

SYNERGIX Object Manager 2009 For Microsoft® Active Directory®

Installation Guide

SYNERGIX, Inc.
All rights reserved
Copyright © 1996 - 2009
www.synergix.com

Table of Contents

Copyright.....	1
Disclaimer.....	1
Trademarks	1
Software License Agreement.....	2
About SYNERGIX Object Manager 2009 for Microsoft® Active Directory®	4
Key Benefits	6
Security Policies	6
VPN Password Expiration Notification.....	6
Security Audit.....	6
On VPN segments	6
Computer Object Management.....	6
Domain Membership	6
Computer account migration.....	7
Hostname.....	7
Description	7
Managed By / Primary User	7
Organize by Chassis Type.....	7
User Object Management.....	8
Account Expiration.....	8
Group Objects	8
Computer Groups	8
Group Policy Objects.....	8
Security Filtering	8
Installing ADOM	9
Technical Support	12

Table of Figures

Figure 1 – Welcome Screen	9
Figure 2 – License Agreement.....	9
Figure 3 – User Information.....	9
Figure 4 – Destination Folder.....	10
Figure 5 – Computer NetBIOS Name Information.....	10
Figure 6 – Computer Domain (FQDN).....	10
Figure 7 – Manual entry, when Computer is part of a workgroup.....	11
Figure 8 – Ready to Install the Application	11
Figure 9 – Updating System	11
Figure 10 – Successful Installation.....	11

The software described in this guide is furnished under a license agreement and may be used only in accordance with the terms of this agreement.

Copyright

All copyrights are exclusively owned by Synergix Inc.

You are NOT allowed to sell, modify and reverse engineer the program without Synergix's written agreement! You are NOT allowed to distribute the registered version of the SYNERGIX Object Manager program without Synergix written agreement!

You can distribute the evaluation version freely without bundling with any other software and as long as no money is asked for it and all files in the package are intact and its use is limited to 30 days.

Registering this product is necessary after the 30 day evaluation period is over.

Disclaimer

UNLESS OTHERWISE PROVIDED BY WRITTEN AGREEMENT WITH SYNERGIX, INC. THIS PUBLICATION AND THE SOFTWARE SOLD WITH THIS PUBLICATION, ARE PROVIDED 'AS IS' WITHOUT WARRANTY OF ANY KIND EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK ARISING OUT OF THE USE OR PERFORMANCE OF THIS PUBLICATION AND SOFTWARE REMAINS WITH YOU. IN NO EVENT WILL SYNERGIX, INC., OR ANY OF ITS SUPPLIERS, BE LIABLE FOR ANY LOST PROFITS, LOST SAVINGS, DIRECT, INCIDENTAL OR INDIRECT DAMAGES OR OTHER ECONOMIC OR CONSEQUENTIAL DAMAGES, EVEN IF SYNERGIX, INC., OR ITS SUPPLIERS, HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SYNERGIX, INC. RESERVES THE RIGHT TO MODIFY THIS DOCUMENT AT ANY TIME WITHOUT OBLIGATION TO NOTIFY ANYONE. IN NO EVENT SHALL SYNERGIX, INC. OR ITS SUPPLIERS LIABILITY UNDER THIS AGREEMENT EXCEED THE SUM OF ANY AMOUNTS PAID HEREUNDER BY THE CUSTOMER TO SYNERGIX OR THE SUPPLIER.

Trademarks

Synergix, Inc. owns a number of registered and unregistered Trademarks and Service Marks (the 'Marks'). These Marks are extremely valuable to Synergix, Inc. and shall not be used by you, or any other person, without Synergix, Inc's express written permission. The Marks include, but are not necessarily limited to the following: OUrganizeIT, Object Manager for Microsoft® Active Directory, imageIT, UNIT, deployIT, trackIT, patchIT, admIT, OptimaX and the Synergix logo. In addition to Synergix, Inc Marks, some Synergix Products may include Trademarks or Service Marks owned by other corporations. These other Marks include, but are not necessarily limited to MICROSOFT® WINDOWS®, which are registered Trademarks of Microsoft Corporation. You shall not use any of the Trademarks or Service Marks of Synergix, Inc., or any other entity, without the express written permission of such Trademark or Service Mark owner.

Synergix, Inc.

Green Brook, NJ 08812

Phone: 201.355.0327
Email: sales@synergix.com
Web: <http://www.synergix.com>

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 THIS 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 PRODUCT DOWNLOAD PAGE OR DURING THE INSTALLATION 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"). Neither the evaluation version nor the REGISTERED version is 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: (1) 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); (2) you retain no copies of the Software and Documentation, including copies stored on a computer; (3) the recipient agrees to the terms and conditions of this Agreement and (4) notify Synergix about the transfer of your rights to new entity.

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, U.S.A. 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 visit SYNERGIX, Inc.'s web site at <http://www.synergix.com> or contact our office.

About SYNERGIX Object Manager 2009 for Microsoft® Active Directory®

Microsoft® Active Directory™ and the Microsoft® Windows™ Operating System built-in functionality falls short on managing VPN connected users, using non-Microsoft VPN client software, in terms of password expiration notification and group policy deployment. Computers that are disconnected from the corporate LAN environment permit users to log in using cached credentials. While this feature offers tremendous value to traveling users, it presents a challenge to IT staff to implement Domain Password Policies in Microsoft® Active Directory® environments. IT staff end up implementing a weak password policy or delay the implementation, leaving the security concerns unresolved.

In addition to the challenges of implementing a strict password policy, the IT staff is also challenged with many more situations dealing with VPN connected users. For instance,

- Login script specified as part of the user property never runs
- Group Policy updates do not apply unless the user remains logged in for extended period of time
- Domain controller security logs do not correctly reflect VPN connected users' login activities
- Applying Group Policy based upon computer chassis type, for instance, to VPN connected laptop computers only.
- Computers disconnected from Microsoft® Active Directory® domain become unmanageable
- Securing Active Directory by automatically expiring user object based upon specified number of days of inactivity.

SYNERGIX Object Manager 2009 for Microsoft® Active Directory® (ADOM) is a unique solution that allows a Microsoft® Windows® based VPN¹ user to change their Active Directory password seamlessly. The user's login behavior to their Windows based laptop i.e. with cache credentials remains the same so no special instructions need to be provided to the laptop users to change their password. All this is achieved without making any schema changes or by installing any software on domain controllers.

ADOM helps organize and secure their computer & user objects in Microsoft® Windows™ Active Directory environment, enabling organizations to better manage Active Directory and meet their SOX, SEC and HIPAA compliance requirements.

- **Manage VPN users' password expiration notification**
- **Seamless method to change password; no change required in user login behavior**

¹ ADOM is VPN client agnostic software.

- **Synchronize cached credentials with domain credentials**
- **No schema changes**
- **No software installation on domain controllers**
- **VPN client software agnostic**
- **Apply Group Policy Objects to VPN connected computers instantaneously**
- **Launch login script when users connect to corporate network via VPN**
- **Manage dormant and inactive user objects**
- Realize targeted ROI on Systems Management Software
MS SMS, LANDesk, HP Radia etc.
- **Associate computer object and last logged on users, by keeping the managedBy attribute up to date.**
- Helps meet security compliance requirements
- **Maintain domain membership of computer objects**

Microsoft® Active Directory™ built-in functionality falls short on managing VPN-connected users, in terms of password expiration notification and group policy deployment. Additionally, it falls short on user and computer object management. Although the default container to add computer and user objects can be changed in Windows 2003 based Active Directory installations, all computer and user objects can end up in the same container unless the OS deployment tools use custom scripts to put them in specific Organizational Units.

For desktop application management and for security policy implementation, IT staff in large organizations typically depends upon third party applications like LANDesk, HP Radia, MS SMS, CA Unicenter, etc. Most of these systems management tools leverage the Organizational Unit in Active Directory to define the scope of system management. Keeping the computer objects properly organized in specific Organizational Unit (by business units, or in relation to OU containing the user object or by chassis type) can become challenging. If the objects are not well placed in the right OU, it can yield unexpected results when systems management software tasks are run, causing major outages and possibly failing on the service level agreements. It is critical that computer objects are managed correctly to reap maximum benefit from the investments made in systems management software and to ensure policies are applied correctly to computer objects. Active Directory Object Manager fills that gap; the post OS deployment and day 2 computer object management is totally automated.

Key Benefits

Security Policies

VPN Password Expiration Notification

Password policies, specifically the password expiration policy, can cause issues to VPN users who typically login using cached credentials. When their password is about to expire, they do not receive password change notification, which ultimately results in their account being locked out. This typically gets resolved by the users having to call the help desk to have their password reset, adding to the help desk cost and also, causing disruption of services to business users.

With ADOM™, VPN users, logging in with cached credentials, are prompted for password change and presented with a custom dialog box to change the Microsoft® Active Directory® password.

Security Audit

On VPN segments

It is typical that most third party (Cisco, MCI, Nortel etc) VPN client users log into their computers using cached credentials. And then, fire up the VPN client to gain access to corporate resources. Under this scenario, neither the security log on the domain controller(s) nor the **Last Logon** attribute of the user object is updated. An audit of active directory environment can report VPN users as inactive users. This scenario can make the SOX, HIPAA and other compliance exercises laboriously and costly.

With ADOM, VPN users logging in with cached credentials and later connecting to corporate resources are tracked in Active Directory® Domain Controller Security logs, just like LAN connected desktop and laptop users. The **Last Logon** attribute is also updated. This enables the auditors to generate accurate usage reports and take appropriate actions to stay compliant with IT security requirements.

Computer Object Management

Domain Membership

Laptop users with elevated privileges may remove their computers from the domain, for non-business / experimental purposes or for business reasons, such as during software product demonstration at client sites, tradeshow or conferences. ADOM helps maintain domain membership. If the computer object in the Active Directory domain becomes defunct or the user removes the computer object from the domain and puts it in a workgroup or another domain, the computer rejoins the domain next time it

connects to the corporate network. All this is achieved without granting the user elevated privileges to his / her workstation or in Active Directory environment.

Computer account migration

ADOM may also be used to help migrate computer accounts from one trusted domain to another trusted domain.

Hostname

The hostname assigned to a Windows based computer at built time may be retained using ADOM. When the user with elevated privileges decides to change the hostname, it is rolled back to the original hostname when the computer is put back on the corporate network (LAN or VPN)

Description

The description attribute of the computer object can be customized and maintained dynamically.

e.g. John Smith, OS Version = 5.1, AV Definition = 5/7/2007 Rev 25

Managed By / Primary User

The 'Managed By' attribute of the computer object is updated and can be used to link the computer object to the primary user's user object.

Organize by Chassis Type

Computer objects are moved in the Active Directory environment and organized in an Organization Unit that reflects the Chassis Type (Desktops or Laptops) and is set relative to the OU where the user object resides.

+ Finance

- + Users -If the primary user's user ID exists here,
- + Desktops -associated Desktop is automatically moved here &
- + Laptops -associated Laptop is automatically moved here.
- + Printers
- + Servers

User Object Management

Account Expiration

Systems Administrators can easily keep track of dormant accounts by enabling the user **Account Expiration** feature. Microsoft Active Directory allows a static entry for Account Expiration, however, ADOM dynamically updates it based upon preconfigured value. For instance, the Systems Administrator can grant 7 days of access from the last successful login.

This feature allows system administrators to expire dormant user accounts thus safeguarding corporate data from unauthorized use. Active users continue to have access to active directory resources without any interruptions.

Group Objects

Computer Groups

ADOM maintains computer object membership in a group that easily differentiates the computer based upon Chassis Type. For instance, all desktop class computers are added to '**Domain Desktops**' group and all laptop class computers are added to '**Domain Laptops**'

This feature allows the systems administrator to configure **Group Policy Objects** and enable them using **Security Filtering** option and make use of the chassis specific groups.

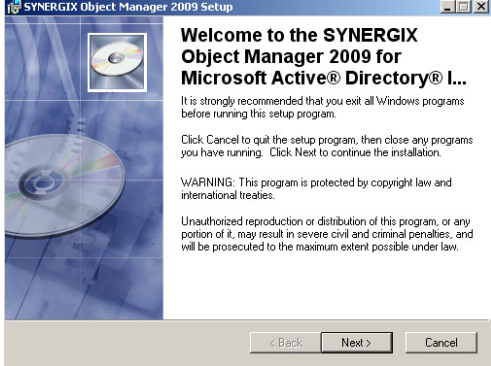
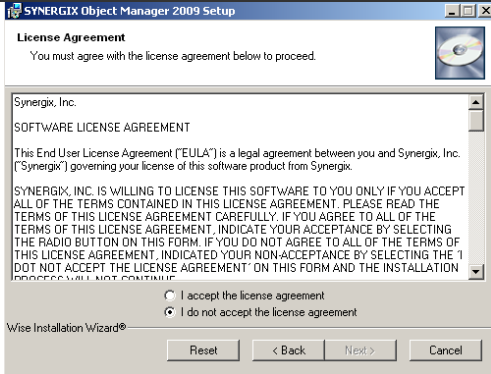
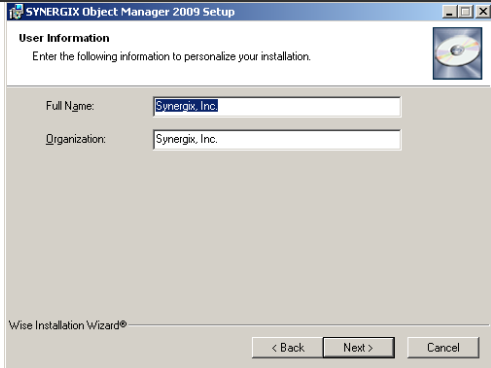
Group Policy Objects

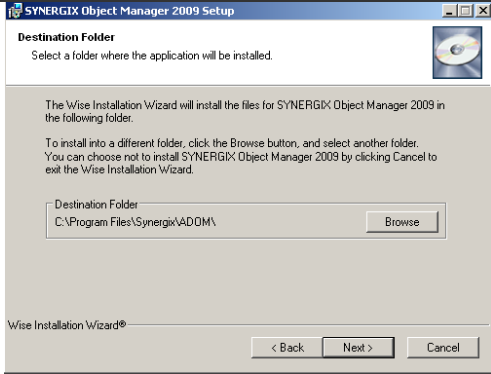
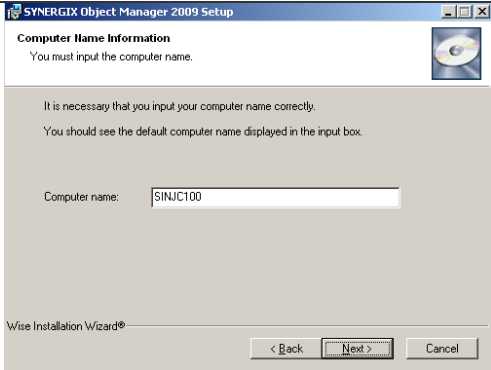
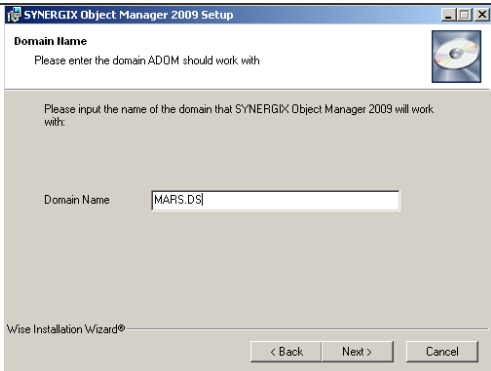
Security Filtering

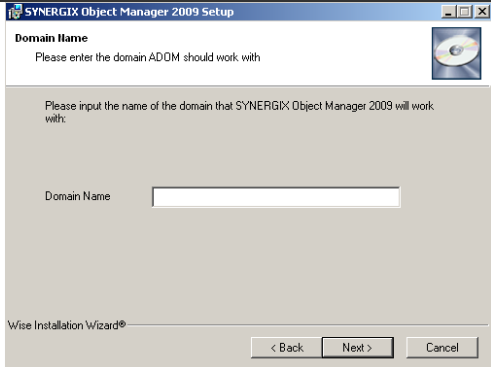
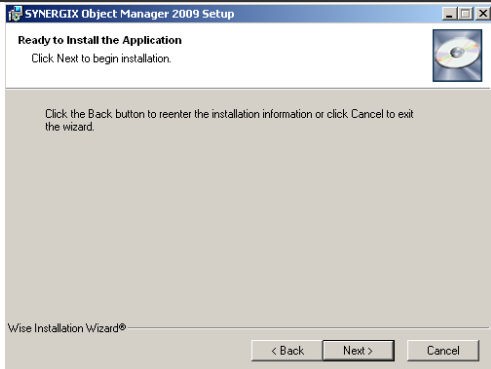
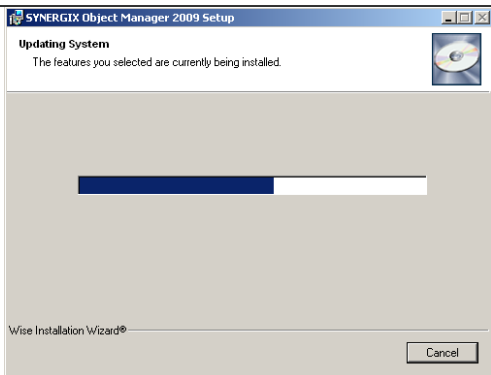
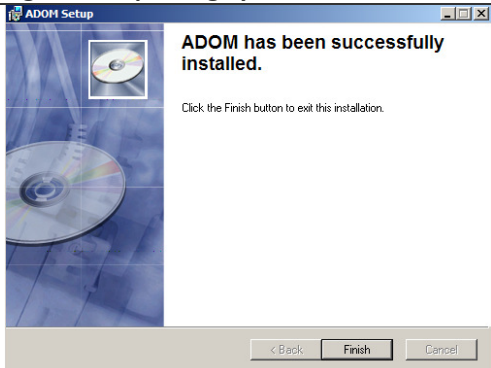
Desktop class and laptop class computers are added to appropriate groups in Active Directory i.e. '**Domain Desktops**' and '**Domain Laptops**'.

These two groups can be used to assign GPO at the domain level and use the **Security Filtering** option to assign policy to appropriate computer objects only.

Installing ADOM

	<p>Ensure that .NET Framework 2.0 or better is installed</p>	
	<p>Start the program setup using MSIEXEC</p> <p><code>MSIEXEC /I ADOM.MSI /!*v ADOM.MSI.LOG</code></p>	
	<p>Click on Next</p>	 <p>Figure 1 – Welcome Screen</p>
	<p>Read through the license agreement. If the terms are acceptable, click on <i>I accept the license agreement</i> radio button and then, click on <i>Next</i>.</p>	 <p>Figure 2 – License Agreement</p>
	<p>In the <i>User Information</i> dialog box, type the <i>Full Name</i> and <i>Organization Name</i> and click on Next.</p>	 <p>Figure 3 – User Information</p>

<p>You may leave the <i>Destination Folder</i> value to default value (recommended).</p> <p>If your current standard operating environment requires for software to be installed on another volume, change the value of Destination Folder by clicking on the <i>Browse</i> button.</p> <p>Click on <i>Next</i></p>	 <p>The screenshot shows the 'Destination Folder' dialog box. It contains instructions on how to choose a folder for installation and a text box with the default path 'C:\Program Files\Synergix\ADOM\'. A 'Browse' button is visible to the right of the text box. At the bottom, there are 'Back', 'Next >', and 'Cancel' buttons.</p> <p>Figure 4 – Destination Folder</p>
<p>The installer will populate the Computer Name edit box with current NetBIOS name of your computer. This value is used by ADOM to roll back the computer name, if the user or a program with local administrative privileges changes the value to non-standard hostname.</p> <p>Change this value only if the current hostname does not comply with your corporate host naming convention.</p>	 <p>The screenshot shows the 'Computer Name Information' dialog box. It instructs the user to input the computer name correctly. A text box contains the value 'SINJC100'. At the bottom, there are 'Back', 'Next >', and 'Cancel' buttons.</p> <p>Figure 5 – Computer NetBIOS Name Information</p>
<p>The Domain Name edit box will be populated with the FQDN of the Microsoft Active Directory domain name that the computer belongs to.</p>	 <p>The screenshot shows the 'Domain Name' dialog box. It asks the user to enter the domain name. A text box contains the value 'MARS.DS\'. At the bottom, there are 'Back', 'Next >', and 'Cancel' buttons.</p> <p>Figure 6 – Computer Domain (FQDN)</p>

<p>If at the time of installation, the computer belongs to a Workgroup instead of an Active Directory domain, the edit box will be blank and must be typed in. After the software is installed and configured with appropriate impersonation [domain] account credentials, the computer will join the specified domain.</p>	 <p>Figure 7 – Manual entry, when Computer is part of a workgroup</p>
<p>Click on <i>Next</i> when ready to install the application.</p>	 <p>Figure 8 – Ready to Install the Application</p>
<p>Please wait while the system is updated with program binaries</p>	 <p>Figure 9 – Updating System</p>
<p>Click on <i>Finish</i> to exit the installation.</p>	 <p>Figure 10 – Successful Installation</p>

The default installation should enable the software for the [VPN Password Expiration Notification feature](#), [Group Policy updates](#), [User Login script](#), [Domain Controller Security Log updates](#). For advanced configuration, please refer to the *SYNERGIX Object Manager – Configuration Guide*.

Technical Support

For technical support, contact support via email at support@synergix.com or visit <http://www.synergix.com/support>

Synergix, Inc.
24 Wingate Way
Green Brook, NJ 08812
www.synergix.com