March 2007
New Firmware and Software Updates

Installation Guide

Document Version 1.0

COPYRIGHT NOTICE

TRADEMARKS

U.S. GOVERNMENT RESTRICTED RIGHTS

Table of Contents

This page is left blank intentionally

Chapter 1 Preface

In March 2007, a number of software and firmware updates were released for Xcalibur Global Software Version 1.1 Rev. 2 and for Chip PC thin client devices.

This document provides instructions for the correct procedures that must be performed when installing the newly released updates.

Intended Audience

This document is targeted at system administrators required to manage Xcalibur Global software and Chip PC thin client devices.

Scope

The scope of this document includes the software and firmware updates released during March 2007 for Xcalibur Global Version 1.1 Rev. 2 and for Chip PC thin client devices.

Objectives

The objective of this document is to describe the correct procedures for installing the Software and Firmware Updates released during March 2007.

Reference Material

For further information, refer to the following Chip PC document:

- How to Install a Software Package into the Xcalibur Global Software Repository, Ref: DG040H
- March 2007 New FW and SW Updates – Release Notes, Ref: DG062N

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** or **Notes** contains supplemental information.

Chapter Overview

This document is divided into the following chapters:

- Chapter 1, “Preface”, provides general information about the document, its scope, objectives and reference material (if applicable).
- Chapter 2, “Procedures”, provides installation procedures when installing the newly released updates, including typical scenarios.
- Appendix A, “How to Locate Installation Policies”, describes how to locate policies that are responsible for Plug-in installations.
- Appendix B, “How to Refresh an Installation Policy”, describes how to refresh (re-apply) an Installation Policy.

Chapter 2 Procedures

Safety and Best Practice Notes

- The procedures described in this document must be carefully followed to ensure a successful installation and prevent data corruption.
- These procedures will cause thin client devices to reboot, therefore it is recommended to perform the procedures at a suitable time when a device reboot will cause minimal disruption to thin client device users.
- The execution of tasks specified in this document depend on the working schedule of the following services
  - Policy Updater
  - Upgrade Service
  - Plugins Service

Note For immediate response, all services should be set at the **IP Scope** level to **Always**.

- It is recommended to only install plug-ins that will actually be used. For example, if you only use RDP there is no need to install ICA.
- It is recommended not to upgrade components (Firmware and/or Plug-ins) that in their current installation are functioning in a satisfactory manner. Upgrade components only under the following circumstances:
  - You specifically need the new features provided by the upgrade.
  - The current installation is not functioning properly.
- New features may require additional licenses.
- If possible, it is strongly recommended that you test the installation procedure on a single client device before performing it on the entire production environment. The purpose of this test is to verify that there are no discrepancies between existing policies and the new software.
- The document “March 2007 New FW and SW Updates – Release Notes”, Ref: DG062N, should be read prior to performing the following procedures.

Licenses

Some of the new features in the March 2007 FW and SW Updates will require the Resource Kit License. The Resource Kit License is a bundled features license combining all tailor made solutions introduced by Chip PC during the last year. Each newly supported feature, which is defined as a Tailored Solution by Chip PC, will be supported using this license.

Important A Resource Kit license must be installed on a thin client before a policy containing Resource Kit features is applied to the client. If the license is installed after the policy has been applied, the policy on the device must be cleared (perform a “Reset to Factory Defaults” selecting only the “Clear Policy” option).

Software Requirements

Depending on the particular features/fixes you intend to implement, you will be required to install different software packages in Xcalibur Global and possibly upgrade device firmware.

Refer to the following table to determine the requirements for your installation:

Feature / Fix	Requirement			
	Plug-in	FW 6.5.5	Resource Kit v.2 + SP4	Installation Scenario
Wireless encryption and authentication	No	**Yes**	**Yes**	2
Host table	No	**Yes**	**Yes**	2
LPR3 Port	No	**Yes**	**Yes**	2
MTU adjusting	No	**Yes**	**Yes**	2
Security options for external storage devices	No	**Yes**	**Yes**	2
Upgrade with local settings restore	No	**Yes**	**Yes**	2
Lock button added to Task Manager	No	**Yes**	**Yes**	2
Internet Explorer URL length	No	**Yes**	**Yes**	2
New High Resolutions	No	**Yes**	**Yes**	2
Default Gateway – remote configuration	No	**Yes**	**Yes**	2

Feature / Fix	Requirement			Installation Scenario
	Plug-in	FW 6.5.5	Resource Kit v.2 + SP4	
Remote installation of certificates and private keys via Xcalibur Global	No	**Yes**	**Yes**	2
Local installation of certificates and private keys on local client device	No	**Yes**	No	2
Device renewal options on local device	No	**Yes**	No	2
Updated Daylight-saving time start dates.	No	**Yes**	**Yes**	2
Plug-in wireless deployment	**Relevant Plug-in**	**Yes**	**Yes**	2
Connection shortcuts in **Start Menu**	**Relevant Plug-in**	**Yes**	**Yes**	2
Smartcard security	**Smartcard Logon**	**Yes**	**Yes**	2
XMLHTTP + XMLSAX in internet explorer[1]	**Internet Explorer**	**Yes**	**Yes**	2
Internet Explorer persistent connection	**Internet Explorer**	**Yes**	**Yes**	2
Internet Explorer renewal option	**Internet Explorer**	No	No	1

[1] Not supported on device models EX5000 and EX5070.

Feature / Fix	Requirement			
	Plug-in	FW 6.5.5	Resource Kit v.2 + SP4	Installation Scenario
ICA persistent connection	**ICA**	**Yes**	**Yes**	2
PNA folders in **Start Menu**	**ICA**	**Yes**	**Yes**	2
Pericom persistent connection	**Pericom**	**Yes**	**Yes**	2
Pericom Device Type for COM port	**Pericom**	**Yes**	**Yes**	2
UltraVNC new resolutions	**UltraVNC**	**Yes**	**Yes**	2
RDP persistent connection	**RDP**	**Yes**	**Yes**	2
RDP mapping external storage into session – bug fix	**RDP**	No	No	1

Installation Scenarios

The installation procedures described in this chapter are divided into different Installation Scenarios. Installation scenarios are defined according to the particular features/fixes you intend to install. Each installation scenario will correspond with a distinctive installation procedure.

Before beginning the installation, it is necessary to select the appropriate installation scenario in order to determine the correct installation procedure.

Review the following sections to determine the installation scenario you should select.

Installation Scenario #1

Select this scenario if you intend only to install one or more updated plug-ins.

Installation Scenario #2

Select this scenario for any installation that does not fit the specifications of Installation Scenario #1.

Prerequisites

Prior to beginning the installation, make sure that the following prerequisites are met:

- An updated backup of the Xcalibur Global database has been performed (using standard SQL tools).
- The user performing the upgrade has been granted all necessary permissions.
- Installation scenario #2 only:

1. **Service Pack SP2** is already installed.
2. **2007 Resource Kit v.1 & SP3** is already installed.

Note **Service Pack SP2** must be installed prior to installing **2007 Resource Kit v.1 & SP3**. For detailed information regarding the installation of these packages refer to the documents:

- “November 2006 New FW and SW Updates - Installation Guide”, Ref: DG042U-1.0
- “January 2007 New FW and SW Updates - Installation Guide”, Ref: DG057U-1.0

Installation Scenario #1

Overview

The procedure outline details the steps required to perform this installation.

The outline can be used as a checklist to keep track of your progress during the installation and help you verify that you have completed all the required steps.

Procedure Outline

1. Verify all prerequisites are met.
   - 1.1 Database backup.
   - 1.2 User permissions.
2. Perform the installation tasks.
   - 2.1 Install new versions of plug-ins to the Software Repository.
   - 2.2 Locate the plug-in installation policies.
   - 2.3 Refresh the plug-in installation policies.

Installation Procedure

#	Task	Notes	Expected behavior
1.	Install the new versions of the plug-ins into the Software Repository.	Refer to the following Chip PC document: How to Install a Software Package into the Xcalibur Global Software Repository (Ref: DG040H).	The plug-ins are installed into the Software Repository overriding the previous plug-in versions.
2.	Locate the plug-in installation policies[2].	Locate the polices that install the plug-ins that have received new versions.	N/A
3.	Refresh the plug-in installation policies[3].	This will cause Xcalibur Global to re-apply the policies and install the new version of the plug-in on the client devices.	Devices get Policy Updates[4] that install[5] the new plug-in versions, overriding the previous plug-in versions.

[2] Refer to Appendix A for information on how to locate install policies.

[3] Refer to Appendix B for information on how to refresh the install policy.

[4] Influenced by the Policy Updater schedule.

[5] Influenced by the Plugins Service schedule.

Installation Scenario #2

Overview

The procedure outline details the steps required to perform this installation.

The outline can be used as a checklist to keep track of your progress during the installation and help you verify that you have completed all the required steps.

Note Depending on the particular features/fixes you intend to install, some of the installation tasks might not be required.

Procedure Outline

1. Verify all prerequisites are met.
   - 1.1 Database backup.
   - 1.2 User permissions.
   - 1.3 2007 Resource Kit v.1 & SP3 installation.
2. Perform the installation tasks.
   - 2.1 Install new plug-ins to the Software Repository.
   - 2.2 Install updated plug-ins to the Software Repository.
   - 2.3 Install the 2007 Resource Kit v.2 & SP4 to the Software Repository.
   - 2.4 Install new firmware version 6.5.5 to the Software Repository.
   - 2.5 Install Resource Kit License (if not already installed).
   - 2.6 Create a policy to save local settings during upgrade.
   - 2.7 Deploy new firmware version to thin client devices.

Installation Procedure

	Task	Notes	Expected Behavior
4.	Install the updated plug-ins to the Software Repository	Refer to the following Chip PC document: "How to Install a Software Package into the Xcalibur Global Software Repository", Ref: DG040H.	The plug-ins are installed to the Software Repository overriding the previous plug-in versions.
5.	Install the new plug-ins to the Software Repository		The plug-ins are installed to the Software Repository.
6.	Install the 2007Resource Kit v.2 & SP4 to the Software Repository.		2007 Resource Kit v.2 & SP4 is installed to the Software Repository.
7.	Install the firmware version 6.5.5 upgrade packages to the Software Repository.		The firmware packages are installed to the Software Repository.
8.	Install the Resource Kit license (if not already installed).	The license is required to activate the tailor made solutions provided by the Resource Kit.	Resource Kit license is installed in the Xcalibur Global Licensing.
9.	Create a policy to save local settings during upgrade[6].	Refer to the following Chip PC document: "How to Use Xcalibur Global to Preserve Local Settings During an Upgrade", Ref: DG064H.	The policy will preserve local settings during the firmware upgrade process.
10.	Deploy the new firmware version 6.5.5 upgrade packages to client devices.	Use Xcalibur Global Policy or the Task Allocation Wizard.	Client devices are upgraded to firmware 6.5.5 and the new versions of existing plug-ins are installed.

[6] Requires the Resource Kit license

Appendix A How to Locate Installation Policies

Appendix A describes how to locate the policies that are responsible for Plug-in installations; this is achieved by using the Show Resulting Policy function.

Overview

In this method, you will generate a resulting policy that resolves the name and location of the Xcalibur Policy that is responsible for installing the selected Plug-in. Refer to Appendix B to learn how to refresh (re-apply) this policy.

Procedure Outline

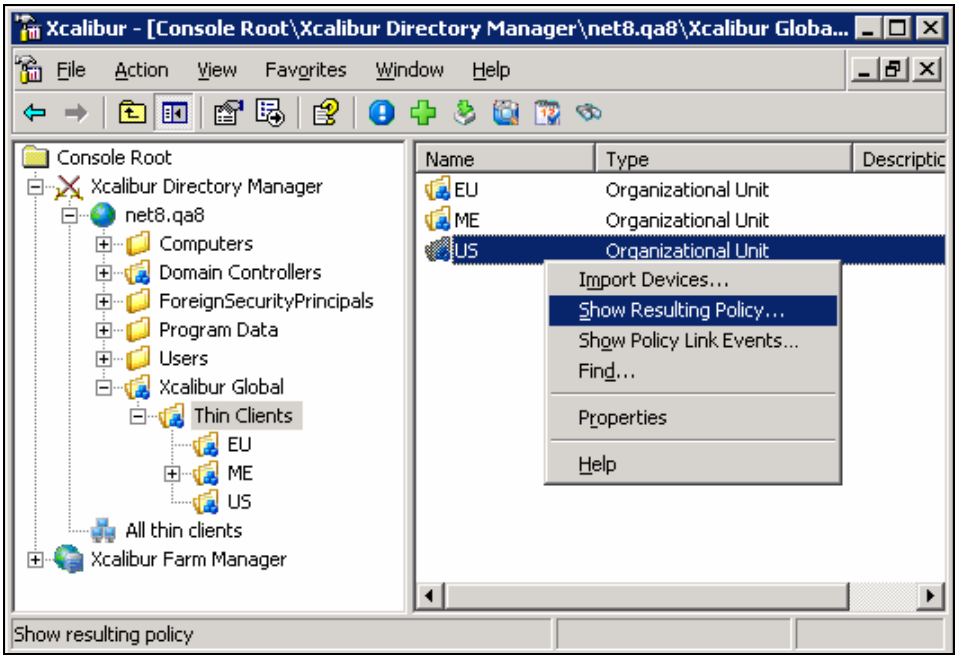
1. Select an OU\device affected by a policy that installs a plug-in you intend to update.
2. Generate Resulting Policy.
   2.1 Browse to the Installation Policy section.
   2.2 Find the name of the Xcalibur Policy responsible for the installation.
   2.3 Find where the policy is linked.
3. Refer to Appendix B.

Procedure

To illustrate the steps of this procedure we shall use an example of an Xcalibur Global environment. In this example:

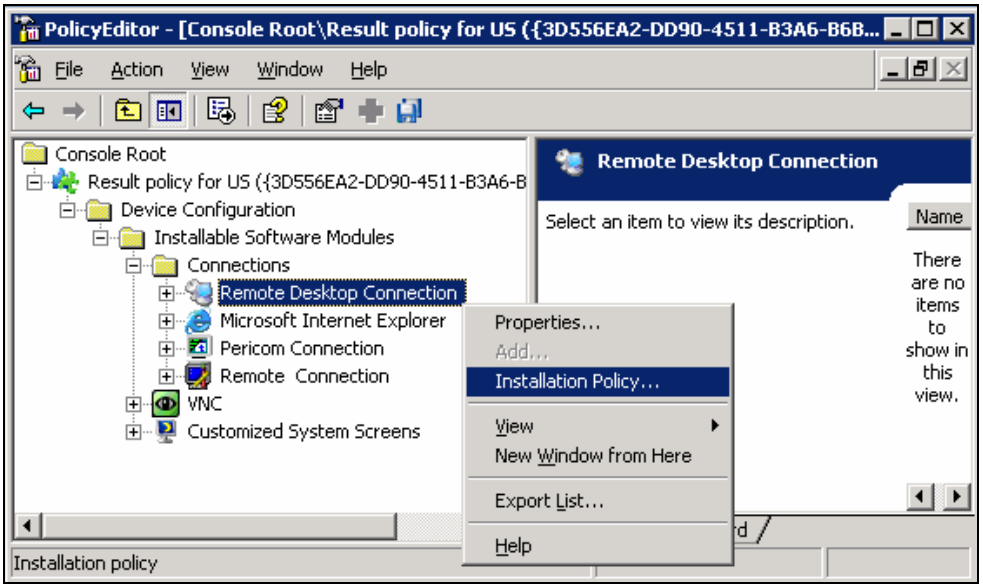
- The target OU is **US**.
- The Plug-in to be updated is **RDP**.
- The name of the installation policy is **Device – RDP 5.2 – Install**.
- The domain is **net8.qa8**.

1. In the **Xcalibur Directory Manager** select and highlight an OU that is affected by a policy that installs a plug-in you intend to update. From the right-click menu select **Show Resulting Policy…**, as illustrated, to display the **PolicyEditor** window.



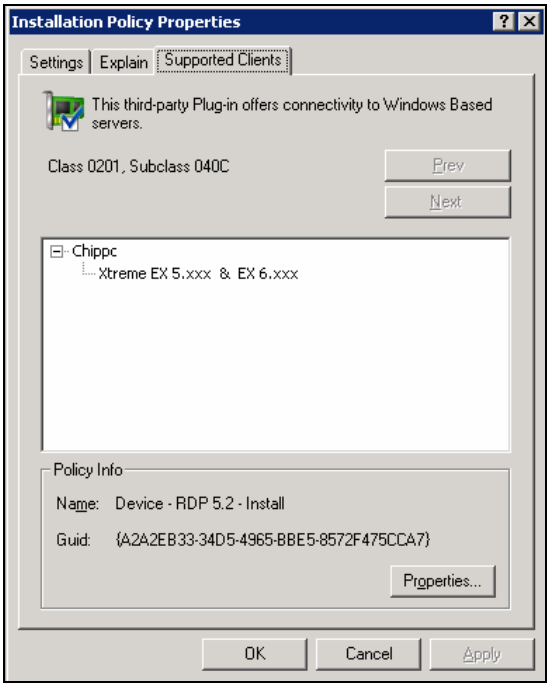
2. The **PolicyEditor** window displays, showing the resulting policy of the OU.

3. In the **PolicyEditor** window, expand **Result policy for *<OU Name>*, Device Configuration, Installable Software Modules, Connections.**



4. Select and highlight the plug-in (in this example **Remote Desktop Connection**), as illustrated above, then from the right-click menu select **Installation Policy…**.to display the **Installation Policy Properties** window.

5. In the **Installation Policy Properties** window, as illustrated, click the **Supported Clients** tab to display the **Supported Clients** tab page.



6. In the **Supported Clients** tab page, as illustrated above, the section **Policy Info** displays the policy name.
7. Write down this policy name for future reference, exactly as it appears (in this example **Device – RDP 5.2 – Install**).

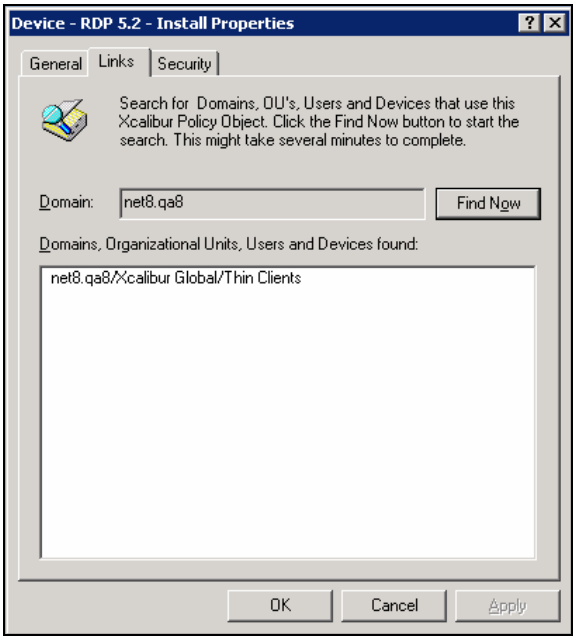
Notes This is the name of the policy responsible for installing the RDP Plug-in on devices residing at the selected level (in this example the **US** Organizational Unit).

8. In the **Supported Clients** tab page, click **Properties…** to display the ***<Policy Name>*** **Properties** window, then click the **Links** tab to display the **Links** tab page.

9. The **Links** tab page, as illustrated, lists the objects to which the installation policy (**Device – RDP 5.2 – Install**) is linked.
10. Write down the name of one object from the list (any object will do) for future reference.

Notes The **Links** tab indicates where the policy responsible for installing the RDP Plug-in is linked (in this example **net8.qa8/Xcalibur Global/Thin Clients**). This information will be used in Appendix B in order to refresh this policy.

Notes In this example the OU **US** whose resultant policy was examined, received the installation policy via inheritance and not as the result of a direct link between the policy and the OU. As a result, the OU **US** does not appear in the list of linked objects and instead one of its parent OUs appears in the list.



11. In the ***<Policy Name>*** **Properties** window, click **OK** to close the window and return to the **Installation Policy Properties** window.
12. In the **Installation Policy Properties** window, click **OK** to close the window and return to the **PolicyEditor** window.
13. In the **PolicyEditor** window, from the main menu select **File, Exit** to close the window and return to the **Xcalibur Directory Manager**.

This page is left blank intentionally.

Appendix B How to Refresh an Installation Policy

Appendix B describes how to refresh an Installation Policy. Refreshing a policy causes Xcalibur Global to re-apply the policy.

Prerequisites

In order to perform the procedures in this appendix the following information that was acquired in appendix A must be available:

- Policy – the name of the installation policy we plan to refresh.
- Object – the name and type of the object to which the policy is linked.

Overview

In this appendix we will locate the object that was selected in the previous appendix and then we will edit the policy that was selected in the previous appendix. We will not change anything in the policy, only open and close the Installation Policy section of the plug-in we have updated; this will refresh the policy and cause Xcalibur Global to re-apply it.

Procedure Outline

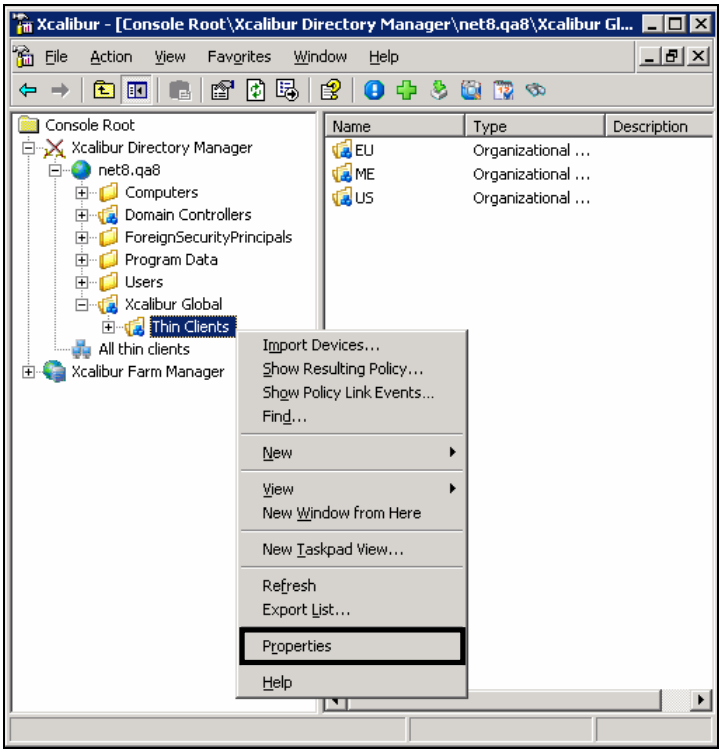
1. Go to the object where the policy is linked. In this example: **net8.qa8/Xcalibur Global/Thin Clients**.
2. Browse to the Xcalibur Policy tab.
3. Edit the policy responsible for installing the Plug-in. In this example: **Device – RDP 5.2 – Install**.
   - 3.1 Browse to the Installation Policy section.
   - 3.2 Open then close the Installation Policy window (causing the Policy to refresh).

Procedure

To illustrate the following procedures we are using an Xcalibur Global environment with the following parameters:

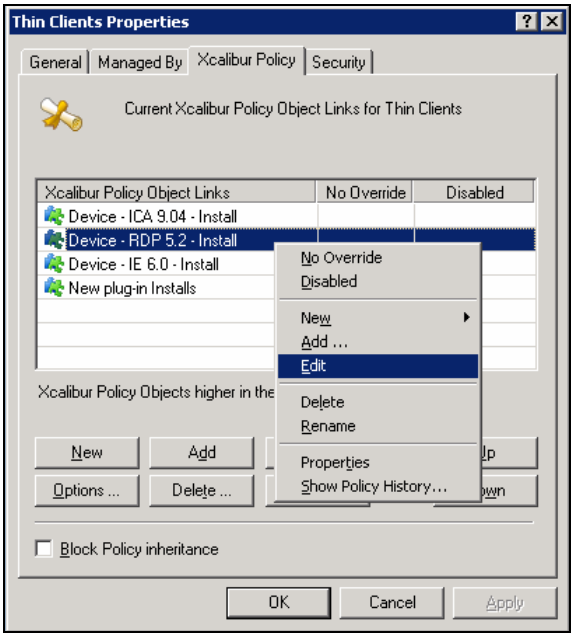
- The domain is **net8.qa8**.
- The plug-in updated is **RDP**.
- The object from appendix A is the OU **Thin Clients** (this is an OU that the installation policy is linked to).
- The policy from appendix A is **Device – RDP 5.2 – Install** (this is the name of the plug-in installation policy).

1. In the **Xcalibur Directory Manager** located the object from appendix A; in our example expand the domain **net8.qa8**, then expand the OU **Xcalibur Global**.
2. Select and highlight the object; in our example the OU **Thin Clients**.
3. From the right-click menu select **Properties**, as illustrated, to display the ***<OU name>*** **Properties** window.

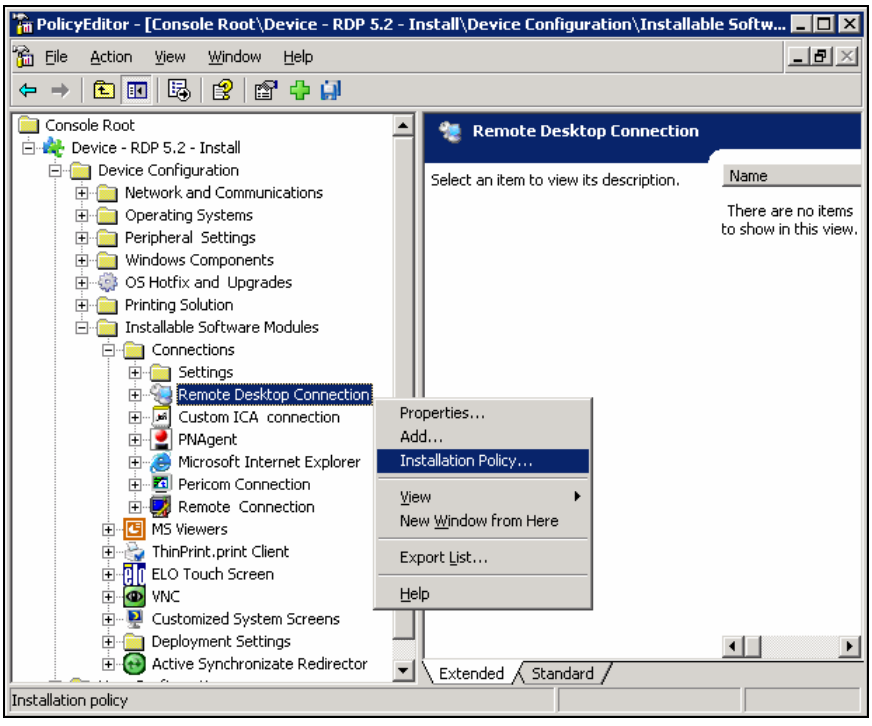


4. In the ***<OU Name>*** **Properties** window (**Thin Client Properties**) click the **Xcalibur Policy** tab to display the **Xcalibur Policy** tab page.

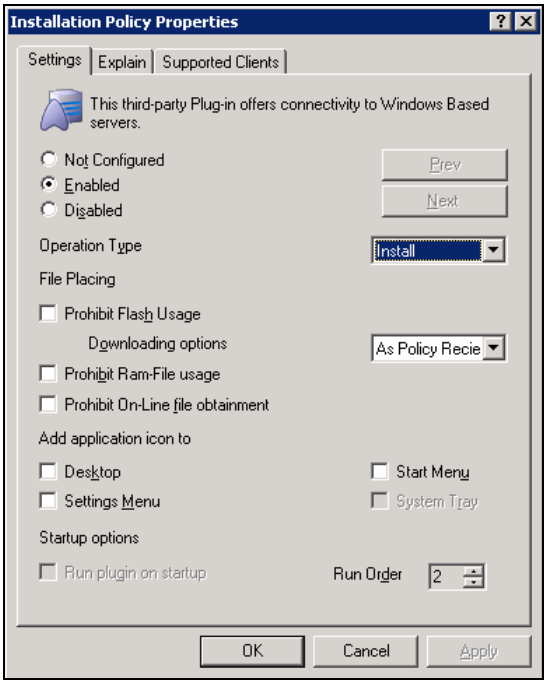
5. In the **Xcalibur Policy** tab page, right click on the policy from appendix A (**Device – RDP 5.2 – Install**), as illustrated, then from the right-click menu select **Edit** to display the **PolicyEditor** window.



6. The **PolicyEditor** window displays the policy settings. In the **PolicyEditor** window expand ***<Policy Name>*, Device Configuration, Installable Software Modules,** and locate the plug-in that has been updated (**Remote Desktop Connection)**. Some of the plug-ins are located ins the sub-branch **Connections**.



7. Select and highlight the plug-in, as illustrated, then from the right-click menu select **Installation Policy…**.to display the **Installation Policy Properties** window, as illustrated.



8. In the **Installation Policy Properties** window click **OK** to close the window and return to the **PolicyEditor** window.

Notes Changing the Installation Policy settings is not necessary, opening and closing the **Installation Policy Properties** window is enough to cause the policy to refresh.

9. In the **PolicyEditor** window from the main menu select **File, Exit** to close the window and return to the ***<OU Name>* Properties** window.
10. In the ***<OU Name>* Properties** window click **OK** to close the window and return to the **Xcalibur Global Management Console**.

Note Following the installation of the 2007 Resource Kit v.1 & SP3, question mark symbols may appear in the policy tree, either when editing a policy or when creating a new policy from a template. This behavior is expected and is by design and in no way should it be interpreted as indicating an error or problem with the functionality of Xcalibur Global.

When this occurs while creating a new policy from a template, a dialog window titled “Custom policy import” will appear. You may ignore all of the options and simply click the “Import” button to proceed with the normal policy creation process.