**Oracle® Enterprise Single Sign-on
Password Reset**

Server Installation and Setup Guide

Release 10.1.4.1.0

**E12630-01**

November 2008

ESSO-PR Server Installation and Setup Guide, Release 10.1.4.1.0

E12630-01

# Table of Contents

# About ESSO-PR

Oracle Enterprise Single Sign-on Password Reset (ESSO-PR) enables workstation users to reset their own Windows domain passwords without the intervention of administrative or help-desk personnel. It provides end users with an alternative means of authenticating themselves by taking a quiz comprising a series of passphrase questions.

Each question is weighted with point values. As the end user answers the quiz questions, ESSO-PR keeps a running score. Points are added to the score for each correct response and points are deducted for each incorrect response. When the end user accumulates sufficient points to meet a preset "confidence level," ESSO-PR permits the end user to select a new password. If the end user's score does not achieve the required confidence level after all questions have been presented, or if it falls below a preset negative value, the quiz ends and the end user is not permitted to reset the password.

The reset service is available to each end user after completing a one-time Enrollment Interview to record passphrase answers. The ESSO-PR Management Console provides easy configuration of the Enrollment Interview and Reset Quiz, including question text, point values, and confidence-level limits. The console also affords convenient reports of enrollment and reset activity and status.

# Abbreviations and Terminology

Following is a list of commonly-used abbreviations and terminology.

| Abbreviation or Terminology | Full Name |
| --- | --- |
| Administrative Console | ESSO-LM Administrative Console |
| Agent | ESSO-LM Logon Manager Agent |
| FTU | First Time Use Wizard |
| ESSO-AM | Oracle Enterprise Single Sign-on Authentication Manager |
| ESSO-PG | Oracle Enterprise Single Sign-on Provisioning Gateway |
| ESSO-KM | Oracle Enterprise Single Sign-on Kiosk Manager |
| ESSO-LM | Oracle Enterprise Single Sign-on |
| ESSO-PR | Oracle Enterprise Single Sign-on Password Reset |

# Before You Begin

## Purpose

This document provides step-by-step installation and configuration instructions for the ESSO-PR server-side software component with enhanced security settings.

## Intended Audience

This document is intended for system and network administrators who are responsible for deploying and securing ESSO-PR on their networks. It is assumed that the reader has a solid grasp of technologies surrounding the configuration of Windows®Server 2003, Windows XP Professional, Windows 2000 Professional, and general technologies regarding the same.

## Best Practices

The following best practices should be observed:

Review the hardware and software requirements in the ESSO-PR Release Notes thoroughly and verify that your environment meets all requirements.

- Avoid installing the ESSO-PR server-side components on a domain controller. Use a member server.
- Ensure that DNS is configured and working properly, including correct enumeration of forward and reverse lookup zones.
- Verify that your servers and workstations have the latest service packs and Windows updates installed on them.

For the creation of service accounts, consider using long, complex passwords and set the accounts to lock out after a specific number of bad password attempts. These actions will prevent a hacker from successfully launching a dictionary attack on service accounts.

| | |
|---|---|
| **Note:** | Generally speaking, Microsoft recommends that IIS servers be installed on member servers. For a full discussion of this matter, visit Microsoft.com. |

# Server Installation Overview

To install the ESSO-PR server components:

1. Log on to the IIS Member Server where you have local administrative rights at the domain level. *Do not* log on at the local machine level.

   Notice that, by default, members of the Domain Administrators group in AD are automatically added to the local administrator's group on the member server. If you are not a member of the Domain Administrators group, add yourself to the local administrators group on the member server. This example designates an "Administrator" account as a member of the Schema Admins group to simplify the process.

2. Locate the .exe or .msi installation file for the ESSO-PR server-side component.

   Whether you receive the ESSO-PR 7.0 CD or download the components, two files exist to install the ESSO-PR server-side components. One is an executable, the other is an MSI, with the .exe containing the .NET framework components.

3. Follow the installation wizard, selecting the defaults and performing the complete installation.

**Note:** The .exe file includes the .NET 2.0 framework. If you are certain that you are running the most recent version of .NET, install from the .msi file.

## Using the Installation Wizard to Install the Server

1. Double-click the **Setup** icon (Oracle_sspr_server_xxx.exe or Oracle_sspr_server_xxx.msi) to launch the Install Wizard:



2. On the License Agreement panel, read the license agreement carefully. Select **I accept the terms in the license agreement** and click **Next >** to continue.
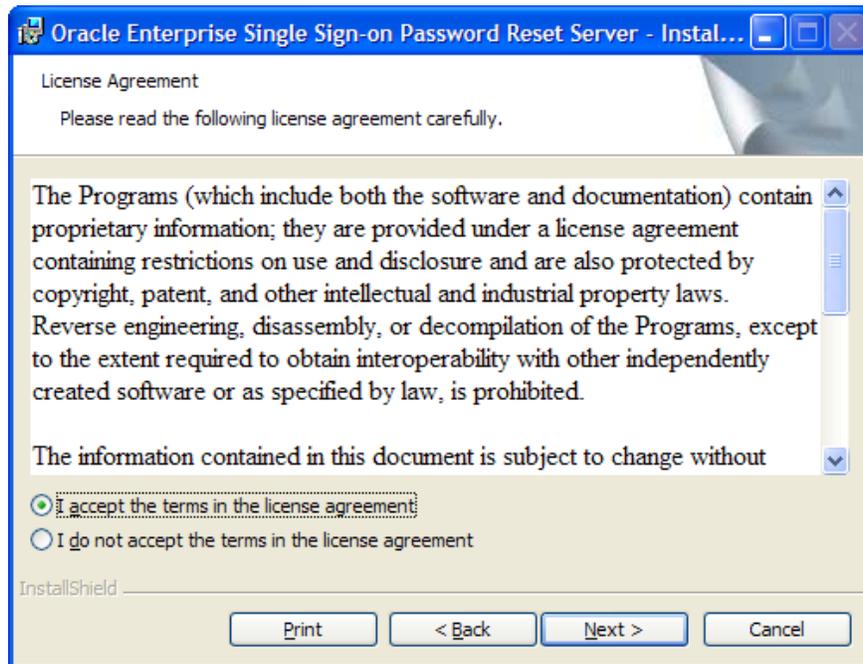
3. Select **Complete** or **Custom** setup type and click **Next >**.(Custom setup allows you to specify an alternate installation directory.) Then click **Next >**.
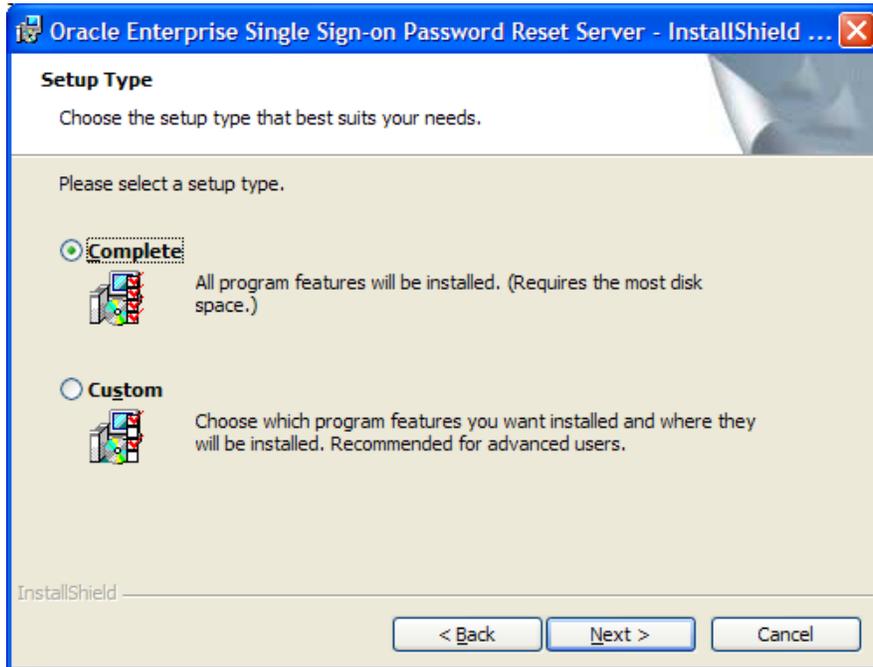


4. Click **Install**.
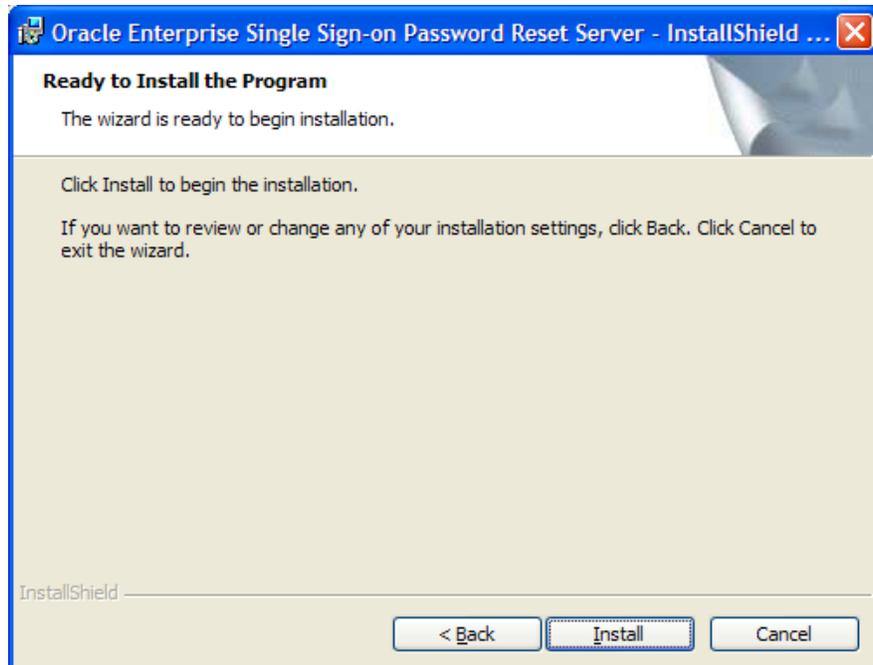
The bar indicates the progress of the installation.



5.   When the installation is complete, click **Finish**.
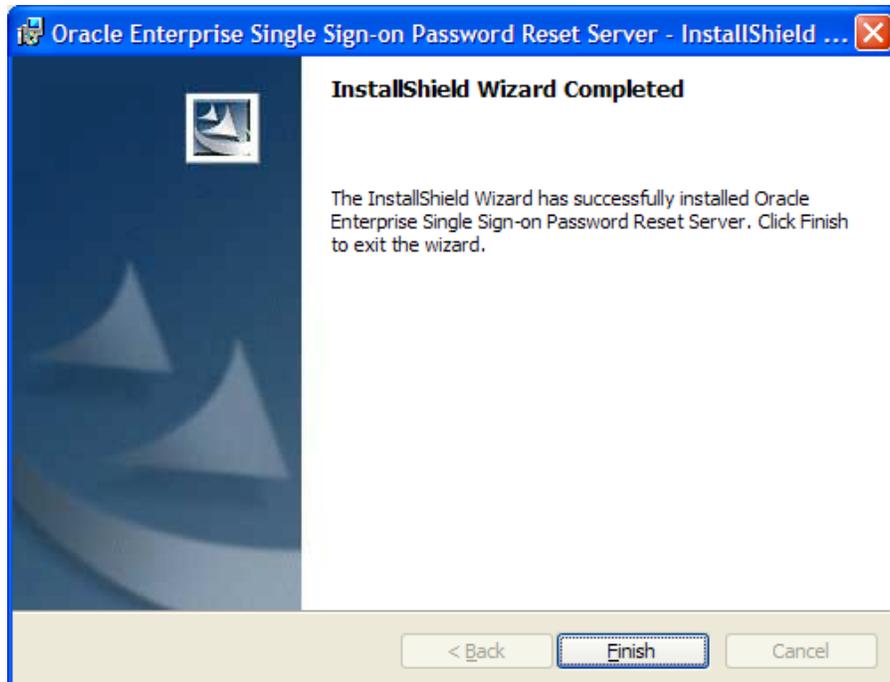
# Creating Service Accounts

Create the following two accounts on your domain controller. These accounts should be ordinary users in the domain users group (default):

- SSPRWEB: This account will be responsible for ESSO-PR IIS functions and will make changes, additions, and so forth, to the organizational unit (OU) that you will create later.
- SSPRRESET: This account will run the actual reset service on the ESSO-PR member server with IIS. It will be responsible for resetting user passwords on the domain level.

| | |
|---|---|
| **Notes:** | Make these accounts members of the local admins group on the local IIS workstation to avoid problems. |
| | These accounts will be the service accounts that ESSO-PR uses to manage the container where user questions and enrollment information will be housed and to handle the actual password reset process. Because these are service accounts, you should use highly complex passwords and prudent practices in terms of user lockout after a certain number of bad attempts. Although this might result in some help desk calls from users who cannot reset their passwords, it will also alert you that someone has been trying to attack these service accounts. For information as to best practices for service accounts and security log monitoring, visit Microsoft's knowledge base. |

# Assigning the SSPRRESET and SSPRWEB Accounts

When a user needs to reset his password, he must verify his identity to the SSPRWEB account first. After the SSPRWEB account confirms the user's identity, it communicates permission to the SSPRRESET account to allow the user to change his password. To assign the authentication and password reset roles, designate properties to SSPRRESET first, and then to SSPRWEB.

## Setting Up the SSPRRESET Account

1.  Run: **Control Panel** > **Administrative Tools** > **Services**.
2.  From the list in the right-hand pane, right-click **Self Service Password Reset**, and select **Properties**.
3.  In the Self Service Password Reset Properties dialog box, select the **Log On** tab.
4.  Select **This account** and enter the account name: `Domain\SSPRRESET`. Then enter and confirm (re-enter) the password for the account.
5.  A dialog box displays to advise you that changes will apply after the service is restarted.
6.  Restart the service as indicated. The SSPRRESET account setup is complete
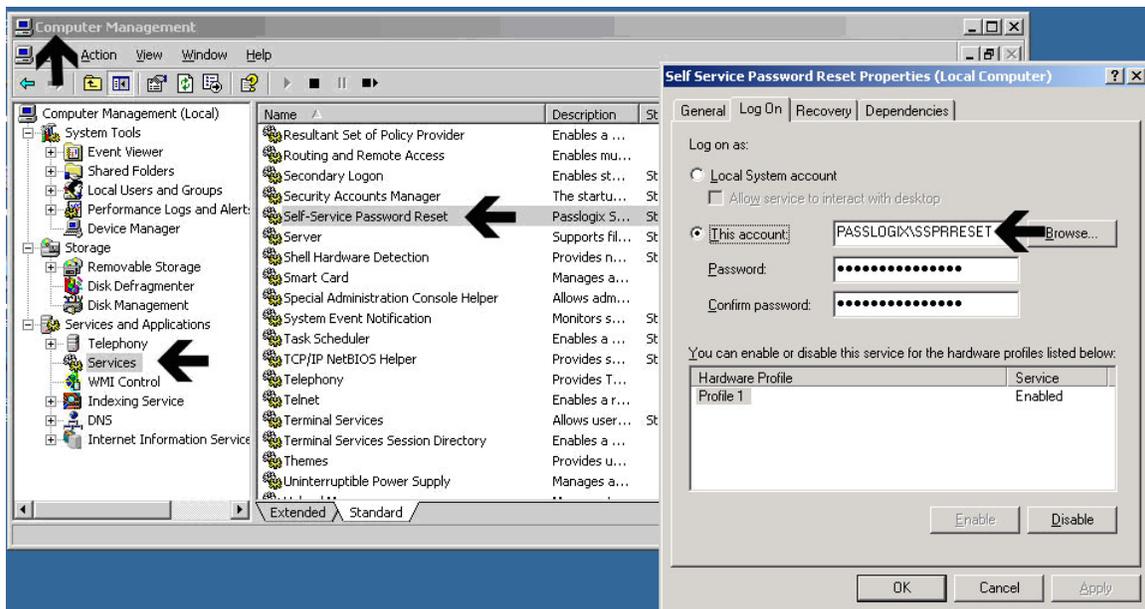


> **Notes:** The SSPRRESET account runs the ESSO-PR password reset service on the IIS server where the server-side components reside.
>
> The SSPRWEB account runs the ESSO-PR virtual website on the IIS server where the server-side components reside.

## Setting Up the SSPRWEB Account

1.  Run: **Control Panel** > **Administrative Tools** > **Internet Information Services**.
2.  Under IIS, locate the vGOSelfServiceReset virtual directory, right-click it, and select **Properties**.
3.  Select the **Directory Security** tab.
4.  In the Authentication and access control section, click **Edit**.
5.  In the Authentication Methods dialog box, under Use the following Windows user account for anonymous access:, enter the name (in Domain\Username format) and password of the SSPRWEB account.
6.  In the Confirm Password window, retype the password and click **OK**.
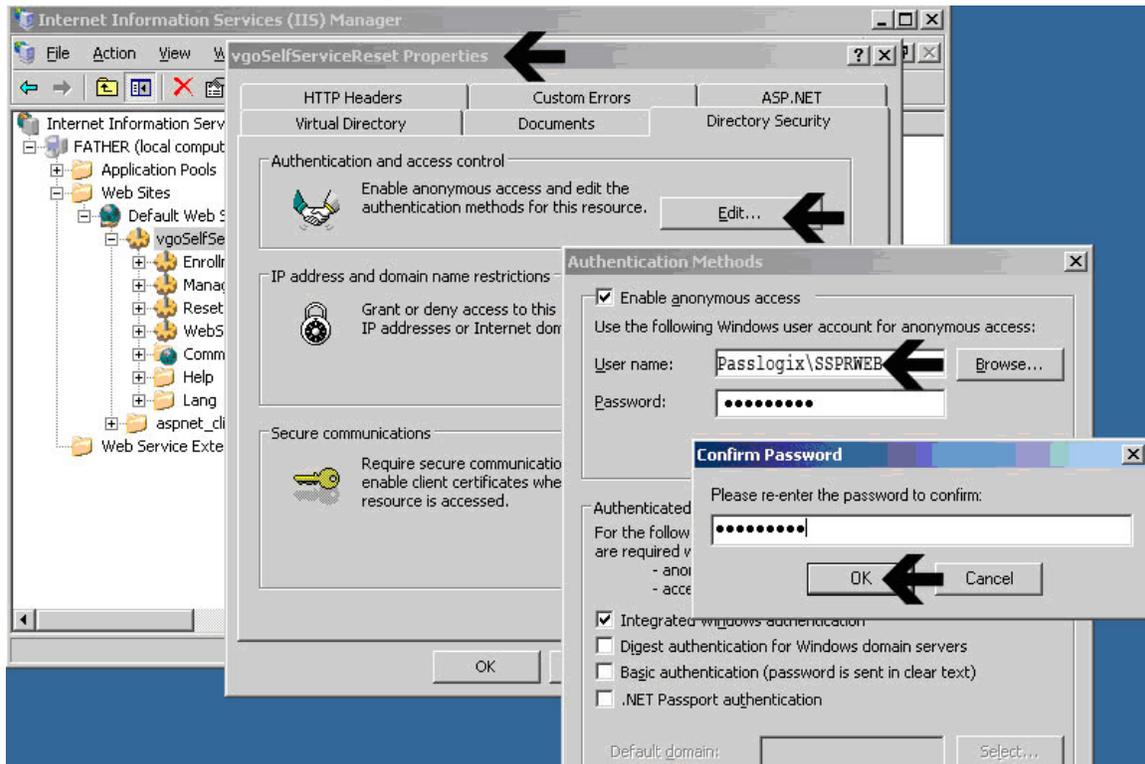


7.  Restart IIS by clicking **Start** > **Run** and entering `iisreset`.

**Note:** If you still have the IIS console open and attempt to browse an item therein, you will receive an error message stating that you must reconnect. If you are prompted, answer yes. This happens because the IIS service was restarted.

The virtual sub-directories under the vgoSelfServiceReset virtual directory should be configured as follows:

| Configuration of v-GO SSPR Virtual Sub-Directories | |
|---|---|
| **Virtual Directory** | EnrollmentClient |
| **Enable Anonymous Access** | NO |
| **Integrated Windows Authentication** | YES |
| **Authentication and Access Control Account** | SSPRWEB |

| | |
|---|---|
| **Virtual Directory** | ManagementClient |
| **Enable Anonymous Access** | NO |
| **Integrated Windows Authentication** | YES |
| **Authentication and Access Control Account** | SSPRWEB |
| | |

| | |
|---|---|
| **Virtual Directory** | ResetClient |
| **Enable Anonymous Access** | YES |
| **Integrated Windows Authentication** | YES |
| **Authentication and Access Control Account** | SSPRWEB |

| | |
|---|---|
| **Virtual Directory** | WebServices |
| **Enable Anonymous Access** | YES |
| **Integrated Windows Authentication** | YES |
| **Authentication and Access Control Account** | SSPRWEB |

**Note:** The only two virtual directories that do not permit anonymous access are EnrollmentClient and ManagementClient.

# Verifying Proper Assignments of SSPRWEB and SSPRRESET Accounts

1. To access the ESSO-PR web-based console, open IIS Manager and navigate down to Default Website, then to vgoSelfServiceReset > ManagementClient. In the right-hand pane, scroll down to the webservice.aspx page and browse it.

**Note:** By default, Windows Server 2003 installation has all Web service extensions disabled. Be sure to activate the required web service extension.
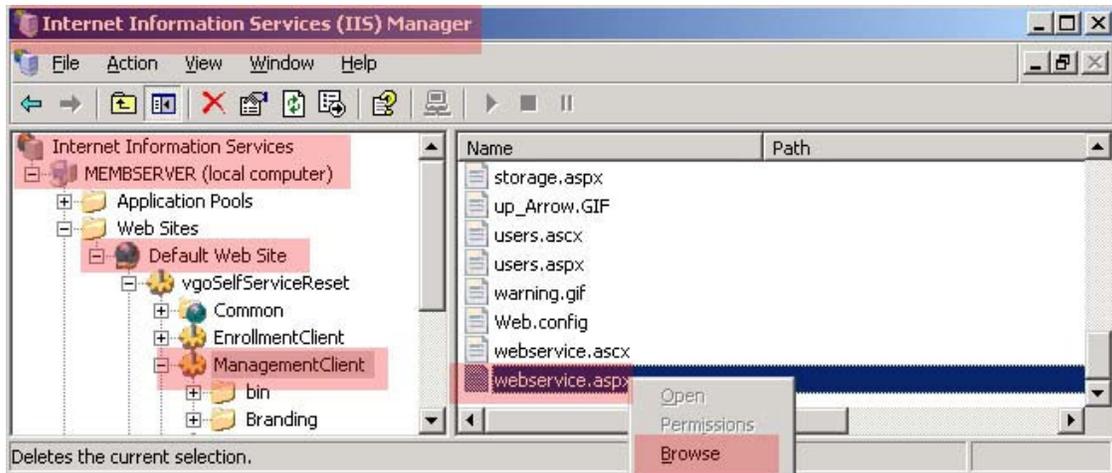


**Note:** When Internet Explorer opens, add this page to your Favorites list for easy access.

2. In the ESSO-PR Management Console web page, locate the System > Web Service Account section. Verify that the SSPRWEB account has been designated as the Current Account.

3.   In the ESSO-PR Management Console Web page, locate the System > Reset Service section. Verify that the SSPRRESET account is listed as the service account for the Reset Service.

| | |
|---|---|
| **Notes :** | If the SSPRRESET account is not listed as the Reset Service account under the Reset Service section of the ESSO-PR Management Console Web page, verify that you are logged in as a local administrator. If it still does not appear, you can manually assign it by specifying the account with the following naming convention: Domainname\SSPRRESET. |
| | If you receive an error message indicating that the account does not have logon rights to a service: |
| | • Navigate to the IIS member server where you installed the ESSO-PR server-side components. |
| | • Check the local administrator's group. |
| | • Verify that the SSPRRESET and the SSPRWEB accounts are both members of the local administrator's group. |
| | • Click on Reset Service in the left pane and verify that the SSPRRESET account is listed as the Reset Service account. |



Notice that the SSPRRESET account has been designated as the service account for the Reset Service.

# Granting Registry Access to the SSPRWEB Account

In order for ESSO-PR to function properly, the SSPRWEB service account needs full permissions to the following registry key on the member server containing the ESSO-PR server side components:

`HKLM\SOFTWARE\PASSLOGIX\SSPR`

**Note:** After applying permissions to this key, drill down several levels to verify that permissions have been propagated throughout.

To avoid possible permissions problems during the configuration of the ESSO-PR server-side components, Passlogix recommends that you make both the SSPRWEB and SSPRRESET accounts members of the local administrator's group on the IIS Member Server where you are installing the ESSO-PR server-side components.

After you have finished the installation and configuration of the `v-GO SSPR` server-side components, you can remove these accounts from the local administrator's group on the member server.

# Enabling Storage in Active Directory

ESSO-PR stores user questions, answers, configuration, and enrollment information within an organizational unit in Active Directory. Select any name for the OU that will identify the unit easily.

Before you proceed, create this organizational unit at the root of your domain. If the OU does not exist when you try to enable storage, you might receive an error message indicating that no such object exists on the server.

**Note:** Before you proceed, create this organizational unit at the root of your domain. If the OU does not exist when you try to enable storage, you might receive an error message indicating that no such object exists on the server.

The Connect As account performs the schema extension. As such, this account must be a member of the Schema Administrator's group and have permissions to create objects within the ESSO-PR OU.



To enable storage in Active Directory:

1.  In the System > Storage screen, select the storage type as AD in the Storage Type drop-down menu.
2.  Enter the fully qualified domain name or the IP address of the domain controller that you want to use.
3.  Enter 389 for the port number. This is the LDAP port used by Active Directory.
4.  Click the **Add** button.
5.  Populate the fields according to the information in the table below.
6.  Click **Submit**.

After a slight delay, the confirmation message, Successfully Saved Changes, is displayed.

| Storage Configuration Screen Label | Explanation |
|---|---|
| Storage Type | The type of directory in which ESSO-PR is installed. This example uses Microsoft Active Directory (AD). |
| Server Name/IP Address, Port Number | The fully qualified domain name or the IP address of the domain controller. The port number for AD is 389. The port number for SSL is 636. |
| Servers | The list of domain controllers to use. This example uses one server: SSPRDC.PASSLOGIX.COM. It is possible to have multiple servers. |
| Server Timeout | The number of seconds in an attempt to establish a connection to the repository before a timeout. |
| Storage Location (DN) OU=SSPR DC=PASSLOGIX DC=COM | The distinguished name (DN) of the ESSO-PR OU that you create within Active Directory. The DN typically includes: The name of the OU that you create The NetBIOS or short name of the domain The extension of the domain; for example, com or .gov. |
| Use SSL | Select to enable secure socket layer. |
| Initialize Storage for ESSO-PR | Make sure that this box is checked. If you do not select this option, you will not be able to enter information into either the Connect As or Password fields. This tells v-GO SSPR whether or not it should extend the schema and create the initial objects. If this box is not checked, v-GO SSPR will only update the storage settings. |
| Connect As | The name of the account that will actually extend the AD schema and add the necessary objects to the ESSO-PR OU. This account should be a member of the Schema Admins group and have permissions to create objects in the ESSO-PR OU. Note: Enter the username in this syntax: Domain\Username |
| Password | The password for the account specified above. |

**Note:** To verify that the ESSO-PR OU is configured correctly, open a fresh instance of Active Directory Users and Computers on your targeted domain controller, using the Advanced view. You should see an OU named SSPR (or the name that you chose) and two subordinate OUs named SystemQuestions and Users. The existence of these two subordinate OUs indicates success.

You can now remove both the SSPRWEB and SSPRRESET accounts from the local administrator's group on the IIS member server where you installed the ESSO-PR server-side components.

# Granting Permissions to the SSPRWEB Account in AD

After creating the OU and subordinate containers within Active Directory, grant limited, specific permissions to the SSPRWEB account for the ESSO-PR OU you created in AD.

> **Note:** If you are familiar with granting advanced permissions to Active Directory objects, make sure that you grant the SSPRWEB account full control to both the ESSO-PR OU and its subordinate containers at the advanced security levels.
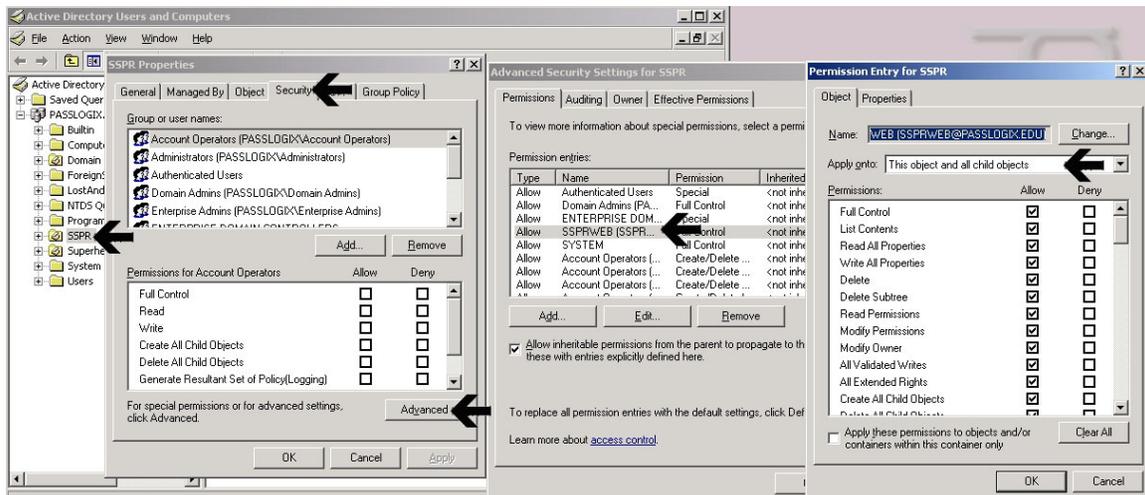
To assign advanced permissions to the SSPRWEB account of the ESSO-PR organizational unit:

1.  Make sure that you have enabled Advanced Features in the View menu under Active Directory Users and Computers.

2.  In the Active Directory Users and Computers window, right-click the ESSO-PR OU and select **Properties**.

3.  Select the **Security** tab.

4.  Click the **Advanced** button at the bottom of the tab to display the Advanced Security Settings for SSPR window.

5.  Select SSPRWEB from the Permission entries list and click **Add**.

6.  Enter the name of the SSPRWEB account. Click **OK**.

7.  On the Permissions Entry for SSPR page, mark the **Full Control** check box in the Allow column.

8.  In the Apply onto: drop-down menu, select **This object and all child objects**.

9.  Click **OK** and close all open windows.

10. Verify that the permissions have been set accordingly.

The SSPRWEB account in Active Directory will have the permissions shown in the following table.

| Organizational Unit | SSPRWEB Account Rights |
| --- | --- |
| SSPR | Full Control |
| SSPR/SystemQuestions | Full Control |
| SSPR/Users | Full Control |

# Delegating Permissions to the SSPRRESET Account

The goal of this procedure is to grant a limited set of rights to the password reset account (SSPRRESET). You will be able to reset user passwords and unlock accounts with this account, but nothing more.

Note that the SSPRRESET account is simply a member of your domain users group. As a fail safe built into AD, this account cannot be used to change the password of a user that has greater rights (such as, an administrator account).

You can assign this right at the organizational unit level or group level. Assigning this right at the user level should not be a general practice and is not recommended.

# Considerations When Planning Account Permissions

The assignment of password reset permissions mandates careful consideration and planning to ensure that the desired accounts, and only the desired accounts, are granted this permission. Some practices and caveats that might help you fine-tune your strategy as you set up these accounts include:

- Consider granting the password reset account granular permissions based on organizational units or specific groups. After applying permissions to either, test to make sure that you have the desired results.
- Do not run the Delegation of Control Wizard at the root of your domain: if you do, you will give the password reset account rights that extend beyond users to objects such as computers and printers.
- Because the password reset account is a member of the domain users group, its password reset permissions are applied to all the members of the domain users group, who are at the same level.

So, if you store all of your users in the default users container in AD and run the Delegation of Control Wizard at that level, it will not permit a domain user account to reset administrator account passwords. Active Directory does not permit users to have admin rights over administrators.

In this scenario, the password reset service account will not be granted permission to reset the password of your administrators. Your administrators will be able to enroll in ESSO-PR and go through the entire password reset dialog. However, when they attempt to reset their passwords, they will receive an error message because the password reset service account is not designed to have permissions to reset the password for users in a higher security group.

Carefully consider whether you want members of your domain administrators group to be able to have their passwords reset by an ordinary user account. While you can grant this level of control to the password reset account, you might decide it is wiser not to do so.

# Delegating Control at the OU Level

Consider an OU structure in Active Directory where users are divided in the following manner:

- OU = Users1
- OU = Users2
- OU = Users (the default user container created in AD)

Assigning users to organizational units makes it possible to manage the SSPRRESET service account permissions of many users in a simple and uniform manner.

In the following example, we will give the SSPRRESET account the authority over the Users2 OU to reset its members' passwords.

1. Go to **Start**>**Administrative Tools**> **Active Directory Users and Computers**.

2. Make sure Advanced Features is checked under the View menu.
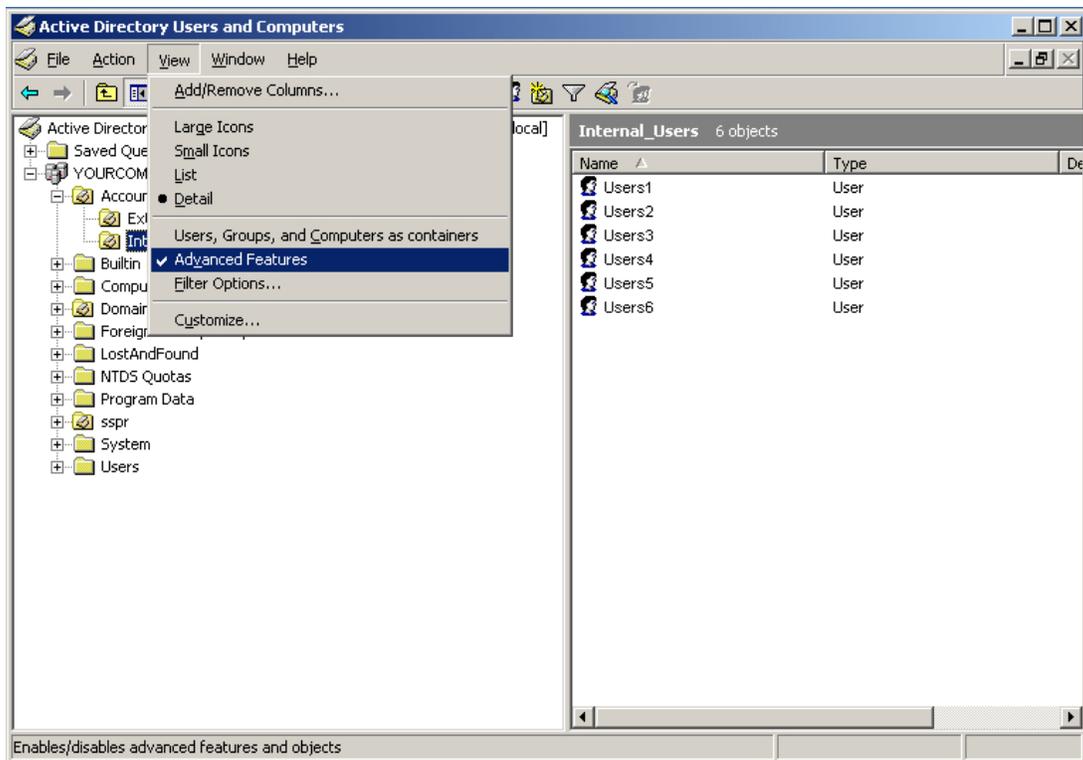


3. Navigate to **Active Directory Users and Computers** > **[YourDomain]** > **[YourOU]**. This example uses YOURCOMPANY.COM> Users2.

4.  Right-click on the OU that you want to control (this example uses the Users2 OU) and select **Properties**.
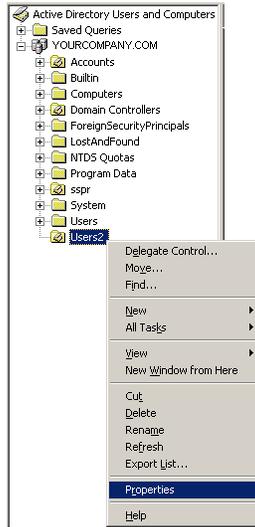


5.  In the Users2 Properties window, select the **Security** tab.
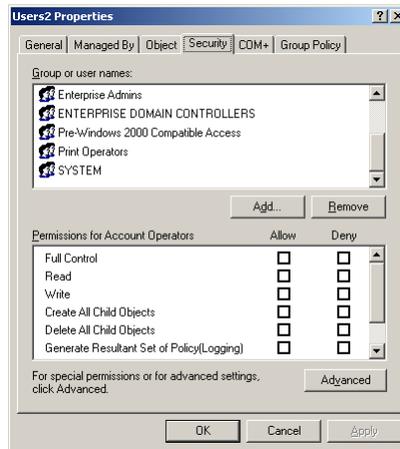
6. Click the **Advanced** button to access Advanced Security Settings.
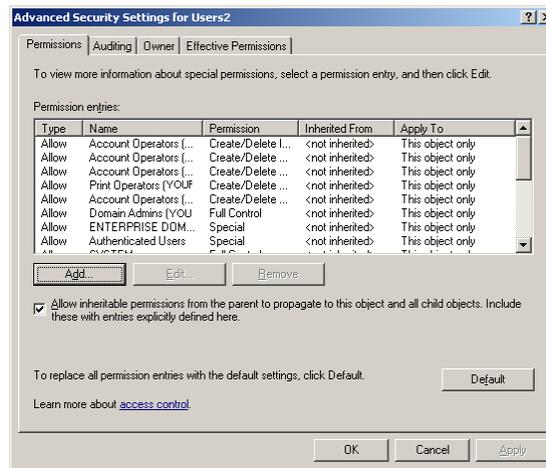


7. Click the **Add** button.
8. In the **Enter the object name to select** field, enter the name of your ssprreset account (or browse to the account using the **Advanced** > **Find** buttons. (You can use the **Check names** button to verify that you have entered the account name correctly.



9. Click **OK**.

10. In the Permission Entry screen's **Apply onto:** dropdown menu, select **User objects**.
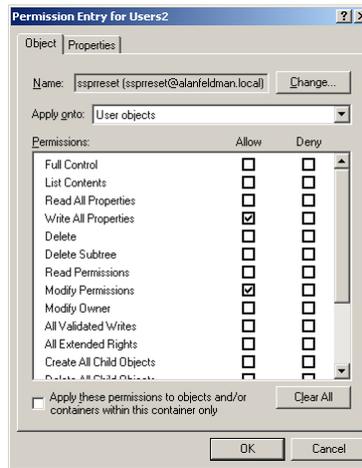


11. In the Permissions window, check **Write All Properties**, **Modify Permissions**, and **Reset password**.
12. Click **OK**.
13. Click OK two more times to close the windows. Your changes take effect immediately.

To verify that permissions were correctly assigned:

1. Right-click on the OU to which you just assigned the new permissions.
2. Select **Properties**.
3. Select the **Security** tab.

The SSPRRESET account should be listed as having Special Permissions. The Advanced tab will indicate that this account has password reset permissions on the OU.

# Making the SSPR Server a Trusted Intranet Site in AD

There are two virtual directories within ESSO-PR that do not permit anonymous access, but that are configured to use integrated Windows authentication (that is, if you are logged onto the domain with your Windows password, you should be able to get to that page).

Because the security for IIS running on Windows Server 2003 is more stringent than IIS on Windows Server 2000, the first time a user attempts to enroll, he might encounter a popup screen requesting username and password, as is customary with any Web site with such settings. You can avoid this behavior (which can lead to undesired help desk calls) by putting the fully qualified domain name of your ESSO-PR IIS server in your list of trusted sites for any user in your domain.

To designate your ESSO-PR server as a trusted intranet site:

- For an individual computer, add the ESSO-PR IIS server's default Web site to your list of trusted intranet sites.
- Within AD, add this site to your list of trusted intranet sites through a group policy.

To accomplish this, you need:

- Domain administrator rights
- The ability to create or modify group policies at the OU or domain level.

In the following example, the ESSO-PR server site is designated as a trusted intranet site for the entire domain. As such, it is a trusted site to all domain users.

| **Note:** | You might choose to create this policy for each OU that contains potential ESSO-PR users for more granular access control. Regardless of your approach, the end result is the inclusion of the ESSO-PR IIS server default Web site as a trusted site. |
|---|---|

To add the ESSO-PR IIS server to the list of trusted sites in your organization, you must first create a policy for Windows clients that do not have the Internet Explorer Enhanced Security Configuration installed (by default, Windows XP and Windows 2000 Professional do not have this feature installed):

1. Remove the Internet Explorer Enhanced Security Configuration settings (`Control Panel > Add/Remove Programs > Add/Remove Windows Components`).
2. De-select (remove) the Internet Explorer Enhanced Security Configuration.

| **Notes:** | You can install this enhanced security feature on your domain controller after having created this policy. Read the dialog box that pops up when you attempt to import the current zone within Group Policy Object Editor. |
|---|---|
| | To create this policy, open Active Directory Users and Computers, right-click on the organizational units that contain users who will be enrolling in ESSO-PR (in this example, at the root level of the domain) and click the **Group Policy** tab. |

3.   Create a policy named SSPR TRUSTED INTRANET SERVER.
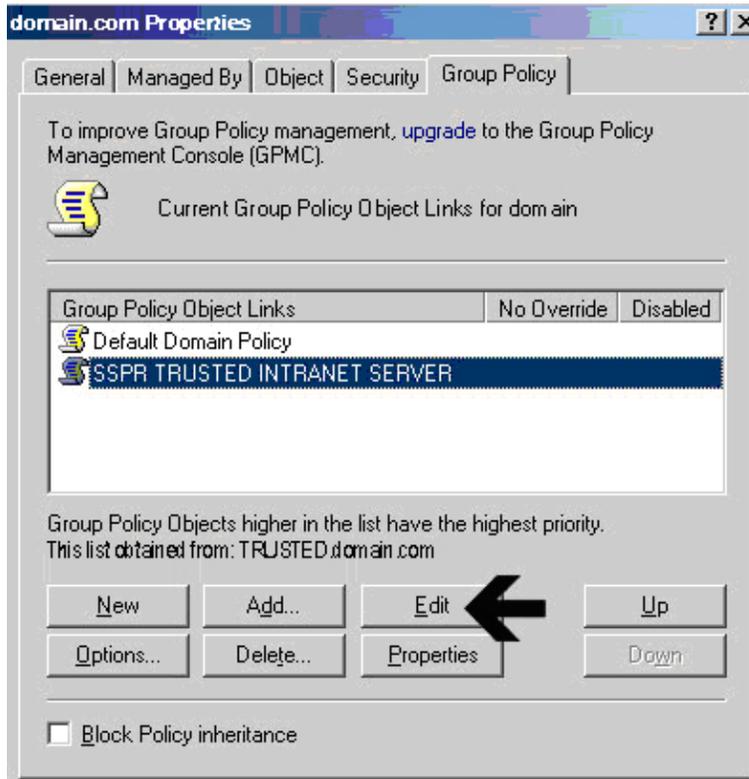


4.   Click **Edit**.
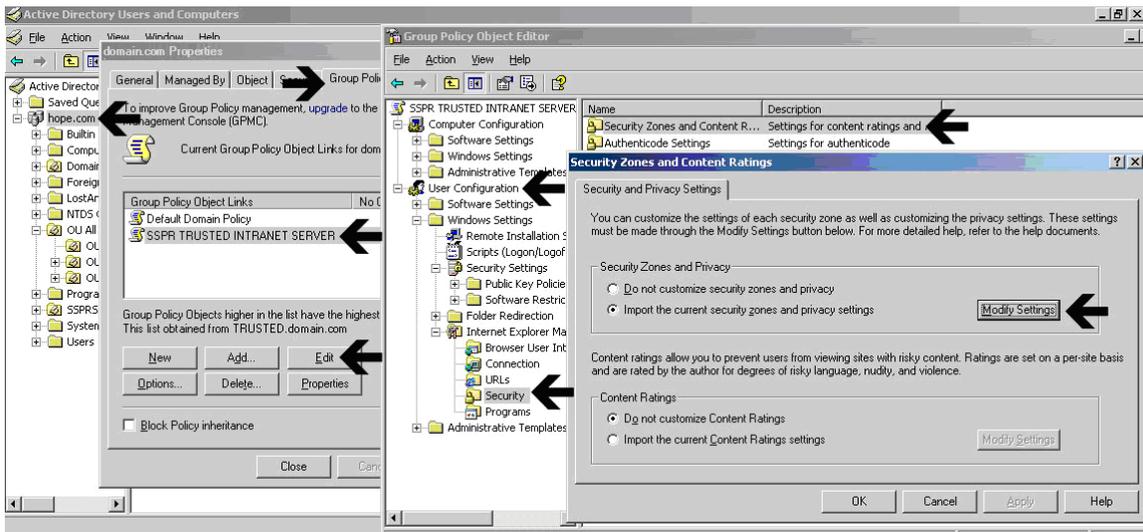


5.   Expand the user configuration portion of the policy in the Group Policy Object Editor.
6.   Navigate to Windows Settings > Internet Explorer Maintenance > Security > Security Zones and Content Ratings.
7.   Click **Modify Settings**.
8.   Read the displayed message and proceed.

> **Note:** This is the same Internet Properties dialog window that is found in Internet Explorer v. 6.0.
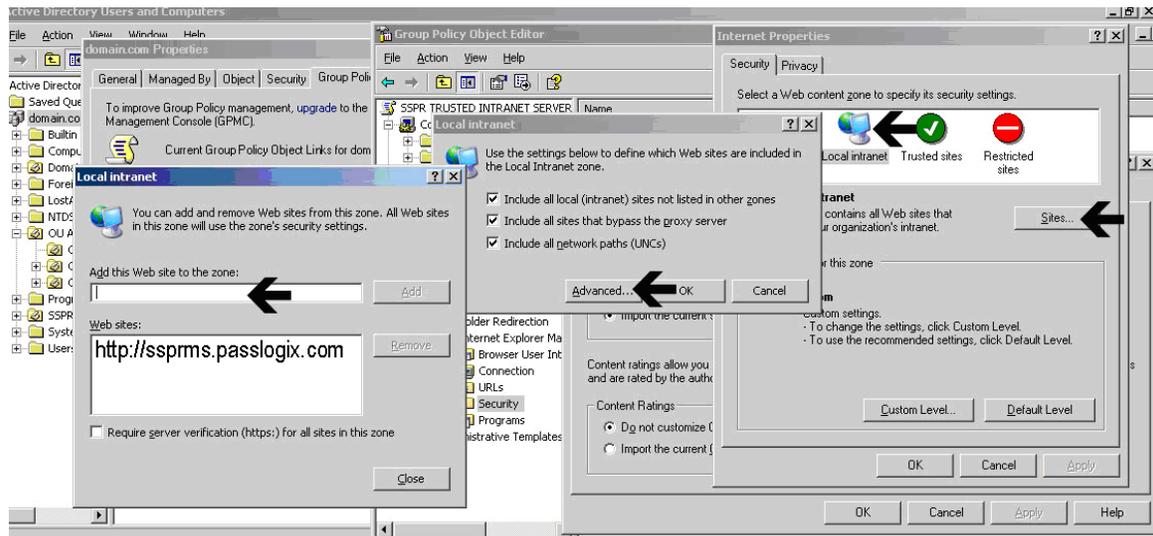


9. In the Internet Properties dialog box, click the **Local intranet zone** icon, then click the **Sites** button.

10. In the Local Intranet dialog box, click **Advanced**.

11. Enter the fully qualified domain name of your ESSO-PR IIS default website where indicated.

12. Click **Close**.

13. Click **OK** and **Apply** as needed to close out of the Group Policy Object Editor.

Depending on the replication speed within your network, it could take some time to replicate this policy throughout your Active Directory structure.

To confirm that this policy was applied at your desired level in AD:

1. Log on as a user who would be affected by this policy (having given AD group policy replication sufficient time).

2. In Internet Explorer, open **Tools** > **Internet Options** > **Security** > **Local Intranet** > **Sites** > **Advanced**.

Internet Explorer should list the site you added in its Trusted Sites window.

# Restricting Access to the Management Console

In order to avoid unauthorized users from accessing the Web-based ESSO-PR management console, perform the following steps:

1.  Open Windows Explorer and navigate to C:\Program Files\Passlogix\ESSO-PR\.
2.  Right-click the Management Client and select **Properties** from the shortcut menu.
3.  In the Properties dialog box, click the **Security** tab.
4.  Click **Advanced**.
5.  Click **Inheritable rights for Users** to clear the selection.
6.  In the dialog box that opens, click **Copy**.
7.  Click **OK**.
8.  In the Security tab, remove unauthorized users.
9.  Click **Add**.
10. Choose an **Advanced** search and select IIS_WPG (for Windows 2003).
11. Click **OK**.

> **Note:** All permissions except Full should be checked under the Allow column.

# Reference and Troubleshooting

## Installation and Configuration Notes

### Using AD or ADAM and IIS Web Services on Different Servers

If IIS and Active Directory or the ADAM instance are on different computers, then you must provide the IIS Web services with a user account that is in the same domain as (or a trusted domain of) AD or ADAM, and that is provided with read/write access to the directory.

### Installing ASP.NET 2.0 With Windows 2000 SP4: "Access is Denied" Error

When you install ASP.NET 2.0 on a computer running on a Windows 2000 Server domain controller with Service Pack 4 (SP4) installed, the built-in IWAM user account (used by IIS Web services with ASP) is not granted Impersonate User rights for ASP.NET 2.0. A request for any ASP resources, including ESSO-PR, can produce an "Access is denied" error message. Microsoft has acknowledged that this is an issue in SP4 (Knowledge Base article 824308) and provides the following workaround to assign "Impersonate a client after authentication" to the IWAM account manually:

1.  Go to Start > Programs > Administrative Tools, and click **Domain Controller Security Policy**.
2.  Click **Security Settings**.
3.  Click **Local Policies**, and then click **User Rights Assignment**.
4.  In the right pane, double-click Impersonate a client after authentication.
5.  In the Security Policy Setting window, click **Define these policy settings**.
6.  Click **Add**, and then click **Browse**.
7.  In the Select Users or Groups window, select the IWAM account name, click **Add**, and then click **OK**.
8.  Click **OK**, and then click **OK** again.
9.  To enforce an update of computer policy, type the following command:
    `secedit /refreshpolicy machine_policy /enforce`
10. At a command prompt, enter `iisreset`.

### Server Error in "/vGOSelfServiceReset/ManagementClient" Application

When you install .NET 2.0 on a computer running a newly installed operating system, the Network Service account must be granted read/write access or you will encounter a server error when you access the ESSO-PR 7.0 Management Console.

To avoid the server error, grant the Network Service account read/write access to the following folder:

C:\Windows\Microsoft.NET\Framework\v2.0.50727\Temporary ASP.NET Files

> **Note:** This is not an ESSO-PR-specific issue. All ASP.NET applications will receive this error if the configuration is not set correctly.

### Group Security Policy: Password History Setting Should Be Increased

ESSO-PR uses the password history setting of the Windows 2000 Group Security Policy. You should allow for one additional prior password in addition to the Enforce password

history setting. For example, if the setting is 3 (ensuring that a user's last three prior passwords cannot be reused), ESSO-PR uses one of these, so the actual setting is 2. Oracle recommends a higher setting for Enforce password history for optimal security.

## Internet Security Settings (Windows 2003 users)

The default settings for Windows 2003 Internet Security settings are more stringent than those for Windows 2000 and XP. You must add the ESSO-PR Web service to the workstation's Trusted Sites Internet zone or the Local Intranet zone in order to use ESSO-PR as a Windows 2003 client.

# Server Registry Settings

## ► Under HKLM\Software\Passlogix\SSPR

| Key | Value Name | Data Type | Data |
|-----|-----------|-----------|------|
| **SSPRService** | Reset_ShowIntroduction | dword REG_DWORD | Set to 1 to display the reset prompt. Set to 0 (default) to suppress the reset prompt. |
| **SSPRService** | Reset_CustomizedErrorMsg | dword REG_DWORD | Set to 1 to activate customizable reset error messages. Set to 0 (default) to use the built-in reset error messages. |
| **Storage** | StorageOrder | string (REG_SZ) | AD or ADAM |
| | | | |
| **Extensions** | | | |

## ► Under HKLM\Software\Passlogix\SSPR\Storage\Extensions\

| Key | Value Name | Data Type | Data |
|-----|-----------|-----------|------|
| **ADAM** | Root | string (REG_SZ) | *ADAM partition root* |
| | Classname | string (REG_SZ) | Adam |
| | | | |

## ► Under HKLM\Software\Passlogix\SSPR\Storage\Extensions\ADAM\

| Key | Value Name | Data Type | Data |
|-----|-----------|-----------|------|
| **Servers** | Server1 | string (REG_SZ) | *server:port (of the ADAM instance)* |
| | | | |

## ► Under HKLM\Software\Passlogix\SSPR\Storage\Extensions\

| Key | Value Name | Data Type | Data |
|-----|-----------|-----------|------|
| **AD** | Root | string (REG_SZ) | *AD root* |
| | Classname | string (REG_SZ) | Ad |
| | | | |

## ► Under HKLM\Software\Passlogix\SSPR\Storage\Extensions\AD\

| Key | Value Name | Data Type | Data |
|-----|-----------|-----------|------|
| **Servers** | Server1 | string (REG_SZ) | *server:port* |

# Installing an ADAM Instance

1. Start ADAMSetup.exe. Select **A unique instance** and click **Next**.
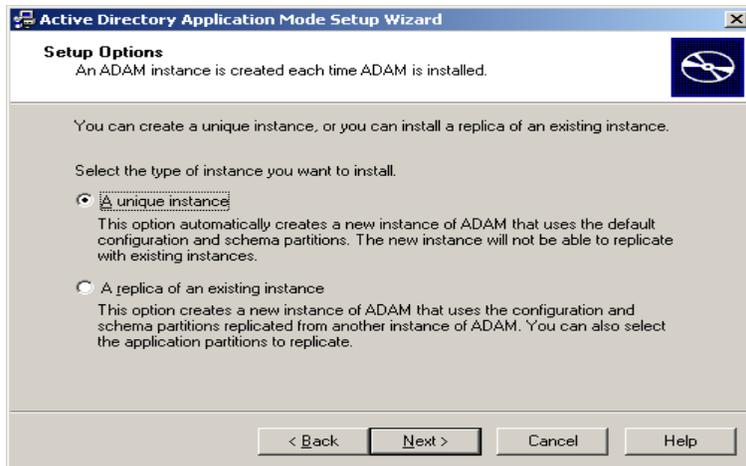


2. Provide your Instance name and click **Next**.

3. Specify port numbers of 10000 and 10001 (ten thousand range, for easy recall) and click **Next**.



4. Specify the root DN (for example, `DC=SSPR,DC=Passlogix,DC=COM`) and click **Next**.
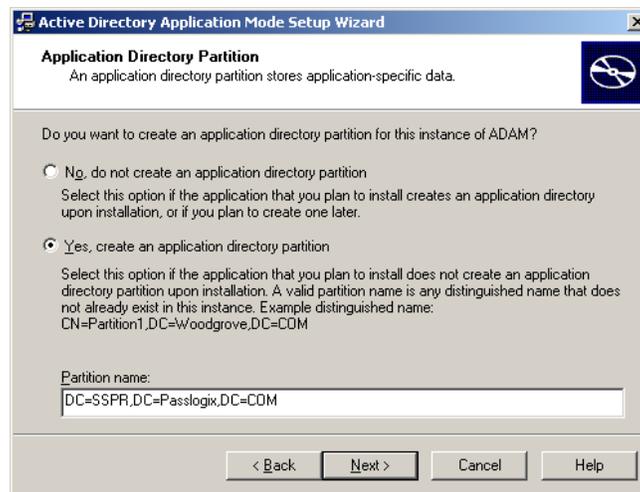
5.   Specify an easy-to-find base location (for example, `%RootDrive%\ADAM\Instance`) and click **Next**.
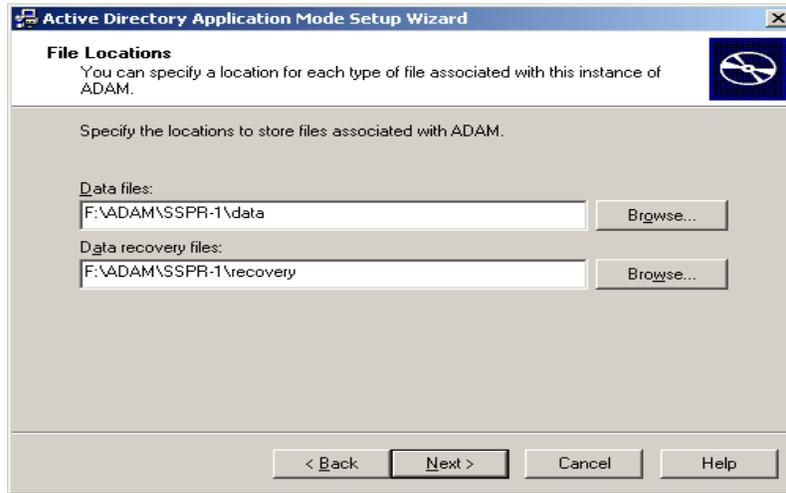


6.   Specify the run privileges and click **Next**.
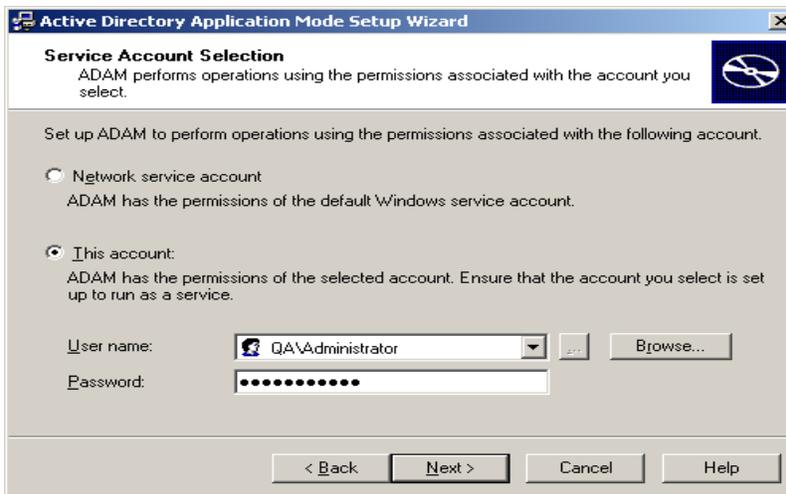
7.  Specify the Administrative Permissions and click **Next**.



8.  Select **Do not import LDIF files** for this instance of ADAM and click **Next**.
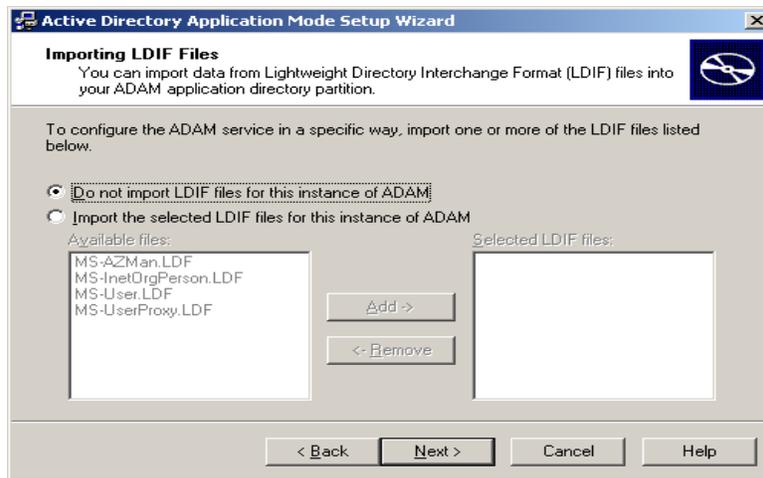
9. Click **Next** as requested to proceed.
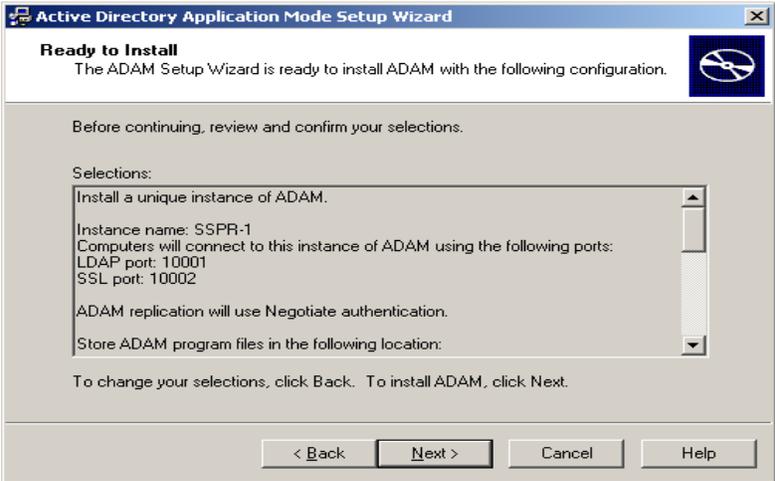


10. Click **Finish**.
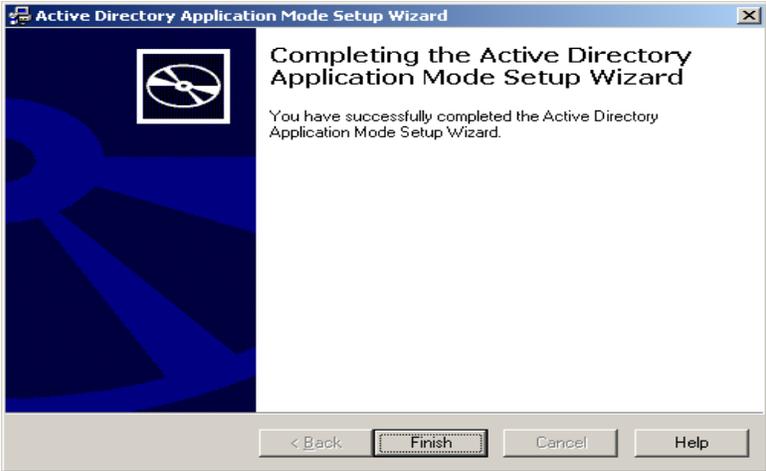
# ITIM Support

## Installation and Setup

The normal ESSO-PR installation includes the ITIM connector. To install ITIM support:

1. Install ESSO-PR Server.
2. Install Sun Java Runtime Environment (JRE) version 1.4 or greater.
3. Install IBM Application Client for WebSphere Application Server.
4. Edit the <SSPR>\WebServices\Connectors\ITIM\exec.bat file as follows:

```
...
line 07: call "C:\Progra~1\WebSphere\AppClient\bin\setupClient.bat"

...

line 10: set SERVER_NAME=iiop://localhost:2809

...
```

5. Replace the bold underlined texts with the WebSphere client installation path and the WebSphere server machine name, respectively. Changes to this file take effect immediately.
6. Turn on logging for the Java module by setting the CREATE_LOG variable to true.

**Note:** All communications between ESSO-PR and the Java module will be output in the log, including user answers.

7. To enable foreign languages, edit
   <SSPR>\WebServices\Connectors\ITIM\languages.txt.
   English is the only language enabled by default; all other languages are disabled. They will not show up in the language dropdown list on the Enrollment page.
8. To enable a language, uncomment the line that contains that language by deleting the apostrophe at the beginning of the line. For example, to enable German:

**Before (German disabled):**

```
...
'de-de=de      '  German
...
```

**After (German enabled):**

```
...
de-de=de       '  German
...
```

The change will not take effect until the IIS service is restarted.