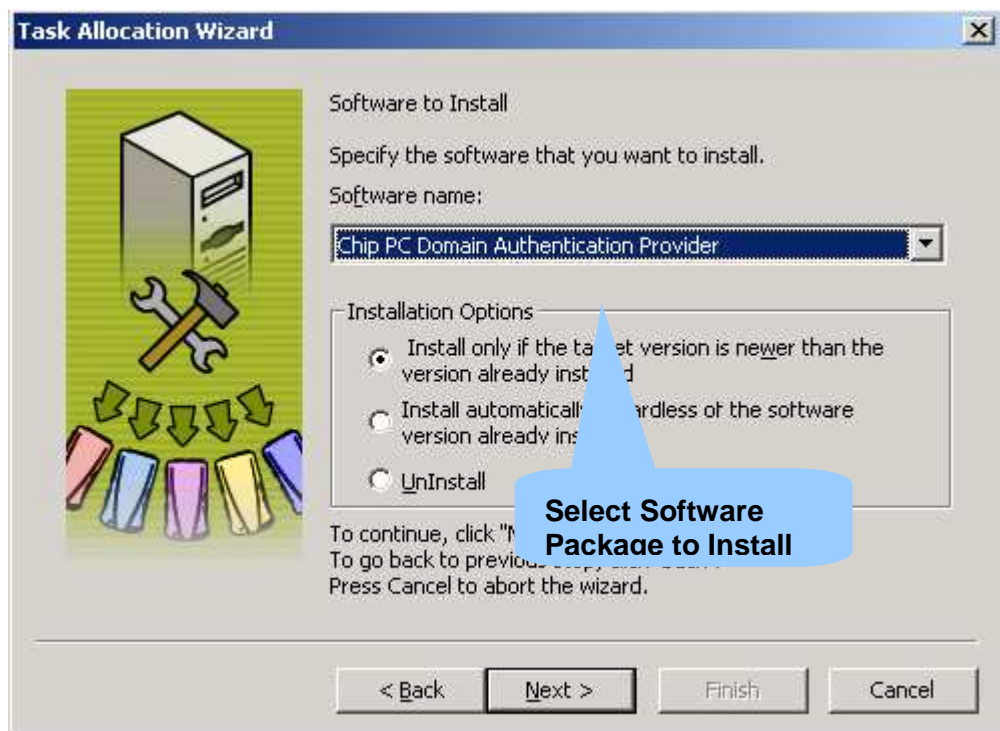
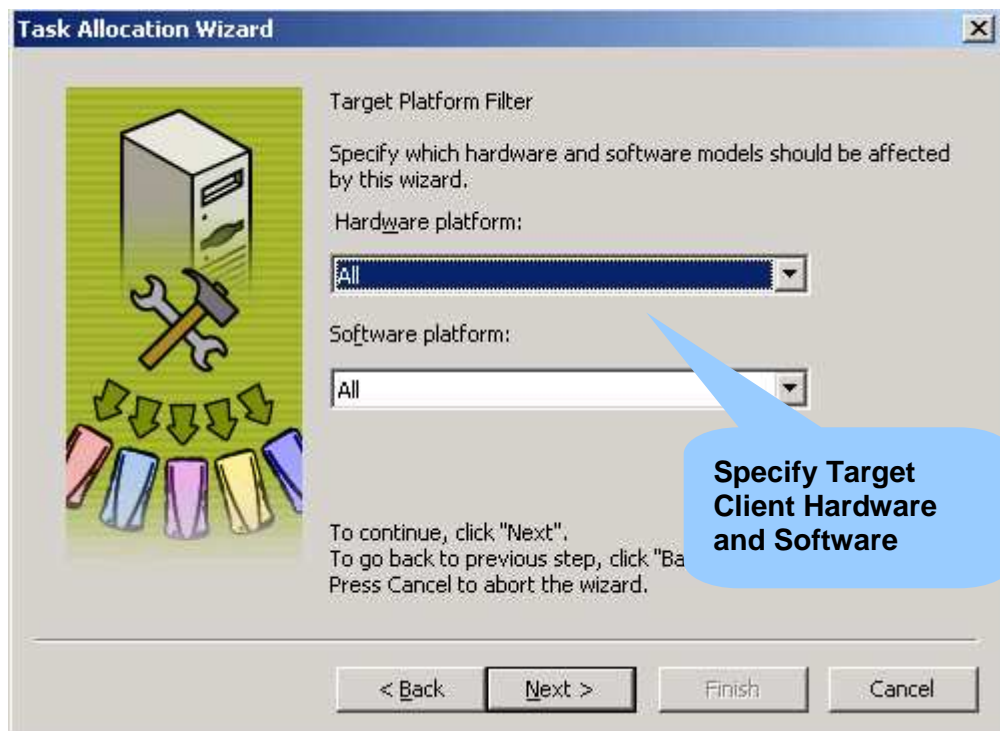
Device MAC	IP Address	SW Platform	Server IP
000535014592	172.16.0.53	6.5.3 Build 120...	172.16.0.
000535014577	172.16.0.54	6.5.1 Build 132...	172.16.0.
00053501415E	172.16.0.51	6.5.1 Build 162...	172.16.0.
00053501456E	172.16.0.52	6.5.3 Build 120...	172.16.0.
00053501416F	172.16.0.55	6.5.3 Build 122...	172.16.0.

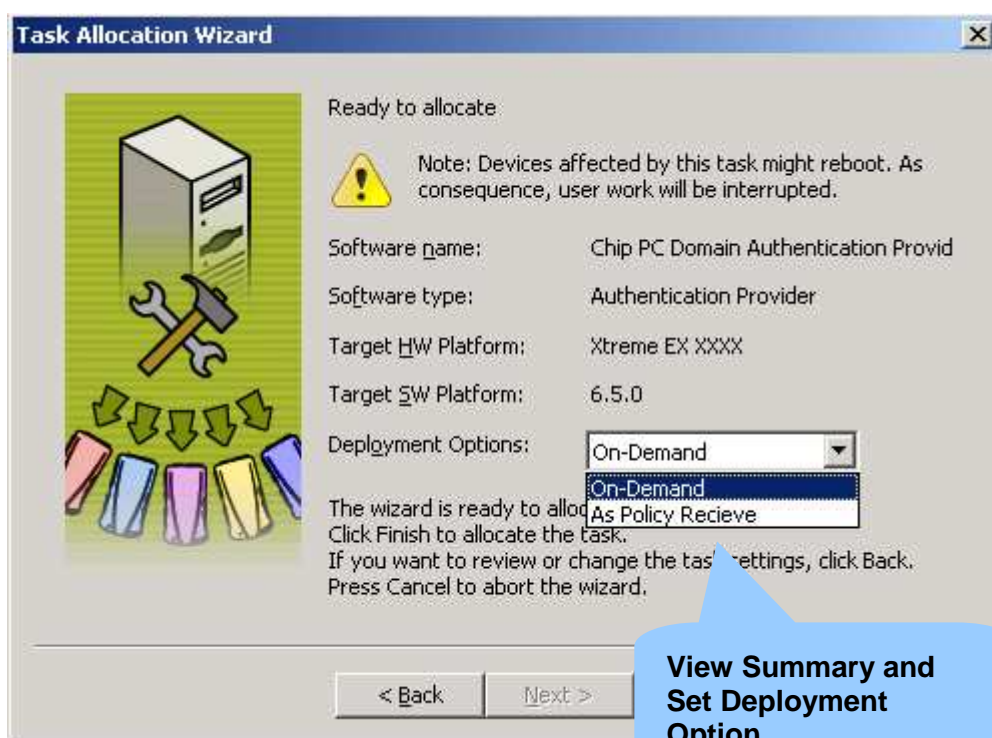
A blue callout bubble points to the table with the text: **Select Thin-Clients from the Farm Manager snap-in**

Task Allocation Wizard:

The Task Allocation Wizard allows you to trigger the software deployment process from the Xcalibur Farm Manager snap-in. This way, you can install software on target devices regardless of the Xcalibur Policy based Software Deployment method. The Task Allocation Wizard is especially useful for troubleshooting and testing scenarios where you want settings to apply immediately on target devices.







How to run the Task Allocation Wizard:

- From the Xcalibur Farm Manager snap-in expand the Farm \ Site \ IP Scope view and select the Thin-Clients on which you want to install software.
- Right click the selected devices and click the All Tasks \ Task Allocation Wizard...option.
- At the Welcome screen press *Next*.
- From the Select Task scroll down menu, choose the type of action to perform (Hotfix / Upgrade Plug-in installation) and then press *Next* to continue.
- To apply this task on clients running a specific hardware and/or firmware versions use the scroll down menus. Choose the All option to affect all the clients that where selected in step 1 and press *Next* to continue.
- From the scroll down menu select the package version that you want to install.
- Installation Options:
 - Install only if target version is newer: Install the software if the client is running an older software version. The software will be installed on clients that do not have this software at all and on clients that run older versions of this software. Clients that already have this software version installed will not be affected by this task.
 - Install automatically regardless of the software version: Force the installation on all selected clients even if this software is already installed.
 - Uninstall: Uninstall this software.

- Press Next to continue.
- View a summary of the task settings. When installing Firmware Upgrades and Hotfixes the Task Allocation Wizard immediately triggers clients address the installation service. However when plug-ins are installed you can choose between two downloading options:
 - As Policy Received: Once the Task settings are sent to the client it triggers an installation request and waits for the Plug-ins Installation Service Working Hours.
 - On-Demand: Installs plug-ins in a dynamic way. Plug-ins are only installed if required. The installation process is initialized once the plug-in is required.
- To complete the Task and apply its setting press Finish.

Recovery

Recovery is the process of restoring the client's firmware. During this process, a recovery image is installed on clients that suffer from a fatal firmware crash.

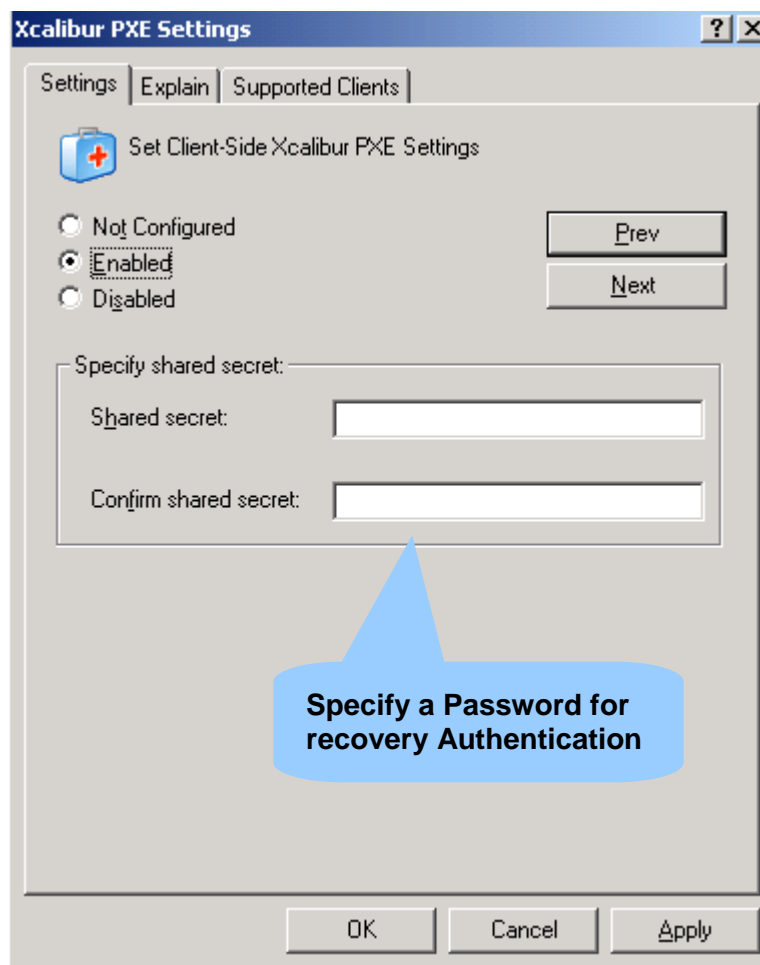
Devices that fail to boot due to a firmware crash automatically enter a recovery state. In this state the client sends a request for recovery to the Recovery Installation Service. This request is first sent by using the Xcalibur Independent Management Protocol. If the initial request fails, the client initiates a second request using PXE protocol. As response the Recovery Installation Service uploads a small-sized firmware version taking less bandwidth therefore shortening the recovery process duration as well as making it more reliable. Once recovery completes a full firmware upgrade can be initialized through the standard upgrade procedures.

Initial settings for Recovery:

As default, no client side settings are required to support recovery. The client's firmware has a built-in mechanism that enters the recovery state in case of a failure.

For increased security, it is possible to set a recovery password (also known as shared secret) that will be used during the recovery process initiation. Once set, both the client and the Recovery Installation Service must be configured with the same shared secret for mutual authentication. In case of a mismatch between the client's and service's password the recovery process is aborted. This allows preventing an unrecognized service from uploading recovery images on client devices.

Using Xcalibur Policy to set Recovery Shared Secret on client devices:



Xcalibur PXE Settings

Settings | Explain | Supported Clients

Set Client-Side Xcalibur PXE Settings

☐ Not Configured
☒ **Enabled**
☐ Disabled

Specify shared secret:

Shared secret:

Confirm shared secret:

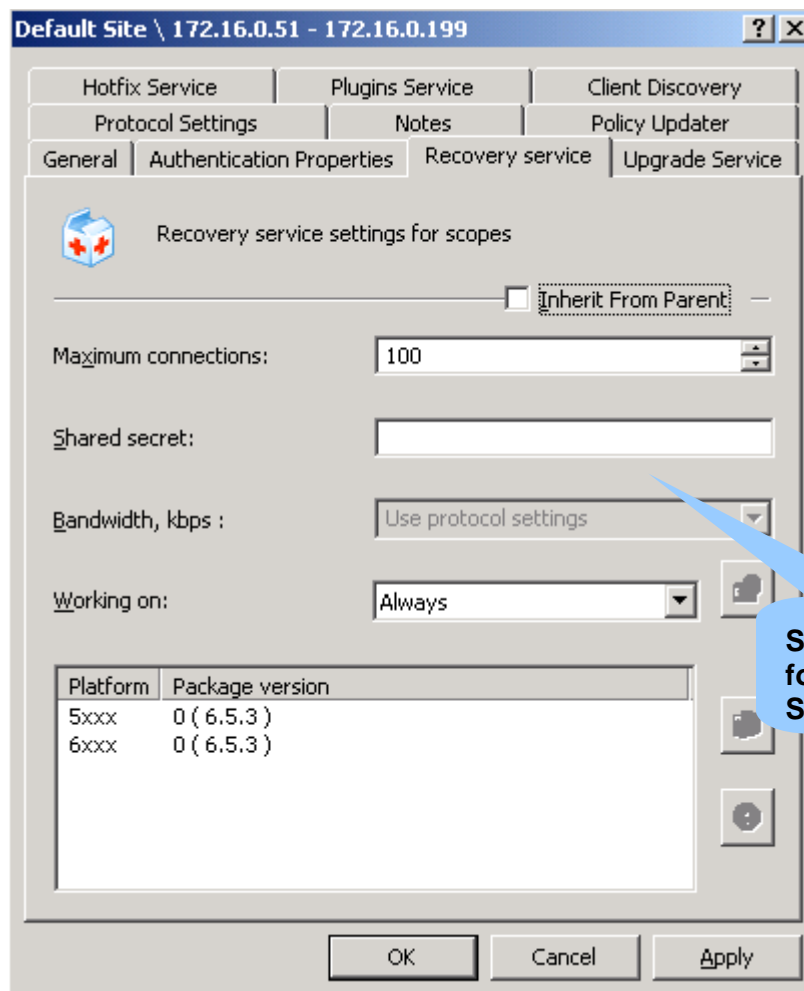
Specify a Password for recovery Authentication

OK Cancel Apply

- Create a new Xcalibur Policy
- In the Policy Tree expand the Device Configuration \ Network and Communications \ Recovery \ PXE container.
- Enable this policy to apply its settings.
- Specify a shared secret, press *OK* and then close all property windows.


Note Xcalibur Policies do not apply on clients that are in Recovery state.

Recovery Installation Service Configuration



Default Site \ 172.16.0.51 - 172.16.0.199

Hotfix Service | Plugins Service | Client Discovery
Protocol Settings | Notes | Policy Updater
General | Authentication Properties | **Recovery service** | Upgrade Service

 Recovery service settings for scopes

☐ Inherit From Parent

Maximum connections: 100

Shared secret:

Bandwidth, kbps : Use protocol settings

Working on: Always

Platform	Package version
5xxx	0 (6.5.3)
6xxx	0 (6.5.3)

OK Cancel Apply

**Set Conditions
for the Recovery
Service**

Recovery Installation Service Configuration:

- From the Xcalibur Farm Manager snap-in right click the Farm / Site or IP Scope, and then click Properties.
- Select the Recovery Service Tab.
- Clear the Inherit from Parent checkbox to disable inheritance.
- Maximum Connections: Set the maximum number of simultaneous client connections that can be connected to this service at the same time.
- Shared Secret: Set a password for the Recovery Service.
- Bandwidth, Kbps: Set the maximum bandwidth to be utilized by each client connection during the recovery process.
- Working on: The Recovery Service constantly listens for client requests. Once a request arrives, it is added to the service queue and will be handled during the service Working Hours.

- Working Hours: Specify when the service becomes operational (e.g. Off-Work hours / Midnight...etc)
- Always: The service immediately answers client requests.
- Manual Permission: Client requests are queued until an administrator manually approves them from the Tasks container.
- Press the Select Package button to browse through the Recovery package list (obtained from the Software Repository) and manually select which Recovery package version to install.
- Press OK to close all property windows.

System Restore

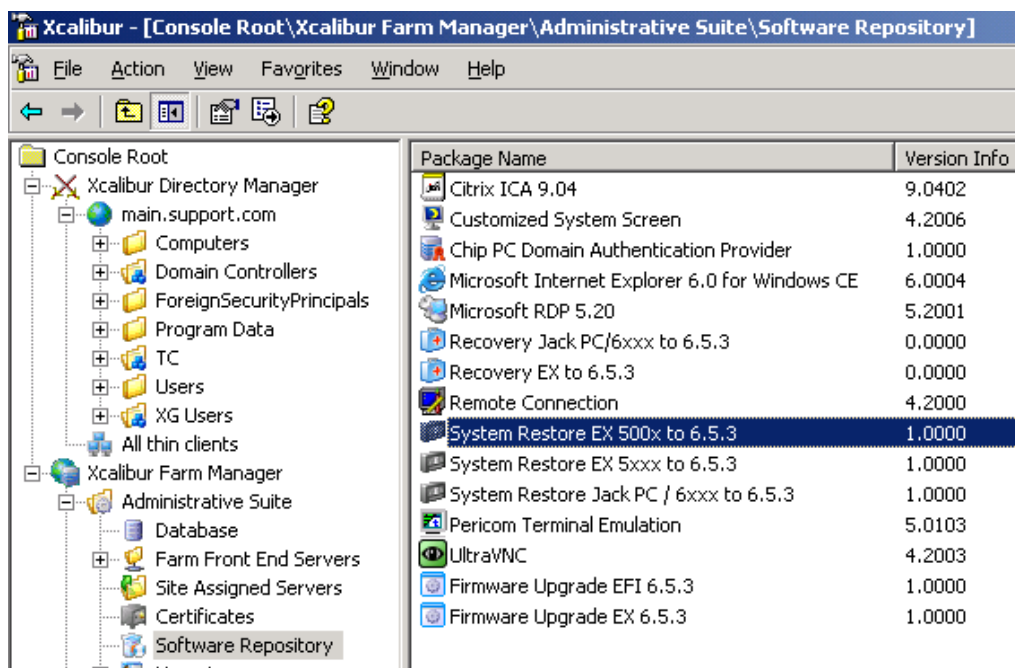
System restore is the process of restoring the client's firmware. During this process, a recovery image is installed on clients that suffer from a fatal firmware crash.

System restore can also be used to create an image once then installing it on multiple Thin-Clients that need to share the same settings.

The system restore image is created by a Thin-Client (see User Guide: Image 6.5.x on www.chippc.com) and stored in the repository container on Xcalibur.

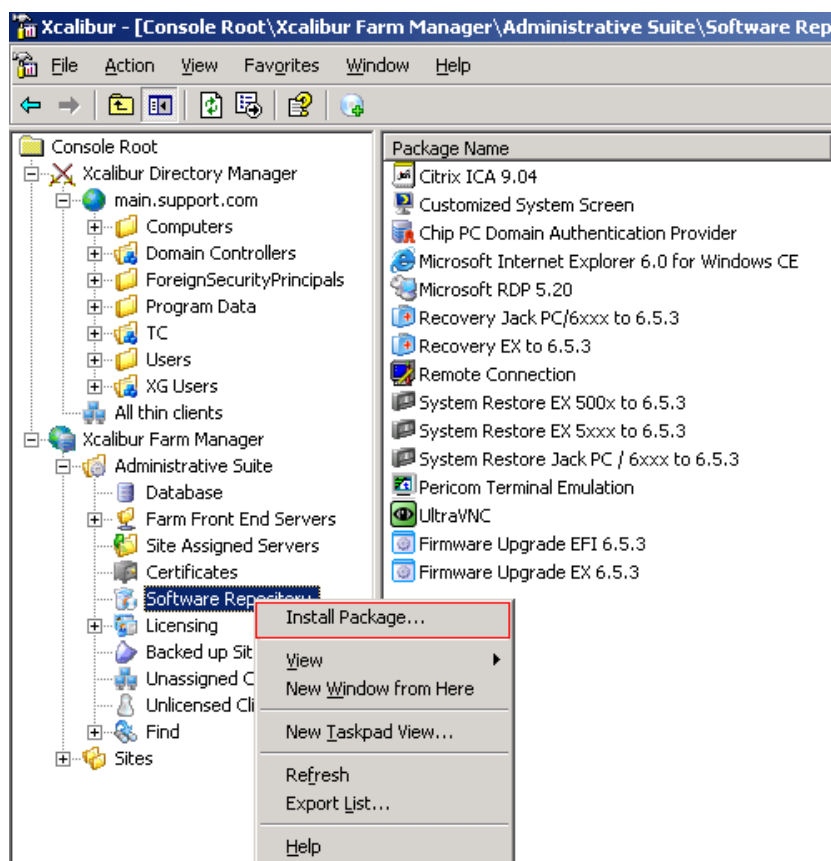
Install Package to Repository

Once a system restore image has been created by the Thin-Client it needs to be uploaded to Xcalibur in order to be available for future recovery.



Install Recovery Package onto Xcalibur:

- Under the Farm Manager, right click the software repository container



- From the dropdown menu choose the Install Package option.
- On the Install Package Wizard click Next to continue



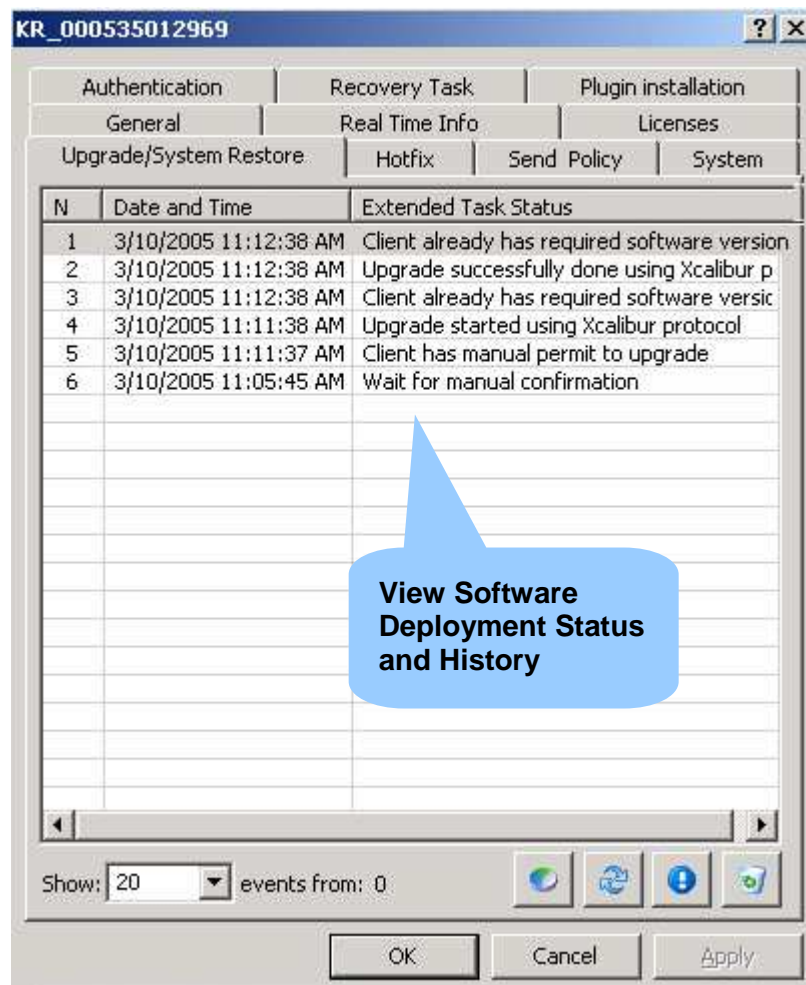
- Click on the Browse button to choose the system restore from its location.
- Click Finish to complete procedure

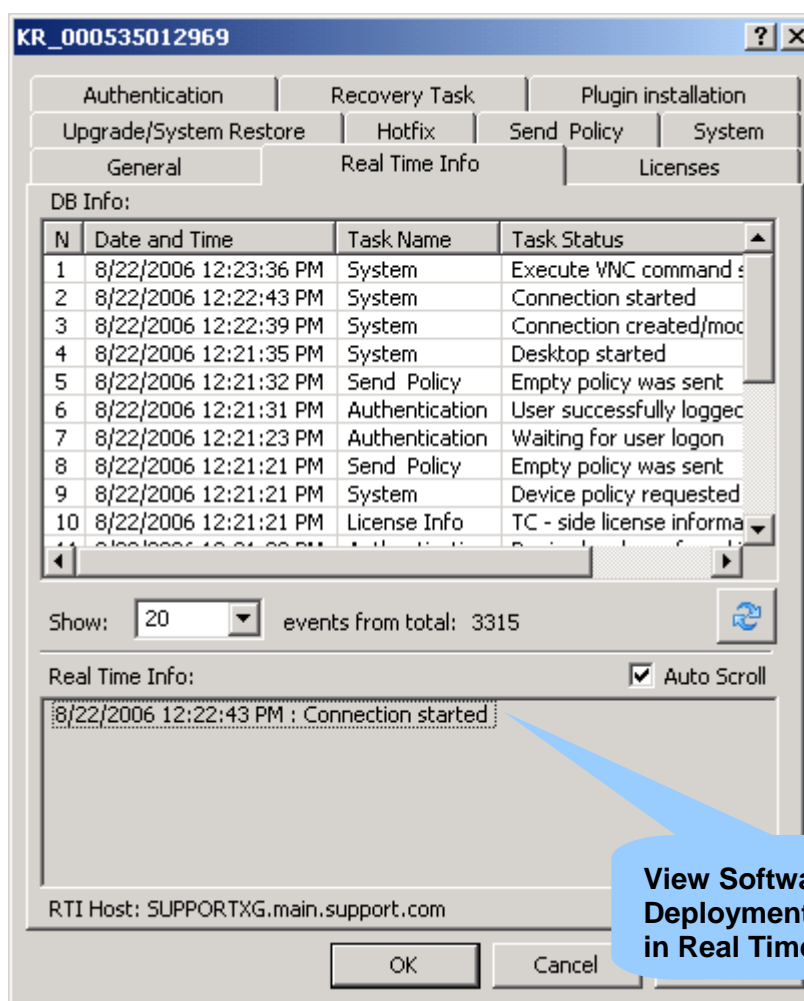
Deploy System Restore on Multiple Thin-Clients

System restore image can be deployed on multiple Thin-Clients through the "Task allocation Wizard" (see p. 90).

Monitoring Software Deployment

From within the Xcalibur Farm Manager you can monitor the software deployment process.





- **Viewing Installation Service Queues:** Under the Farm \ Site \ Tasks \ % installation Service Name% container you can view the installation service queue and manually Decline or/ Accept client requests.
- **Viewing Software Deployment History:** Information regarding software deployment history can be viewed under each client's properties, within the Upgrade, Hotfix, Recovery and Plug-in Installation tabs.
- **Monitoring Software Deployment in Real Time:** Real time information including policy application, software deployment and more is displayed under the Client Properties \ Real Time Info tab.

Appendix A Advanced Features

In addition to the features detailed in the previous chapters, the following advanced features are available:

- ThinX (Linux) Device Management
- Session Desk
- Super User
- VDI Broker
- Microsoft SMS Integration

Technical information regarding the above features is available in separate documents as follows:

- *How to Setup NFS for Xcalibur Global* (Ref# DL121H)
- *How to Use a Superuser* (Ref# DG079H)
- *Xcalibur Global – Session Desk* (Ref# DG077U)
- *Xcalibur Global - VDI Broker* (Ref# DG076U)
- *Asset Management of Chip PC Thin Clients via Microsoft SMS 2003* (Ref# DG078B)