Password Manager Windows Desktop Client

EmpowerID provides an extension that allows organizations to plug into Password Manager to customize the Windows logon experience beyond that supplied by the standard Windows GINA and Credential Provider tools. GINA (Windows XP, Server 2003) and Credential Provider (VISTA, Windows 7, Server 2008) are DLLs that Windows loads and executes during the booting process to provide the Windows Logon and Windows Security screens or user icons that users see when initially logging into, locking, or unlocking a computer. These native tools provide the functionality that allows workstation users to authenticate themselves by submitting correct username and password combinations.

The Problem

The GINA and Credential Providers are helpful tools—for users who remember their password. But what happens when they forget their password and cannot log into or unlock their machines? With the native GINA and Credential Provider they cannot progress any further without administrative or helpdesk intervention. These users cannot access their systems, their productivity is lost, and the business costs associated with password recovery increase.

The Solution

The EmpowerID GINA and Credential Provider extensions solve this problem by extending the password recovery functionality of the EmpowerID Password Manager with user-friendly buttons added to the Windows Logon and Credential Provider screens. These buttons allow users who have enrolled themselves into the Password Recovery Service to reset their passwords by clicking the "Self-Service" options provided at logon and supplying the answers to their password reset questions.

GINA extension

Credential Provider extensions

The sections in this topic describe how to deploy the EmpowerID GINA and Credential Provider extensions in your environment and is divided into the following activities:

- Installing, configuring and testing the EmpowerID GINA extension for Windows XP
- Installing, configuring and testing the EmpowerID Credential Provider extension for VISTA and Windows 7
- Automating deployment across your network
- Making Group policy settings

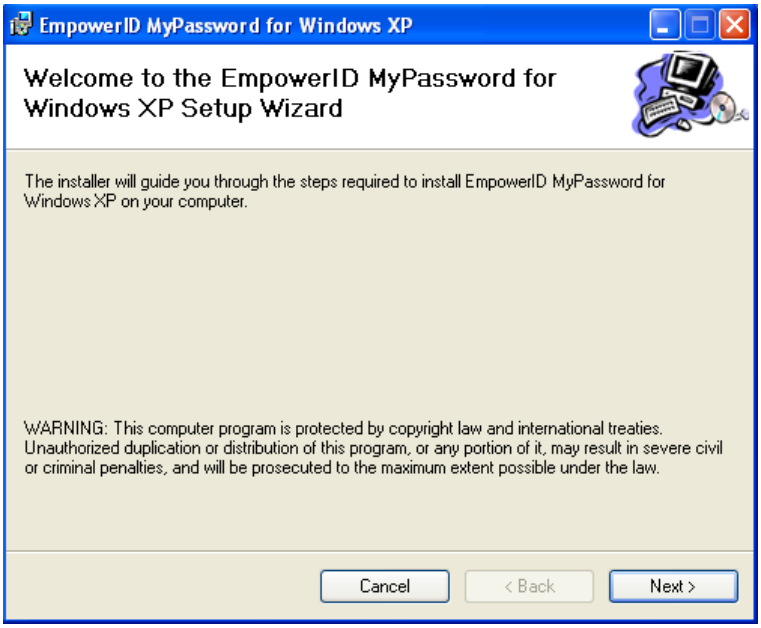
Installing the EmpowerID Password Extension adds the following Operating System-dependent registry values to the Microsoft Hive.

- **Windows XP:** EmpowerID GINA extension adds pwgina.dll to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon
- **Vista and Windows 7:** EmpowerID Credential Provider extension adds the subkey D8D0B103-A64C-43d7-9E8D-62166802D62E with a data value of ResetMyPasswordCP to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers.

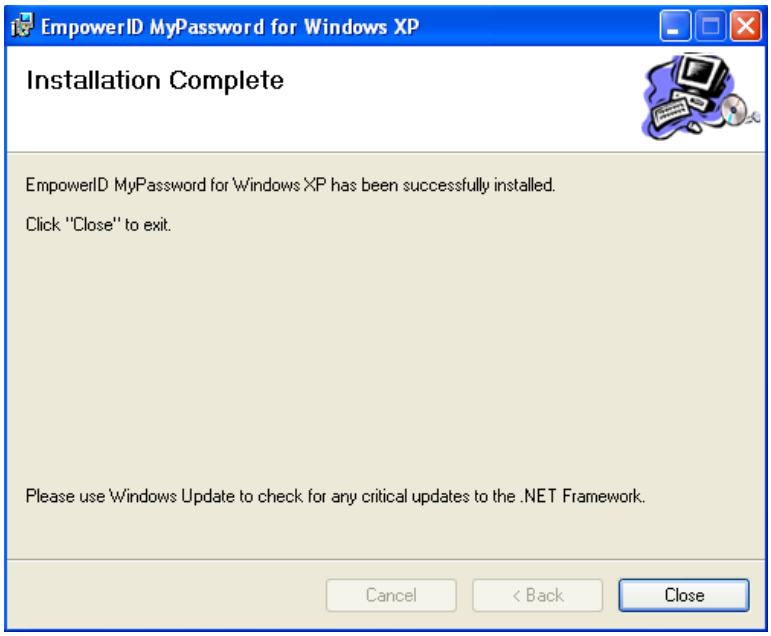
Note: Installing the EmpowerID Password Extension utility on a computer where any other third-party extension is installed will disable that third-party extension. When you uninstall the EmpowerID Password Extension utility, the previous extension will be re-enabled.

To install, configure, and test the EmpowerID GINA extension for Windows XP

1. Uninstall any prior versions of the GINA extension
2. Double-click on the EmpowerIDMyPasswordForWindowsXP.msi.
2. In the Setup Wizard that opens, click **Next**.



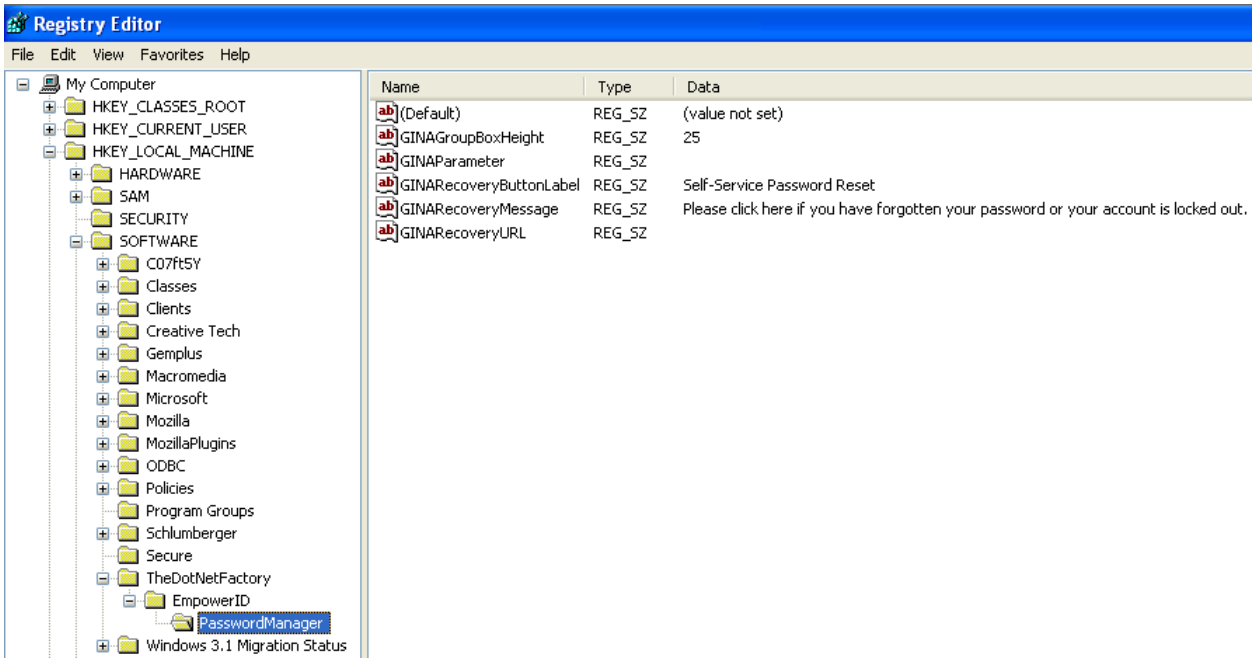
3. When the wizard completes the installation, click **Close**.



4. Open Registry Editor and navigate to *HKEY_LOCAL_MACHINE\SOFTWARE\TheDotNetFactory\PasswordManager* and set the GINARecoveryURL value and customize any of the other optional settings (for details on the keys and what they do see the GINA keys section below)

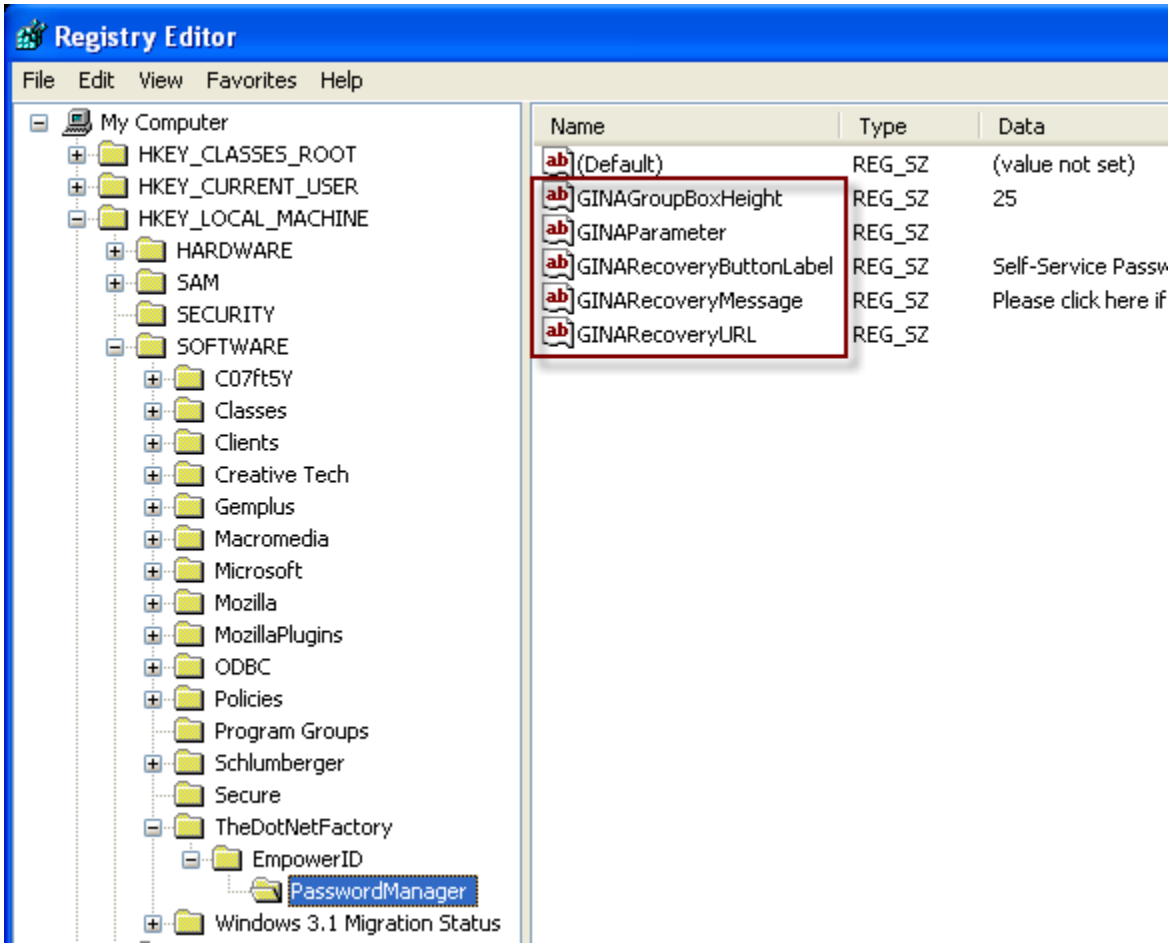
5. Reboot the machine. The extension will show on the Windows logon screen after a reboot.

GINA Keys



These keys above control the details of what is displayed in the Windows logon extension when users logon or lock their computers.

The details pane contains customizable entries: **GINAGroupBoxHeight, GINARecoveryButtonLabel, GINARecoveryMessage,** and **GINARecoveryURL**.



• **GINAGroupBoxHeight:** This value controls the height of the box that appears at the bottom of the Windows logon screen. This allows you to control the box size to accommodate longer RecoveryMessage values if necessary. The default value is 25. Changing the value of this entry is optional.

• **GINARecoveryButtonLabel:** This is the text that displays to the user on the Recovery Button EmpowerID places on the Windows Logon screen. The default value is “Self-Service Password Reset”. Changing the value of this entry is optional.

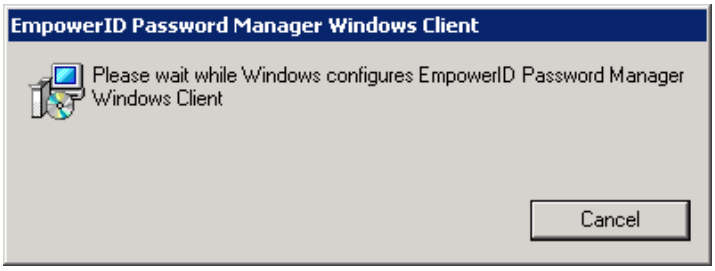
• **GINARecoveryMessage:** This is the text description that displays to the user in the pane that hosts the Recovery Button. The default value is, “Please click here if you have forgotten your password or your account is locked out.” Changing the value of this entry is optional.

• **GINARecoveryURL:** This is the URL that opens the Password Recovery Center in your environment. Right-click on this entry and modify the value to equal the URL of Password Recovery Center in your environment. The URL should read: *http://%yourserver%/adselfservice/recoverycenter/question.aspx*

NOTE: You must configure this setting manually after installation.

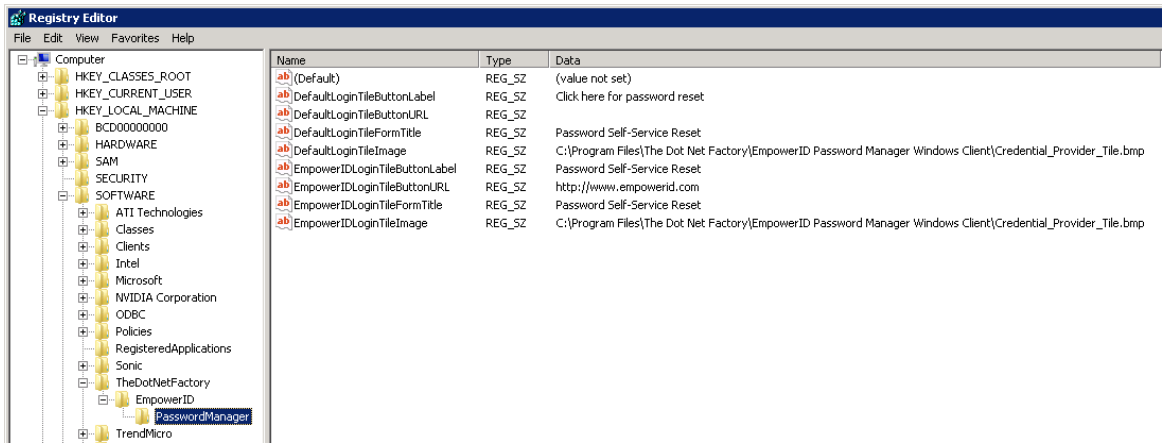
To install the EmpowerID Credential Provider extension for Vista or Windows 7

1. Double-click on the EmpowerIDCredentialProvider32.msi (x86) or EmpowerIDCredentialProvider64.msi (x64) depending the machine.
2. A message box appears stating that Windows is configuring EmpowerID MyPassword. You can click Cancel to abort the installation.

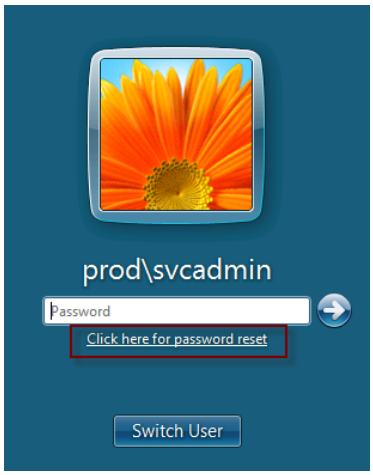


3. Open Registry Editor and navigate to *HKEY_LOCAL_MACHINE\SOFTWARE\TheDotNetFactory\EmpowerID\PasswordManager* and set the DefaultLoginTileButtonURL value and the EmpowerIDLoginTileButtonURL. Here you can also customize any of the other optional settings (for details on the keys and what they do see the Credential Provider keys section below)

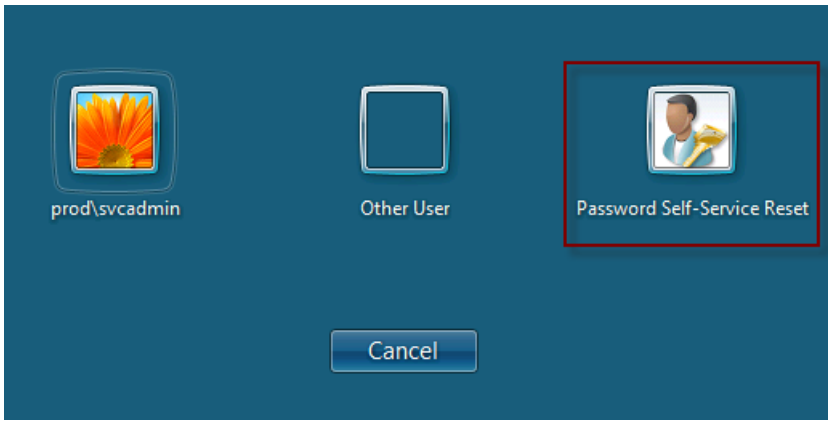
Credential Provider Keys



These key controls what displays to users when they need to logon, have locked their machines, or go to switch user mode

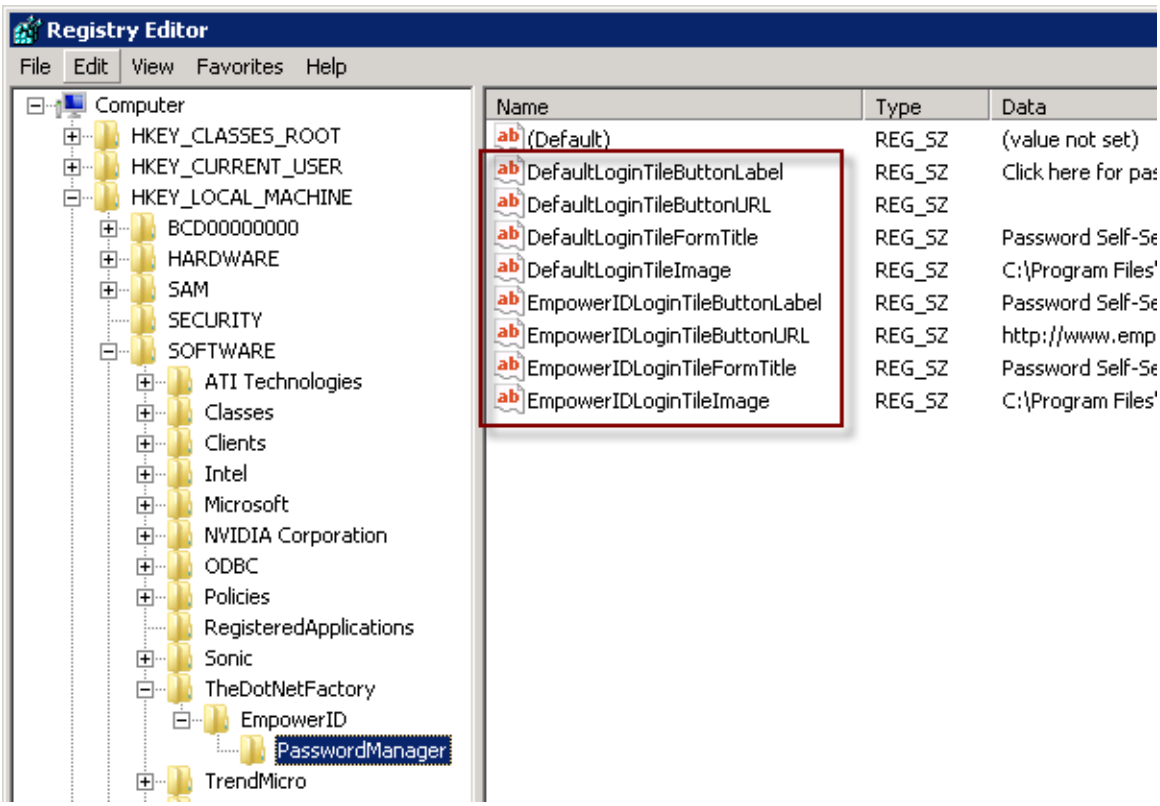


DefaultLoginTile



EmpowerIDLoginTile

The details pane contains customizable entries: **DefaultLoginTileButtonLabel**, **DefaultLoginTileButtonURL**, **DefaultLoginTileFormTitle, DefaultLoginTileImage, EmpowerIDLoginTileButtonLabel, EmpowerIDLoginTileButtonURL, EmpowerIDLoginTileFormTitle,** and **EmpowerIDLoginTileImage**.



• **DefaultLoginTileButtonLabel:** This is the text that displays to the user on the Default Login link that EmpowerID places below the Windows Logon password field. The default value is “Click here for password reset”. Changing the value of this entry is optional.

• **DefaultLoginTileButtonURL:** This is the URL that opens the Password Recovery Center in your environment. Right-click on this entry and modify the value to equal the URL of Password Recovery Center in your environment. The URL should read: *http://%yourserver%/adselfservice/recoverycenter/question.aspx*

NOTE: You must configure this setting manually after installation.

• **DefaultLoginTileFormTitle:** This is the title on the limited browser that opens to the DefaultLoginTileButtonURL when the user clicks the DefaultLoginTileButtonLabel. The default value is “Password Self-Service Reset”. Changing the value of this entry is optional.

• **DefaultLoginTileImage:** This is the image that appears for the Credential Provider. The default value is “C:\Program Files\The Dot Net Factory\EmpowerID Password Manager Windows Client\Credential_Provider_Tile.bmp”.

• **EmpowerIDLoginTileButtonLabel:** This is the text that displays below the EmpowerIDLoginTileImage that displays in switch user selection. The default value is “Password Self-Service Reset”. Changing the value of this entry is optional.

• **EmpowerIDLoginTileButtonURL:** This is the URL that opens the Password Recovery Center in your environment. Right-click on this entry and modify the value

to equal the URL of Password Recovery Center in your environment. The URL should read: *http://%yourserver%/adselfservice/recoverycenter/question.aspx*

NOTE: You must configure this setting manually after installation.

• **EmpowerIDLoginTileFormTitle:** This is the title on the limited browser that opens to the EmpowerIDLoginTileButtonURL when the user clicks the EmpowerIDLoginTile. The default value is “Password Self-Service Reset”. Changing the value of this entry is optional.

• **EmpowerIDLoginTileImage:** This is the image that appears for the Credential Provider tile that EmpowerID adds to the switch user selection. The default value is “C:\Program Files\The Dot Net Factory\EmpowerID Password Manager Windows Client\Credential_Provider_Tile.bmp”.

CONFIGURING DEFAULT SETTINGS USING GROUP POLICY OBJECTS AND .ADM FILES

The GINA extension and Credential Provider default settings may be configured to match your desired settings prior to installation. Your PCs will then automatically receive the correct settings via Group Policy administrative templates (for information on GPO deployment see the DEPLOYING THE WINDOWS DESKTOP CLIENT USING GPO section of this document).

1. Copy the administrative template file(s) (GINAEmpowerIDPasswordManager administrative template or CredentialProviderEmpowerIDPasswordManager administrative template file) to the inf directory in the SystemRoot (example: c:\Windows\inf) folder on your Windows Domain Controller.

2. You will need to determine what the best approach is for your environment and whether you want to use an existing GPO or create a new GPO. Open the desired GPO in the Group Policy Management Editor.

3. Expand the Computer Configuration node and the Policies node. On the Administrative Templates folder, right click and select Add/Remove Templates from the menu.

4. Click the Add button on the Add/Remove Templates dialog

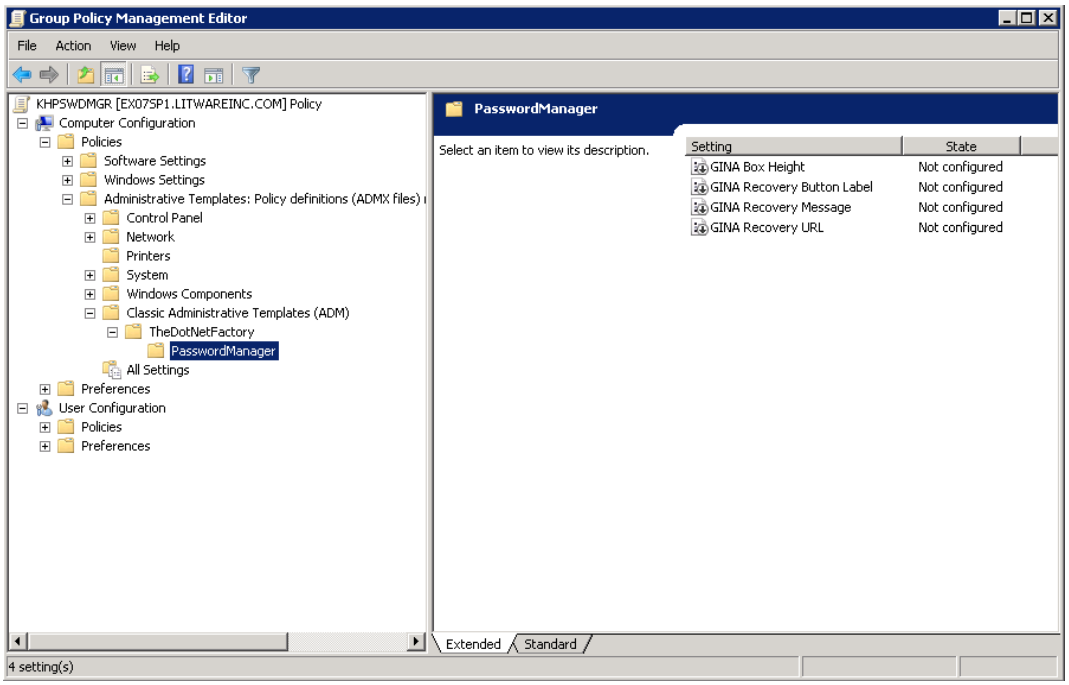
5. On the Policy Templates file selection, select the desired .adm file and click Open

6. Click Close on the Add/Remove Templates dialog

7. Expand the Administrative Templates folder and locate the folder called TheDotNetFactory (depending on the OS you may also need to expand the Classic Administrative Templates folder as well).

8. Expand the TheDotNetFactory folder, and select the PasswordManager folder

9. Each of the settings listed here can be configured by enabling them and entering the desired values (see the details on the keys above for more information)



NOTE: These settings are applied after the Group Policy is applied

DEPLOYING THE WINDOWS DESKTOP CLIENT USING GPO:

Group Policy deployment can be used to install the Password Manager for Windows client. If you are deploying through GPO, the best practice recommendation would be to create a separate GPO for each msi type based on OS and processor type. WMI filters can be used to do this and documentation on WMI filters can be found on http://technet.microsoft.com. It is also recommended that you test your GPO before doing a full deployment.

1. Copy the .msi file to a network share that is accessible to all workstations where you wish to install the Windows Desktop Client. Be sure this network share is configured to ensure that Everyone has only Read access to the folder and that Domain Admins have Full Control, Change, and Read access to the folder.

2. Create a new GPO object for the deployment or select an existing GPO object to use.
   Note: This GPO object must be linked to all of the computers, sites, domains, or organizational units where you want to use the GINA Extension or Credential Provider.

3. Open the desired GPO in the Group Policy Management Editor.

4. Expand the Computer Configuration folder, expand the Policies folder, expand the Software Settings folder, right-click the folder Software installation, and select New | Package.

5. On the Open dialog search for and select the .msi (be sure to use the network path and not the local path)

6. Click Open

7. Select the deployment method and click OK

8. Verify and configure the properties of the installation if needed.

   Note: The GINA Extension or Credential Provider will be installed on each computer linked to the GPO object according to your organization's group policy. The installation of the GINA Extension on each end-user computer starts when the computer is restarted. All computers have to be restarted after you have installed the ADPassword GINA extension. If a computer does not restart automatically, you should restart it manually. You will need to do this for computers running Microsoft Windows XP. The Dot Net Factory GINA Extension acts as an enhancement to the system file msgina.dll. It is absolutely prohibited to remove the msgina.dll. Otherwise, the system can become unstable and may not load Windows.