Pass-through Authentication Rules

Technical Brief

Document Version 1.0

November 2006

COPYRIGHT NOTICE

This product and/or associated software are protected by copyright, international treaties and various patents.

This manual and the software, firmware and/or hardware described in it are copyrighted. You may not reproduce, transmit, transcribe, store in a retrieval system, or translate into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual, or otherwise, any part of this publication without express written permission from Chip PC.

CHIP PC SHALL NOT BE LIABLE FOR TECHNICAL OR EDITORIAL ERRORS OR OMISSIONS CONTAINED HEREIN; NOR FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES RESULTING FROM THE FURNISHING, PERFORMANCE, OR USE OF THIS MATERIAL.

The information contained in this document represents the current view of Chip PC on the issues discussed as of the date of publication. Because Chip PC must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Chip PC, and Chip PC cannot guarantee the accuracy of any information presented after the date of publication.

This Guide is for informational purposes only. CHIP PC MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

TRADEMARKS

Chip PC, Xcalibur, Xtreme PC, Jack PC, and the Chip PC logo are either trademarks or registered trademarks of Chip PC.

Products mentioned in this document may be registered trademarks or trademarks of their respective owners

The Energy Star emblem does not represent endorsement of any product or service.

U.S. GOVERNMENT RESTRICTED RIGHTS

The Software and documentation are provided with RESTRICTED RIGHTS.

You agree to comply with all applicable international and national laws that apply to the Software, including the U.S. Export Administration Regulations, as well as end-user, end-use and country destination restrictions issued by U.S. and other governments.

The information and specifications in this document are subject to change without prior notice.

Images are for demonstration purposes only.

Table of Contents

Chapter 1 Preface 5
Intended Audience 5
Scope 5
Objectives 5
Prerequisites 5
Reference Materials 5
Document Features 6
Conventions 6
Chapter Overview 6
Chapter 2 Introduction 7
What is Pass-through Authentication? 7
What are Pass-through Authentication Rules? 7
Chapter 3 Basic Principles 9
How do Pass-through Authentication Rules work? 9
Illustration & Example 10
Chapter 4 User Interface 11
The Primary Screen 11
Primary Screen Structure 11
The Test Screen 12
Test Screen Structure 12

Chapter 5 Scripts 13

Definitions 13

Split Scripts Functionality 14

Split Scripts Syntax 16

Split Script Examples 17

Merge Scripts Functionality 18

Merge Script Examples 19

Appendix A Configuring The Various Clients 21

Configuring ICA 21

Configuring RDP 22

Configuring Internet Explorer 23

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 (or later) product versions:

- Xcalibur Global, Version 1.1, Revision 2 + Service Pack 2
- ChipPC client device firmware, Version 6.5.4
- Internet Explorer plug-in, Version 6.0
- Citrix ICA plug-in, Version. 9.18
- Microsoft RDP plug-in, Version.5.2

Objectives

The objective of this document is to provide the technical know-how and understanding that is required to correctly and effectively use the Pass-through Authentication Rules.

Prerequisites

This document assumes that the reader has a working understanding of the use of Xcalibur Global policies; this should include the creation and modification of such policies.

More information on this topic is available in the reference materials detailed in following section.

Reference Materials

Xcalibur Global - Administrator's Guide, Ref: DG018U

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”, introduces the concepts of Pass-through Authentication Rules.
- Chapter 3, “Basic Principles”, describes the basic principles behind the operation method of Pass-through Authentication Rules.
- Chapter 4, “User Interface”, described the interface used to configure the Pass-through Authentication Rules.
- Chapter 5, “Scripts”, explains how to use the split scripts and merge scripts. The chapter covers functionality, syntax and examples.
- Appendix A, “Configuring The Various Clients”, describes the specific procedures for configuring Pass-through Authentication Rules for each of the supported clients.

Chapter 2 Introduction

This chapter introduces the concepts of Pass-through Authentication and Pass-through Authentication Rules.

What is Pass-through Authentication?

Pass-through Authentication allows transparent forwarding of user credentials to client applications. The client application (e.g. ICA, I.E., RDP) then passes the credentials to the server thus allowing single user sign-on.

Pass-through Authentication prevents the need for the user to re-enter his credentials.

What are Pass-through Authentication Rules?

Pass-through Authentication Rules are a set of scripts that allow manipulating the user credentials (User name / Password / Domain name) prior to passing them through to the client application.

For example, you can create a pass-though authentication rule that cuts the first part of the original domain name prior to passing it to the PNAgent client.

This way, when user alex@first.second.com logs-on to a device, the Pass-through Authentication rule transparently modifies the logon name to alex@second.com and then passes it to the PNAgent client.

This page is left blank intentionally.

Chapter 3 Basic Principles

This chapter will describe the basic principles behind the operation method of Pass-through Authentication Rules.

How do Pass-through Authentication Rules work?

The "Pass-through Authentication Rules" process is based on two steps.

Step 1 – Split the original data

A "Split Script" (defined later in document) is applied to the values of the following variables:

- User Name.
- Domain Name.

The "Split Script" dissects and filters out segments of the original values and creates new strings that can be used in Step 2 by the "Merge Scripts".

Step 2 – Merge the dissected data

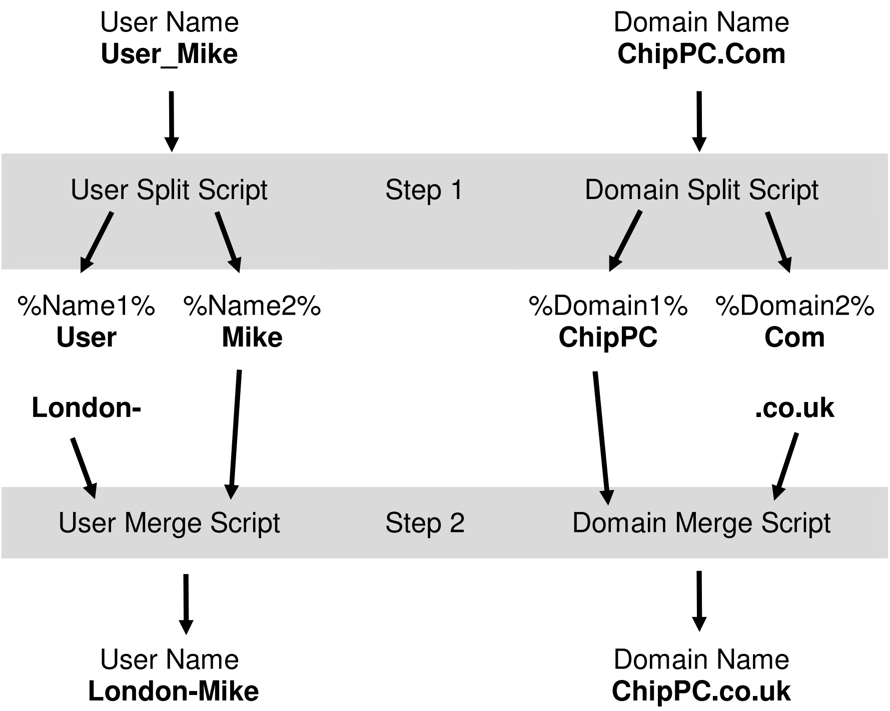
"Merge Scripts" (defined later in document) are used to join the strings created in Step 1 with other strings, thus creating new values for the following variables:

- User Name.
- Domain Name.
- Password.

Illustration & Example

The following flow chart illustrates a scenario where the original User Name (User_Mike) and Domain Name (ChipPC.Com) are first dissected by a Split Script (as shown in Step 1) and then merged with additional values by a Merge Script (as shown in Step 2) so that the end-results that are passed-through to the client application are:

- User Name: London-Mike
- Domain Name: ChipPC.co.uk



In Step 1, the User Split Script splits the User Name (User_Mike) into three strings:

1. The string “User” which is stored in the variable %Name1%.
2. The string “_” which is discarded.
3. The string “Mike” which is stored in the variable %Name2%.

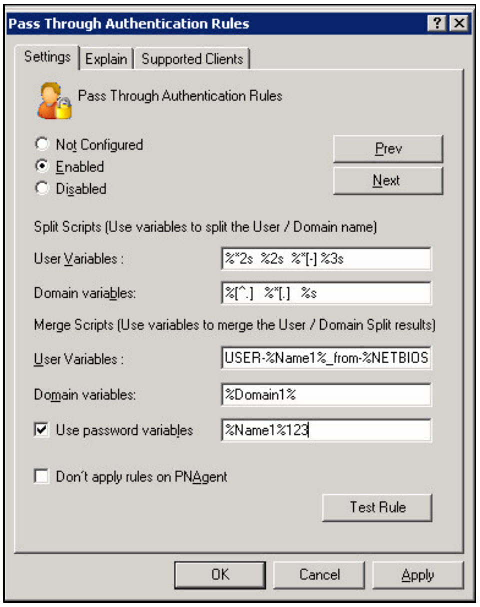
In Step 2, the User Merge Script appends the string stored in the variable %Name2% to a pre-defined string “London-“. The output of the User Merge Script is a new User Name (London-Mike) which is passed on to the client application.

Chapter 4 User Interface

The “Pass-through Authentication Rules” are configured via an Xcalibur Global policy option (See Appendix A). The user interface is composed of two screens:

4. The Primary screen, which is the first screen to appear when you enter the “Pass-through Authentication Rules” settings.
5. The Test screen, which is opened when pressing the “Test Rule” button in the Primary screen.

The Primary Screen


Pass Through Authentication Rules
?
Settings
Explain
Supported Clients
Pass Through Authentication Rules
Prev
Next
Test Rule
OK
Cancel
Apply

○ Not Configured
● Enabled
○ Disabled

Split Scripts (Use variables to split the User / Domain name)

User Variables : %*2s %2s %*[-] %3s

Domain variables: %[^.] %*[.] %s

Merge Scripts (Use variables to merge the User / Domain Split results)

User Variables : USER-%Name1%_from-%NETBIOS

Domain variables: %Domain1%

☑ Use password variables %Name1%123

☐ Don’t apply rules on PNAgent

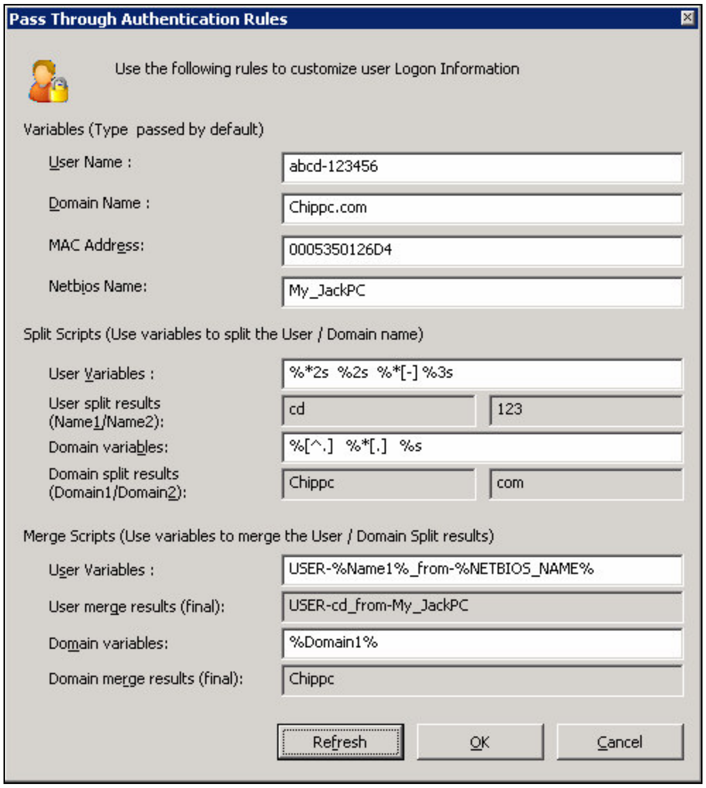
Primary Screen Structure

1. **Split Scripts section:**
Displays the scripts that will be applied to the values of User Name and Domain Name.
2. **Merge Scripts section:**
Displays the scripts that will be used to create new values for the User Name Domain Name and Password (optional).
3. **"Don't apply rules on PNAgent" checkbox:**
Prevent pass-through rules from applying on PNAgent logon (only available for ICA client).
4. **“Test Rule” button:**
Opens the Test screen.

The Test Screen

This screen lets you build and test scripts.

Once the script construction and testing is complete, pressing OK will transfer the scripts to the Primary screen.



Pass Through Authentication Rules

Use the following rules to customize user Logon Information

Variables (Type passed by default)

User Name : abcd-123456

Domain Name : Chippc.com

MAC Address: 0005350126D4

Netbios Name: My_JackPC

Split Scripts (Use variables to split the User / Domain name)

User Variables : %*2s %2s %*[-] %3s

User split results (Name1/Name2): cd 123

Domain variables: %[^.] %*[.] %s

Domain split results (Domain1/Domain2): Chippc com

Merge Scripts (Use variables to merge the User / Domain Split results)

User Variables : USER-%Name1%_from-%NETBIOS_NAME%

User merge results (final): USER-cd_from-My_JackPC

Domain variables: %Domain1%

Domain merge results (final): Chippc

Test Screen Structure

1. **Variables Section:**
   Type here the variables that the “Pass-through Authentication Rules” would normally receive from the environment. These values will be used to simulate the results of the scripts.
2. **Split Scripts Section:**
   Type here the Split Scripts that will manipulate the original values of the User Name and Domain Name.
3. **Merge Scripts Section:**
   Type here the Merge Scripts that will create new values for the User Name and Domain Name.
4. **Refresh button:**
   Press this to display the script results in the grayed out fields below the script sections.

Chapter 5 Scripts

This chapter explains how to use the split scripts and merge scripts. The chapter covers functionality, syntax and examples.

Definitions

This section describes the components that are used to construct Split Scripts and Merge Scripts.

- **Filter:** A Filter is a function that can read a segment from an existing string.
- **Storing Filter:** A Storing Filter will store the segment it read into a new variable.
- **Discarding Filter:** A Discarding Filter will not store the segment it has read.
- **Split Script:**
  - A Split Script is a combination of filters, applied to a single string.
  - A Split Script can store up to two segments of the original string into two new variables.
  - The purpose of the Split Scripts is to create additional working blocks for the Merge Scripts.
- **Merge Script:** A Merge Script is a list of variables and text that are joined together to created a new value.

Split Scripts Functionality

The following rules determine the functionality of the Split Scripts:

1. **The Split Scripts can manipulate the values of the following variables:**

   5.1 User Name.

   5.2 Domain Name.

2. **Each script can contain 1 or more filters.**

   Example:

   - If F1, F2 and F3 represent filters, a script could be “F1 F2”, “F3 F1 F2”, just “F2” or any other combination.

3. **Filters within a script may be separated by spaces.**

   Example:

   - If F1, F2 and F3 represent filters, a script “F1 F2 F3” would be the same as “F1F2F3”.

4. **For each original variable value that the script manipulates:**

   5.3 The first filter manipulates the original string.

   5.4 The later filers manipulate the string that is leftover from the previous filter (this could be null).

   Example:

   - If the original value is “ABCD1234” and we use the script “F1 F2 F3”.
   - F1 will work on the string “ABCD1234” and might, for example, read the first 4 characters (“ABCD”).
   - F2 will than work on the remaining string “1234”.
     - If F2 were to now read the 4 characters of the string, F3 will receive an empty string to work with.
     - If F2 were to read 2 characters of the string (“12”), F3 will receive the string “34” to work on.

5. **Each script may contain both types of filters:**

   5.5 Storing Filters (as previously defined).

   5.6 Discarding Filters (as previously defined).

6. **Storing Filters store their strings into new variables.**

   5.7 Only the first 2 Storing Filters in a script will store their strings into new variables.

   5.8 Base on the original variable (Domain Name or User Name), the results of the two Storing Filters will be saved in the following new variables:

Original Variable	Storing Filter	New Variable
User Name	1st	%Name1%
User Name	2nd	%Name2%
Domain	1st	%Domain1%
Domain	2nd	%Domain2%

1st or 2nd refers to the position of the filter within the script.

Split Scripts Syntax

The syntax for all types of filters is the same (case sensitive):

Filter Syntax	Explanation
%s	The complete string (See example #1 below).
%*n*s	The first *n* characters of the string (See examples #2-4 below).
%[*string*]	The first characters read until a character that **is not** found in the *string* is reached. The *string* can be a list of particular characters, a singe range or multiple ranges. Examples: [abcdef],[0-9],[a-z],[c-f],[q-z],[1-5 h-m u-z] (See examples #5-6 below).
%[^*string*]	The first characters read until a character that **is** found in the *string* is reached. (See examples #7-8 below).

- **Storing Filter:** By default, every filter will store the resulting string and will therefore become a Storing Filter.
- **Discarding Filter:** to create a Discarding Filter, add an asterisk (*) after the percent (%) sign. This will cause the filter to discard, rather than store, the resulting string.

Split Script Examples

The table below illustrates the outcome of various Split Scripts when applied on the User Name: **abcd-123456**

#	Filter Syntax	Resulting value of variable	
		%Name1%	%Name2%
1	%s	abcd-123456	
2	%3s	abc	
3	%3s %s	abc	d-123456
4	%3s %5s	abc	d-123
5	%[a-c] %4s	abc	d-12
6	%[abcdefg] %[-12]	abcd	-12
7	%[^0-9 -] %[^5-9]	abcd	-1234
8	%[^0-9 -] %*[-] %[^5-9]	abcd	1234
9	%*2s %2s %*[-] %3s	cd	123

Note Additional information about the filter syntax can be found at the following link: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/vccore98/HTML/_crt_format_specification_fields_.2d_.scanf_and_wscanf_functions.asp

Merge Scripts Functionality

The following rules determine the functionality of the Merge Scripts:

1. **The following variables can receive new values from a Merge Script:**
   - User Name.
   - Domain Name.
   - Password.
2. **Merge Scripts can use the following variables to create new strings:**
   - %Name1%
   - %Name2%
   - %Doman1%
   - %Domain2%
   - %NETBIOS_NAME%
   - %MAC_ADDRESS%
3. **The Merge Script joins the strings from the variables it contains.** A new string is created by appending the strings contained in the variables according to their order of appearance in the Merge Script.
4. **Additional text can be added to the final output string.** By placing additional strings anywhere in the script, they will be merged into the final output string according to their order of appearance in the Merge Script.

Merge Script Examples

Variables	Sample Values
%Name1%	abcd
%Name2%	1234
%Domain1%	chippc
%Domain2%	com
%NETBIOS_NAME%	MY_TERMINAL
%MAC_ADDRESS%	00053501ABCD

Script: %Name1%@%Domain1%.%Domain2%

Result: abcd@chippc.com

Script: USER-%Name1%_from-%NETBIOUS_NAME%

Result: USER-abcd_from-MY_TERMINAL

This page is left blank intentionally.

Appendix A Configuring The Various Clients

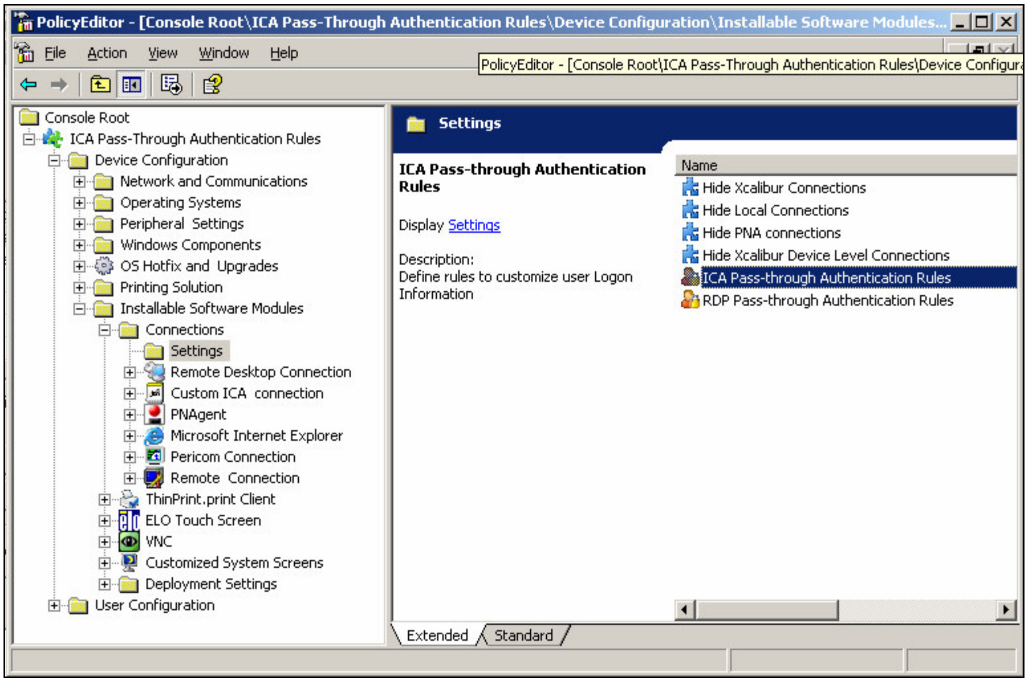
The Pass-through Authentication Rules are configured via an Xcalibur Global policy option. Although a common user interface is used (see Chapter 4), each client application has its own individual Pass-through Authentication Rules that are configured in a separate policy option. This appendix will describe where to configure the Pass-through Authentication Rules for the following clients:

- ICA
- RDP
- Internet Explorer

Configuring ICA

1. In the Xcalibur Global policy editor, expand the following path, as illustrated below:

   <*policy name*> \ Device Configuration \
   Installable Software Modules \ Connections \ Settings


PolicyEditor - [Console Root\ICA Pass-Through Authentication Rules\Device Configuration\Installable Software Modules...
File
Action
View
Window
Help
PolicyEditor - [Console Root\ICA Pass-Through Authentication Rules\Device Configura
Console Root
ICA Pass-Through Authentication Rules
Device Configuration
Network and Communications
Operating Systems
Peripheral Settings
Windows Components
OS Hotfix and Upgrades
Printing Solution
Installable Software Modules
Connections
Settings
Remote Desktop Connection
Custom ICA connection
PNAgent
Microsoft Internet Explorer
Pericom Connection
Remote Connection
ThinPrint.print Client
ELO Touch Screen
VNC
Customized System Screens
Deployment Settings
User Configuration
Settings
Name
Hide Xcalibur Connections
Hide Local Connections
Hide PNA connections
Hide Xcalibur Device Level Connections
ICA Pass-through Authentication Rules
RDP Pass-through Authentication Rules
Extended
Standard

ICA Pass-through Authentication Rules

Display Settings

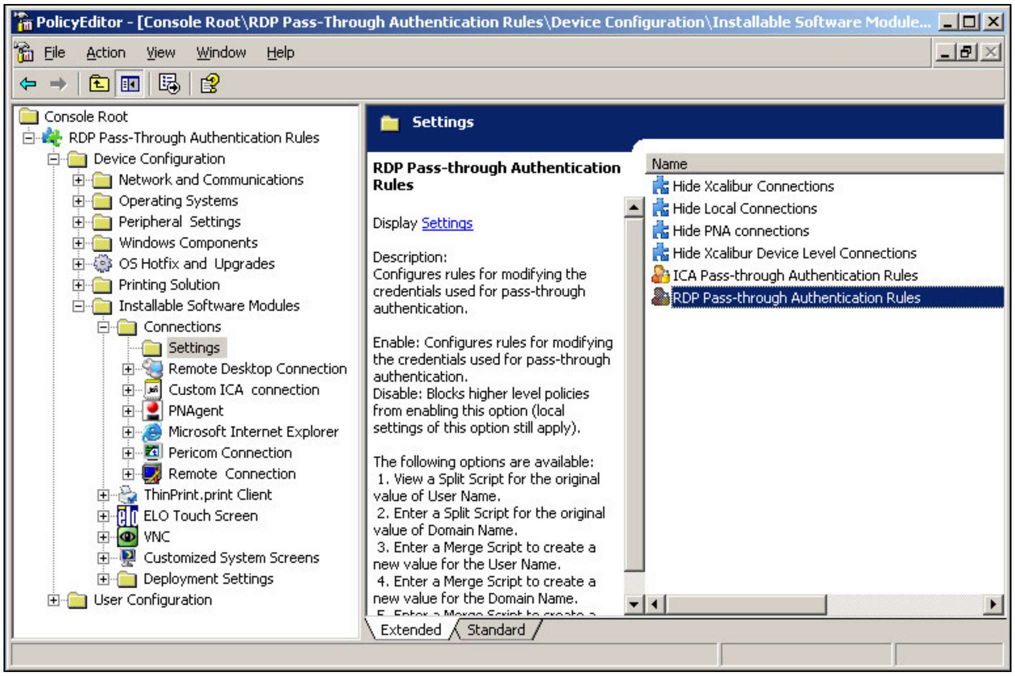
Description:
Define rules to customize user Logon Information

2. Double click on the **ICA Pass-through Authentication Rules** option to open the window for configuring the ICA Pass-through Authentication Rules.

Configuring RDP

1. In the Xcalibur Global policy editor, expand the following path, as illustrated below:

   <*policy name*> \ Device Configuration \
   Installable Software Modules \ Connections \ Settings


PolicyEditor - [Console Root\RDP Pass-Through Authentication Rules\Device Configuration\Installable Software Module...
File
Action
View
Window
Help
Console Root
RDP Pass-Through Authentication Rules
Device Configuration
Network and Communications
Operating Systems
Peripheral Settings
Windows Components
OS Hotfix and Upgrades
Printing Solution
Installable Software Modules
Connections
Settings
Remote Desktop Connection
Custom ICA connection
PNAgent
Microsoft Internet Explorer
Pericom Connection
Remote Connection
ThinPrint.print Client
ELO Touch Screen
VNC
Customized System Screens
Deployment Settings
User Configuration
Settings
Name
Hide Xcalibur Connections
Hide Local Connections
Hide PNA connections
Hide Xcalibur Device Level Connections
ICA Pass-through Authentication Rules
RDP Pass-through Authentication Rules
Extended
Standard

RDP Pass-through Authentication Rules

Display Settings

Description:
Configures rules for modifying the credentials used for pass-through authentication.

Enable: Configures rules for modifying the credentials used for pass-through authentication.
Disable: Blocks higher level policies from enabling this option (local settings of this option still apply).

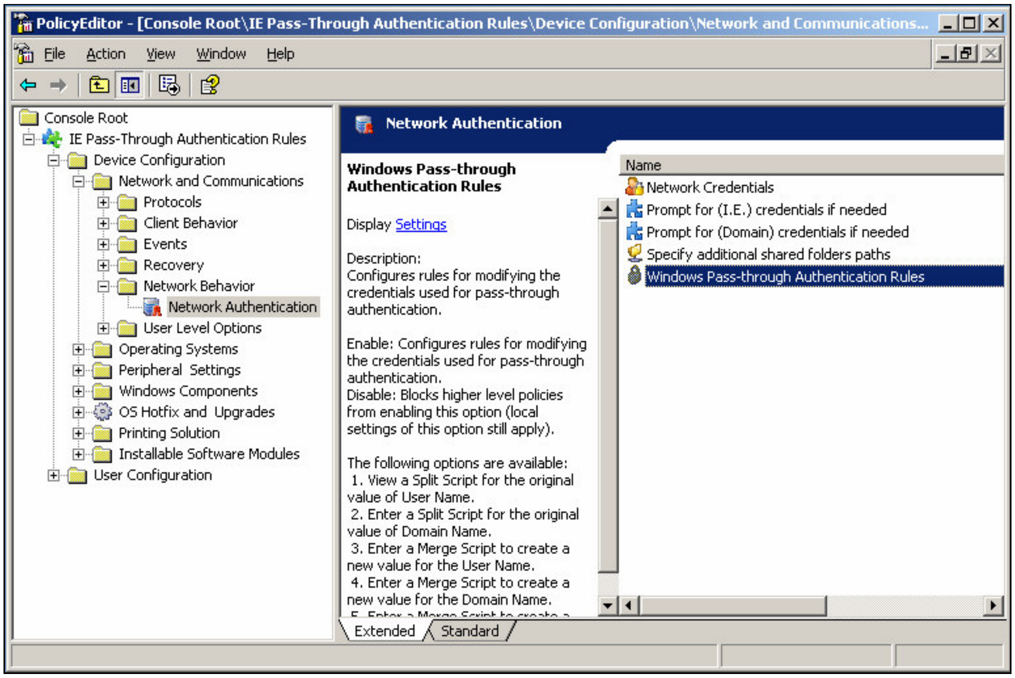
The following options are available:
1. View a Split Script for the original value of User Name.
2. Enter a Split Script for the original value of Domain Name.
3. Enter a Merge Script to create a new value for the User Name.
4. Enter a Merge Script to create a new value for the Domain Name.
5. Enter a Merge Script to create a

2. Double click on the **RDP Pass-through Authentication Rules** option to open the window for configuring the RDP Pass-through Authentication Rules.

Configuring Internet Explorer

1. In the Xcalibur Global policy editor, expand the following path, as illustrated below:

   <policy name> \ Device Configuration \ Network and Communications \ Network Behavior \ Network Authentication


PolicyEditor - [Console Root\IE Pass-Through Authentication Rules\Device Configuration\Network and Communications...
File
Action
View
Window
Help
Console Root
IE Pass-Through Authentication Rules
Device Configuration
Network and Communications
Protocols
Client Behavior
Events
Recovery
Network Behavior
Network Authentication
User Level Options
Operating Systems
Peripheral Settings
Windows Components
OS Hotfix and Upgrades
Printing Solution
Installable Software Modules
User Configuration
Network Authentication
Name
Network Credentials
Prompt for (I.E.) credentials if needed
Prompt for (Domain) credentials if needed
Specify additional shared folders paths
Windows Pass-through Authentication Rules
Extended
Standard

Windows Pass-through Authentication Rules

Display Settings

Description:
Configures rules for modifying the credentials used for pass-through authentication.

Enable: Configures rules for modifying the credentials used for pass-through authentication.
Disable: Blocks higher level policies from enabling this option (local settings of this option still apply).

The following options are available:
1. View a Split Script for the original value of User Name.
2. Enter a Split Script for the original value of Domain Name.
3. Enter a Merge Script to create a new value for the User Name.
4. Enter a Merge Script to create a new value for the Domain Name.
5. Enter a Merge Script to create a

2. Double click on the **Windows Pass-through Authentication Rules** option to open the window for configuring the Internet Explorer Pass-through Authentication Rules.