Using the Smartcard Logon Plug-in

Technical Brief

Document Version 1.0

COPYRIGHT NOTICE

TRADEMARKS

U.S. GOVERNMENT RESTRICTED RIGHTS

Table of Contents

This page is left blank intentionally.

Chapter 1 Preface

This chapter provides general information about the document.

Intended Audience

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

Scope

This document is applicable to the following product versions:

- Xcalibur Global 1.1 rev.2
- ChipPC client device firmware 6.5.4
- Smartcard Logon plug-in 4.2

Objectives

The objective of this document is to provide the technical knowledge and understanding that is required to correctly and effectively use the Smartcard Logon plug-in on Chip PC thin clients.

Prerequisites

1. This document assumes that the reader has at least a mid-level technical understanding in the field of Xcalibur Global administration.
2. To implement the procedures in this document, the user will need a smartcard with a Smartcard Logon certificate or a Smartcard User certificate. For detailed instructions on installing a certificate onto a smartcard, refer to the Microsoft document: “Certificate enrollment using smart cards” at http://support.microsoft.com/kb/257480

Reference Materials

- “Xcalibur Global - Administrator’s Guide”, Ref: DG018U
- “How to Install a Software Package into the Xcalibur Global Software Repository”, Ref: DG040H
- “How to Install a License File into the Xcalibur Global Database”, Ref: DG060H
- “How to Use the Task Allocation Wizard to Install a Plug-in via Xcalibur Global”, Ref: DG059H.
- “How to Install the VNC Plug-in via Xcalibur Global”, Ref: DG026H

Document Features

Conventions

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

Caution	Text marked **Caution** contains warnings about possible loss of data.

Important	Text marked **Important** contains information that is essential to completing a task.

Note Text marked **Note** contains supplemental information.

Chapter Overview

This document is divided into the following chapters:

- Chapter 1, “Preface”, provides general information about the document.
- Chapter 2, “Introduction”, This chapter provides general information regarding the plug-in functionality and relevant smartcard information.
- Chapter 3, “Managing the Smartcard Logon Plug-in via Xcalibur Global”, describes how to configure and deploy the Smartcard Logon plug-in to thin clients via the Xcalibur Global management software.
- Appendix A, “Implementing a Typical Smartcard Logon Solution”, describes a typical implementation of a smartcard single sign-on solution.

Chapter 2 Introduction

This chapter provides general information regarding the plug-in functionality and relevant smartcard information.

Smartcard Concepts

PIN Code

Each smartcard has a Personal Identification Number (PIN). This PIN code can be used as a password to control access to the information stored on the smartcard.

Certificate

Each smartcard can store one or more certificates. A certificate is a file with information that can be used for authentication, logon, encryption and other purposes.

Plug-in Functionality

The Smartcard Logon plug-in enables the use of a smartcard to secure the thin client and prevent unauthorized access to the device.

security is achieved by using the following methods:

- Authentication of smartcard certificate:
  1. The plug-in reads the values of certain fields in the certificate that is stored on the smartcard.
  2. The plug-in compares the values it has read to corresponding values entered during the plug-in configuration.
  3. If any one of the values that is read from the smartcard, does not match the corresponding pre-configured value, then access to the client device is blocked.
  4. If all values match, the plug-in uses the credentials stored in the smartcard in order to execute an automatic logon to the client device.

  The fields that can be examined in the authentication process are:
  - Issuer CN
  - Principal Domain Name
  - Certificate Validity Date
- Requiring a PIN Code - The plug-in can require the user to enter a PIN code. The user will be able to work on the thin client only if the correct PIN code is entered.
- Smartcard removal behavior – if the smartcard is removed the plug-in can restart, logoff or lock the client device.

Supported Smartcards & Readers

Smartcards

The Smartcard Logon plug-in has been successfully tested with the following smartcards:

- Instant EID, SETEC (www.setec.com)
- NetMaket EiD, NetMaker (www.netmaker-cg.com)

Card Readers

The Smartcard Logon plug-in has been successfully tested with the following card readers:

- Manufacturer: SCM Microsystems (www.scmmicro.com)
- Models:
  - SCR331
  - SCR335
  - SCR338 (keyboard)
  - SCR3310
  - SCR3311

Important	The items listed above are the only smartcards and card readers that are officially approved by Chip PC for use with the Smartcard Logon plug-in. To verify the possible compatibility of other smartcards and card readers that are not included in the lists above, please contact Chip PC support at: http://www.chippc.com/support/request-support/

Chapter 3 Managing the Smartcard Logon Plug-in via Xcalibur Global

The following chapter describes how to configure and deploy the Smartcard Logon plug-in to thin clients via the Xcalibur Global management software.

Installing the Smartcard Logon Plug-in into Xcalibur Global

Complete the following installation steps to enable the management of the Smartcard Logon plug-in via Xcalibur Global:

1. Install the plug-in software package into the Xcalibur Global Software Repository.
   For detailed instructions, refer to the document: “How to Install a Software Package into the Xcalibur Global Software Repository”, Ref: DG040H.
2. Install the plug-in license file into the Xcalibur Global Licensing.
   For detailed instructions, refer to the document: “How to Install a License File into the Xcalibur Global Database”, Ref: DG060H.

Deploying the Smartcard Logon Plug-in to Thin Clients

The Smartcard Logon plug-in can be deployed to thin clients using one of the following methods:

- The Task Allocation Wizard
  For detailed instructions, refer to the document: “How to Use the Task Allocation Wizard to Install a Plug-in via Xcalibur Global”, Ref: DG059H.
- An Xcalibur Policy
  For detailed instructions, refer to the document: “How to Install the VNC Plug-in via Xcalibur Global”, Ref: DG026H (the same procedure used for the VNC plug-in applies to the Smartcard Logon plug-in).

Note The actual execution of the installation tasks will depend on the working schedule of the **Policy Updater** and the **Plugins Service**.

Configuring the Smartcard Logon Plug-in

The following procedure describes the method for configuring the Smartcard Logon plug-in via an Xcalibur Global Policy.

The method is based on the following steps:

1. Select the OU containing the target device.
2. Create an Xcalibur Policy that is linked to the selected OU.
3. Configure the Xcalibur Policy to configure the Smartcard Logon plug-in.

Procedure

Select the OU Containing the Target Device

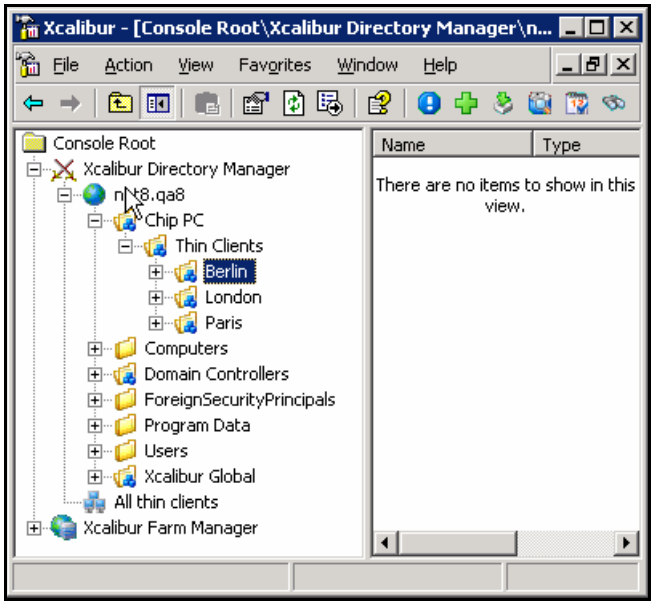
- The OU in our example is **Berlin**
- The Domain in our example is **net8.qa8**

1. Launch the Xcalibur Global Management Console.

   From the Task Bar select:

   Start \ Programs \ Xcalibur Global 1.1 \ Management Console.

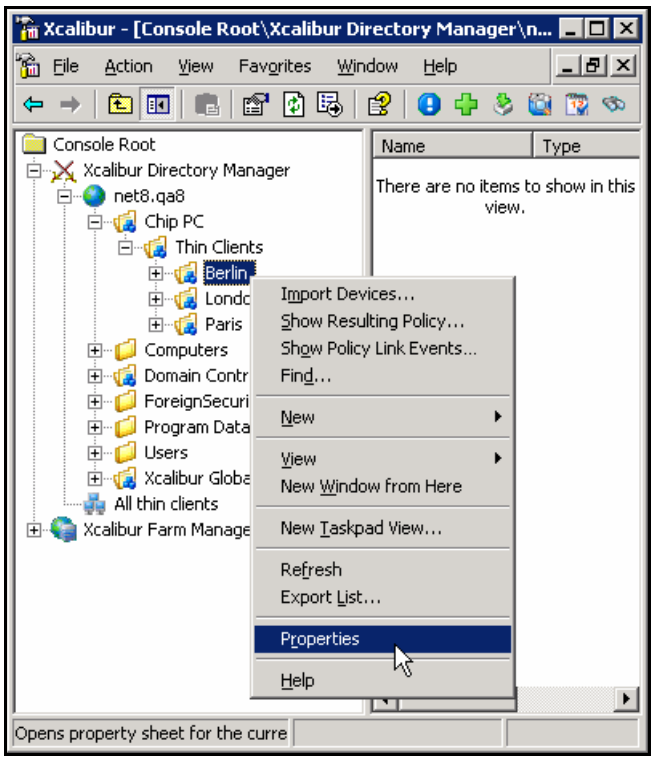
2. Expand the folders containing the OU.
   In this example expand:
   Xcalibur Directory Manager \ net8.qa8 \ Chip PC \ Thin Clients



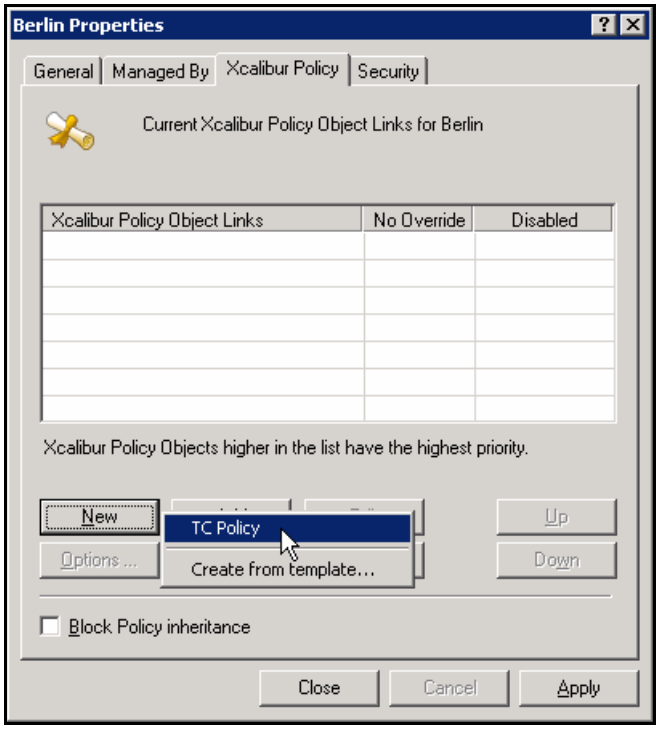
3. Select the OU **Berlin**.

Create an Xcalibur Policy that is linked to the selected OU

1. Right-click on the OU (Berlin) to open a drop-down menu.
2. Select **Properties** from the drop-down menu, as displayed:



3. The ***<OU>* Properties** window will open.
4. Select the **Xcalibur Policy** tab.
5. Click the **New** button and select **TC Policy** from the drop-down menu.

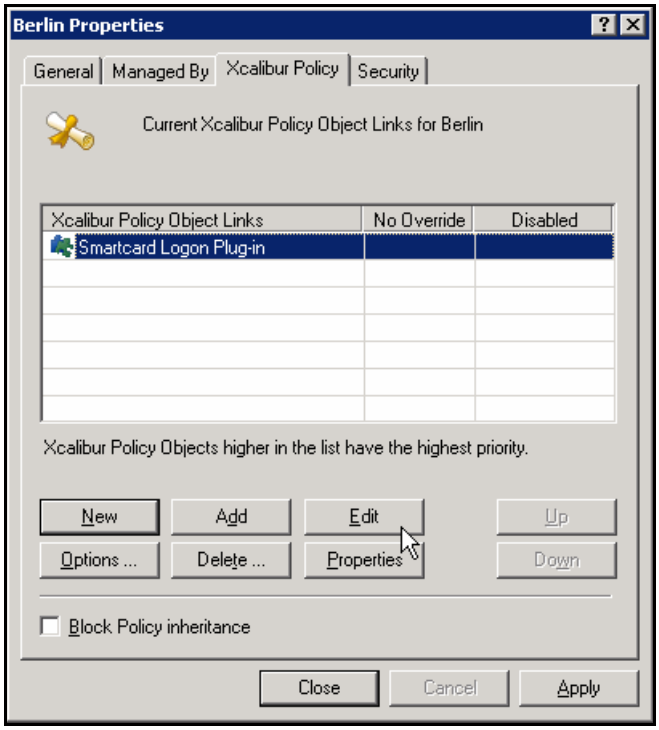


6. A **New Xcalibur Policy Object** is created in **the Xcalibur Policy Object Links** column.

7. Enter a new name for the policy. In this example, we will use the name **Smartcard Logon Plug-in**. Press **Enter**.

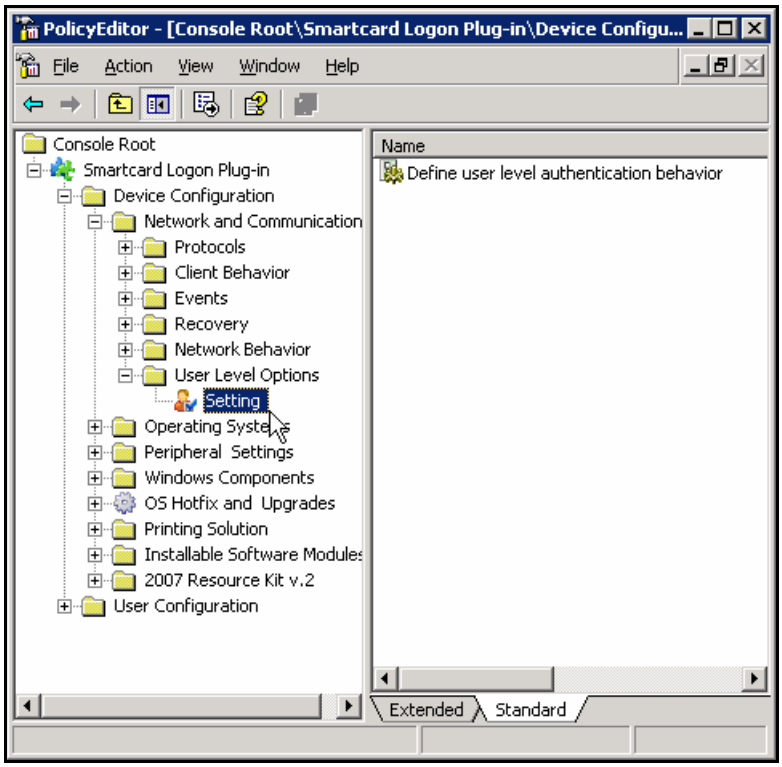
Configure the Xcalibur Policy to configure the Smartcard Logon plug-in.

1. Select the newly created policy.
2. Click **Edit** to open the **Xcalibur Policy Editor**



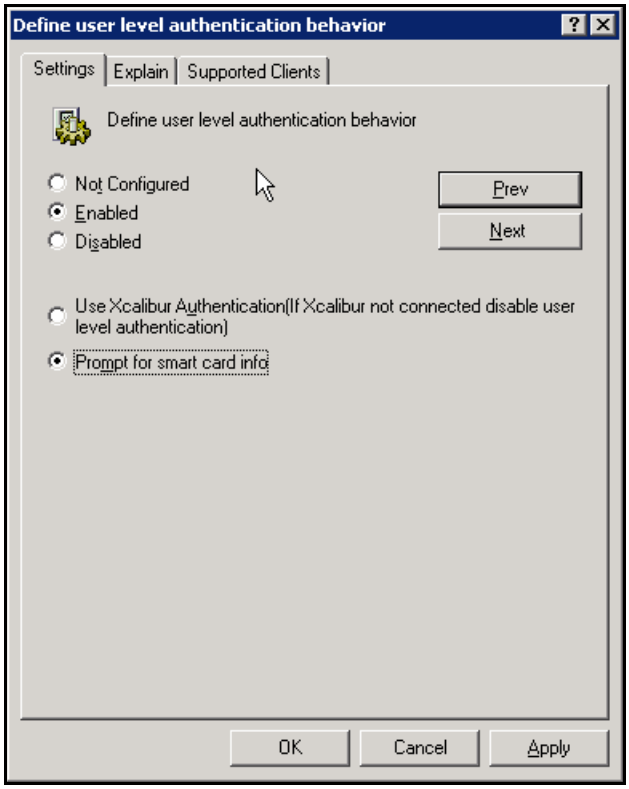
3. The **Xcalibur Policy Editor** window will open.
4. Expand the following policy branch:

   ***<policy name>* \ Device Configuration \ Network and Communications \ User Level Options**
5. Select the **Setting.**



6. In the right pane, double-click on **Define user level authentication behavior**.

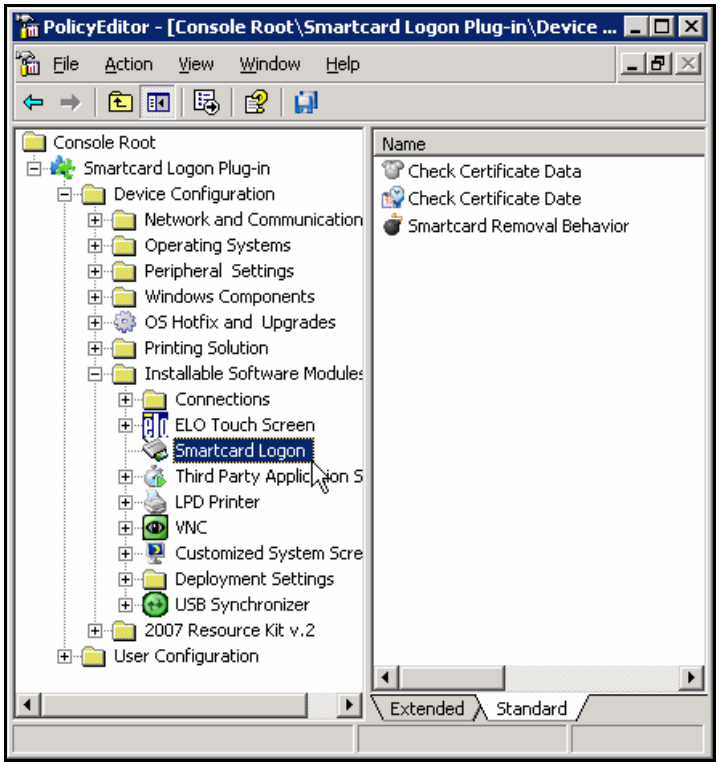
7. The **Define user level authentication behavior** window will open.
8. Select the **Enabled** option.
9. Select the **Prompt for smart card info** option.



Note The purpose of this option is to configure the thin client to refer to the smartcard for user level authentication credentials. The alternative option is to refer to Xcalibur Global for these credentials.

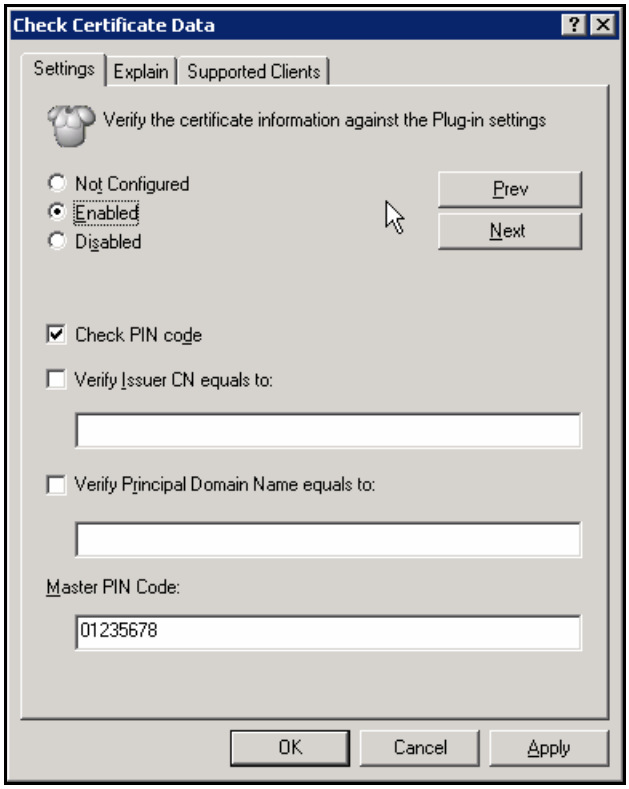
10. Click **OK** to save your settings and exit the Define user level authentication behavior window.

11. Expand the following policy branch:
    ***<policy name>* \ Device Configuration \ Installable Software Modules**
12. Select the **Smartcard Logon** object**.**



13. In the right pane, double-click on **Check Certificate Data**.

14. The **Check Certificate Data** window will open.
15. Select the **Enabled** option.
16. The **Check PIN code** is enabled by default.



17. Enable or disable any of the following fields:

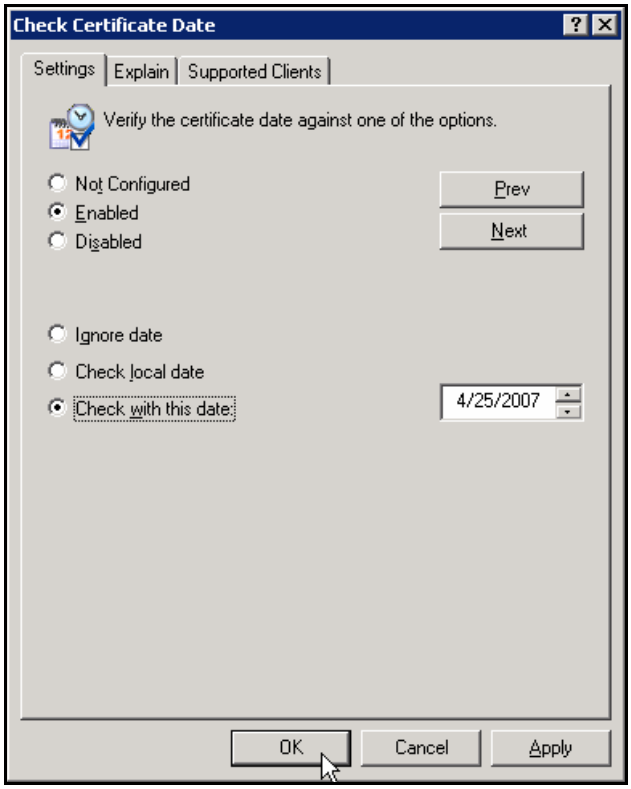
    Check PIN code – enabling this option will require the user to enter the correct PIN code in order to use the smartcard to logon to the thin client.

    Verify Issuer CN equals to – enabling this option will check if the string entered in the corresponding field is identical to the **Issuer CN** field of the certificate that is stored on the smartcard. If the verification fails, login will fail.

    Verify Principal Domain Name equals to – enabling this option will check if the string entered in the corresponding field is identical to the **Principal Domain Name** field of the certificate that is stored on the smartcard. If the verification fails, login will fail.

18. Enter a string into the **Master PIN Code** field. This string will allow you to override the plug-in protection and access the plug-in configuration on a thin client without requiring a successful user logon. The Master PIN Code is intended for administrative purposes only and should not be disclosed to the end user.
19. Click **OK** to save your settings and exit the Check Certificate Data window.

20. In the right pane, double-click on **Check Certificate Date**.
21. Select the **Enabled** option.



22. Select one of the following options:

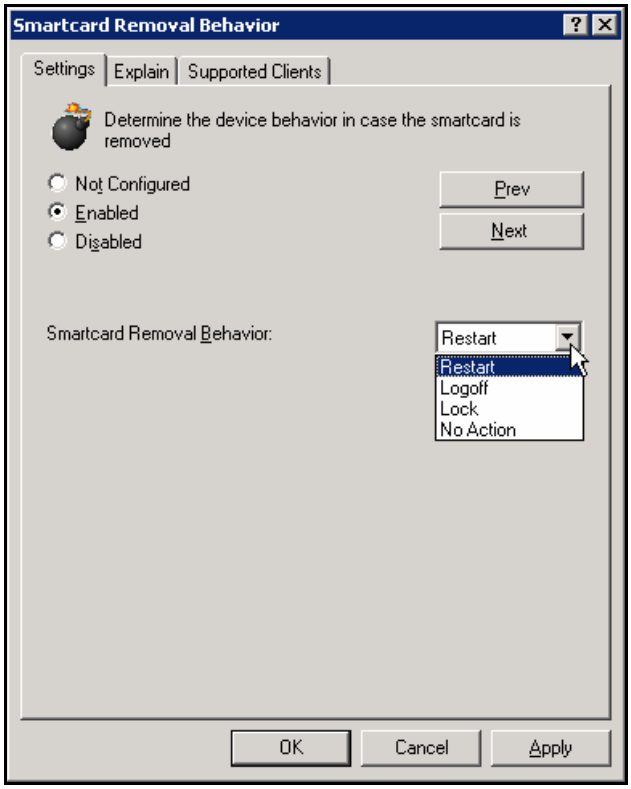
    Ignore date – selecting this option will cause the thin client to ignore the validity dates of the certificate stored on the smartcard (if the certificate has expired it will still be used for authentication).

    Check local date – selecting this option will verify that the thin client's current date falls between the certificate's **valid from** date and it's **valid to** date. If the verification fails, login will fail.

    Check with this date – selecting this option will verify that the date specified in the corresponding field falls between the certificate's **valid from** date and it's **valid to** date. If the verification fails, login will fail.

23. Click **OK** to save your settings and exit the Check Certificate Date window.

24. In the right pane, double-click on **Smartcard Removal Behavior**.
25. Select the **Enabled** option.



26. Select a value for the **Smartcard Removal Behavior** field from the drop-down list. The selected value will determine the thin client's behavior if the smartcard is remove or the card reader is disconnected. The following values are available:

    Restart – the device will reboot.

    Logoff – the current user will be logged-off.

    Lock – the device will enter a "locked" state that prevents any access to the device. The original smartcard (the one used for the logon) must be re-inserted into the reader to "unlock" the device.

    No Action – the device will continue its operation unaffected.
27. Click **OK** to save your settings and exit the Smartcard Removal Behavior window.
28. In the Xcalibur Policy Editor, select **File** and then **Exit** from the menu.
29. From the **Xcalibur Policy** tab, click **OK** to close the window and return to the **Xcalibur Management Console**.

This page is left blank intentionally.

Appendix A Implementing a Typical Smartcard Logon Solution

The following appendix describes a typical implementation of a smartcard single sign-on solution with the following features:

- Secure thin client access
- Once the smartcard is successfully verified, a session (RDP/ICA) starts automatically.
- Provide PIN code to logon to the session (single sign-on)

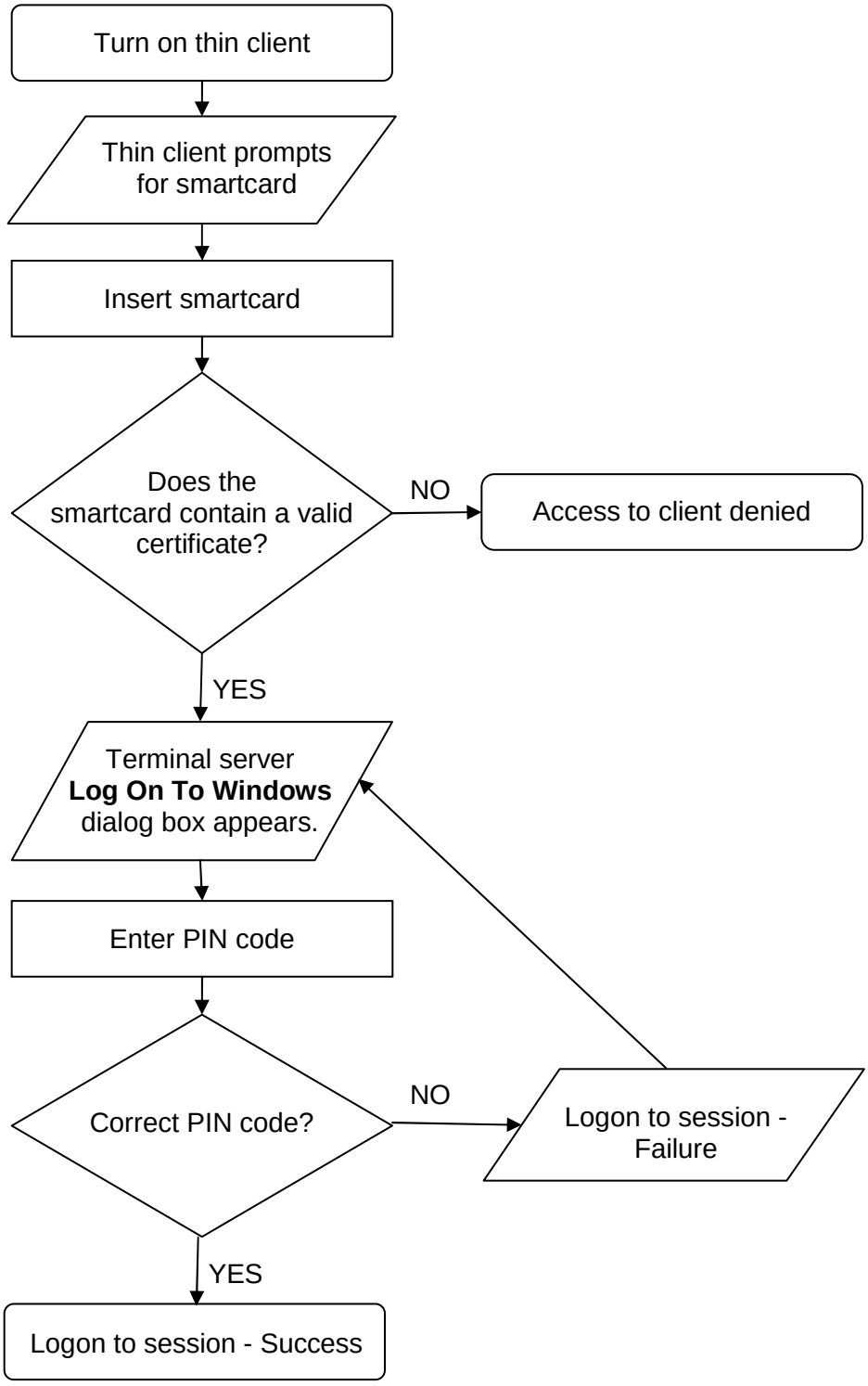
Solution Overview

The following table provides an overview of the solution's configuration steps and their effects.

Table 1 - Solution Configuration Steps

#	Step	Effect
1	In the Smartcard Logon plug-in: 1. Disable the **Check PIN code** option. 2. Enable checking one or more of the available certificate fields.	1. Prevents redundant entry of PIN code when accessing the thin client (PIN code will be required when accessing session). 2. Access to the thin client is granted only when using a smartcard with a valid certificate.
2	Create a connection on the thin client and create an **auto-start connection shortcut** on the client's desktop.	A session is automatically opened as soon as the smartcard is verified.
3	Configure the terminal server to support smartcard logon.	When a session to the terminal server is opened, the server will prompt for a PIN code. If the correct PIN code is entered, the credentials from the certificate on the smartcard will automatically be used to logon.

The following flow chart describes the user experience:



Solution Configuration

The following section provides a detailed guide to configuring the steps described in **Table 1** in the previous section.

Step 1

Configure the Smartcard Logon plug-in by following the procedure described is chapter 3 of this document.

In the plug-in configuration, use the following settings:

1. Disable the **Check PIN code** option.
2. Enable checking one or more of the available certificate fields.

Step 2

Create a connection on the thin client and create an auto-start connection shortcut on the client's desktop.

Follow the procedure described in the document: "How to Create an RDP Connection via Xcalibur Global", Ref: DG036H.

In the connection configuration, use the following settings:

1. Disable the **Automatic Logon** option.
2. Enable **Smart Cards** in the **Local devices** section.
3. In the **On policy receive** drop-down list, select **create autostart connection shortcut on desktop**.

Note A Citrix ICA connection may, alternatively, be used.

Step 3

Configure the server to support smartcard logon.

1. Perform configuration procedures required by the server vendor.
2. Install the following software on the server:
   2.1 Smartcard reader drivers.
   2.2 Smartcard CSP.

Optional Configuration

The following section describes optional settings that can be configured to increase the overall security of the solution.

The table below describes optional Xcalibur Policy settings and their effects:

Table 2 – Optional Security Settings

Option	Setting	Effect	
After user logged off from all sessions, perform device Log-Off	Enabled	Forces the client device to log-off when the last session is closed.	**Cumulative Effect** The client device reboots as soon as the last session is closed. A smartcard and PIN code are required to access the device and start a new session.
Map Logoff to Reboot	Enabled	Forces the client device to reboot when the user logs-off the device.	