



## DPRA Server Installation and Setup Guide





## DPRA Server Installation and Setup Guide

**Note:**

Before using this information and the product it supports, read the information in "Notices," on page 37.

This edition applies to version 6.0 of this adapter and to all subsequent releases and modifications until otherwise indicated in new editions.

© **Copyright International Business Machines Corporation 2005, 2007. All rights reserved.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

## Table of Contents

---

Before You Begin.....	6
Purpose .....	6
Intended Audience .....	6
System Platform Requirements and Necessary Accounts .....	6
Best Practices .....	6
Installing the Server.....	7
Step by Step: Installing the TAM E-SSO: Desktop Password Reset Adapter Server.....	8
Creating Service Accounts.....	9
Assigning the SSPRRESET and SSPRWEB Accounts .....	10
Setting Up the SSPRRESET Account.....	10
Setting Up the SSPRWEB Account.....	11
Verifying Proper Assignments of SSPRWEB and SSPRRESET Accounts.....	13
Granting Registry Access to the SSPRWEB Account.....	16
Enabling Storage in Active Directory.....	17
Granting Permissions to the SSPRWEB Account in AD.....	20
Delegating Permissions to the SSPRRESET Account.....	22
Considerations When Planning TAM E-SSO: Desktop Password Reset Adapter Account Permissions.....	22
Running the Delegation of Control Wizard at the OU Level .....	22
Granting the Password Reset Account Permissions at the Group Level .....	25
Making the TAM E-SSO: Desktop Password Reset Adapter Server a Trusted Intranet Site in AD.....	28
Restricting Access to the Management Console.....	31
Reference and Troubleshooting .....	32
Installation and Configuration Notes .....	32
Using AD/ADAM and IIS Web Services on Different Servers.....	32
Installing ASP.NET 2.0 With Windows 2000 SP4: "Access is Denied" Error.....	32
Access Denied Writing to Temporary ASP.NET Files.....	32
Windows Installer Error 1720 .....	33
Group Security Policy: Password History setting should be increased.....	33
Internet Security settings (Windows 2003 users) .....	33
TAM E-SSO: Desktop Password Reset Adapter Registry Settings .....	34
Installing an ADAM Instance.....	35
ITIM Support.....	37
Installation and Setup .....	37

## Before You Begin

---

### Purpose

This document provides step-by-step installation and configuration instructions for IBM Tivoli Access Manager for Enterprise Single Sign-On Desktop Password Reset Adapter (TAM E-SSO: Desktop Password Reset Adapter) software server-side component with enhanced security settings.

### Intended Audience

This document is written for system and network administrators who are responsible for deploying and securing TAM E-SSO: Desktop Password Reset Adapter 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.

### System Platform Requirements and Necessary Accounts

Please see the Release Notes for the latest system requirements.

### Best Practices

The following best practices should be observed:

- Avoid installing the TAM E-SSO: Desktop Password Reset Adapter server-side components on a Domain Controller. Use a member server.<sup>1</sup>
- Ensure that DNS is configured and working properly, including correct enumeration of forward and reverse lookup zones.
- Ensure that your servers and workstations have the latest service packs and Windows updates installed on them.
- For the creation of service accounts, consider long complex passwords and set the accounts to lock out after a finite set of bad password attempts. This will prevent a hacker from attempting a dictionary attack on service accounts.

---

<sup>1</sup> Generally speaking, Microsoft recommends that IIS servers be installed on member servers. For a full discussion of this matter, visit [Microsoft.com](http://Microsoft.com).

## Installing the Server

---

To install the TAM E-SSO: Desktop Password Reset Adapter server components:



**Do NOT install the TAM E-SSO: Desktop Password Reset Adapter server-side components on a Domain Controller.**

1. Log onto the IIS Member Server where you have local administrative rights at the domain level. *Do not* log on at the local machine level.<sup>2</sup>
2. Locate the .exe or .msi installation file for the TAM E-SSO: Desktop Password Reset Adapter server-side component.<sup>3</sup>

**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.

3. Follow the installation wizard, selecting the defaults and performing the Complete installation as in Figure 1.

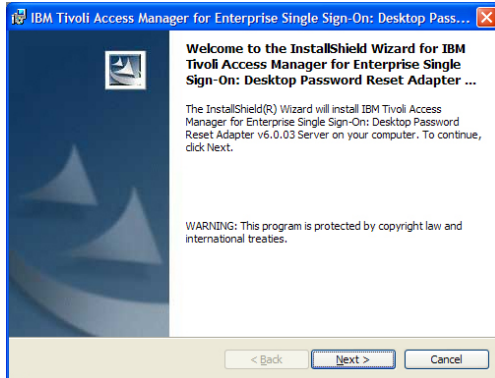
---

<sup>2</sup> By default, members of the Domain Admins 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 Administrator's group, add yourself to the local administrator's group on the member server. This example designates an "Administrator" account as a member of Schema Admins group to simplify the process.

<sup>3</sup> Whether you receive the TAM E-SSO: Desktop Password Reset Adapter 6.0 CD or download the components, two files exist to install the TAM E-SSO: Desktop Password Reset Adapter server-side components. One is an executable, the other is an MSI, with the .exe containing the .NET framework components.

## Step by Step: Installing the TAM E-SSO: Desktop Password Reset Adapter Server

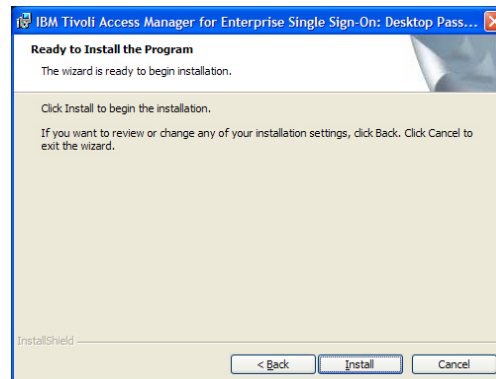
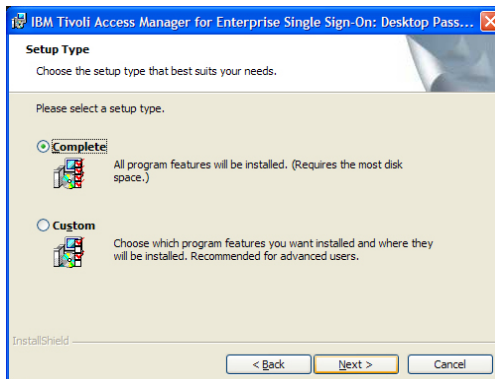
1. Double click the IBM\_SSPR\_Server\_<versionnumber>. (EXE or MSI) The Install Wizard appears:
2. Select I accept the terms in the license agreement and click **Next**.



Click **Next**.



3. Select a complete installation and click **Next**.
4. Click **Install**.



5. The installer indicates its progress.
6. When the installation is complete, click **Finish**.

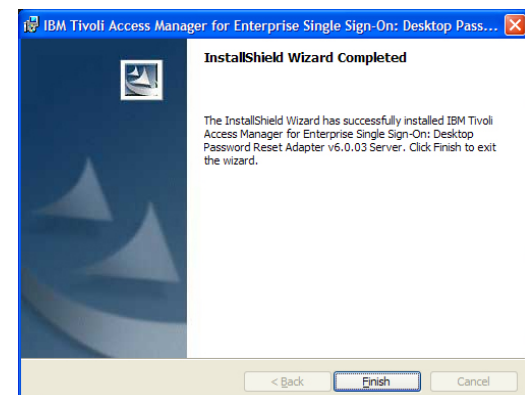
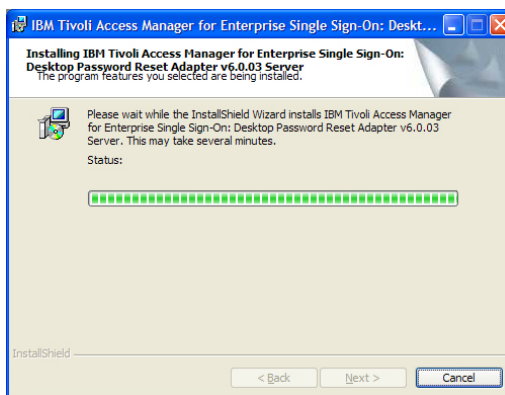


Figure 1. TAM E-SSO: Desktop Password Reset Adapter Installation Wizard



## Creating Service Accounts<sup>4</sup>

---

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 TAM E-SSO: Desktop Password Reset Adapter IIS functions and will make changes, additions, etc., to the Organizational Unit (OU) that you will create later.
- **SSPRRESET:** This account will run the actual reset service on the TAM E-SSO: Desktop Password Reset Adapter member server with IIS. It will be responsible for resetting user passwords on the domain level.

**Note:** Make these accounts members of the local admins group on the local IIS box to avoid problems.

---

<sup>4</sup> These will be the service accounts used by TAM E-SSO: Desktop Password Reset Adapter to manage the container where user questions and enrollment information will be housed and to handle the actual password reset process. Since 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 may result in some helpdesk calls from users who cannot reset their passwords, it will also alert you that somebody has been trying to attack these service accounts. For information as to best practices for service accounts and security log monitoring, visit Microsoft's knowledgebase.

## Assigning the SSPRESET 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 SSPRESET account to allow the user to change his password. To assign the authentication and password reset roles, designate properties to SSPRESET first, and then to SSPRWEB.

### Setting Up the SSPRESET Account

1. Run: **Control Panel > Administrative Tools > Services**. (See Figure 2.)
2. From the list in the right pane, right-click **Self Service Password Reset**, and select **Properties**.
3. The **Self Service Password Reset Properties** dialog displays.
4. Select the **Log On** tab.
5. Select **This account** and enter the account name: **Domain\SSPRESET**. Then enter and confirm the password for the account.

A dialog appears to advise you that changes will apply after the service is restarted.

6. Restart the service as indicated.

The SSPRESET account setup is complete.

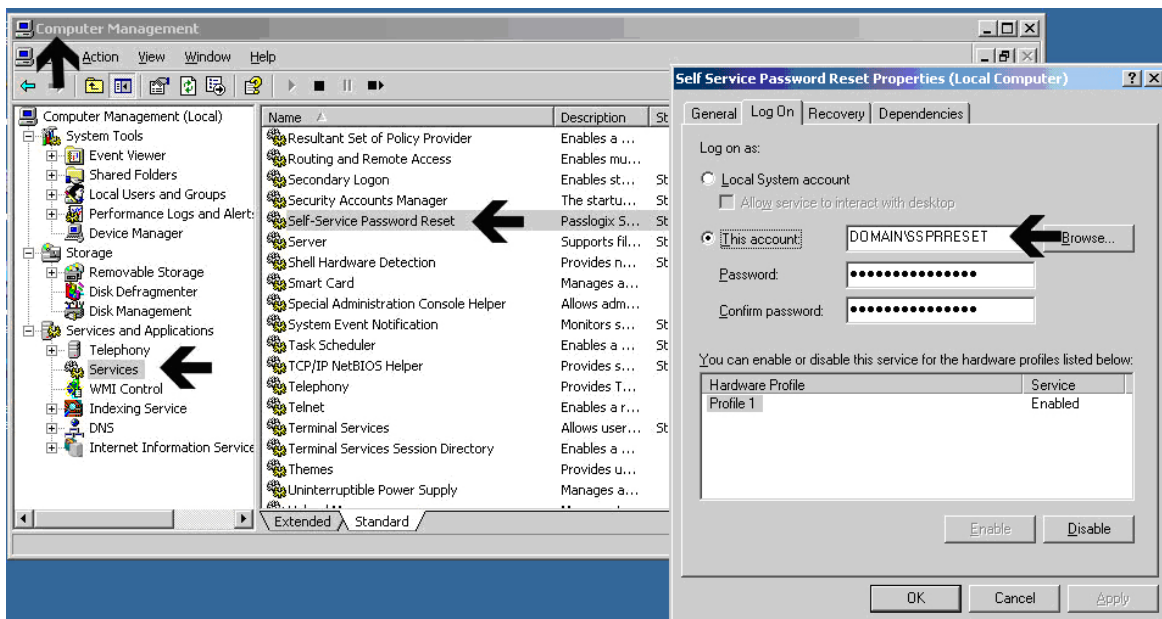


Figure 2. Setting Up the SSPRESET account

**Note:** The SSPRESET account runs the TAM E-SSO: Desktop Password Reset Adapter password reset service on the IIS server where the server-side components reside.

**Note:** The SSPRWEB account runs the TAM E-SSO: Desktop Password Reset Adapter 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**. (See Figure 3.)
2. Under IIS, locate the **vgoSelfServiceReset** virtual directory, and right-click it and select **Properties**.
3. Select the **Directory Security** tab.
4. In the **Authentication and access control** section, click **Edit**.
5. The **Authentication Methods** dialog displays.
6. Under **Use the following Windows user account for anonymous access**:, enter the name (in **Domain\Username** format) and password of the SSPRWEB account.
7. At the **Confirm Password** window, retype the password and click **OK**.

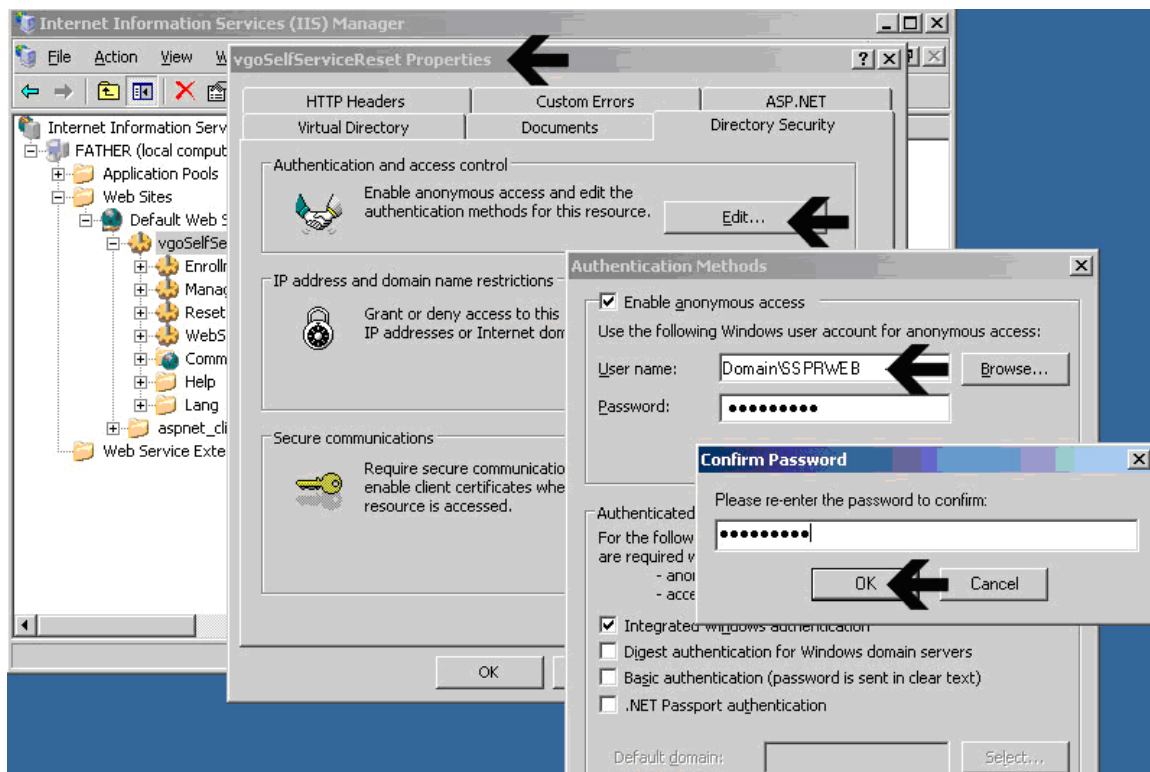


Figure 3. Setting Up the SSPRWEB account

8. Restart IIS by clicking **START > RUN** and typing **iisreset**.

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

9. The virtual sub-directories under the **vgoSelfServiceReset** virtual directory should be configured as in Table 1.

**Table 1. Configuration of TAM E-SSO: Desktop Password Reset Adapter  
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

To access the TAM E-SSO: Desktop Password Reset Adapter web-based console, open IIS Manager and navigate down to **Default Website**, then to **vgoSelfServiceReset > ManagementClient**. In the right pane, scroll down to the **webservice.aspx** page and browse it (see Figure 4).

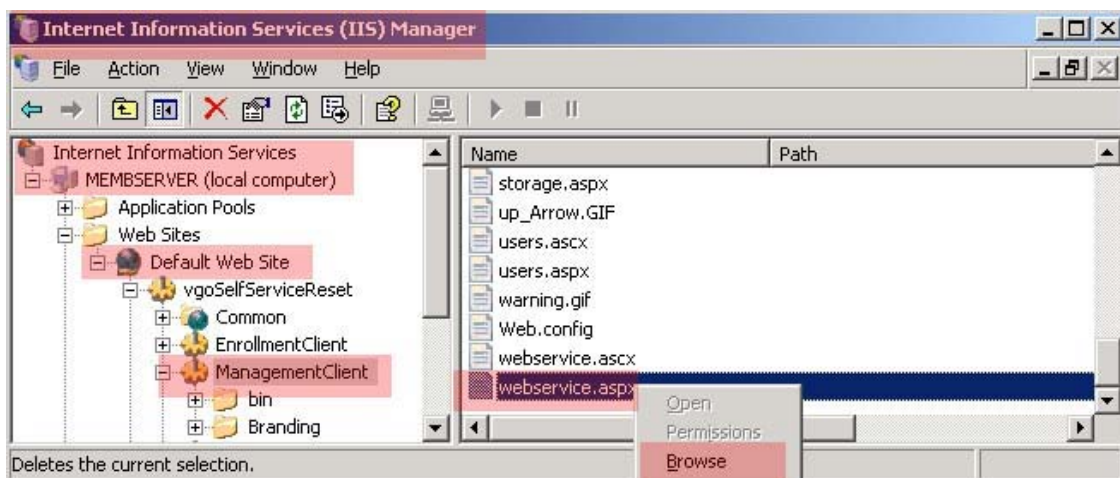


Figure 4. Browse webservice.aspx Page.

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

**Note:** If you receive the error: 'The current identity (NT AUTHORITY\NETWORK SERVICE) does not have write access to 'C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\Temporary ASP.NET Files'', follow the procedure in **Access Denied Writing to Temporary ASP.NET Files** in the **Reference and Troubleshooting** section.

In the TAM E-SSO: Desktop Password Reset Adapter **Management Console** web page, locate the **System > Web Service Account** section. Verify that the SSPRWEB account has been designated as the **Current Account** as in Figure 5.

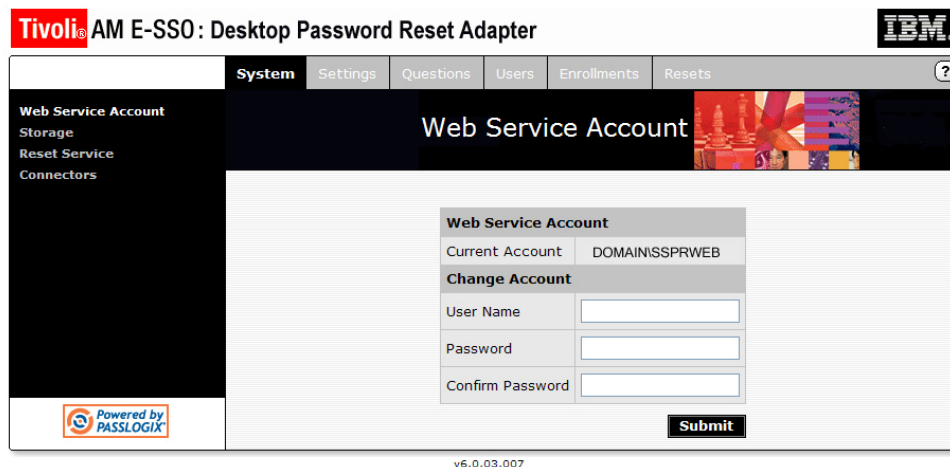



Figure 5. Verify that the SSPRWEB account is the *Web Service Account*.

In the TAM E-SSO: Desktop Password Reset Adapter *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 (Figure 6).

**Note:** If the *SSPRRESET* account is not listed as the Reset Service account under the *Reset Service Section* of the *TAM E-SSO: Desktop Password Reset Adapter Management Console* web page, make sure 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:**

1. Navigate to the IIS member server where you installed the TAM E-SSO: Desktop Password Reset Adapter server-side components (see Figure 6).
2. Check the local administrator's group.
3. Verify that the SSPRRESET and the SSPRWEB accounts are both members of the local administrator's group.
4. Click on *Reset Service* in the left pane and make sure that the SSPRRESET account is listed as the *Reset Service* account.

**Tivoli** AM E-SSO : Desktop Password Reset Adapter **IBM**

System Settings Questions Users Enrollments Resets ?

Web Service Account  
Storage  
Reset Service  
Connectors

### Reset Service

Current Status	
Status	Started
Account	DOMAIN\SSPRRESET

**Change Service Account**

User Name

Password

Confirm Password

**Service Options**

Listening Port

Domain

**Submit**

Powered by PASSLOGIX

v6.0.03.007

Figure 6. Verify that the SSPRRESET account is the *Reset Service Account*.

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

## Granting Registry Access to the SSPRWEB Account

---

In order for TAM E-SSO: Desktop Password Reset Adapter to function properly, the SSPRWEB service account needs full permissions to the following registry key on the member server containing the TAM E-SSO: Desktop Password Reset Adapter 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 TAM E-SSO: Desktop Password Reset Adapter server side components, it's recommended that both the DPRARWEB and SSPRRESET accounts be made members of the local administrator's group on the IIS Member Server where you are installing the TAM E-SSO: Desktop Password Reset Adapter server-side components.

Once you have finished the installation and configuration of the TAM E-SSO: Desktop Password Reset Adapter server-side components, you may remove these accounts from the local administrator's group on the member server.



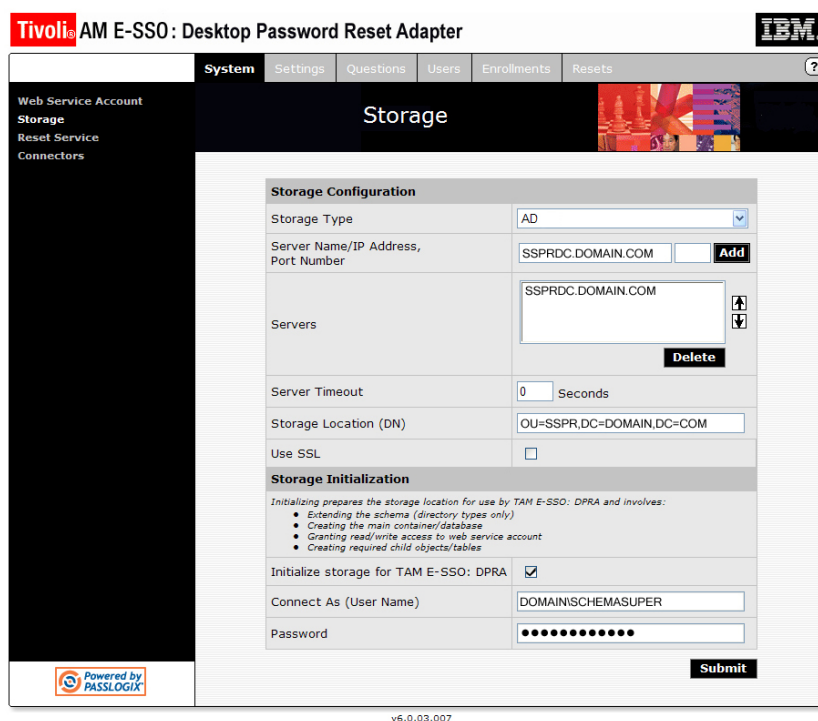
## Enabling Storage in Active Directory

TAM E-SSO: Desktop Password Reset Adapter 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 may receive an error message indicating that no such object exists on the server.**

The **Connect As** account is the one that performs the schema extension. As such, this account needs to be a member of the Schema Administrator's group and have permissions to create objects within the Password Reset OU.



The screenshot displays the 'Storage' configuration page of the TAM E-SSO: Desktop Password Reset Adapter. The interface includes a top navigation bar with tabs for System, Settings, Questions, Users, Enrollments, and Resets. A left sidebar lists options: Web Service Account, Storage, Reset Service, and Connectors. The main content area is titled 'Storage' and contains two sections: 'Storage Configuration' and 'Storage Initialization'.

**Storage Configuration**

- Storage Type: AD (selected from a dropdown)
- Server Name/IP Address, Port Number: SSPRDC.DOMAIN.COM (with an 'Add' button)
- Servers: A list containing SSPRDC.DOMAIN.COM (with 'Add' and 'Delete' buttons)
- Server Timeout: 0 Seconds
- Storage Location (DN): OU=SSPR,DC=DOMAIN,DC=COM
- Use SSL: ☐

**Storage Initialization**

Initializing prepares the storage location for use by TAM E-SSO: DPRA and involves:

- Extending the schema (directory types only)
- Creating the main container/database
- Granting read/write access to web service account
- Creating required child objects/tables

Initialize storage for TAM E-SSO: DPRA: ☒

Connect As (User Name): DOMAINSCHEMASUPER

Password: [masked]

A 'Submit' button is located at the bottom right of the form. The footer of the page indicates 'v6.0.03.007'.

Figure 7. Enabling storage in Active Directory

To enable storage in Active Directory:

1. In the **System > Storage** screen, select the storage type as AD in the **Storage Type** dropdown menu.
2. Enter the fully-qualified domain name or the IP address of the Domain Controller that you want to use.
3. Enter **389<sup>5</sup>** for the port number.
4. Click the **Add** button.
5. Populate the fields according to the information in Table 2.
6. Click **Submit**.

After a slight delay, the confirmation message **Successfully Saved Changes** displays.

Table 2. Storage Configuration Screen Explanations	
Screen Label	Explanation
<b>Storage Type</b>	The type of directory in which TAM E-SSO: Desktop Password Reset Adapter is installed. This example uses Microsoft Active Directory (AD).
<b>Server Name/IP Address, Port Number</b>	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.
<b>Servers</b>	The list of domain controllers to use. This example uses one server: <b>SSPRDC.DOMAIN.COM</b> . It is possible to have multiple servers.
<b>Server Timeout</b>	The number of seconds in an attempt to establish a connection to the repository before a timeout.
<b>Storage Location (DN)</b>  <b>OU=SSPR</b> <b>DC=DOMAIN</b> <b>DC=COM</b>	The distinguished name (DN) of the TAM E-SSO: Desktop Password Reset Adapter TAM E-SSO: Desktop Password Reset Adapter OU that you create within Active Directory. The DN typically includes: The name of the OU that you create The netbios/short name of the domain The extension of the domain, e.g., com, .gov, etc.
<b>Initialize Storage for TAM E-SSO: Desktop Password Reset Adapter</b>	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 <b>Connect As</b> or <b>Password</b> fields. This tells TAM E-SSO: Desktop Password Reset Adapter whether or not it should extend the schema and create the initial objects. If this box is not checked, TAM E-SSO: Desktop Password Reset Adapter will only update the storage settings.
<b>Connect As</b>	The name of the account that will actually extend the AD schema and add the necessary objects to the TAM E-SSO: Desktop Password Reset Adapter OU. This account should be a member of the Schema Admins group and have permissions to create objects in the TAM E-SSO: Desktop Password Reset Adapter OU.  <b>Note:</b> You should enter the username in this syntax: <b>Domainname/Username</b>
<b>Password</b>	The password for the account specified above.

<sup>5</sup> This is the LDAP port used by Active Directory.

**Note:** To verify that the TAM E-SSO: Desktop Password Reset Adapter 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 **TAM E-SSO: Desktop Password Reset Adapter** (or the name that you chose) and two sub OUs named **SystemQuestions** and **Users**. The existence of these two sub OUs indicates success.

You can now remove both the SSPRWEB and SSPRESET accounts from the local administrator's group on the IIS member server where you installed the TAM E-SSO: Desktop Password Reset Adapter server-side components.

## Granting Permissions to the SSPRWEB Account in AD

After creating the OU and sub containers within Active Directory, grant limited, specific permissions to the SSPRWEB account for the TAM E-SSO: Desktop Password Reset Adapter OU you created in AD (see Figure 8).

**Shortcut:** 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 TAM E-SSO: Desktop Password Reset Adapter OU and its sub-containers at the advanced security levels.

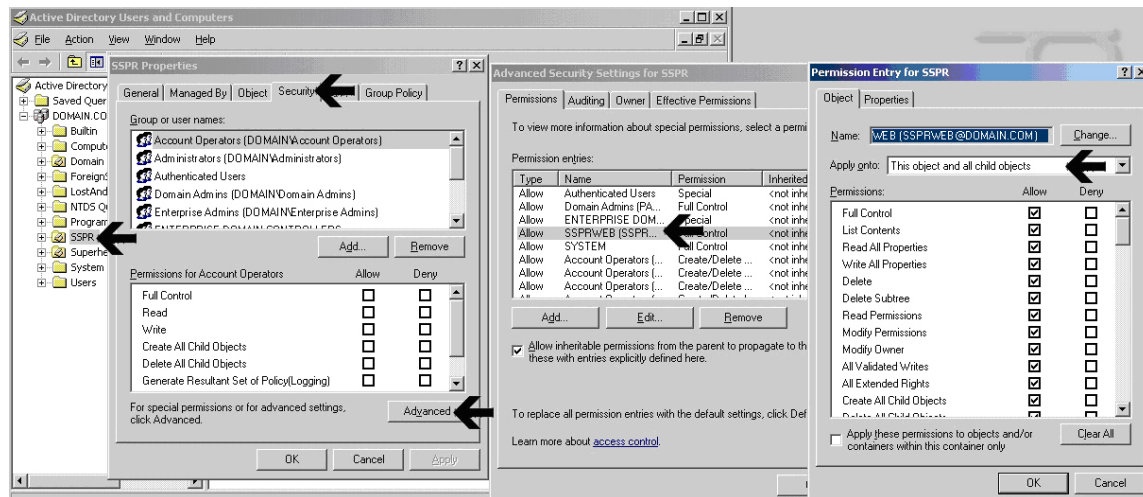


Figure 8. Assign advanced permissions to the SSPRWEB account.

To assign advanced permissions to the SSPRWEB account of the TAM E-SSO: Desktop Password Reset Adapter 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 **SSPR** Organizational Unit 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** window.
5. Click the **Add** button.
6. Enter the name of the SSPRWEB account.
7. Click **OK**. The **Permissions Entry** page displays.
8. Check the **Full Control** box in the **Allow** column.
9. In the **Apply onto:** dropdown menu, select **This object and all child objects**.
10. Click **OK** and close all open windows.
11. Verify that the permissions have been set accordingly.

The SSPRWEB account will have the permissions in Table 3 when configured correctly.

**Table 3. SSPRWEB Account Permissions in Active Directory**

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 the password reset account (SSPRRESET) a limited set of rights. This account should be able to reset user passwords and unlock accounts but nothing more.

Bear in mind that the SSPRRESET account is simply a member of your Domain User's group and, as a failsafe built into AD, will not be able to change the password of a user that has greater rights (e.g., an administrator account).

There are several ways to delegate the password reset permissions:

- At the Organizational Unit level by running the Delegation of Control Wizard
- At the Group level by setting advanced permissions manually

Assigning this right at the User level should not be a general practice and is not recommended.

### Considerations When Planning TAM E-SSO: Desktop Password Reset Adapter Account Permissions

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

- 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: This will give the password reset account rights that extend beyond users to objects such as computers, printers, etc.
- Since 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 doesn't 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 TAM E-SSO: Desktop Password Reset Adapter and go through the entire password reset dialog, but when they attempt to reset their passwords, they will receive an error message. This is because the password reset service account is not designed to have permissions to reset the password for users in a higher security group.

- Please note, you need to consider carefully whether you want members of your domain administrator's 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 may decide it is wiser not to do so.

### Running the Delegation of Control Wizard 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 run the *Delegation of Control Wizard* on each OU, and grant the SSPRRESET service account permissions to users contained within the OU.

In the following example, we will give the SSPRRESET account the authority over the **Users2** OU to reset its members' passwords using the *Delegation of Control Wizard* (Figure 9):

1. Navigate to **Active Directory Users and Computers > [YourDomain] > [YourOU]**. This example uses **DOMAIN.COM > Users2**.
2. Right-click on the OU that you want to control (this example uses the **Users2** OU) and select *Delegate Control*.

This launches the *Delegation of Control Wizard*. (Figure 9)

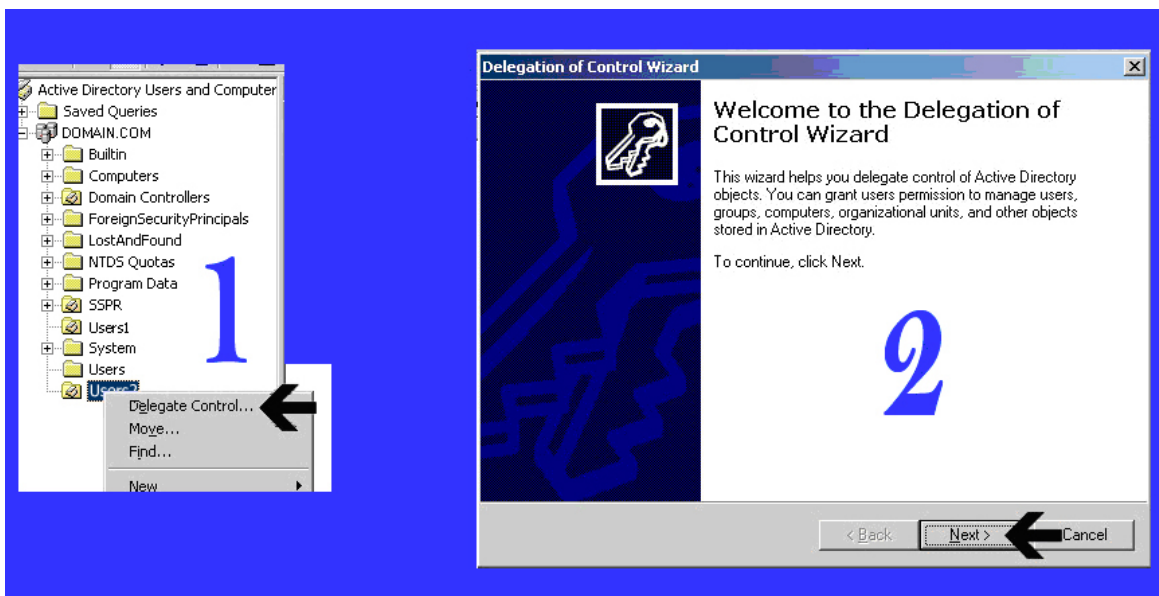


Figure 9. Using the Delegation of Control Wizard

3. In the *Wizard* dialog box, click *Next*.
4. Add the SSPRRESET account to the *Users or Groups* list in the dialog box (Figure 10).
5. Click *Next* to display the *Tasks to Delegate* dialog box (Figure 10).
6. Select the *Create a custom task to delegate* radio button (Figure 10).
7. Click *Next*.

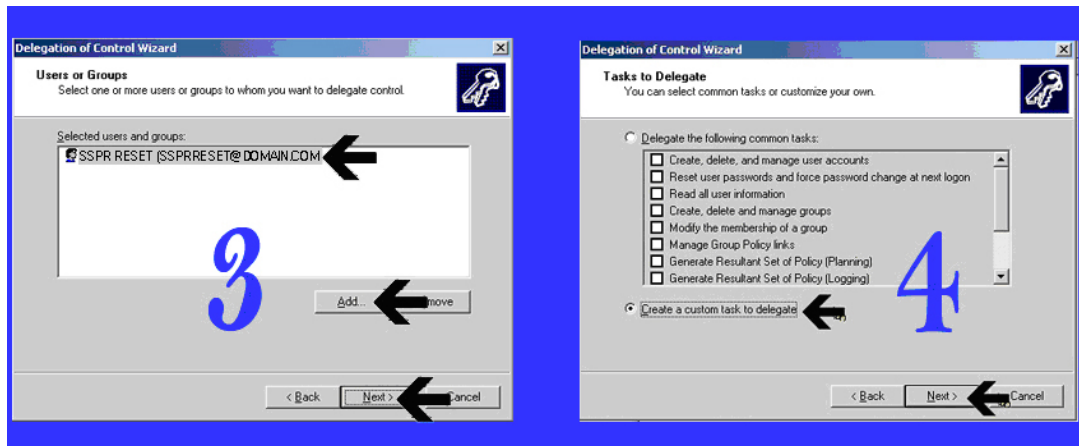


Figure 10. Add OU to SSPRESET account (3) and create a custom task (4).

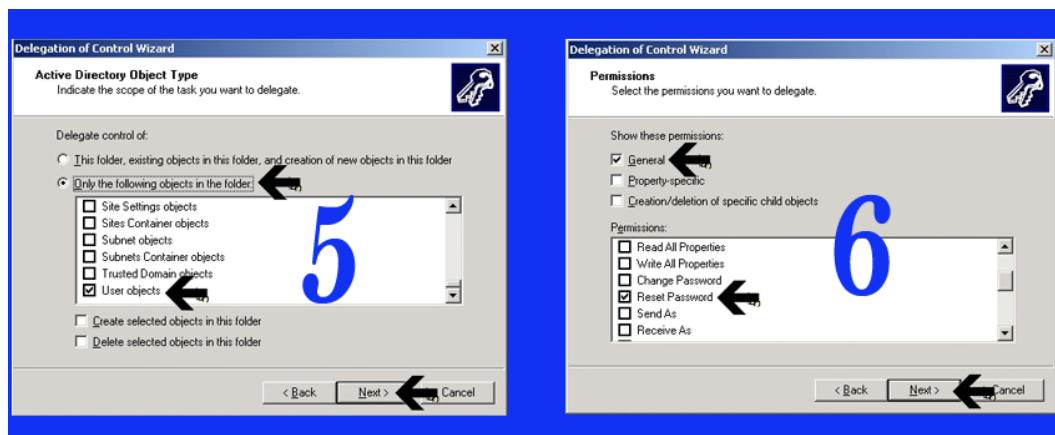


Figure 11. Select User objects (5), General permissions > Reset Password (6).

8. In the **Active Directory Object Type** dialog box, select the **Only the following objects in the folder** radio button. (Figure 11)
9. Scroll down to **User** objects and check the box. (Figure 11)
10. Click **Next**. (Figure 11)
11. In the **Permissions** dialog box, make sure that only the **General** check box is selected.
12. Scroll down to **Reset Password** and check the box.
13. Click **Next**.
14. The final screen of the **Wizard** summarizes the controls you've just assigned. (Figure 12)
15. Click **Finish**.



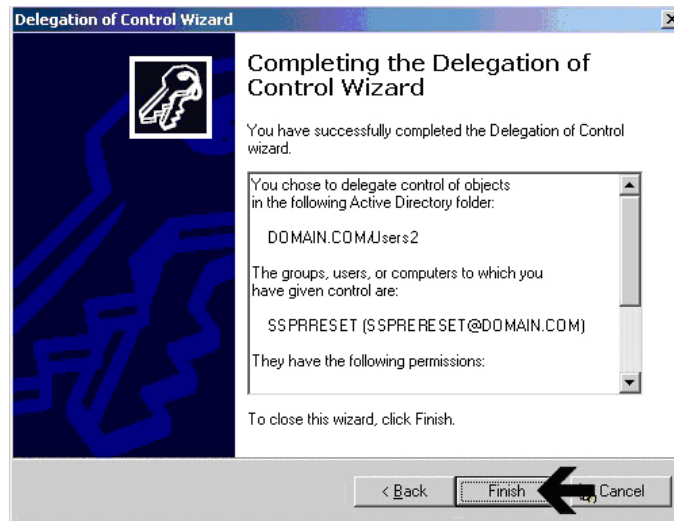


Figure 12. Summary of assigned controls

To verify that permissions were correctly assigned:

1. Right-click on the OU for which you just ran the *Delegation of Control Wizard*.
2. Select *Properties*.
3. Select the *Security* tab.

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

**Note:** When using the *Delegation of Control Wizard* at the OU level, make sure that permissions for the Password Reset account are explicitly set.

## Granting the Password Reset Account Permissions at the Group Level

If you have not separated users into Organizational Units as discussed previously, you can assign advanced security manually for the SSPRESET Account to specific groups.

**Note:** The delegation of control wizard is NOT available at the group level.

To assign the SSPRESET account permission for groups manually:

1. Navigate to **Active Directory Users and Computers > [YourDomain] > [YourGroup]**. This example uses **DOMAIN.COM > Users2 > GROUP1**. (Figure 13)
2. Right-click the *Group* object to display its *Properties* dialog box. (Figure 13)
3. Select the *Security* tab. (Figure 13)
4. Click the *Advanced* button. (Figure 13)

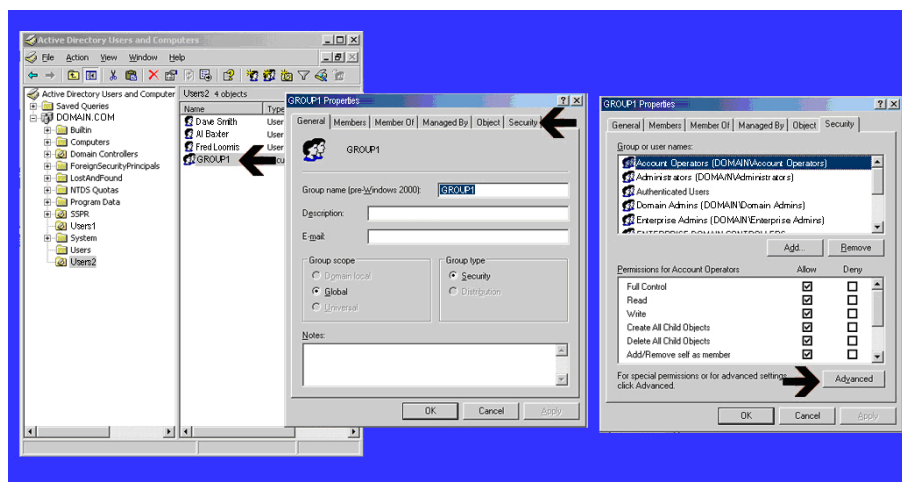


Figure 13. Selecting Advanced Settings for the Group.

5. The **Advanced Security Settings** screen displays. (Figure 14).
6. Click **Add**.
7. A screen displays prompting you to **Enter the object name to select**. (Figure 14)

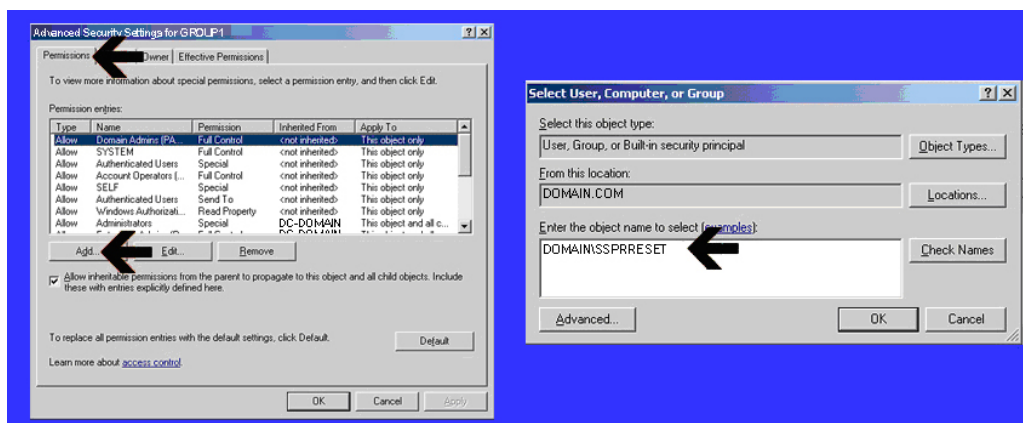


Figure 14. Enter the SSPRESET account.

8. Enter the name of the SSPRRESET account.
9. Click **OK**.
10. The **Permission Entry** screen displays. (Figure 15)

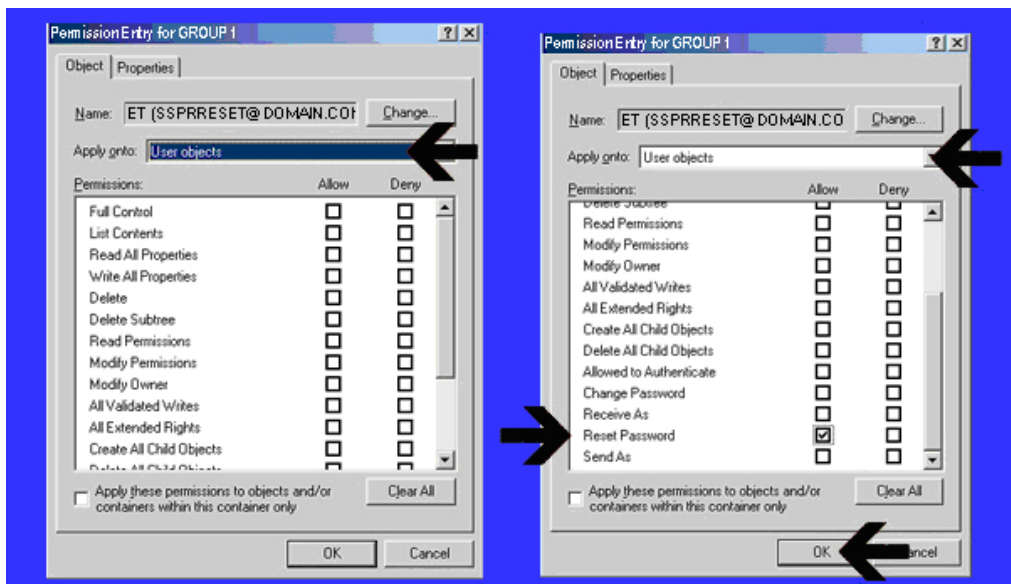


Figure 15. Assign reset password control over the User object.

11. From the **Apply onto:** drop down box, select **User objects**. (Figure 15)
12. Scroll down to **Reset Password** and check its box. (Figure 15)
13. Click **OK** and **Apply**.

To verify that permissions were correctly assigned:

1. Right-click on the group that you just assigned to the SSPRRESET account.
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 group.

## Making the TAM E-SSO: Desktop Password Reset Adapter Server a Trusted Intranet Site in AD

---

There are two virtual directories within TAM E-SSO: Desktop Password Reset Adapter that do not permit anonymous access, but that are configured to use integrated Windows authentication (i.e., if you are logged onto the domain with your Windows password, you should be able to get to that page).

Since 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 may encounter a popup screen requesting his username and password, as is customary with any website with such settings. You can avoid this behavior (which can lead to undesired helpdesk calls) by putting the fully-qualified domain name of your TAM E-SSO: Desktop Password Reset Adapter IIS server in your list of trusted sites for any user in your domain.

To designate your TAM E-SSO: Desktop Password Reset Adapter server as a trusted intranet site:

- For an individual computer, add the TAM E-SSO: Desktop Password Reset Adapter IIS server's default website in your list of trusted intranet sites.
- Within AD, add this site to your list of trusted intranet sites via a group policy.

To accomplish this, you need:

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

In the example below the TAM E-SSO: Desktop Password Reset Adapter Server site will be designated as a trusted intranet site for the entire domain. As such, it shall be a trusted site to all domain users.

**Note:** You may choose to create this policy for each OU that contains potential TAM E-SSO: Desktop Password Reset Adapter users for more granular access control. Regardless of your approach, the end result is the inclusion of the TAM E-SSO: Desktop Password Reset Adapter IIS server default website as a trusted site.

To add the TAM E-SSO: Desktop Password Reset Adapter IIS server to the list of trusted sites in your organization, it is necessary to begin by creating 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**.

**Note:** 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 Unit(s)** that contain users who will be enrolling in TAM E-SSO: Desktop Password Reset Adapter (in this example, at the root level of the domain) and click the **Group Policy** tab.

3. Create a policy named **TAM E-SSO: Desktop Password Reset Adapter TRUSTED INTRANET SERVER**. (Figure 16)

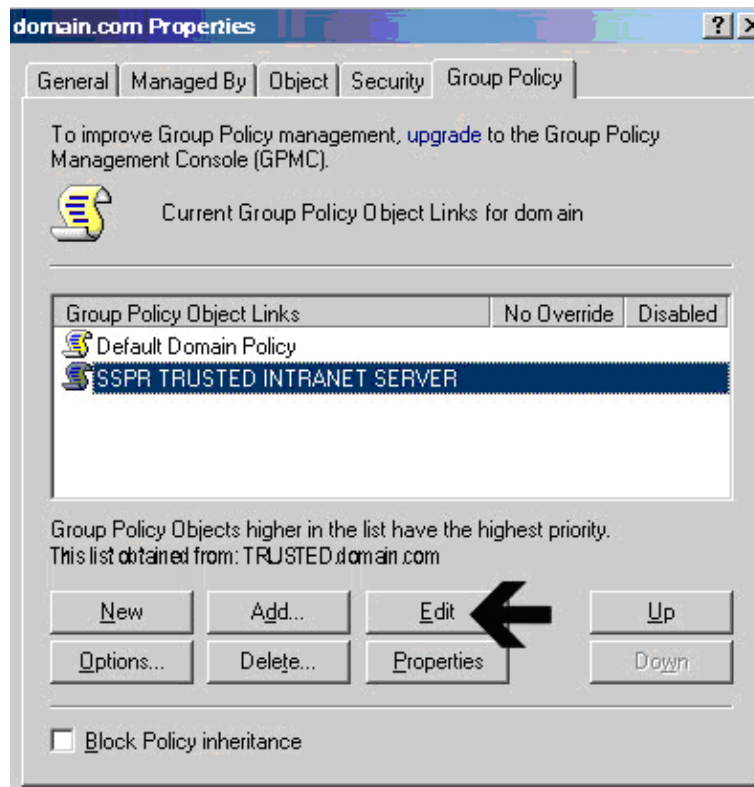


Figure 16. Create a policy for trusted intranet servers.

4. Click the **Edit** button. (Figure 16)

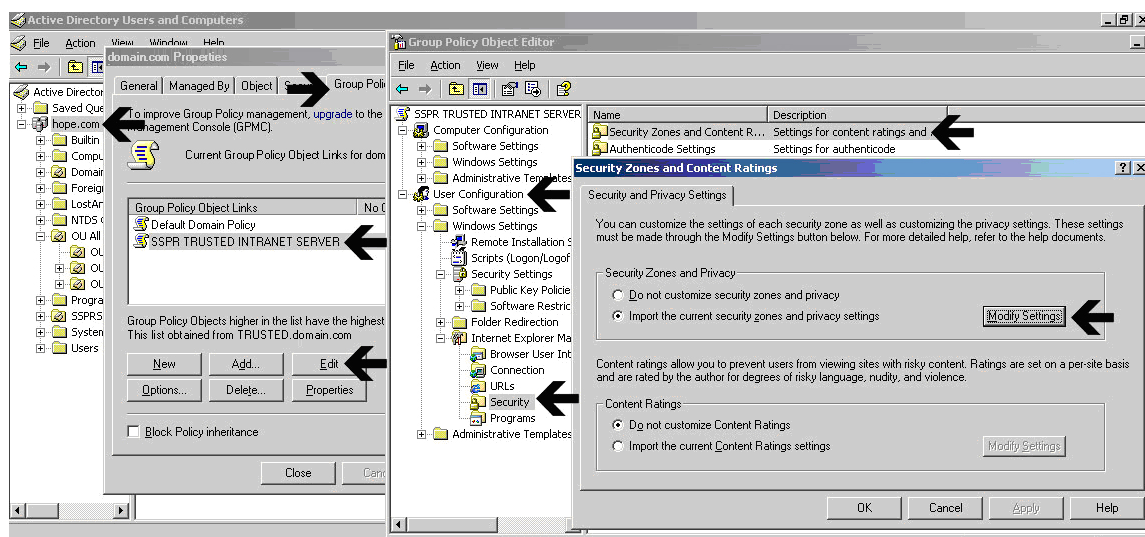
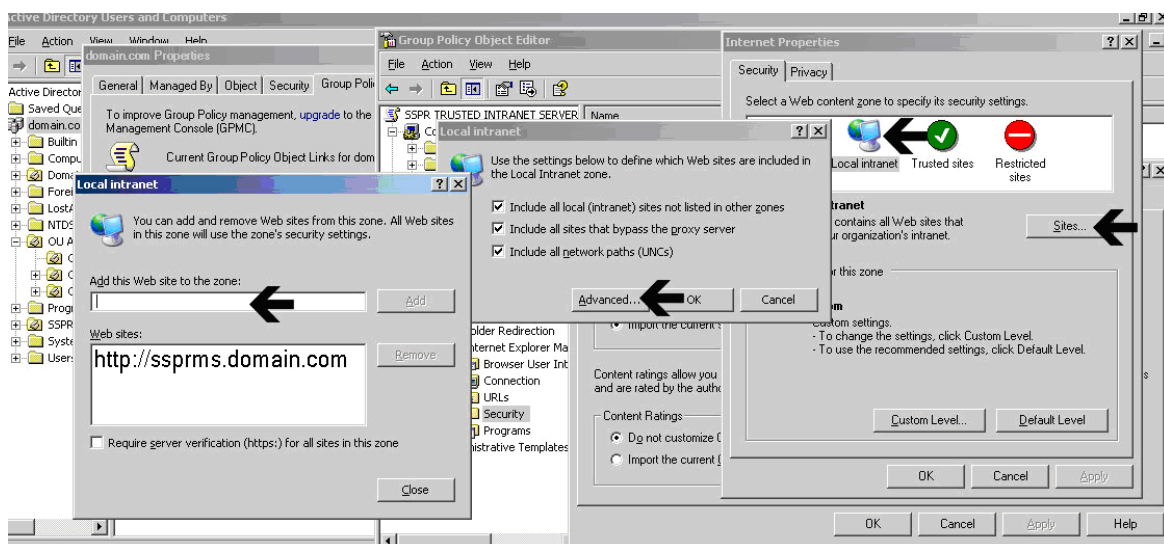


Figure 17. Editing the policy

5. Expand the user configuration portion of the policy in the **Group Policy Editor**. (Figure 17)
6. Navigate to **Windows Settings > Internet Explorer Maintenance > Security > Security Zones and Content Ratings**. (Figure 17)
7. Click **Modify Settings**. (Figure 17)  
A message displays.
8. Read the message and proceed. (Figure 17)

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



**Figure 18. Enter the fully-qualified domain name of your trusted site.**

9. Click on the **Sites** button. (Figure 18)
10. Click on the **Advanced** button. (Figure 18)
11. Enter the fully-qualified domain name of your TAM E-SSO: Desktop Password Reset Adapter IIS default website where indicated. (Figure 18)
12. Click **Close**. (Figure 18)
13. Click **OK** and **Apply** as needed to close out of the Group Policy Object Editor. (Figure 18)

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 TAM E-SSO: Desktop Password Reset Adapter management console, perform the following steps:

1. Open **Windows Explorer** and navigate to **C:\Program Files\v-GO SSPR\**
2. Right-click the **Management Client** and select **Properties** from the shortcut menu.
3. In the **Properties** dialog, click the **Security** tab.
4. Click **Advanced**.
5. Click **Inheritable rights for Users** to clear the selection. A dialog appears.
6. 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/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/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 TAM E-SSO: Desktop Password Reset Adapter 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. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then 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, type `iisreset`.

#### *Access Denied Writing to Temporary ASP.NET Files*

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 a server error will be encountered when accessing the TAM E-SSO: Desktop Password Reset Adapter 6.0 Management Console.

To do this, 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 a TAM E-SSO: Desktop Password Reset Adapter specific issue. All ASP.NET applications will receive this error if the configuration is not correctly set.



### ***Windows Installer Error 1720***

Error 1720 occurs during TAM E-SSO: Desktop Password Reset Adapter client software installation when the logged-on user does not have sufficient rights to install software on the workstation. You must log on to workstation as a user with Administrator rights or contact support personnel.

### ***Group Security Policy: Password History setting should be increased***

TAM E-SSO: Desktop Password Reset Adapter makes use of 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), TAM E-SSO: Desktop Password Reset Adapter uses one of these, so the actual setting is 2. A higher setting for Enforce password history is recommended 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 TAM E-SSO: Desktop Password Reset Adapter Web service to the workstation's Trusted Sites Internet zone or the Local Intranet zone in order to use TAM E-SSO: Desktop Password Reset Adapter as a Windows 2003 client.

## TAM E-SSO: Desktop Password Reset Adapter Registry Settings

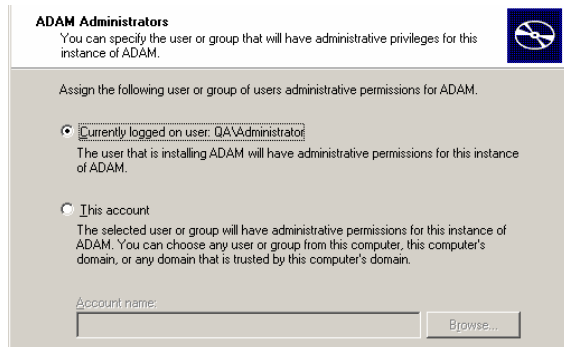
### TAM E-SSO: Desktop Password Reset Adapter Server Registry

► Under HKLM\Software\Passlogix\SSPR			
Key	Value Name	Data Type	Data
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\			
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

<p><b>1</b> Start <b>ADAMSetup.exe</b>.</p> <div> <p><b>Setup Options</b> An ADAM instance is created each time ADAM is installed.</p> <p>You can create a unique instance, or you can install a replica of an existing instance.</p> <p>Select the type of instance you want to install.</p> <p><input checked="" type="radio"/> <b>A unique instance</b> This option automatically creates a new instance of ADAM that uses the default configuration and schema partitions. The new instance will not be able to replicate with existing instances.</p> <p><input type="radio"/> <b>A replica of an existing instance</b> This option creates a new instance of ADAM that uses the configuration and schema partitions replicated from another instance of ADAM. You can also select the application partitions to replicate.</p> </div> <p>Select <b>A unique instance</b> and click <b>Next</b></p>	<p><b>2</b> Provide your Instance name and click <b>Next</b>.</p> <div> <p><b>Instance Name</b> The instance name is used to differentiate this instance of ADAM from other ADAM instances on this computer.</p> <p>Type a name for this instance. The name should reflect the use for which this instance of ADAM is intended.</p> <p>Instance name: <input type="text" value="SSPR-1"/></p> <p>Example: Addressbook1</p> <p>The ADAM service name is created when the instance name is combined with the product name. It will be displayed in the list of Windows services.</p> <p>ADAM service name: ADAM_SSPR-1</p> </div>
<p><b>3</b> Specify port numbers of 10000 and 10001 (Ten thousand range, for easy recall) and click <b>Next</b>.</p> <div> <p><b>Ports</b> Computers will connect to this instance of ADAM using specific ports on all of the IP addresses associated with this computer.</p> <p>The ports displayed below are the first available for this computer. To change these ports, type the new port numbers in the text boxes below.</p> <p>If you plan to install Active Directory on this computer, do not use 389 for the LDAP port or 636 for the SSL port because Active Directory uses these port numbers. Instead, use available port numbers from the following range: 1025-65535.</p> <p>LDAP port number: <input type="text" value="10001"/></p> <p>SSL port number: <input type="text" value="10002"/></p> </div>	<p><b>4</b> Specify the root DN (e.g., <b>DC=SSPR, DC=Passlogix, DC=Com</b>) and click <b>Next</b>.</p> <div> <p><b>Application Directory Partition</b> An application directory partition stores application-specific data.</p> <p>Do you want to create an application directory partition for this instance of ADAM?</p> <p><input type="radio"/> <b>No, do not create an application directory partition</b> Select this option if the application that you plan to install creates an application directory upon installation, or if you plan to create one later.</p> <p><input checked="" type="radio"/> <b>Yes, create an application directory partition</b> Select this option if the application that you plan to install does not create an application directory partition upon installation. A valid partition name is any distinguished name that does not already exist in this instance. Example distinguished name: CN=Partition1,DC=Woodgrove,DC=COM</p> <p>Partition name: <input type="text" value="DC=QA-2003-1,DC=QA,DC=Passlogix,DC=Com"/></p> </div>
<p><b>5</b> Specify an easy-to-find base location (e.g., <b>%RootDrive%\ADAM\Instance</b>) and click <b>Next</b>.</p> <div> <p><b>File Locations</b> You can specify a location for each type of file associated with this instance of ADAM.</p> <p>Specify the locations to store files associated with ADAM.</p> <p>Data files: <input type="text" value="F:\ADAM\SSPR-1\data"/> <input type="button" value="Browse..."/></p> <p>Data recovery files: <input type="text" value="F:\ADAM\SSPR-1\recovery"/> <input type="button" value="Browse..."/></p> </div>	<p><b>6</b> Specify the run privileges and click <b>Next</b>.</p> <div> <p><b>Service Account Selection</b> ADAM performs operations using the permissions associated with the account you select.</p> <p>Set up ADAM to perform operations using the permissions associated with the following account.</p> <p><input type="radio"/> <b>Network service account</b> ADAM has the permissions of the default Windows service account.</p> <p><input checked="" type="radio"/> <b>This account:</b> ADAM has the permissions of the selected account. Ensure that the account you select is set up to run as a service.</p> <p>User name: <input type="text" value="QA\Administrator"/> <input type="button" value="Browse..."/></p> <p>Password: <input type="password" value="....."/></p> </div>

## 7 Specify the Administrative Permissions and click **Next**.



**ADAM Administrators**  
You can specify the user or group that will have administrative privileges for this instance of ADAM.

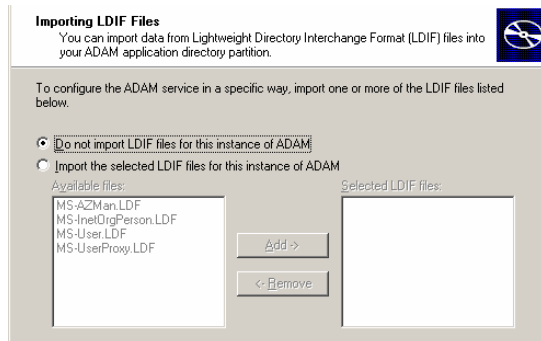
Assign the following user or group of users administrative permissions for ADAM.

☒ **Currently logged on user: QA\\Administrator**  
The user that is installing ADAM will have administrative permissions for this instance of ADAM.

☐ **This account**  
The selected user or group will have administrative permissions for this instance of ADAM. You can choose any user or group from this computer, this computer's domain, or any domain that is trusted by this computer's domain.

Account name:

## 8 Select **Do not import LDIF files for this instance of ADAM** and click **Next**.



**Importing LDIF Files**  
You can import data from Lightweight Directory Interchange Format (LDIF) files into your ADAM application directory partition.

To configure the ADAM service in a specific way, import one or more of the LDIF files listed below.

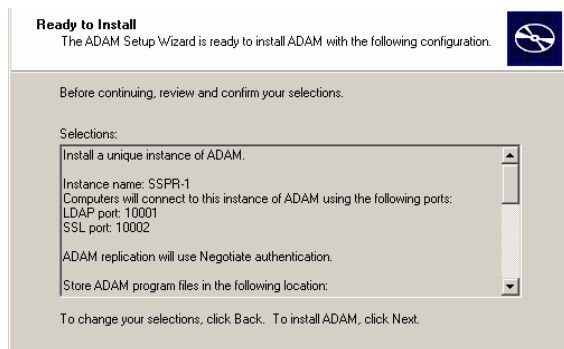
☒ **Do not import LDIF files for this instance of ADAM**

☐ Import the selected LDIF files for this instance of ADAM

Available files:  
MS-AZMan.LDF  
MS-InetOrgPerson.LDF  
MS-User.LDF  
MS-UserProxy.LDF

Selected LDIF files:

## 9 Click **Next** as requested to proceed.



**Ready to Install**  
The ADAM Setup Wizard is ready to install ADAM with the following configuration.

Before continuing, review and confirm your selections.

Selections:

Install a unique instance of ADAM.

Instance name: SSPP-1  
Computers will connect to this instance of ADAM using the following ports:  
LDAP port: 10001  
SSL port: 10002

ADAM replication will use Negotiate authentication.

Store ADAM program files in the following location:

To change your selections, click Back. To install ADAM, click Next.

## 10 Click **Finish**.



**Completing the Active Directory Application Mode Setup Wizard**

You have successfully completed the Active Directory Application Mode Setup Wizard.

## ITIM Support

### Installation and Setup

The normal TAM E-SSO: Desktop Password Reset Adapter installation includes the ITIM connector. To install ITIM support:

1. Install TAM E-SSO: Desktop Password Reset Adapter 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 will take effect immediately.
6. Turn on logging for the Java module by setting the **CREATE\_LOG** variable to **true**.

**Note:** All communications between TAM E-SSO: Desktop Password Reset Adapter 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.

---

## Appendix. Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing  
IBM Corporation  
North Castle Drive  
Armonk, NY 10504-1785  
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation  
Licensing  
2-31 Roppongi 3-chome, Minato-ku  
Tokyo 106-0032, Japan

**The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:**

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged should contact:

IBM Corporation  
2ZA4/101  
11400 Burnet Road  
Austin, TX 78758  
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

---

## Trademarks

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both:

AIX  
DB2  
developerWorks  
eServer  
IBM  
iSeries  
Lotus  
Passport Advantage  
pSeries  
RACF  
Rational  
Redbooks  
Tivoli  
WebSphere  
zSeries

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Intel, Intel Inside (logos), MMX and Pentium are trademarks of Intel Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a trademark of Linus Torvalds in the U.S., other countries, or both.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Other company, product, and service names may be trademarks or service marks of others.









Printed in USA

GI11-8068-01

