Software Installation Guide

SYNERGIX ADCE - Active Directory Client Extensions for MS Windows™

This guide explains how to install the SYNERGIX ADCE software product on current versions of Microsoft® Windows™ computers.

SYNERGIX ADCE software addresses issues encountered by business users who connect to Active Directory domain based resources, typically over VPN connections (legacy or SSL based) or over WiFi connections and using cached credentials. The software includes features such as Password Change Notification, Password Change synchronization, Group Policy update, User Logon Script execution, Kerberos Ticket refreshes, Duplicate DNS record reconciliation and many more.

The Secure Network Connection feature of ADCE serves dual purposes. It limits inbound and outbound network connectivity until an authorized user logs in. This feature also enables Fast Logon Optimization and defers the processing of otherwise synchronous and slow group policy processing.

SYNERGIX, INC.

www.synergix.com

Published: Jan 2012

Table of Contents

Legal Disclaimer i

Software License Agreement iv

Terms And Definitions vi

Introduction 1

Software Requirements 2

- Server Requirements 2
- Client Requirements 2

Starting SYNERGIX ADCE Installation 3

- Interactive Installation 3
- Silent Installation 8

Installing Group Policy Administrative Template File 10

Creating New Domain Group Policy Object 11

Editing Domain Group Policy Object 12

- Editing Domain Group Policy Object Scope Options 13
- Editing Domain Group Policy Object Status 16

Adding Administrative Template File to a GPO 18

Configuring Software Settings (Illustrations) 21

- Product Activation Key 21
- Customize User Interface Footer Section Controls 22
- Execute User Logon Scripts 23

Legal Disclaimer

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in, or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Synergix.

Synergix may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided, in any written license agreement from Synergix, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2011 Synergix, Inc. All rights reserved.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Document Summary

SYNERGIX Active Directory Client Extensions (ADCE) software **Installation Guide** provides step-by-step instructions to the systems administrator responsible for the product installation, which involves configuration of the ❶Microsoft® Windows™ Client Operating System[1] ❷ Microsoft® Active Directory Domain Environment and ❸ Group Policy Objects that are required for the product to function optimally.

[1] Supported Microsoft Windows Operating Systems only i.e. Windows XP and above

Software Installation Guide

SYNERGIX ADCE - Active Directory Client Extensions for MS Windows™

SYNERGIX Active Directory Client Extensions [ADCE] for Microsoft® Windows™ is a unique software solution that bridges the gap between LAN connected computers and remote (VPN or WiFi) computers. SYNERGIX Active Directory Client Extensions software is VPN client software agnostic tool; it works on legacy VPN client software ex. Cisco VPN Client Software, MCI, Nortel, Microsoft and on SSL based VPN software such as from Juniper.

Remote users logging in from a domain computer or even from a personal computer in a workgroup or untrusted domain environment to their corporate network using VPN client software are presented with several challenges; these translate into poor user experience and increased desktop management and support costs. SYNERGIX ADCE software addresses several of such challenges:

- **Enforce** domain password policy changes on VPN users
- **Manage** Group Policy refreshes on VPN connected computer
- **Execute** user login scripts when user [VPN] connects to corporate network
- **Execute** VPN connect and **VPN disconnect** scripts
- **Map** user's home drive to home path when user [VPN] connects to corporate network
- **Update** Kerberos tickets and group membership without logging off the user or restarting remote computer
- **Update** computer object attributes dynamically ex. description, location, managedBy
- **Secure** dormant accounts
    - **Update** user object attributes dynamically ex. account expires
- **Manage** Duplicate DNS records
- **Maintain** domain membership of trusted computer objects
- **Centrally manage** local administrator and backup administrator account credentials
- **Map** domain user account to a local account
- **Local account** can be granted elevated privileges
- **Improve** the Return on Investment, on desktop management software that tie into Active Directory

SYNERGIX ADCE requires Microsoft® .NET Framework 2.0 or higher version. Microsoft® .NET Framework 1.1 may be required for the Windows Installer.

Synergix, Inc.

Software License Agreement

This End User License Agreement (“EULA”) is a legal agreement between you and Synergix, Inc. (“Synergix”) governing your license of this software product from Synergix.

SYNERGIX, INC. IS WILLING TO LICENSE THIS SOFTWARE TO YOU ONLY IF YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT. PLEASE READ THE TERMS OF THIS LICENSE AGREEMENT CAREFULLY. IF YOU AGREE TO ALL OF THE TERMS OF THIS LICENSE AGREEMENT, INDICATE YOUR ACCEPTANCE BY SELECTING THE RADIO BUTTON ON THE ONLINE FORM. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS LICENSE AGREEMENT, INDICATED YOUR NON-ACCEPTANCE BY SELECTING THE ‘I DOT NOT ACCEPT THE LICENSE AGREEMENT’ ON THE WINDOWS INSTALLER DIALOG BOX AND THE INSTALLATION PROCESS WILL NOT CONTINUE.

LICENSE: Synergix grants you a non-exclusive license to use the software ("Software") and any accompanying documentation ("Documentation"). The evaluation version is not sold, but licensed. You may use the Software solely for your own customary business or personal purposes. You may only use the Software in accordance with the Documentation. You may not rent, lease, sublicense or lend the Software. You may, however, permanently transfer all of your rights under this Agreement to another person or legal entity provided that: ❶ you transfer to the person or entity all of the Software and Documentation (including all copies, updates, upgrades, prior versions, component parts, the media and printed materials, and this Agreement); ❷ you retain no copies of the Software and Documentation, including copies stored on a computer; and ❸ the recipient agrees to the terms and conditions of this Agreement.

You may not make or have made, or permit to be made, any copies of the Software or portions thereof, except as necessary for backup or archival purposes in support of your use of the Software as permitted hereunder. You may not copy the Documentation. You may not attempt to alter, disassemble, decompile, decrypt or reverse engineer the Software.

PROPRIETARY RIGHTS: You acknowledge that the Software is proprietary to Synergix, Inc. and its suppliers and that title and other intellectual property rights therein remain with Synergix, Inc. and its suppliers. Except as stated above, this Agreement does not grant you any right to patents, copyrights, trade secrets, trademarks (whether registered or unregistered), or any other rights, franchises or licenses in respect of the Software. You may not adopt or use any trademark or trade name that is likely to be similar to or confusing with that of Synergix or its products or any of its suppliers or take any other action which impairs or reduces the trademark rights of Synergix or its suppliers.

CONFIDENTIALITY: You agree to hold the Software in confidence, disclosing the Software only to authorized users having a need to use the Software as permitted by this Agreement and to take all reasonable precautions to prevent disclosure to other parties.

REMEDIES AND TERMINATION: Unauthorized use, copying or disclosure of the Software, or any breach of this Agreement will result in automatic termination of this license and will make available to Synergix, Inc. other legal remedies. In the event of termination, you must destroy all copies of the Software and all of its component parts. All provisions of this Agreement relating to disclaimers of warranties, limitation of liability, remedies, damages, and Synergix, Inc.'s proprietary rights shall survive termination.

LIMITED WARRANTY AND DISCLAIMER: Synergix, Inc. warrants to the original purchaser ("Customer")

for thirty (30) days from the date of original purchase from Synergix, Inc. or its authorized retailer that the Software will perform in substantial conformance with the Documentation when the Software is used as authorized. Synergix, Inc. warrants the media containing the Software against failure during the above warranty period. Synergix, Inc. makes no warranty or representation that the Software will meet your specific requirements, that the operation of the Software will be uninterrupted or error free, or that all defects in the Software will be corrected. Synergix, Inc. makes no warranty, implied or otherwise, regarding the performance or reliability of any third party products (software or hardware) not provided by Synergix, Inc.. THE INSTALLATION OF ANY THIRD PARTY PRODUCTS OTHER THAN AS AUTHORIZED BY SYNERGIX, INC. WILL VOID THIS WARRANTY. IN ADDITION, USE, MODIFICATION, AND/OR REPAIR OF THE SOFTWARE OTHER THAN AS AUTHORIZED BY SYNERGIX, INC. WILL VOID THIS WARRANTY.

EXCEPT FOR THE ABOVE EXPRESS LIMITED WARRANTY, SYNERGIX, INC. MAKES AND YOU RECEIVE NO WARRANTIES OR CONDITIONS ON THE SOFTWARE, EXPRESS, IMPLIED, STATUTORY, OR IN ANY OTHER PROVISION OF THIS AGREEMENT OR COMMUNICATION WITH YOU, AND SYNERGIX, INC. SPECIFICALLY DISCLAIMS ANY IMPLIED WARRANTY OR CONDITION OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR NON INFRINGEMENT OF THIRD PARTY RIGHTS.

LIMITATION OF LIABILITY: TO THE EXTENT PERMITTED BY APPLICABLE LAW, SYNERGIX, INC. AND ITS SUPPLIERS SHALL NOT BE LIABLE FOR ANY DAMAGES, INCLUDING LOSS OF DATA, LOST PROFITS, COST OF COVER OR OTHER SPECIAL, INCIDENTAL, CONSEQUENTIAL OR INDIRECT DAMAGES ARISING FROM THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE OR FAILURE OF THE SOFTWARE, HOWEVER CAUSED AND UNDER ANY THEORY OF LIABILITY. THIS LIMITATION WILL APPLY EVEN IF SYNERGIX, INC. HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. YOU ACKNOWLEDGE THAT THE PURCHASE PRICE REFLECTS THIS ALLOCATION OF RISK. BECAUSE SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

EXPORT CONTROLS: You agree that you will not export or re-export the Software in any form in violation of any applicable laws or regulations of the United States or the country in which you obtained them.

U.S. GOVERNMENT RESTRICTED RIGHTS: The Software and Documentation are provided with RESTRICTED RIGHTS. Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs (c)(1) and (2) of the Commercial Computer Software Restricted Rights at 48 CFR 52.227-19, as applicable.

GENERAL: The laws of the State of New Jersey govern this Agreement. You agree that this Agreement shall not be subject to the United Nations Convention on Contracts for the International Sale of Goods (1980). This Agreement is the entire agreement held between us and supersedes any other communications or advertising with respect to the Software. If any provision of this Agreement is held invalid, the remainder of this Agreement shall continue in full force and effect.

If you have any questions, please see SYNERGIX, Inc.'s web site at http://www.synergix.com

BY USING THIS DOCUMENT FOR REVIEW, DOWNLOADING OUR SOFTWARE, INSTALLING IT FOR EVALUATION PURPOSES OR FOR COMMERCIAL USE, THE USER AGREES TO HAVE READ AND UNDERSTAND THE FOREGOING AGREEMENT AND TO BE BOUND BY ALL ITS TERMS.

TERMS AND DEFINITIONS[2]

ACTIVE DIRECTORY

Active Directory is a technology created by Microsoft that provides a variety of network services, including:

- Lightweight Directory Access Protocol LDAP is the industry standard directory access protocol, making Active Directory widely accessible to management and query applications. Active Directory supports LDAPv3 and LDAPv2.
- Kerberos-based authentication
- DNS-based naming and other network information (Guts of DNS, Stable DNS is needed for AD to work properly)
- Central location for network administration and delegation of authority
- Information security and single sign-on for user access to networked based resources
- The ability to scale up or down easily
- Central storage location for application data
- Synchronization of directory updates amongst several servers

FORESTS, TREES AND DOMAINS

All objects inside a common directory database is known as domain. Each domain stores information only about the objects that belong to that domain. A tree consists of a single domain or multiple domains in a contiguous namespace. A forest is a collection of Trees and represents the outermost boundary within which users, computers, groups, and other objects exist. The forest is the security boundary for Active Directory.

The Active Directory framework that holds the objects can be viewed at a number of levels. At the top of the structure is the *forest.* A forest is a collection of multiple trees that share a common global catalog, directory schema, logical structure, and directory configuration. The forest, tree, and domain are the logical parts in an Active Directory network.

The Active Directory forest contains one or more transitive, trust-linked *trees*. A tree is a collection of one or more *domains* and domain trees in a contiguous namespace, again linked in a transitive trust hierarchy. Domains are identified by their DNS name structure, the namespace.

SCHEMA

The Microsoft Active Directory schema contains formal definitions of every object class that can be created in an Active Directory forest. The schema also contains formal definitions of every attribute that can exist in an Active Directory object. This section provides the reference for each schema object and provides a brief explanation of the attributes, classes, and other objects that comprise the Active Directory schema.

[2] Reference: Wikipedia.org, Microsoft

OBJECTS AND OBJECT ATTRIBUTES

Everything that Active Directory tracks is considered an object. An object is any user, system, computer, resource, or service tracked within Active Directory. The generic term object is used because Active Directory is capable of tracking a variety of items, and many objects can share common attributes.

An Active Directory structure is a **hierarchical framework** of objects. The objects fall into two broad categories: resources (e.g., printers) and security principals (user or computer accounts and groups). Security principals are Active Directory objects that are assigned unique security identifiers (SIDs) used to control access and set security.

Each object represents a single entity — whether a user, a computer, a printer, or a group — and its **attributes**. Certain objects can also be containers of other objects. An object is uniquely identified by its name and has a set of attributes — the characteristics and information that the object can contain — defined by a schema, which also determines the kind of objects that can be stored in Active Directory.

Each attribute object can be used in several different schema class objects. The schema object exists to allow the schema to be extended or modified when necessary. However, because each schema object is integral to the definition of Active Directory objects, deactivating or changing these objects can have serious consequences because it will fundamentally change the structure of Active Directory itself. A schema object, when altered, will automatically propagate through Active Directory and once it is created it can only be deactivated — not deleted. Changing the schema usually requires a fair amount of planning.

INTRODUCTION

Microsoft provides several Windows based tools to manage the Active Directory environment. They generally require the Windows Server 2003 Administration Tools Pack or the Remote Server Administration Tool to be installed on the each of the administrators' machines in order for them to manage the Active Directory environment.

LAN connected computers and users interactively logging into Active Directory from such computers get a rich experience and seamless access to Active Directory domain resources. In contrast, remote users connecting the corporate network via VPN i.e. using cached credentials may experience issues. These issues include password change notification, group policy updates, user login script execution, DNS duplicate records and several others. SYNERGIX ADCE addresses several of these issues and allow the administrators to manage remote computers and remote users like LAN connected computers and users.

- **Enforce** domain password policy changes on VPN users
- **Manage** Group Policy refreshes on VPN connected computer
- **Execute** user login scripts when user [VPN] connects to corporate network
- **Execute** VPN connect and **VPN disconnect** scripts
- **Map** user's home drive to home path when user [VPN] connects to corporate network
- **Update** Kerberos tickets and group membership without logging off the user or restarting remote computer
- **Update** computer object attributes dynamically ex. description, location, managedBy
- **Secure** dormant accounts
    - **Update** user object attributes dynamically ex. account expires
- **Manage** Duplicate DNS records
- **Maintain** domain membership of trusted computer objects
- **Centrally manage** local administrator and backup administrator account credentials
- **Map** domain user account to a local account
- **Local account** can be granted elevated privileges
- **Improve** the Return on Investment, on desktop management software that tie into Active Directory

SOFTWARE REQUIREMENTS

SYNERGIX ADCE for Microsoft® Windows™ is client based software. No schema changes are required in the Active Directory forest environment nor is any server software required on a domain server.

Server Requirements

	None

Client Requirements

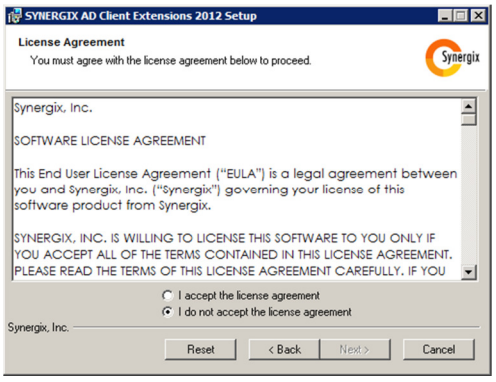
Client Computer Operating System	Ex. Windows Server XP Windows Vista Windows 7.0 Windows Server 2003 Windows Server 2008
Client Computer Operating Platform	Ex. 32 bit 64 bit
Client Computer Role	Ex. Domain Member or Workgroup Computer
.NET Framework	Ex. .NET Framework 2.0 or above SP1

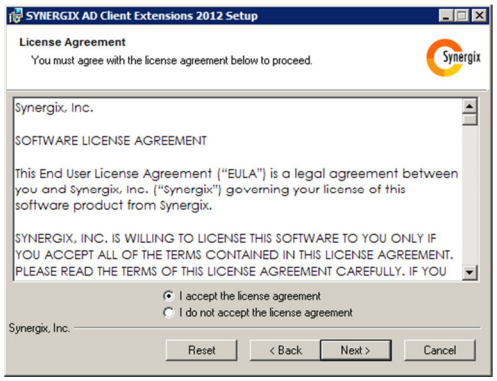
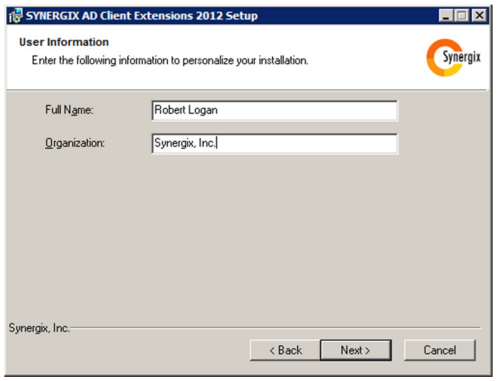
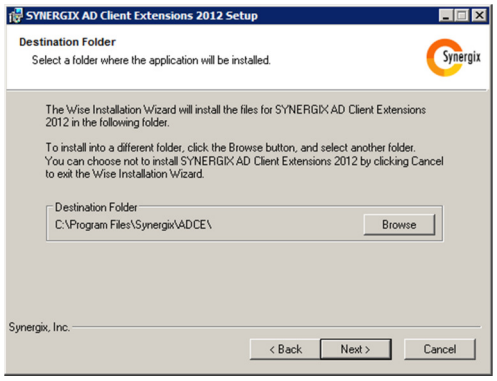
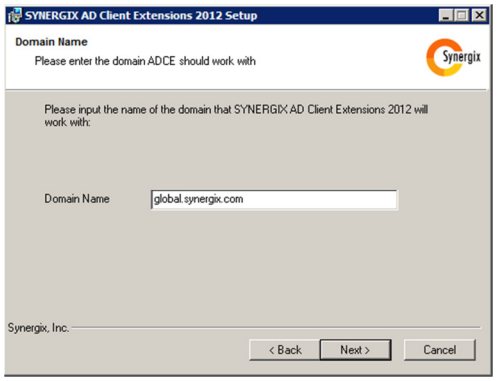
STARTING SYNERGIX ADCE INSTALLATION

Interactive Installation

This section of the document guides you through interactive installation process of SYNERGIX Active Directory Client Extensions.

You must have administrative privileges in order to perform the installation or your system must be configured to *Allow install with elevated privileges* (http://msdn.microsoft.com/en-us/library/ms813108.aspx)

Task	Illustration
Login to the client computer using an administrative account	
Locate ADCE software installation package file (MSI formatted file). Double click on the MSI file to launch the software installation wizard. **Note:** The same MSI package file will install on 32 bit and on 64 bit platforms.	
When the Welcome dialog box is displayed, click on *Next* button.	
Review the content of the *End User License Agreement*. By default, *I do not accept the license agreement* radio button is selected	

Review the content of the *End User License Agreement*. Select ***I accept the license agreement*** radio button, if you wish to proceed with the software installation.	
In the User Information dialog box, enter *Full Name* and *Organization.*	
Review *Destination Folder* setting. The default *Destination Folder* is set under the \Program Files\ folder. It is generally not necessary to change this setting.	
In the *Domain Name* dialog box, ensure that your Active Directory domain FQDN is displayed. Correct it as needed. **Note:** It is required that you type the Active Directory Domain Name in FQDN format	

In the *Recommended Configuration Changes* dialog box, review the settings and check / uncheck the options as appropriate for your environment. The 6 digit numbers displayed in parenthesis indicate the KB article published by the vendor. You may visit Microsoft website to get more information on specific settings.

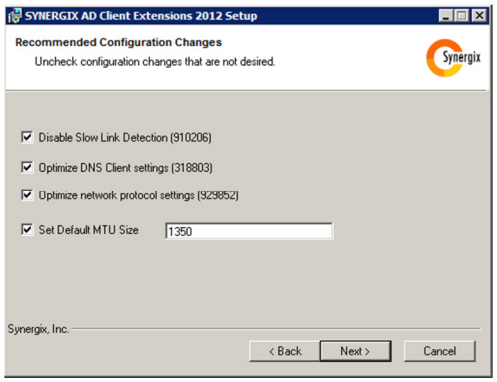
1. (910206) In order to facilitate the download of Group Policy object over a slow link network connection, the registry setting is modified to facilitate this setting.

2. (318803) Disables caching of negative DNS responses

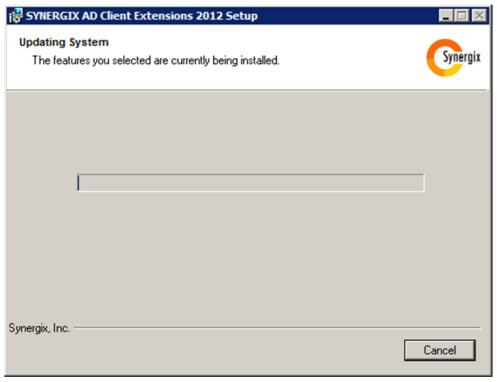
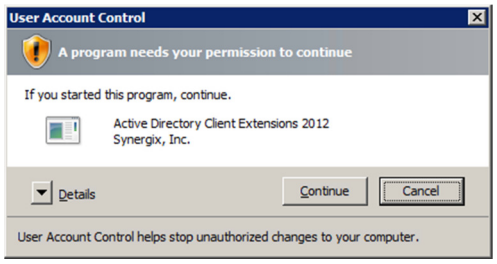
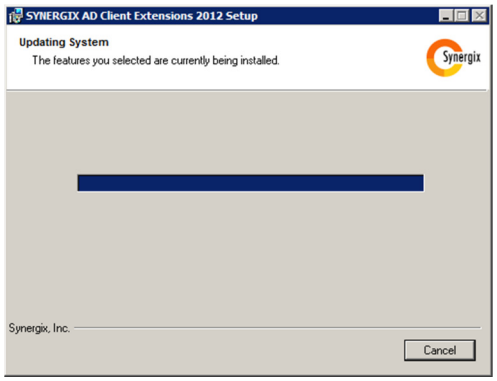
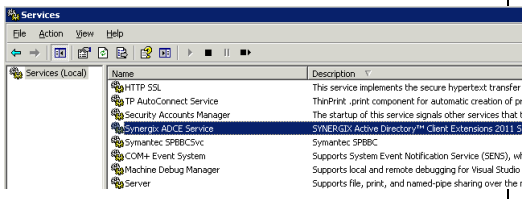
3. (929852) Optimizes network protocol settings

4. In order to reduce network packet fragmentation and optimize data transmission over a VPN connection, it is generally recommended to adjust the MTU size.

Note: It is strongly recommended that the *Recommended Configuration Changes* are left as shown i.e. they are checked.



When you're ready to start the installation, click on *Next* button.

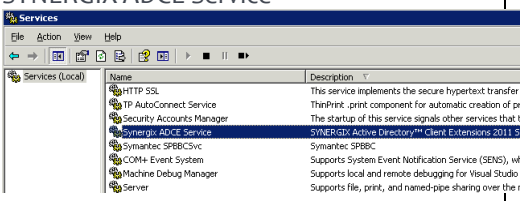
Please wait while the system is updated.	
The User Account Control (UAC) feature in Windows Operating System will prompt you to continue with the installation. Click on Continue button.	
The installation will resume after the prompt in UAC dialog is acknowledged.	
Check the status of the installation and then, click on *Finish* button to complete the installation.	
Immediately after the software installation has completed, ***SYNERGIX ADCE Service*** will start running.	SYNERGIX ADCE Service 

And ***SYNERGIX ADCE Client*** application will be displayed in the System Tray.	 SYNERGIX ADCE Client
Immediately after the software installation has finished and the program (service and client components) started, following features of the software will work without requiring any configuration changes: ❶ Domain Password Change Notification ❷ Group Policy Refresh ❸ Kerberos Ticket Refreshes For additional product features to work, you will be required to configure a Group Policy Object. You must add the Group Policy Administrative Template file provided and configure the settings as appropriate for your environment.	

Silent Installation

This section of the document guides you through silent installation process of SYNERGIX Active Directory Client Extensions.

You must have administrative privileges in order to perform the installation or your system must be configured to *Allow install with elevated privileges* (http://msdn.microsoft.com/en-us/library/ms813108.aspx)

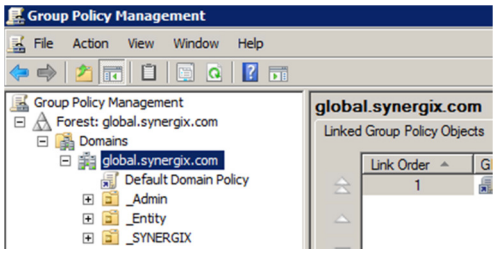
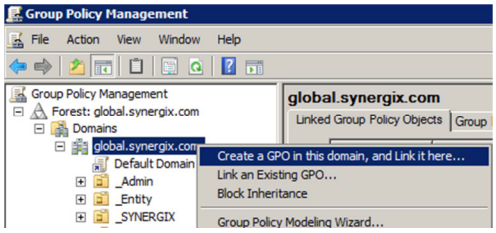
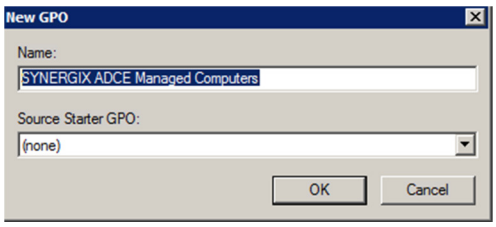
Task	Illustration
Login to the client computer using an administrative account	
Locate ADCE software installation package file (MSI formatted file). **Note:** The same MSI package file will install on 32 bit and on 64 bit platforms.	
Start the command prompt	
Run following command. It will silently install SYNERGIX ADCE software and generate a verbose log file, when `/l*v` parameter is specified. `msiexec /i ADCE.MSI /qb-! /l*v ADCE.MSI.log`	`msiexec /i ADCE.MSI /qb-! /l*v ADCE.MSI.log`
Immediately after the software installation has completed, ***SYNERGIX ADCE Service*** will start running.	SYNERGIX ADCE Service 
And ***SYNERGIX ADCE Client*** application will be displayed in the System Tray.	 SYNERGIX ADCE Client
When the software installation has finished	

and the program (service and client components) started, following features of the software will work without requiring any configuration changes: ❶ Domain Password Change Notification ❷ Group Policy Refresh ❸ Kerberos Ticket Refreshes For additional product features to work, you will be required to configure a Group Policy Object. You must add the Group Policy Administrative Template file provided and configure the settings as appropriate for your environment.	

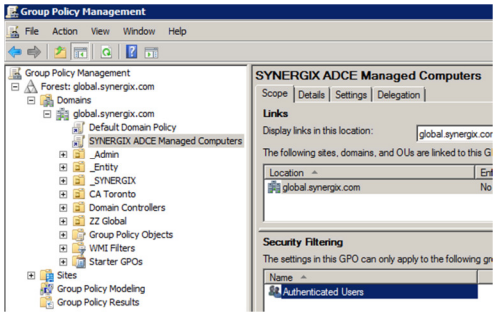
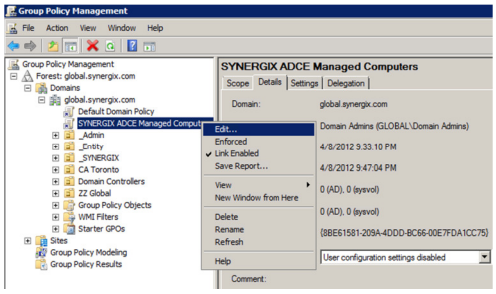
INSTALLING GROUP POLICY ADMINISTRATIVE TEMPLATE FILE

Task	Illustration
Login to administrator computer (domain computer running Windows XP or Windows 7.0) using an administrative account.	
Extract **SYNERGIX-ADCE.adm** file from the downloaded compressed file.	
The Administrative Template file **SYNERGIX-ADCE.adm** must be copied to %SystemRoot%\INF folder (default in Windows XP environment) or %SystemRoot%\PolicyDefinitions (default in Windows VISTA and Windows 7.0 environments)	C:\Windows\INF (XP) or C:\Windows\PolicyDefinitions (Win 7)

CREATING NEW DOMAIN GROUP POLICY OBJECT

Task	Illustration
Login to the Administrator's workstation	
Launch GPMC.MSC	
Select the container where the new GPO will be created and linked. In the illustration, the default naming context is chosen	
Right click on the container object and select *Create and Link a GPO Here …*	
Enter *New GPO* name Ex. **SYNERGIX ADCE Managed Computers Policy**	
Click on OK. New GPO is created and linked to the selected container object.	

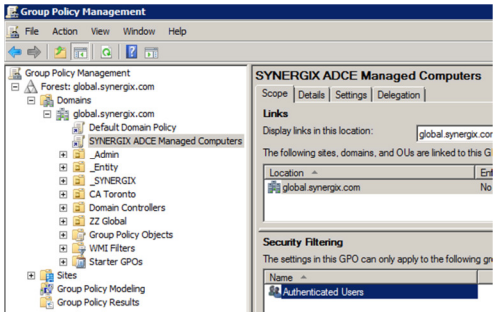
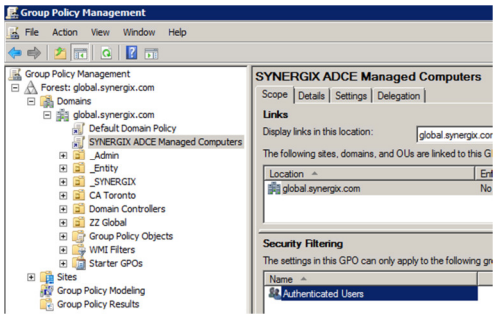
EDITING DOMAIN GROUP POLICY OBJECT

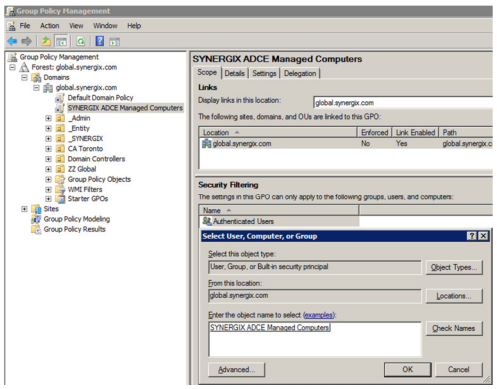
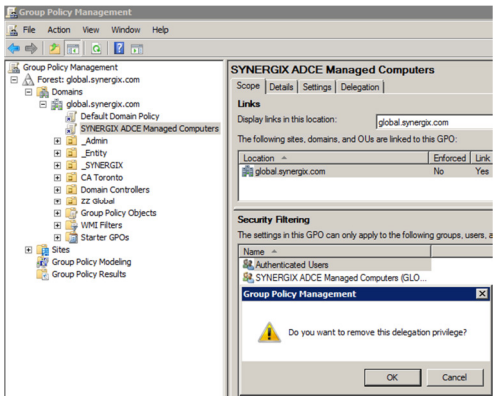
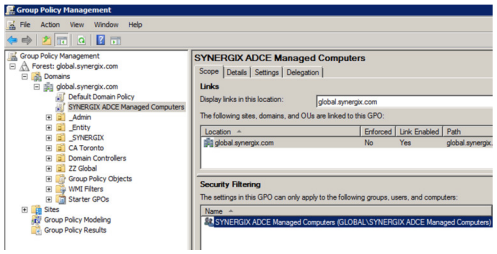
Task	Illustration
Login the Administrator's workstation	
Launch GPMC.MSC	
Select the container where the new GPO is created.	
Select the new GPO that was recently created Ex. **SYNERGIX ADCE Managed Computer Policy**	
Right mouse click on the GPO and select *Edit*. This will launch the Group Policy editor Ex. **SYNERGIX ADCE Managed Computer Policy**	

Editing Domain Group Policy Object Scope Options

This section of the document guides you through setting the Scope Options in the selected Group Policy Object. The steps outlined in this section are optional.

In its default configuration, the GPO scope includes the "*Authenticated Users*" security principal in the Security Filtering section of the GPO. It means all computer objects and user objects that are in the Organizational Unit or the domain container that the GPO is linked to, will be in scope of the GPO. If you desire to narrow down the scope, you may remove the "*Authenticated Users*" security principal and in its place, add the "SYNERGIX ADCE Managed Computers" security group which only contains computer objects on which the software is installed. Please note that the security group "SYNERGIX ADCE Managed Computers" is also used for license monitoring purposes (refer to the section on configuring Product Activation Key)

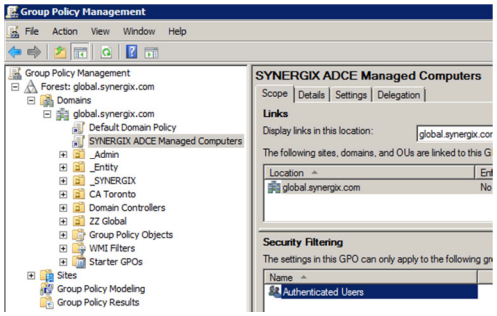
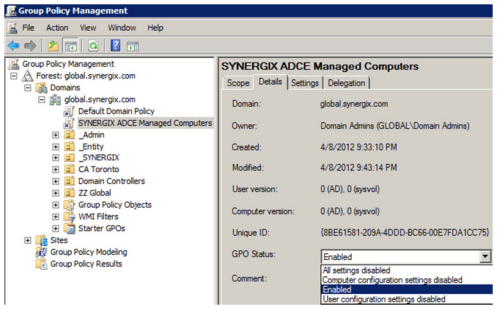
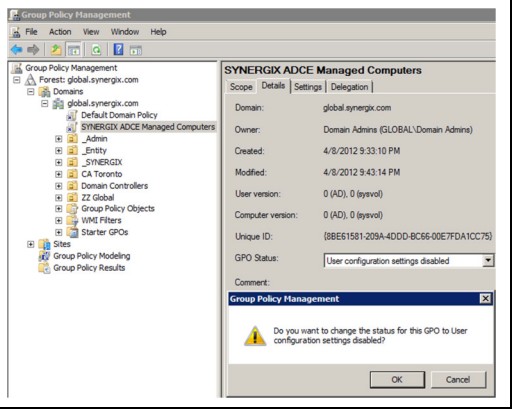
Task	Illustration
Login the Administrator's workstation	
Launch GPMC.MSC	
Select the container where the new GPO is created.	
Select the new GPO that was recently created Ex. **SYNERGIX ADCE Managed Computer Policy**	
Select the Scope tab and verify the security principal under Security Filtering. By default, it will contain *Authenticated Users*	

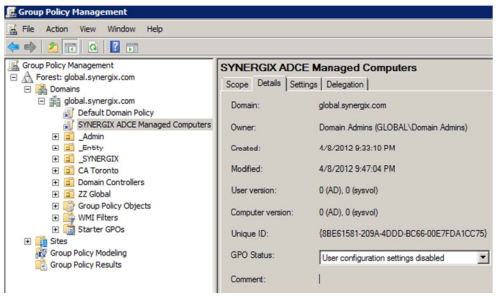
Click on Add. Select **SYNERGIX ADCE Managed Computers** security group and click on OK	
Select *Authenticated User* and click on Remove. When prompted to remote the delegation privilege, click on OK	
Verify that the Security Filtering setting now contains only the **SYNERGIX ADCE Managed Computers** security group.	

Editing Domain Group Policy Object Status

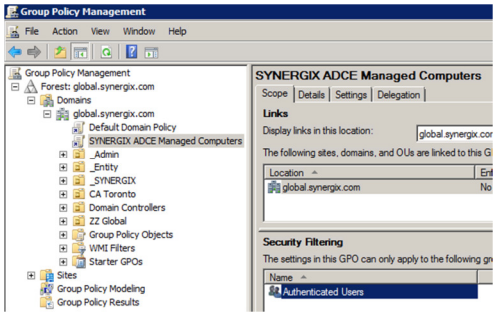
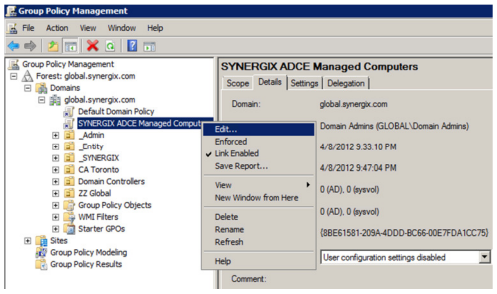
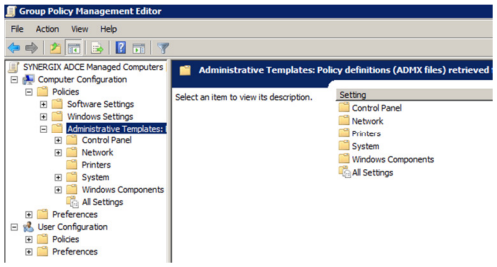
This section of the document guides you through changing the GPO Status. The steps outlined in this section are optional.

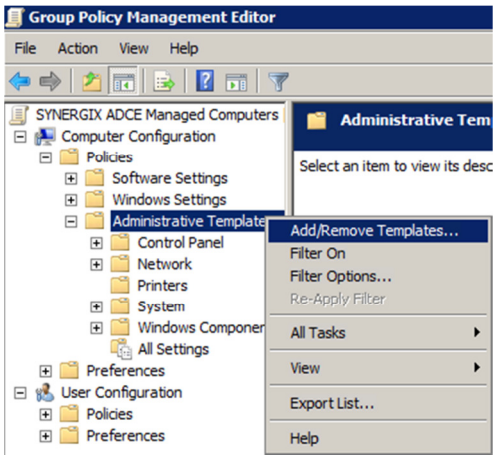
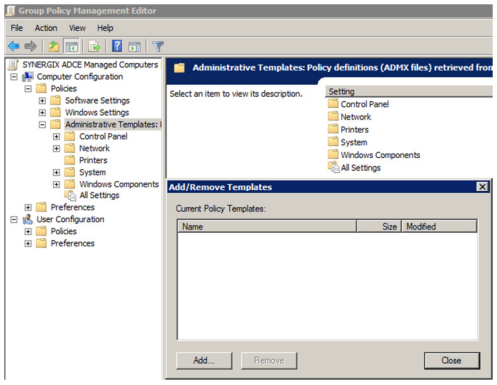
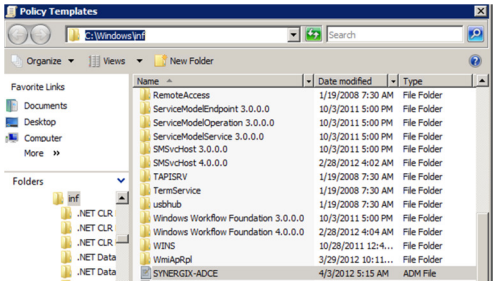
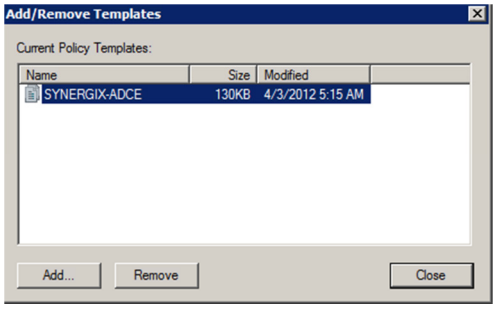
In its default configuration, the GPO status for both the COMPUTER configuration and the USER configuration is enabled. SYNERGIX ADCE software manages all of its configuration parameters in the COMPUTER configuration only. Follow the steps provided in this section of the document if you wish to disable the USER configuration part of the GPO.

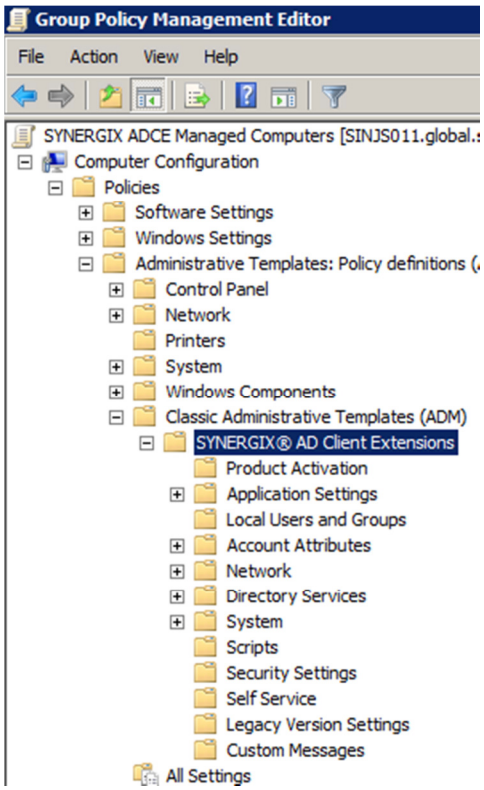
Task	Illustration
Login the Administrator's workstation	
Launch GPMC.MSC	
Select the container where the new GPO is created.	
Select the new GPO that was recently created Ex. **SYNERGIX ADCE Managed Computer Policy**	
Select the Details tab. By default, the GPO Status will be **Enabled** i.e. both the COMPUTER and USER configuration settings will be enabled.	
From the drop down list, select *User Configuration settings disabled.* When prompt to change the GPO status, click on OK.	

Verify that the *User Configuration settings disabled* displays in the GPO Status field.	

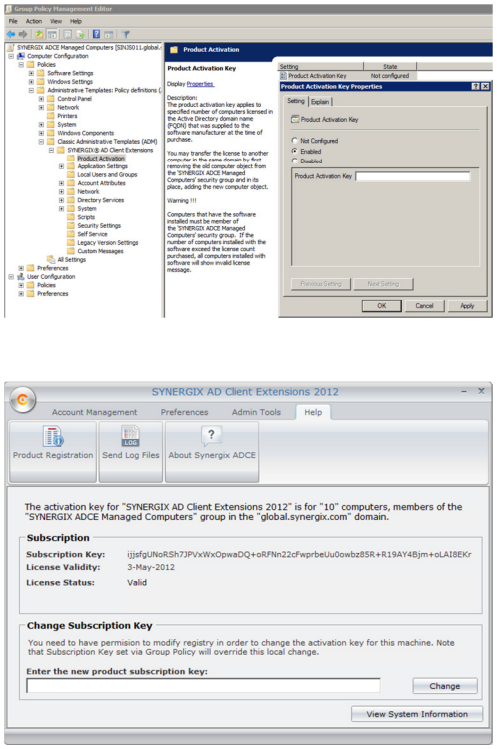
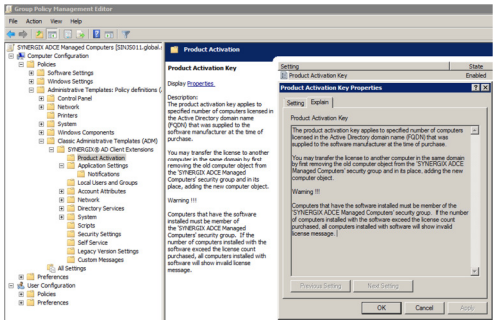
ADDING ADMINISTRATIVE TEMPLATE FILE TO A GPO

Task	Illustration
Login the Administrator's workstation	
Launch GPMC.MSC	
Select the container where the new GPO is created.	
Select the new GPO that was recently created Ex. **SYNERGIX ADCE Managed Computer Policy**	
Right mouse click on the GPO and select *Edit*. This will launch the Group Policy editor Ex. **SYNERGIX ADCE Managed Computer Policy**	
Under Computer Configuration, select Administrative Templates	

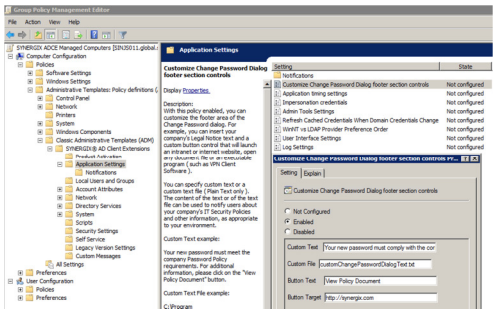
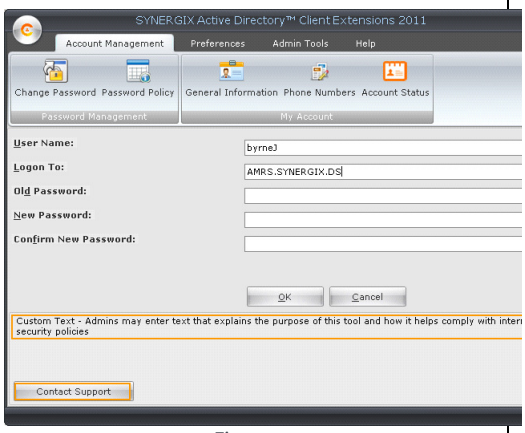
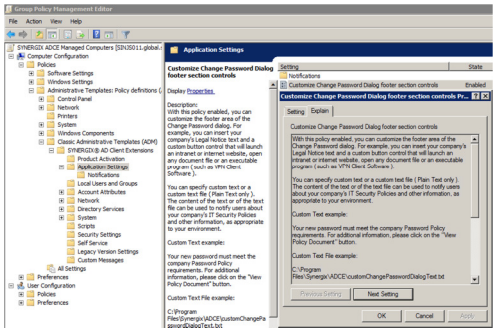
Right mouse click on Administrative Templates. From the context sensitive menu, select Add / Remove Templates …	
You will see list of Administrative Template files that are already added in the Group Policy Editor console. Click on **Add** button.	
Select **SYNERGIX-ADCE.adm** file from the list and click on Open button.	
You will notice that SYNERGIX-ADCE template file in the Current Policy Templates list. Click on Close button to return back to Group Policy Editor	

In the Group Policy Editor tree view, you should notice that the SYNERGIX Active Directory Client Extensions node added.	
Explore various settings that are configurable using Group Policy object.	

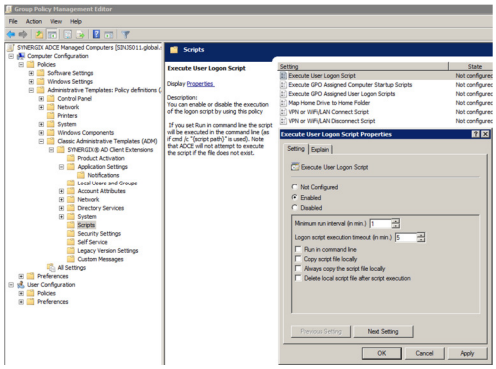
Product Activation Key

Task	Illustration
For illustration purposes, the **Product Activation Key** setting is opened. Under the Setting tab, 2 options are provided 1. Enable the setting 2. Product Activation Key You may paste the long product activation key provided by the software vendor, in the textbox control. When the **Product Activation Key** settings are configured, specific number of computer objects that are members of designated security group (by default, the **SYNERGIX ADCE Managed Computer** security group) will have the product license. **Note:** The Product Activation Key contains your Active Directory domain FQDN, Active Directory security group (SYNERGIX ADCE Managed Computers) and the license count.	 Figure 1 **Product Activation Key validated**
The Explain tab of the selected Group Policy setting provides precise information on the use of the setting.	

Customize User Interface Footer Section Controls

Task	Illustration
For illustration purposes, the **Customize User Interface footer section controls** is opened. Under the Setting tab, 4 options are provided 3. Enable the setting 4. Custom Text 5. Custom File 6. Button Text 7. Button Target When the **Customize User Interface footer section control** settings are configured, the user interface of the software will display custom information. This helps the system administrators notify the users about the use of the software and provide specific URL on their intranet website or on the Internet.	  Figure 1 **Customize User Interface footer section controls**
The Explain tab of the selected Group Policy setting provides precise information on the use of the setting.	

Execute User Logon Scripts

Task	Illustration
Double click on a setting. For illustration purposes, the **Execute User Logon Script** setting is opened. Under the Setting tab, 7 options are provided 1. Enable the setting 2. Minimum run interval (mins) 3. Logon script time out (mins) 4. Run in command line 5. Copy the script file locally 6. Always copy the script file locally 7. Delete local script file after script Setting **Minimum run interval (mins)** to a low value, for example to 1 minute, will ensure that the User Logon Script is executed every time VPN connection is established. If you wish to have the User Logon Script execute only once per day, set the value to 1,440 mins	

For your comments, please contact:

Synergix, Inc.

1200 Route 22 East, Suite 2000

Bridgewater, New Jersey 08807

+1 908 988 4688

http://www.synergix.com