Lepide Active Directory Self-Service

Steps to Deploy GINA/CP

Table of Contents

1. Introduction

Lepide Active Directory Self-Service provides a comprehensive means of providing automation for the necessary tasks related to manage the Active Directory in an organization.

GINA/CP helps you to access LADSS functionalities through the login screen. It allows users to easily unlock account or reset password directly from the lock screen. However, the GINA/CP installer has to be installed at client systems to avail the benefits.

The GINA/CP installer can be deployed at client systems through two ways:

1. **Direct installation at client systems:** Installation at individual systems
2. **Through GPO:** For bulk installation
3. **Remote Installation of Agents:** Select computers to install the agents.

If you have any questions at any point in the process, you can contact our Support Team. The contact details are listed at the end of this document.

2. Direct Installation at Client Systems

Follow the below mentioned steps to set up GINA/CP at individual client systems:

1. Login to LADSS admin section.
2. Click on "Configuration" tab and go to GINA/CP Installer page.
3. Download the GINA/CP Installer file.
4. Double-click the installer file and accept the license agreement after reading it.
5. Click "Next."
6. The Web Server Information page will open. You need to make changes in this section as per your network.
7. Click "Next: and follow the simple screen instructions to install it directly at individual client systems.

> NOTE: Perform the following steps on the Web Server Information page.
> - Enter the Web Server URL where LADSS is installed instead of local host.
> - Enter the selected Port Number in case it has been changed while installing LADSS.
> - If LADSS is installed in a secure network, then change "http" to "https."
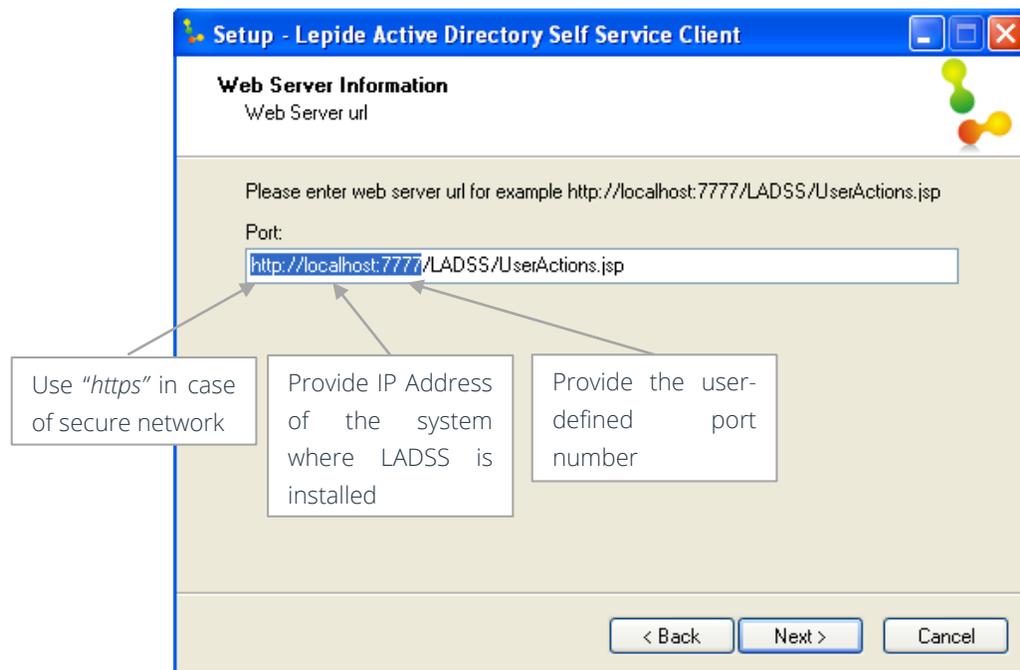
Check the following image.

Figure 1: Page of Instalaltion Wizard to change the URL

TIP: In case, you click "Next" mistakenly and install the file without providing the correct URL, kindly uninstall the application and install it again with the correct path.

3. Installation through GPO

GINA/CP can be deployed over network wide systems at one go through a customized group policy. The group policy can be applied at:

- Computer startup/shutdown
- User logon/logoff

We recommend you to create it for computer startup/shutdown (however, it includes some extra steps).

3.1 Install through a Group Policy at Startup/Shutdown

Follow the below mentioned steps to get GINA/CP activated through GPO on a particular domain:

In LADSS admin section, go to the GINA/CP Installer page and download it.

Figure 2: Download GINA/CP Installer

In the following steps, you will find how to:

- Create a Security Group
- Create a Group Policy
- Perform Administrative Template Settings
- Applying the GPO

3.1.1 Create a Security Group

1. Go to "Administrative Tools" and open "Active Directory Users and Computers" console.

2. Right-click on any OU, select "New" and click "Group" to create a new group.

3. Provide group name in the respective fields.

4. Select group scope as "Global" and group type as "Security" (these are default settings).
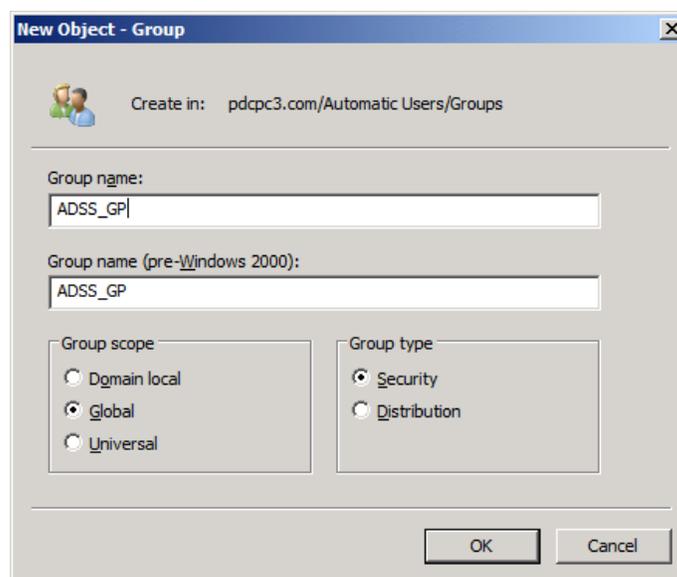
5. Click "OK."

Figure 3: Create a new group

6. The new group will be reflected under the respective section. Double-click on it or right-click and open "Properties."
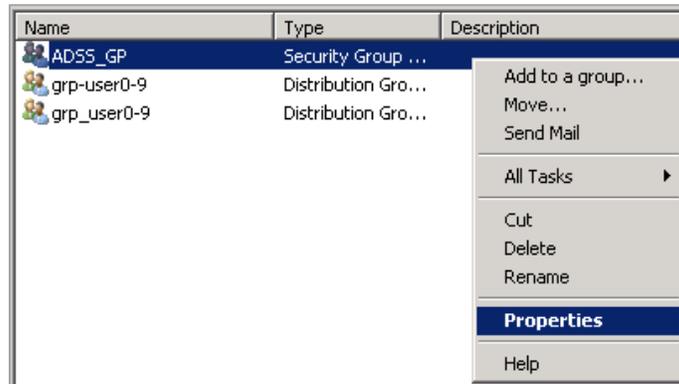

Figure 4: Option to view the properties of security group

7. Select "Members" and click "Add" to add all the computers where you want to deploy GINA/CP settings.
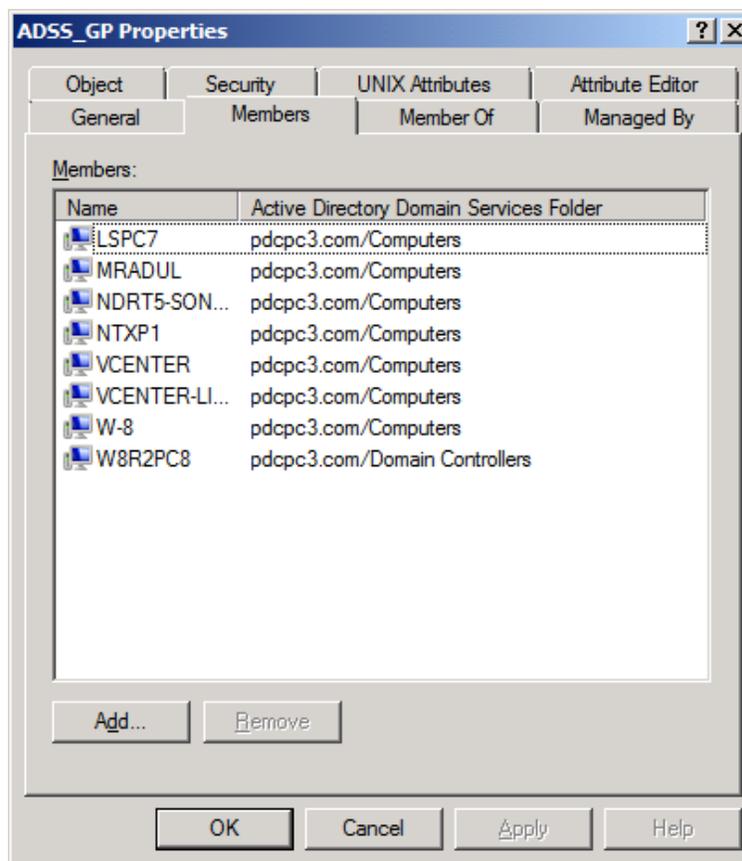

Figure 5: Add Computers as the Group Members

8. Click "OK", once you have added the computers.

9. Close "Active Directory Users and Computers" console.

In the next section, you will how to create a Group Policy add script at Computer Startup/Shutdown.

3.1.2 Create a Group Policy

1. Now go to "Administrative Tools" and open "Group Policy Management." (Execute *"gpmc.msc"* on Run or Command Prompt to access it.)

2. Under Group Policy Management, select the domain where GINA/CP settings are to be activated and right-click on it to create a new GPO.
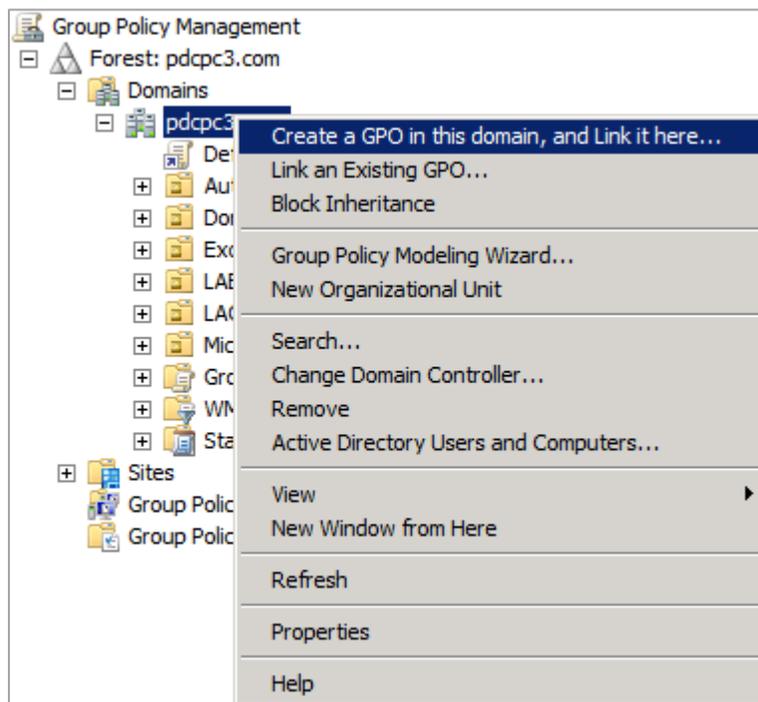
Figure 6: Option to create a Group Policy

NOTE: You can create a new Group Policy on OUs as well instead of a domain.

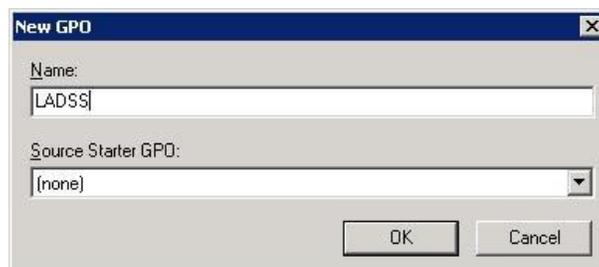3. Provide a name to the new Group Policy and click "OK."

Figure 7: Create GPO

The new GPO will be listed under the current domain.

4. Right-click on it and select "Edit."

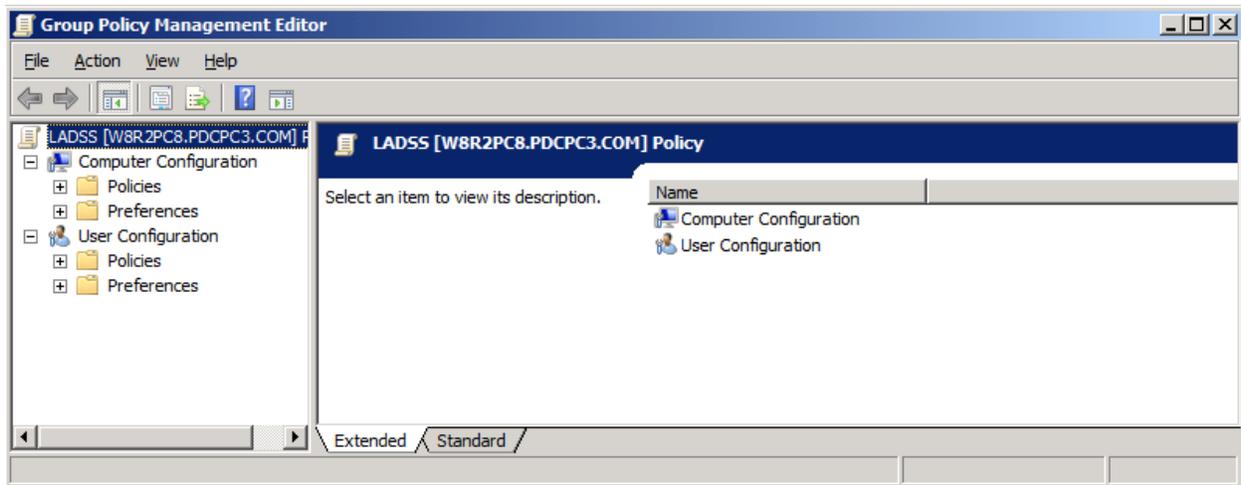5. "Group Policy Management Editor" opens automatically and the new GPO will be highlighted.

Figure 8: Group Policy Management Editor

6. Go to "Computer Configuration", and expand "Policies" folder.

7. Navigate to "Windows Settings", expand the node and click on "Scripts (Startup/Shutdown)".
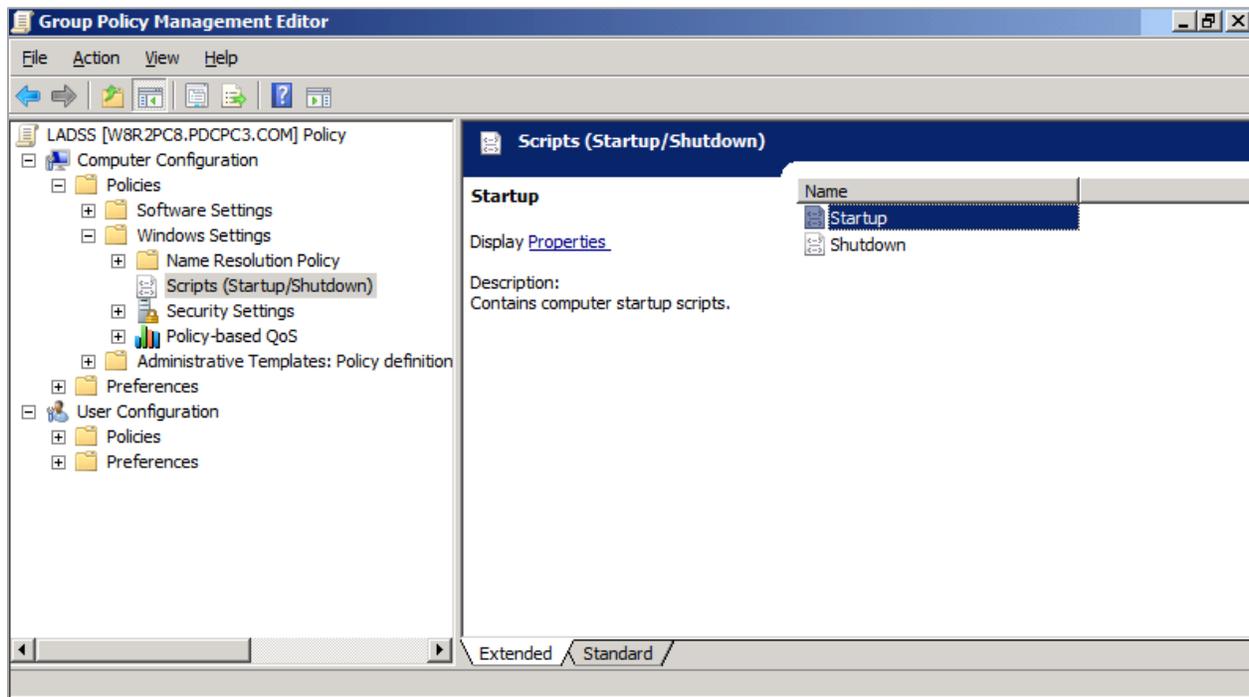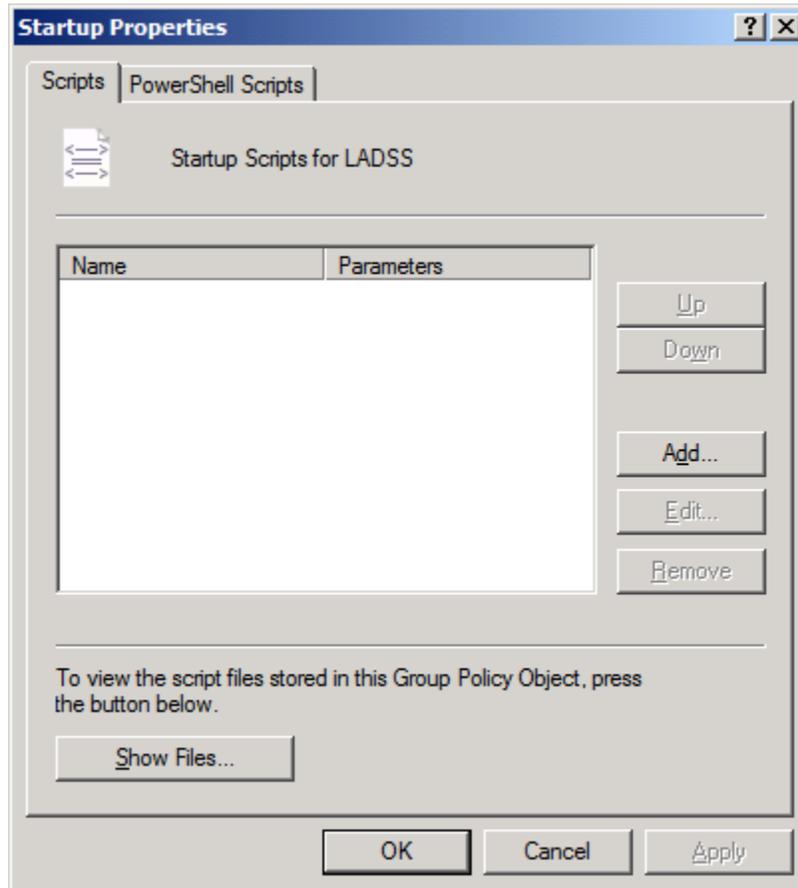
Figure 9: Start/Shutdown Scripts

NOTE: The script can be inserted either at Startup or during Shutdown. Here, we are performing it at startup.

8. Double-click 'Startup' to access its properties.

Figure 10: Properties of the Startup Script

9. Click "Show Files" to access its window that shows the details regarding the script files stored in this Group Policy Object.

10. Now, copy the GINA/CP installer file (from the downloaded location) to here.
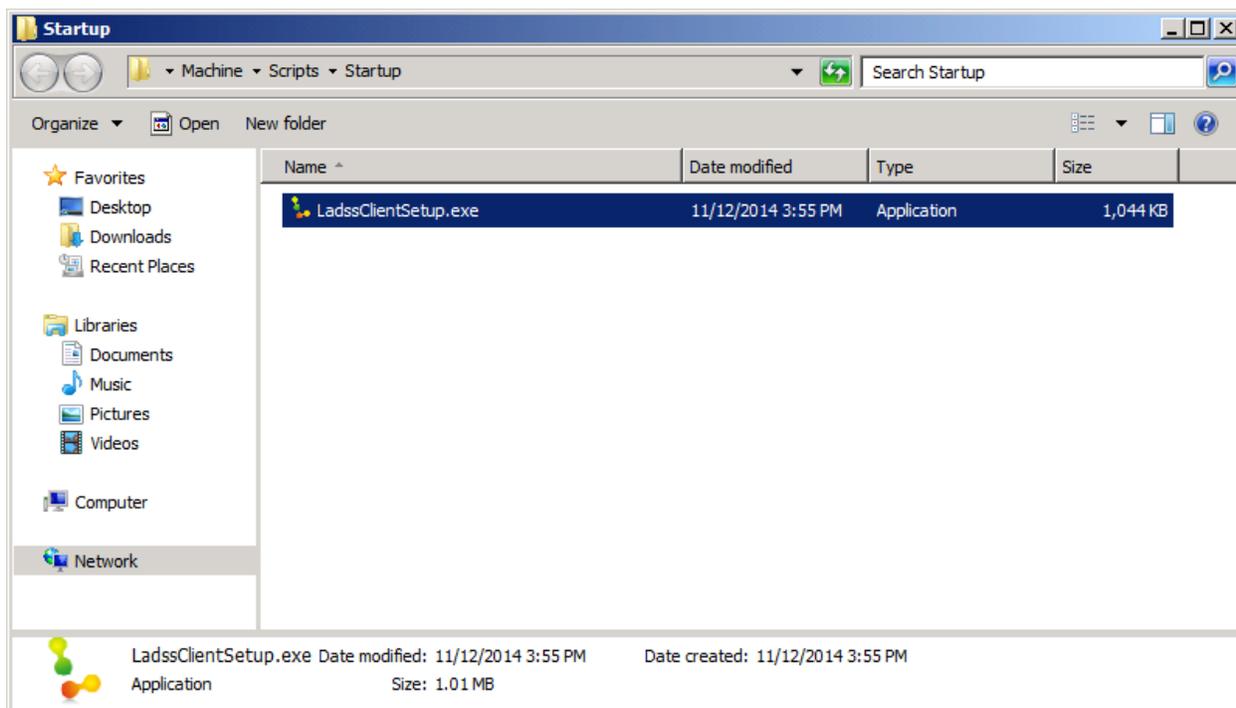
Figure 11: Add Files to run at Startup

11. Close the window.

12. Now, in 'Startup Properties', click "Add" to access "Add a Script" dialog box.

13. Click "Browse" and select the GINA/CP installer file. The setup file will be selected in "Script Name" text field.

14. Provide script parameters by typing '/VERYSILENT' and provide the URL from where LADSS is being accessed after leaving a single space.

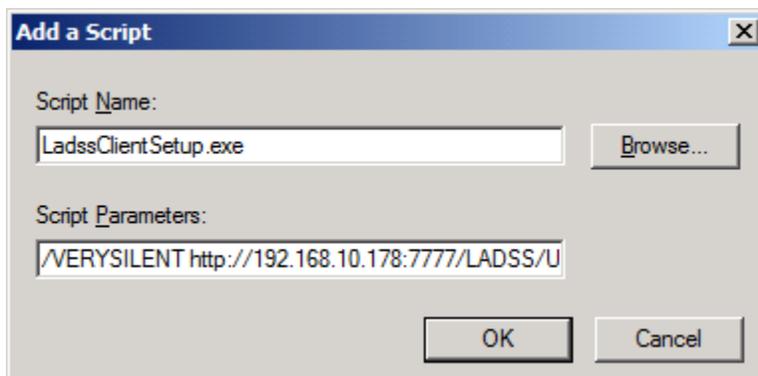   Example URL: *http://192.168.10.178:7777/LADSS/UserActions.jsp*

15. Click "OK."

Figure 12: Add a script
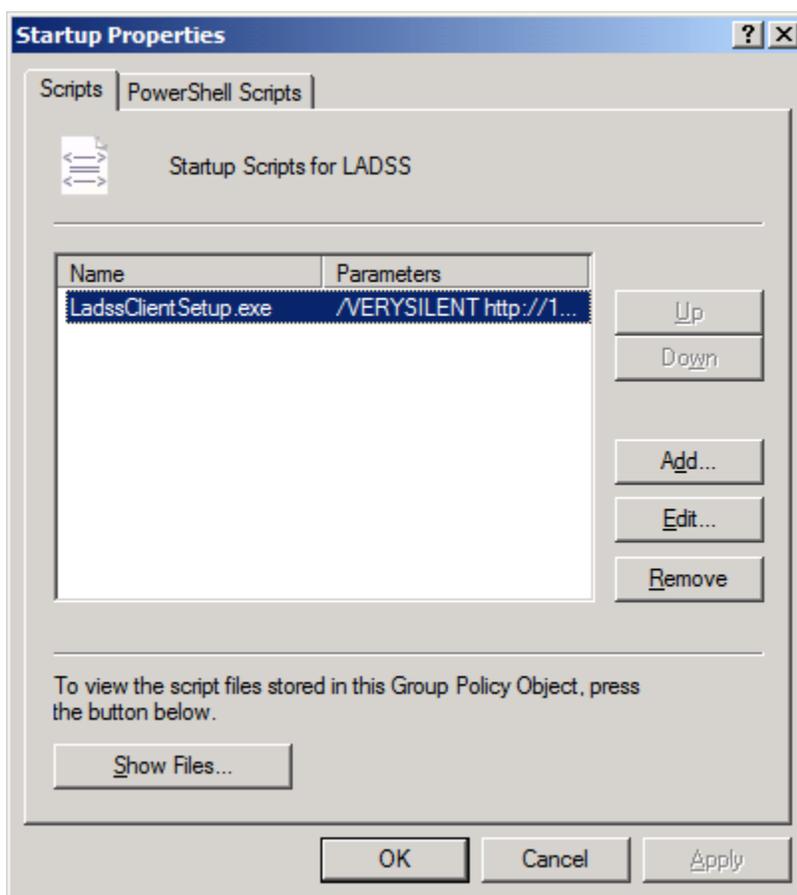
16. The script will be successfully added.

Figure 13: Added the startup script

17. Click "Apply" and "OK" to complete the process.

This is how you can create a Group Policy for deploying GINA/CP installation at all added client systems. However, before updating the Group Policy, you need to configure few 'Administrative Template Settings' as shown in the next section.

3.1.3 Administrative Template Settings

Perform the following steps.

1. In the same Group Policy Management Editor section, under Computer Configuration, expand Policies, navigate to Administrative Template section and expand it in the following order.

   Computer Configuration →Policies →Administrator Templates → System

2. Navigate to 'System' and expand it.

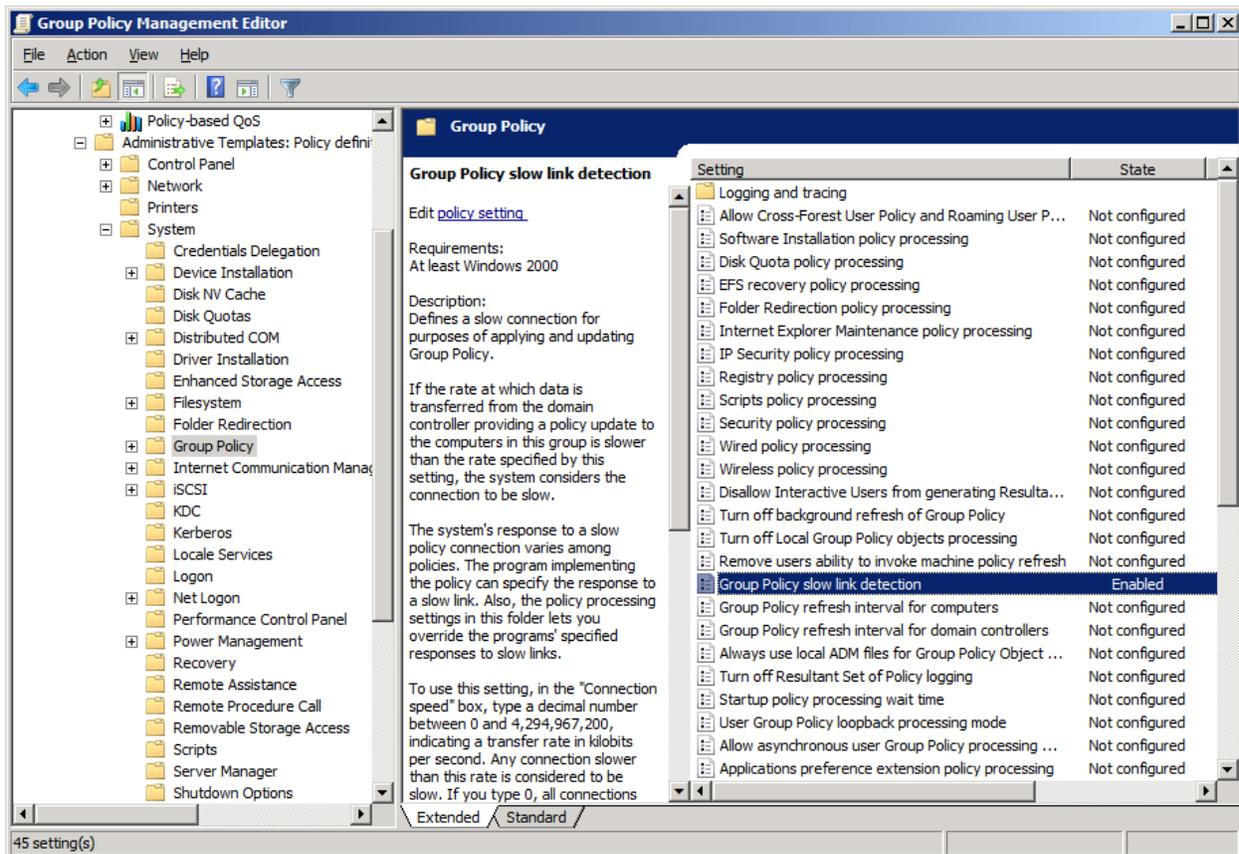3. Under 'System', navigate to "Group Policy" and double-click "Group Policy slow link detection.'

Figure 14: "Group Policy slow link detection" policy

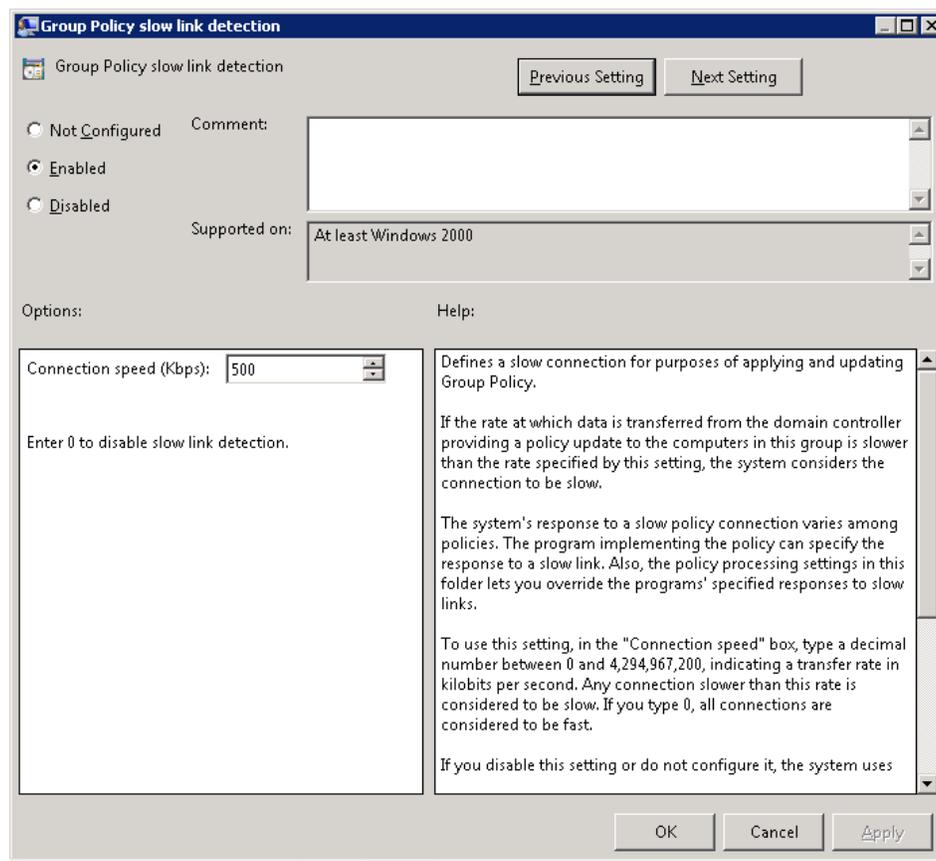4. Double-click it to select its properties.

Figure 15: Enable the policy

5. Select "Enabled."

6. Click "Apply" and "OK."

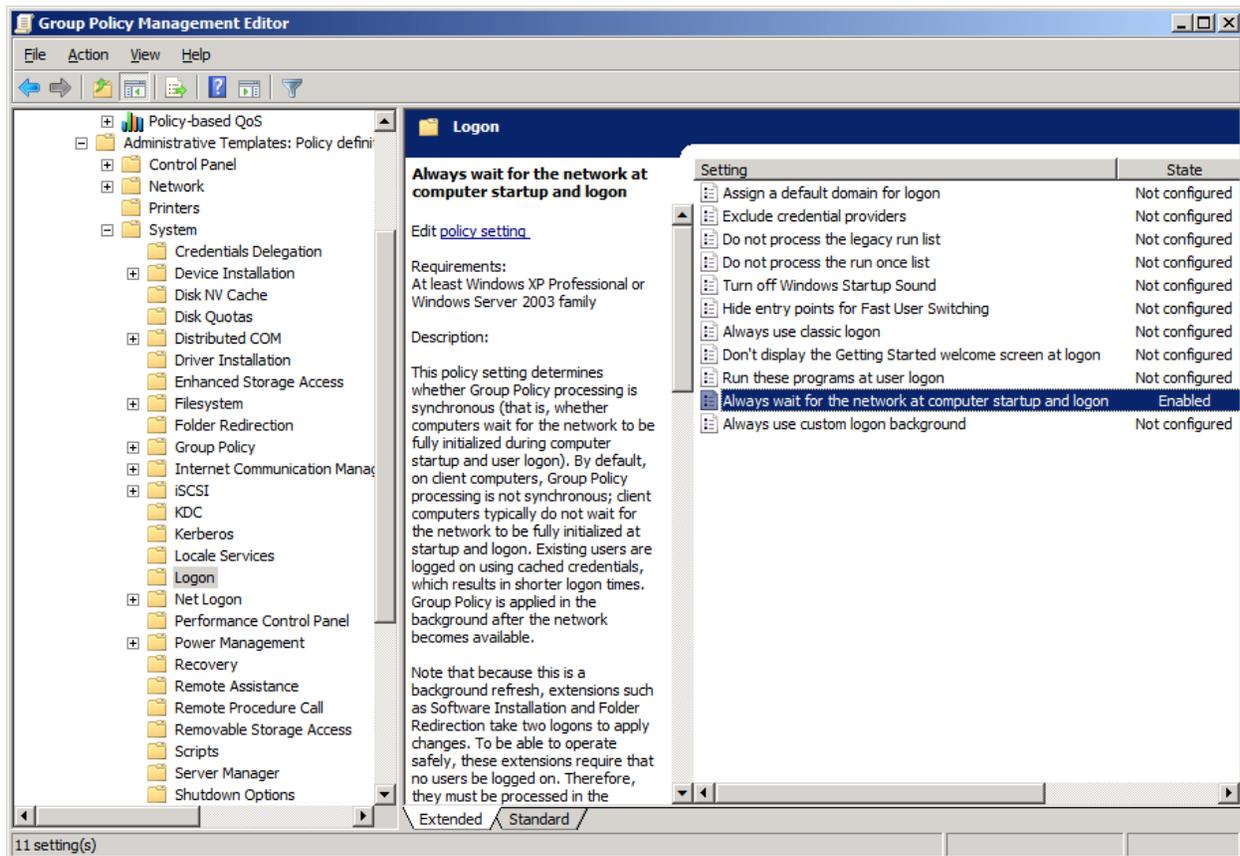7. In "System", now navigate to "Logon."

Figure 16: "Always wait for the network at computer startup and logon" policy

8. Double-click 'Always wait for the network at computer startup and logon' and enable it the same way.

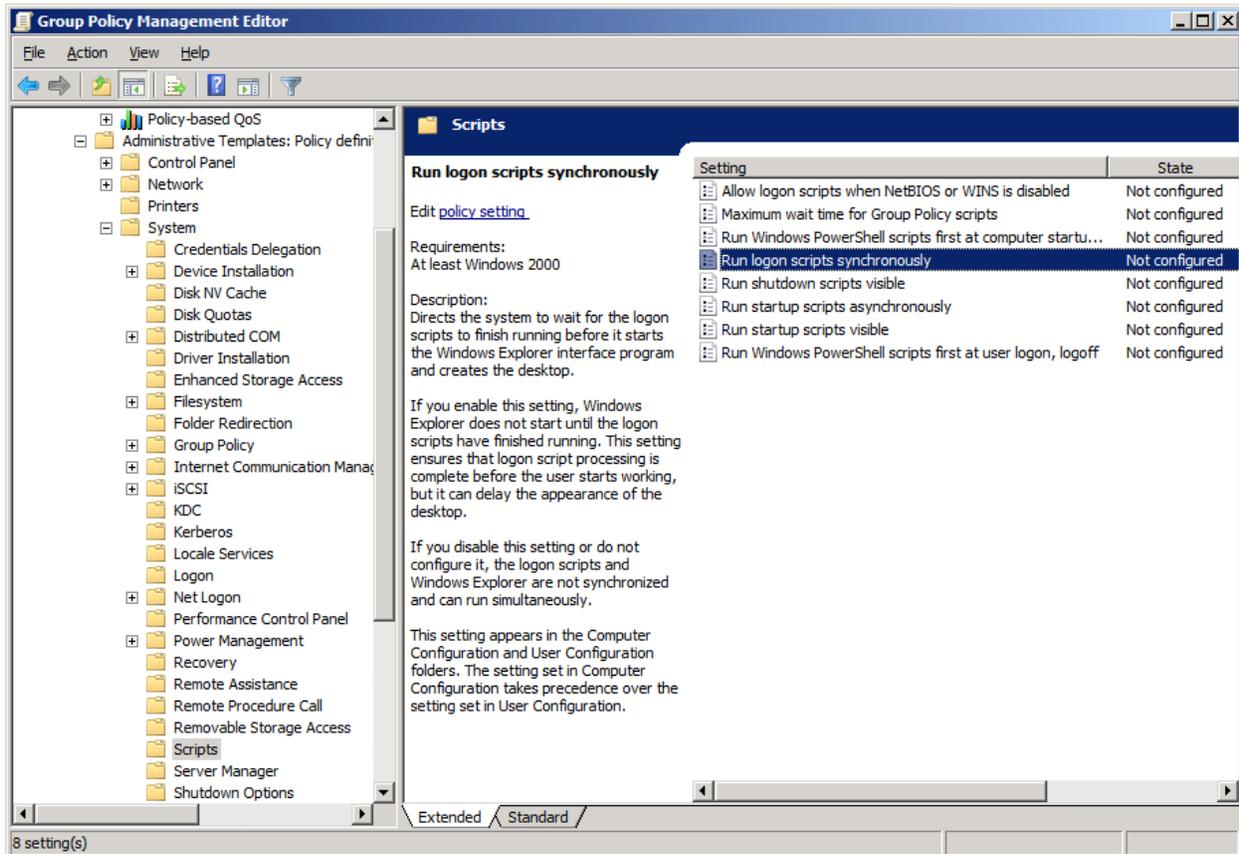9. Finally navigate to 'Scripts' in "System".

Figure 17: "Run logon scripts synchronously" policy

10. Double-click "Run logon scripts synchronously" and enable it.

11. Double-click "Maximum wait time for Group Policy scripts" and enable it.

That is it; the required administrative template settings will be successfully configured. The last section deals with GPO application.

3.1.4 GPO Application

The next process is to apply the created GPO to the desired computers within the network.

1. In the same 'Group Policy Management Editor' section, right-click on the newly created Group Policy and click 'Properties'.
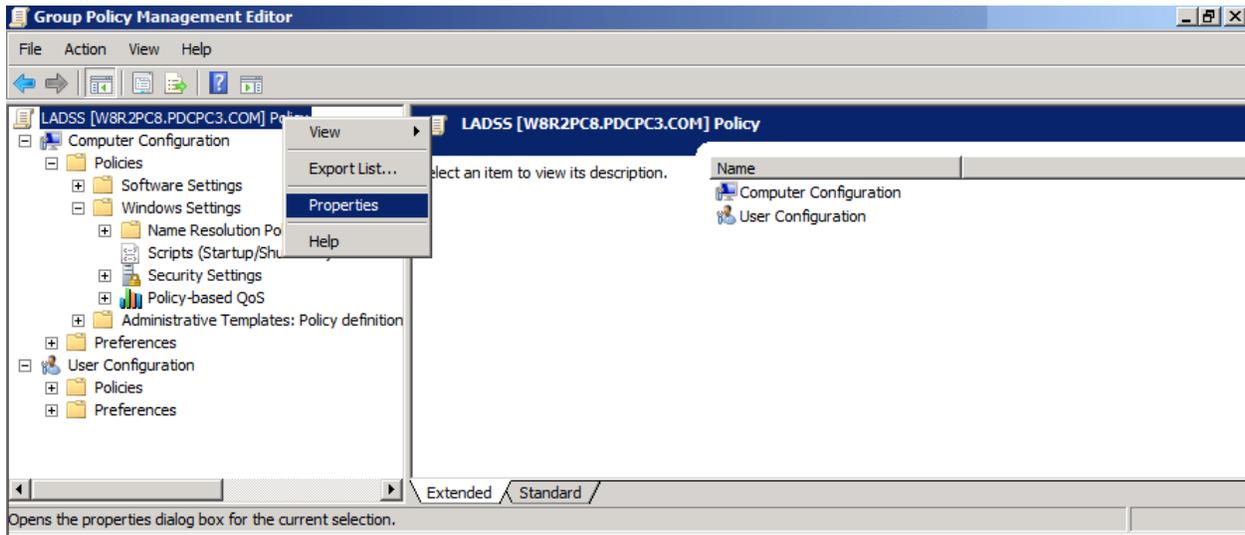
Figure 18: Option to view Properties of a GPO

2. In "Properties" dialog box, click "Security" tab.

3. Select "Authenticated Users" and enable "Read" checkbox.

4. (Important) Now, uncheck "Apply Group Policy" checkbox.

5. Leave rest all checkboxes as it is.
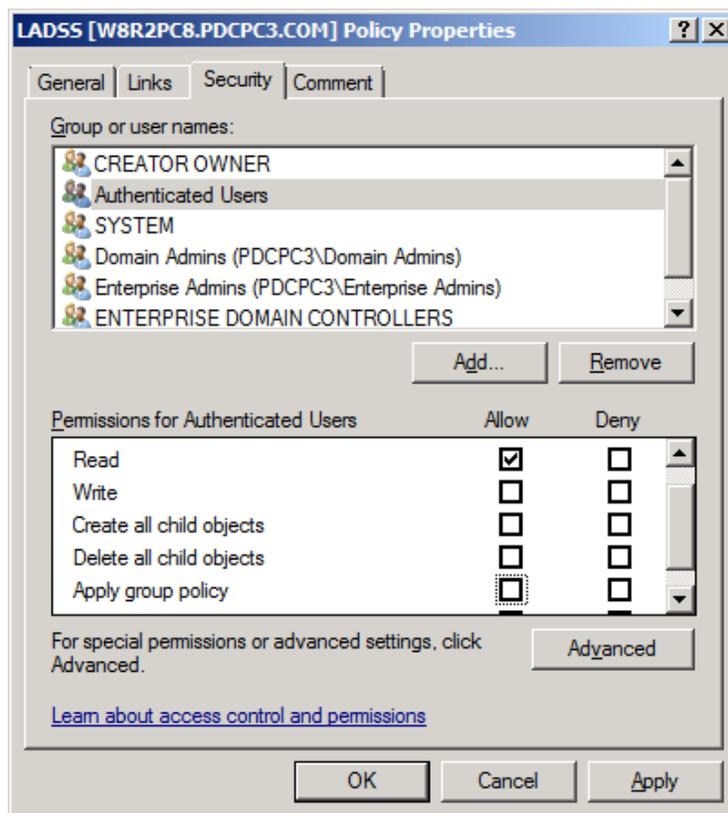
6. Click "Apply."

Figure 19: Properties of a GPO

7. Now, click "Add" and enter the name of the security group created at the first step.

8.   Click "Check Names" to authenticate entry of correct group.

> NOTE: If you face trouble in manually entering the group name, you can use the 'Advanced' tab to explore the group name.

9. Click "OK."

10. The added group will be reflected under "Security" tab.

11. Now select the group, enable 'Read' and 'Apply Group Policy' checkbox.

12. Click "Apply" and "OK."

13. Now, the final step is to update the Group Policy.

14. Execute "gpupdate" command on Run or Command Prompt.

15. Restart all the client systems where the GPO is to be applied.

Once the client systems reboot, you can find 'Reset Password/Unlock Account' link appears on the Windows logon screen. Thus, you can successfully deploy GINA/CP through GPO at computer startup/shutdown.

3.2 Install through Group Policy at User Logon/Logoff

This is an alternate way to install the GINA/CP installer files at client systems through user logon/logoff. This procedure involves less steps; however, there is a drawback. The script will be executed only when users who have administrative rights logon or logoff to the respective client systems.

The steps are almost similar for creating the GPO and adding script. To deploy GINA/CP through this method, follow the below mentioned steps:

1. In LADSS admin section, go to GINA/CP Installer page.

2. Download the GINA/CP Installer and configure it on Domain Controller. Do it by simply pasting the installer file in the public folder of the server where LADSS is installed.

3. Now go to 'Administrative Tools' and open 'Group Policy Management'.

4. Under "Group Policy Management", select the domain where GINA/CP settings are to be activated and right-click on it to create a new GPO.
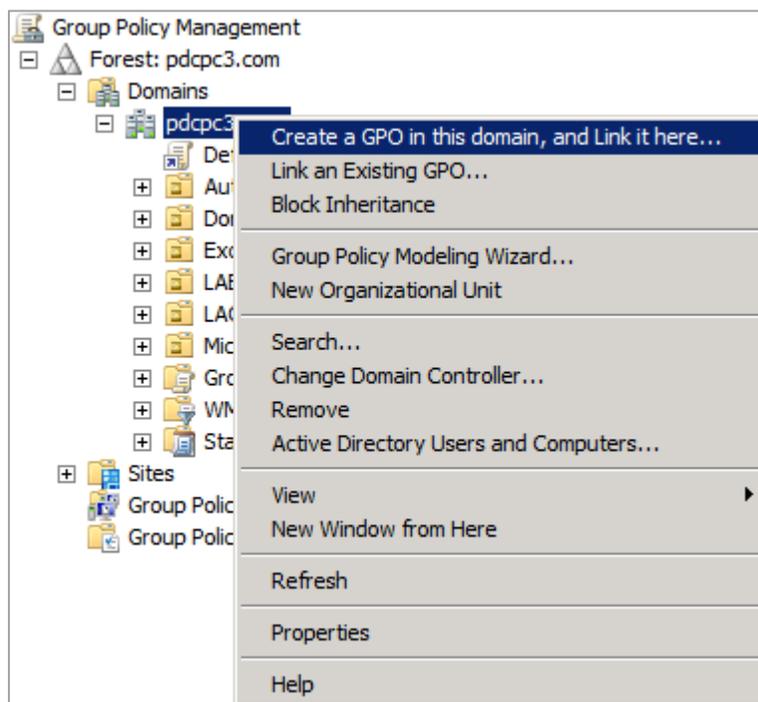

Figure 20: Option to create a GPO

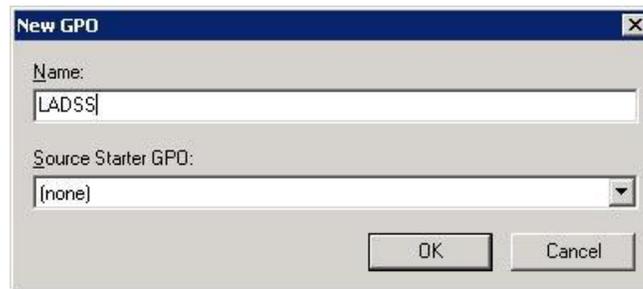5. Provide a name to the new GPO and click "OK."

Figure 21: Option to create a GPO

The new GPO will be listed under the current domain.

6. Right-click on it and select "Edit" to access "Group Policy Management Editor."

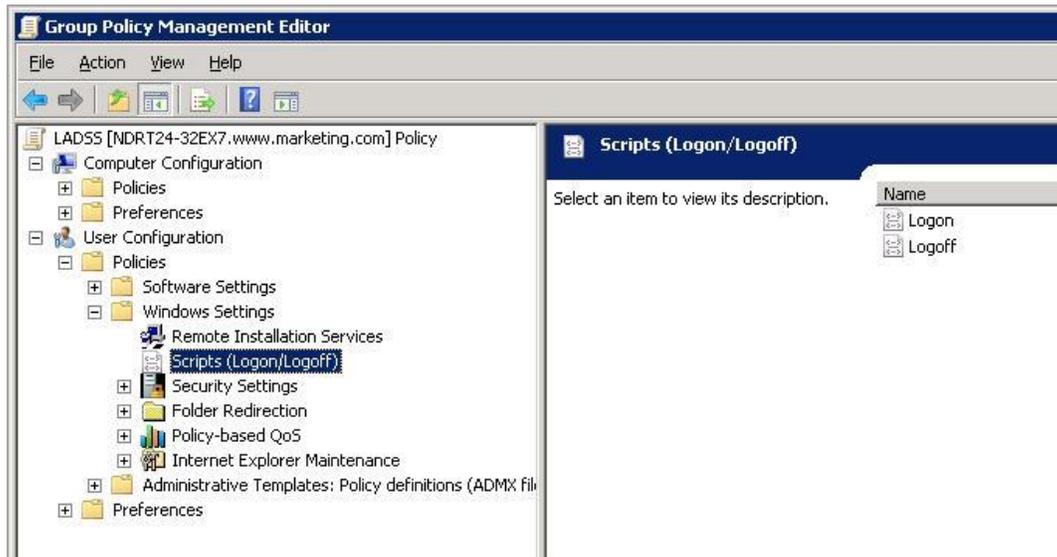7. Go to 'User Configuration', and expand 'Policies' folder.

Figure 22: Logon/Logoff Scripts

8. Double-click 'Logoff' and the logoff properties wizard will open up.

NOTE: The script can be inserted at either Logon or Logoff but it is preferable to activate the script at logoff.

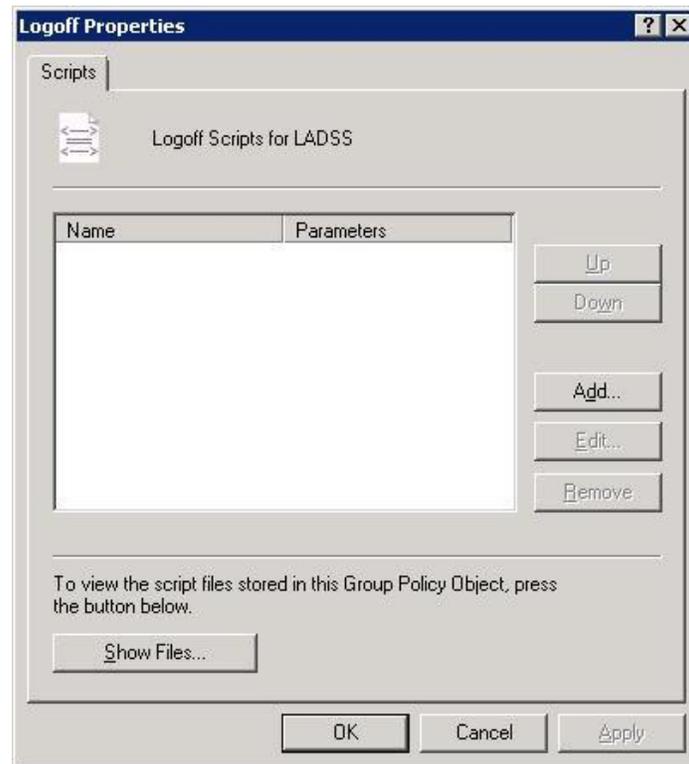9. Click 'Add' to open up the script addition window

Figure 23: Add Logoff Script

10. Provide complete path of the installer exe file in the Script Name text field

NOTE: If LADSS is installed at a client site, then provide the IP address of the system where GINA/CP scheduler exe was placed in the public folder.

11. Provide script parameters by typing '/VERYSILENT' and provide the URL from where LADSS is being accessed. (Example URL: http://192.168.10.195:7777/LADSS/UserActions.jsp)
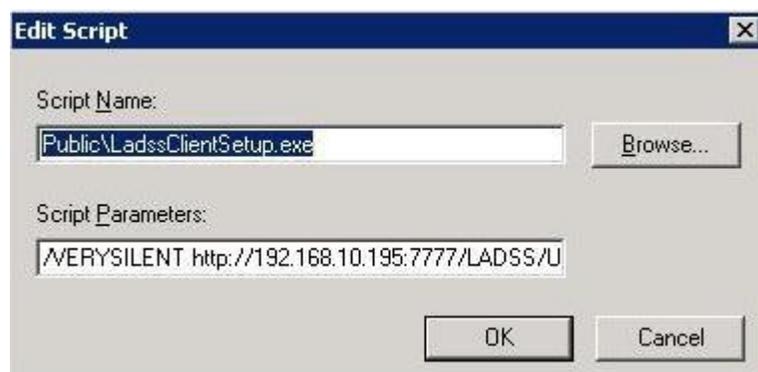
12. Click "OK."

Figure 24: Edit Script
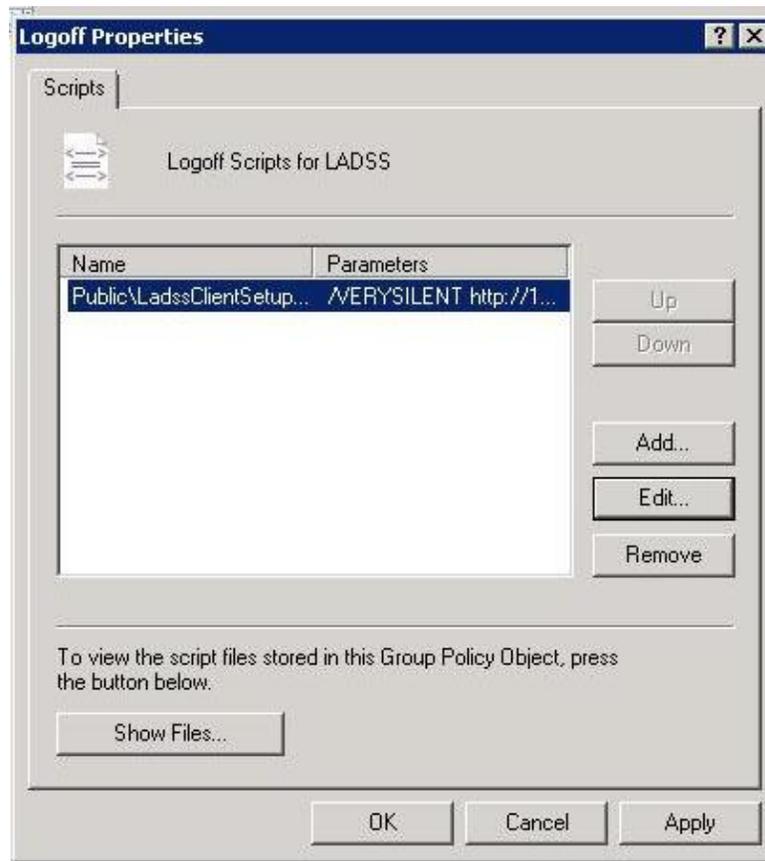
13. The script will be successfully added.

Figure 25: Added the logoff script

14. Click 'Apply' and then 'Ok' to confirm.

15. Now, the final step is to update the Group Policy. Go to Run or Command Prompt, enter *'gpupdate'* and hit enter.

16. Logoff and then Login all the client systems where the GPO is to be applied. In case, the GPO is not updated, reboot the client systems.

4. Remote Installation of Agents

Perform the following steps

1. Go to "Configuration" tab and select "GINA/CP Installer".

2. Select "Remote Agent Installation" option from the drop-down menu.

Figure 26: Install GINA/CP

3. Select the domain where you want to install the agent(s).

4. Click "Add" to access the menu.

Figure 27: Option to select computers

5. This menu contains the following three options. You can select anyone to add the computers for installing agents on them. Let us have a look at these options.

   A. **Specific Computer:** This option lets you add the computer directly by providing its name or IP Address. Selecting it will display the following pop-up.

Perform the following steps.

    i.   Type the name or IP Address of the desired computer.

    ii.   Click "Add" to add this computer. The computer is added to the list below.

    iii.   You can add multiple computers.

    iv.   Click "OK" once you are done. This will take you back to the previous screen of remote agent installation, which will now display the added computers.

B.   **IP Address:** This option lets you add the computers between the provided IP address range.

Perform the following steps.

    i.   Enter the start and end IP Address.

Figure 28: Add Computers through IP Address range

ii. Click "Ok" to add the computers of which IP Addresses fall between the specified range. It takes you back to the previous screen of remote agent installation, which will now display the added computers.

C. **Computer Discover from AD:** This option lets you add the computers from Active Directory. Clicking it will display the list of all available computers in Active Directory.
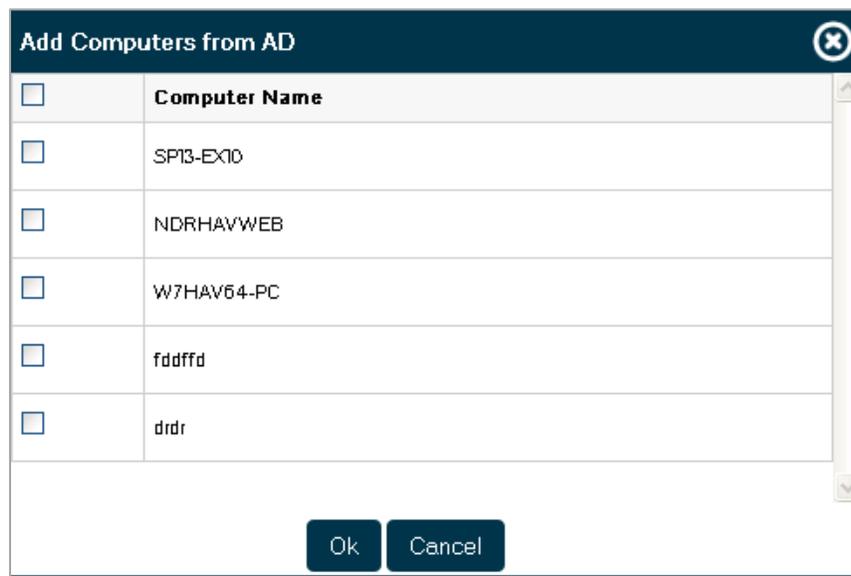
Figure 29: Add computers from Active Directory

Check the computers where you want to install the agents and click "OK". It takes you back to the main screen, which will now display the list of added computers.

6. While adding the computers using any of the above methods, if any computer(s) is/are already added then software will display the following message. The remaining computer(s) not added already will be added.
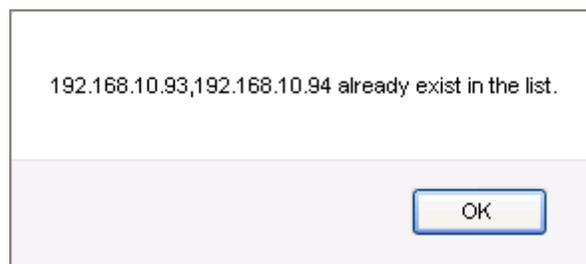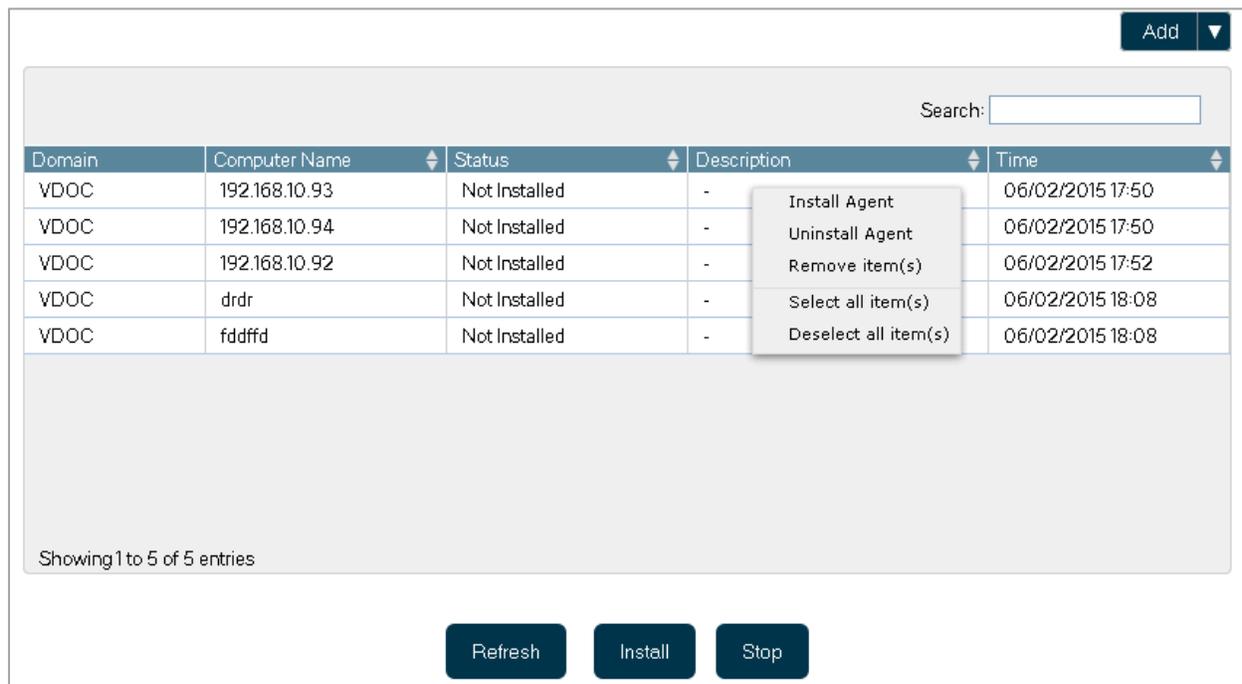
Figure 30: Computer already exists in the list

7. Once you have added the computers, now you can select the exact computers to proceed with installation.

Figure 31: Added the computers.

8. You can right click on any entry in the list to access the context menu, which has the following options.

    a. **Install Agent:** This option lets you install the agent(s) on the selected computer(s).

    b. **Uninstall Agent:** This option lets you uninstall the agent(s) from the selected computer(s).

    c. **Remove item(s):** This option lets you remove the selected computer(s) from the list. Follow the steps below to remove the items.

    d. **Select all item(s):** This option lets you select all computers at once.

    e. **Deselect all item(s):** This option lets you deselect all computers at once.

9. Click the computers in the list to select them.

10. Click "Install" button. Alternatively, you can right click and select "Install Agent" option. It starts the agent installation process.

Figure 32: Installing GINA/CP Agents

You can click "Stop" to cancel the current process.

11. This will start the process to install the agents on the selected computers. Once completed, the following message box appears on the screen.
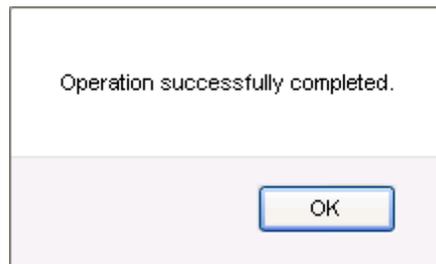
Figure 33: Agents has been installed.

NOTE: To uninstall the agent, you have to select the computer(s) from the list and do a right click.

5. Conclusion

Using this process, GINA/CP can be activated on any domain server. Now, users will get an option to 'Reset Password/Unlock Account' directly at their logon screen (as shown below).

Figure 34: GINA/CP option at logon screen

Domains users just need to click on the respective option to perform the required task.
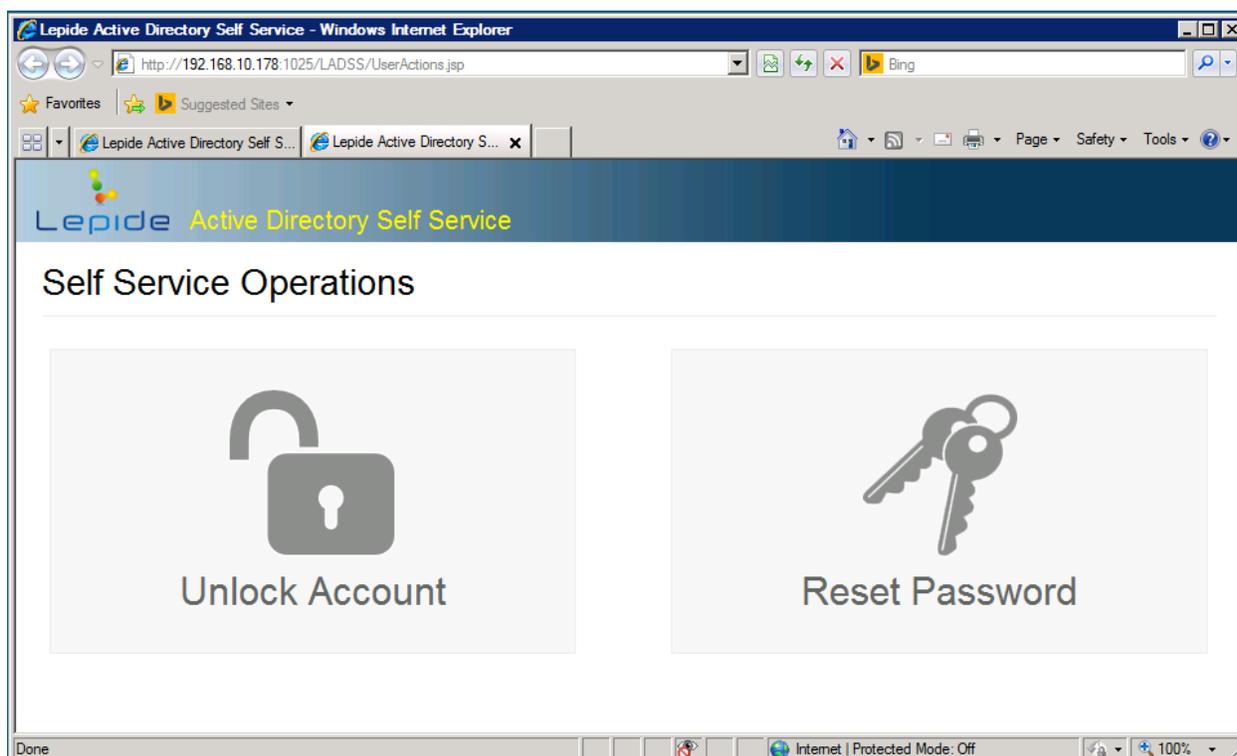
Figure 35: Self-service options

To read more about the solution visit http://www.lepide.com/active-directory-self-service/.

6. Support

If you are facing any issue while installing, configuring or using the solution, then you can connect with our team.

Product experts

USA/Canada: +1-800-814-0578

UK/Europe: +44 (0) -845-594-3766

Rest of the World: +91 (0) -991-004-9028

Technical gurus

USA/Canada: +1-800-814-0578

UK/Europe: +44(0)-800-088-5478

Rest of the World: +91(0)-991-085-4291

You can also visit http://www.lepide.com/contactus.html to chat live with our team and to know more about our support team.

You can email your queries at the following addresses.

sales@Lepide.com for Sales

support@Lepide.com for Support

7. Copyright

Lepide Active Directory Self-Service, any and all components, any and all accompanying software, files, data and materials, this guide, and other documentation are copyright of Lepide Software Private Limited, with all rights reserved under the copyright laws. This user guide cannot be reproduced in any form without the prior written permission of Lepide Software Private Limited. No Patent Liability is assumed, however, on the use of the information contained herein.

© Lepide Software Private Limited, All Rights Reserved.

8. Warranty Disclaimers and Liability Limitations

Lepide Active Directory Self-Service, any and all components, any and all accompanying software, files, data, and materials are distributed and provided AS IS and with no warranties of any kind, whether expressed or implied. In particular, there is no warranty for any harm, destruction, impairment caused to the system where these are installed. You acknowledge that good data processing procedure dictates that any program, listed above, must be thoroughly tested with non-critical data before there is any reliance on it, and you hereby assume the entire risk of all use of the copies of Lepide Active Directory Self-Service and the above listed accompanying programs covered by this License. This disclaimer of warranty constitutes an essential part of this License.

In no event does Lepide Software Private Limited authorize you or anyone else to use Lepide Active Directory Self-Service and the above listed accompanying programs in applications or systems where Lepide Active Directory Self-Service and the above listed accompanying programs' failure to perform can reasonably be expected to result in a significant physical injury, or in loss of life. Any such use is entirely at your own risk, and you agree to hold Lepide Software Private Limited harmless from any and all claims or losses relating to such unauthorized use.

9. Trademarks

Lepide Active Directory Self-Service is a registered trademarks of Lepide Software Pvt Ltd.

All other brand names, product names, logos, registered marks, service marks and trademarks (except above of Lepide Software Pvt. Ltd.) appearing in this document are the sole property of their respective owners. These are purely used for informational purposes only. We have compiled a list of such trademarks, but it may be possible that a few of them are not listed here.

Windows®, Active Directory®, AD®, Group Policy Management Console®, and Group Policy Mangement Editor® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.