Installing Access Manager Agent for Microsoft SharePoint 2007

Author:	Jeff Nester Sun Microsystems Jeff.Nester@sun.com
Date:	06/22/09
Version	1.1 (Changed the encrypted replay password example)
Description:	Paraphrased version of the "***Sun Java System Access Manager Policy Agent 2.2 Guide for Microsoft IIS 6.0 With Outlook Web Access 2007/ SharePoint 2007***" specifically addressing the installation and configuration of the Access Manager Agent for SharePoint 2007.

Table of Contents

Installing Access Manager Agent for Microsoft SharePoint 2007

In order to simplify the steps for installing the Access Manager Agent for Microsoft SharePoint 2007, I have taken content from "***Sun Java System Access Manager Policy Agent 2.2 Guide for Microsoft IIS 6.0 With Outlook Web Access 2007/SharePoint 2007***" and created a step by step guide for installing the Agent. The original document can be found at http://docs.sun.com/app/docs/doc/820-4581

How does the Agent work?

The following describes the process that is implemented by the Agent to provide Single Sign On (SSO) to SharePoint:

1. User access the SharePoint app first time.
2. Agent checks for SSO cookie and since it doesn't find it, redirects to Access Manager for authentication
3. Authentication takes place at Access Manager and the post-auth plugin (ReplayPasswd) encrypts the password and set it as a session attribute.
4. The user is redirected to the SharePoint/Agent and the agent checks for the SSO token and then uses it and retrieves the encrypted password from the session.
5. It then decrypts the encrypted password and retrieves the original password, after which it does the base-64 encoding required by Basic Authentication.
6. It constructs the authorization header and sends it to IIS. And thus IIS allows the access to the resource.

Before You Begin

Access Manager must already be installed and running correctly. This document does not describe that process.

Locate the Agent zip file at https://cds.sun.com/is-bin/INTERSHOP.enfinity/WFS/CDS-CDS_SMI-Site/en_US/-/USD/ViewProductDetail-Start?ProductRef=Agt-2.2-01-IIS6.0-OTH-G-F@CDS-CDS_SMI

> **Note** – Prior to unzipping the product binaries, as shown in this task, you must copy the agent .zip file to a directory. For example, create a directory "Agents" in C:\ and copy the .zip file to that Agents directory. The directory to which you install the web agent is referred to as the Policy Agent base directory, or PolicyAgent-base.

For the directory scenario described in the preceding paragraph, the location of PolicyAgent-base varies as follows:

- The 64–bit Agent for IIS 6.0 version & the OWA 2007 version:
  These two versions of the agent use the following location for PolicyAgent-base:

  C:\Agents\iis_v6_x64_WINNT_agent\web_agents\iis6_agent

- The SharePoint 2007 version:

This version of the agent uses the following location for PolicyAgent-base:

C:\Agents\iis_v6_WINNT_agent\web_agents\iis6_agent

Unzip the product binaries.

Create Agent Deployment Configuration File

The agent for Microsoft IIS 6.0 provides a Visual Basic (VB) script to help you create agent configuration files. When you run it, the VB script prompts for information related to the Web Site Identifier, the agent you are installing, and Access Manager. The script creates an agent configuration file based on the information you provide.

> **Note** – When you are deploying the agent on multiple web sites, you must create a unique agent configuration file for each of the web sites. Use the following steps to create multiple agent configuration files. However, ensure that you give a unique file name to each of the configuration files.

1. Change to the directory:
   PolicyAgent-base\bin

   This directory stores the VB script required to create the agent configuration file.

2. Open a command window as described in the substeps that follow.
   a) Click Start.
   b) Select Run.
   c) Type cmd.

3. Issue the following command (be aware that the command is case sensitive):

   cscript IIS6CreateConfig.vbs defaultConfig

IIS6CreateConfig.vbs	A VB script that saves your responses to prompts about the Microsoft IIS 6.0 host and the Access Manager host in a file.For this example, the file is labeled defaultConfig.
defaultConfig	The agent configuration file created by this command and for which you provide the actual name. This is a text file to which the output of the commands entered while running the script are written.

> **Note** – Give a unique name for this agent configuration file since you will need the same file to unconfigure the agent. The script prompts for information as it progresses with the creation of the agent configuration file.

Configure AMConfig.properties file for Access Manager

In order to achieve SSO with Microsoft SharePoint using the Agent for Microsoft IIS 6.0, a post-authenitcation module is required to be deployed on Access Manager.

Perform the steps in this task on the Access Manager host.

1. Set the JAVA_HOME variable to the location in which JDK binaries are installed.
2. Execute DESgenKey.class as follows:

   # java -classpath am_sdk.jarPath com.sun.identity.common.DESGenKey
   where am_sdk.jarPath is a place holder for the path to the am_sdk.jar file.

   For example:

   java -classpath /opt/SUNWam/lib/am_sdk.jar com.sun.identity.common.DESGenKey

   Key ==> cIlz47oZBJs=

   Note – The am_sdk.jar file, which is an Access Manager JAR file, is typically found in the lib folder of the Access Manager installation, such as /opt/SUNWam/lib in a package installation or sun/webserver7/https-hostname/web-app/hostname/amserver/WEB-INF/lib in single war file installation.

3. Add the string produced in the previous step to a newly created text file as described in the substeps that follow:

   a) Copy the string produced in the previous step.
   b) Create a file, which for this example is named des_key.txt, in a directory of your choosing. The des_key.txt name is used in this guide as an example. Name the file differently if you wish.
   c) Save the copied string in the des_key.txt file.

4. Configure the com.sun.am.replaypasswd.key property in the AMConfig.properties configuration file as described in the substeps that follow.

   a) Open the AMConfig.properties configuration file.
   b) Add the following property to the file:

      com.sun.am.replaypasswd.key

   c) Copy the string from the des_key.txt file.
   d) Add the copied string as the value of the com.sun.am.replaypasswd.key property.

For example, if the string in the des_key.txt file is wuqUJyr=5Gc=, then the new property would be set as follows:

```
com.sun.am.replaypasswd.key = wuqUJyra5Gc=
```

5. Configure a property specific to Microsoft Office SharePoint in the AMConfig.properties file as described in the substeps that follow.
   a) Add the respective property and corresponding value to the file as indicated:

      For SharePoint, an optional property allows you to set an attribute in the Access Manager repository LDAP other than uid that allows users to log in to Access Manager to in turn log in to SharePoint:

      ```
      com.sun.am.sharepoint_login_attr_name = SharePoint-login-value
      ```

      where,SharePoint-login-value is a placeholder that represents an attribute in the user repository used by SharePoint to authenticate.

      For example:

      ```
      com.sun.am.sharepoint_login_attr_name = displayName
      ```

      The example purposes, a user has a uid of ak1234 and a displayName of andy. In this example, the user logs in to Access Manager using the uid (ak1234). However, the SharePoint repository has a record for andy, not ak1234, and the user uses andy to log in to the SharePoint application.

      Therefore, this property maps ak1234 to andy as the user accesses the SharePoint application after authenticating with Access Manager.

      In other words, this property provides a method for mapping any user attribute used by SharePoint to authenticate to the attribute used by Access Manager to authenticate.

   b) Save and close the AMConfig.properties file.

5. Restart Access Manager.

Configure the ReplayPasswd Post-Authenticaiton Plug-in for Access Manager

1. Deploy the post-authentication plug-in, ReplayPasswd, as described in the substeps that follow. This step requires the use of Access Manager Console.

   a) Log in to Access Manager as amadmin.
   b) With the Access Control tab selected, click the name of the realm you wish to configure.
   c) Click the Authentication tab.

d) Click Advanced Properties.
   The Advanced Properties button is in the General section.

e) Scroll down to the Authentication Post Processing Classes field.
f) Add the text related to Authentication Post Processing Classes in the manner appropriate for the Access Manager version you are using:

- Access Manager 7.0 series from Patch 7 forward
  For these patches of the Access Manager 7.0 series, execute the following substeps:

  i. In the Authentication Post Processing Classes field, enter the required text:

     ```
     com.sun.identity.authentication.spi.ReplayPasswd
     ```

  ii. Click Add.

- Access Manager 7.1 series from Patch 1 forward
  For these patches of the Access Manager 7.1 series, execute the following substeps:
  i. In the Authentication Post Processing Classes section, enter the required text:

     ```
     com.sun.identity.authentication.spi.ReplayPasswd
     ```

  ii. Click Add.

g) Click Save.
h) Click Log Out to log out of the Access Manager Console.

8) Verify the deployment of the post-authentication plug-in, RedplayPasswd, as described in the substeps that follow:
   a) Stop Access Manager.
   b) Access the AMConfig.properties configuration file.
   c) Note the value of the following property before changing it to message, as indicated:

      ```
      com.iplanet.services.debug.level = message
      ```

      You must change this value back to its original value at the completion of this step.

   d) Save and close the file.
   e) Start Access Manager.
   f) Log in to Access Manager Console using amadmin
   g) Click Log Out to immediately log out of the Access Manager Console.
   h) Change directories to the Access Manager debug log files.
   i) Verify the existence of a file named ReplayPasswd.

      The existence of this file indicates the successful deployment of the post-authentication plug-in.

j) Reset the debug value to its original value.
k) Restart Access Manager.

Deploy the Agent

1. Verify that settings are correct in the defaultConfig file.
2. Change to the following directory:

```
PolicyAgent-base\bin
```

3. Deploy the agent using the cscript command:

```
cscript SPAdmin.vbs -config defaultConfig
```

SPAdmin.vbs	SPAdmin.vbs VB scripts that can be used to install the required ISAPI filter. The SPAdmin.vbs script installs the ISAPI filter amsharepointfilter32.dll.
-config	The option that allows the output to be used to configure Agent for Microsoft IIS 6.0 to protect Microsoft SharePoint.

4. Accept the default when presented with the following prompt:

   Enter the Agent Resource File Name [IIS6Resource.en]:

   Here is an example of the execution:

```
The preceding prompt appears in the following context:

Microsoft (R) Windows Script Host Version 5.6
Copyright (C) Microsoft Corporation 1996-2001. All rights reserved.
Copyright c 2004 Sun Microsystems, Inc. All rights reserved

Use is subject to license terms

Enter the Agent Resource File Name [IIS6Resource.en]:

After you accept the default, a message such as the following should
appear:

Creating the Agent Config Directory
Creating the AMAgent.properties File
Updating the Windows Product Registry
Completed Configuring the IIS 6.0 Agent
```

Modify the Agent Properties File

For the task presented in this section, you must edit the web agent AMAgent.properties configuration file.

The same property and respective value added to the AMConfig.properties configuration file must now be added to the web agent AMAgent.properties configuration file.

1. Open the web agent AMAgent.properties configuration file.

2. Add the following property to the file:

   ```
   com.sun.am.replaypasswd.key
   ```

3. Copy the string from the des_key.txt file.
4. Add the copied string as the value of the com.sun.am.replaypasswd.key property.

   For example, if the string in the des_key.txt file is wuqUJyr=5Gc=, then the new property would be set as follows:

   ```
   com.sun.am.replaypasswd.key = wuqUJyra5Gc=
   ```

Configure SharePoint for Basic Authentication

To protect Microsoft SharePoint with this agent you must ensure that the authentication method for the Microsoft IIS 6.0 Server is set to Basic authentication as described below:

1. As an administrator, log in to Windows 2003 Server where Microsoft Office SharePoint is running.
2. In the Microsoft Windows Start menu, choose run.
3. Type the following: inetmgr
4. Click OK.
5. Expand the local computer.
6. Expand the Web Sites folder.
7. Right click the SharePoint site that you are protecting with the agent.

   The agent-protected SharePoint site is typically the site using port 80 (SharePoint — 80).

8. In the options list, click Properties.

   The Default Web Site Properties dialog box appears.

9. Select the Directory Security tab.
10. Click Edit in the Authentication and access control section.
11. Select Basic authentication in the Authenticated access section.

    Ensure that no other authentication option is checked.

12. Click OK.
13. Click OK again to close the Web site properties.

Modify the signout.aspx File to Properly Handle the Logout Process

It is necessary to modify the signout.aspx file so that when a users logs out of SharePoint they are also logged out of Access Manager. This is done by the following:

1. Back up the signout.aspx file.

   This file is typically available in the following directory:

   ```
   C:\Program Files\Common Files\Microsoft Shared\web serverextensions\12\TEMPLATE\LAYOUTS
   ```

2. Open the signout.aspx file.
3. Replace the lines of code indicated within this step.
   Original Code Snippet (replace this code snippet):

   ```
   function _spBodyOnLoad() {
      try {
         document.execCommand("ClearAuthenticationCache");

         }
      catch (e) {
         window.close();
         }
   }
   ```

   With the following (Note: replace the amHost and amPort with the correct values):

   ```
   function _spBodyOnLoad()
   {
        window.location="https://amHost:amPort/amserver/UI/Logout";
   }
   ```

4. Save and close the signout.aspx file.
5. Restart the Microsoft IIS 6.0 server using the iisreset command.

At this point the Agent is installed and should be working!