Sun OpenSSO Enterprise Policy Agent 3.0 Guide for Microsoft Internet Information Services (IIS) 6.0

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

Part No: 821–0334
December 8, 2009

091211@23031

Sun OpenSSO Enterprise Policy Agent 3.0 Guide for Microsoft Internet Information Services (IIS) 6.0

Last updated December 8, 2009

The IIS 6.0 policy agent is a version 3.0 web agent that functions with Sun™ OpenSSO Enterprise to protect resources deployed on Microsoft® Internet Information Services (IIS) 6.0.

Contents

For general information about web policy agents, including the new features for version 3.0 agents, see *Sun OpenSSO Enterprise Policy Agent 3.0 User's Guide for Web Agents*.

Supported Platforms, Compatibility, and Coexistence for the IIS 6.0 Agent

Supported Platforms for the IIS 6.0 Agent

TABLE 1 Supported Platforms for the IIS 6.0 Agent

Agent For	Support Platforms
Microsoft Internet Information Services (IIS) 6.0	Microsoft Windows Server 2003, 32–bit and 64–bit systems

- Minor versions of Microsoft IIS 6.0 are supported.
- Minor versions of the supported OS, including updates, service packs, and patches, are also supported.

Compatibility With Access Manager 7.1 and Access Manager 7 2005Q4

Access Manager 7.1 and Access Manager 7 2005Q4 are compatible with version 3.0 policy agents. However, because Access Manager 7.1 and Access Manager 7 2005Q4 do not support centralized agent configuration, a version 3.0 agent deployed with Access Manager must store its configuration data locally in the `OpenSSOAgentBootstrap.properties` and `OpenSSOAgentConfiguration.properties` files. The `OpenSSOAgentBootstrap.properties` file contains the information required for the agent to start and initialize itself.

A version 3.0 agent automatically detects the host server it is accessing. In the case of Access Manager 7.1 or Access Manager 7 2005Q4, a version 3.0 agent will switch to "local" mode and use the properties from the agent's `OpenSSOAgentConfiguration.properties` file.

Coexistence With Version 2.2 Policy Agents

OpenSSO Enterprise supports both version 3.0 and version 2.2 agents in the same deployment. The version 2.2 agents, however, must continue to store their configuration data locally in the `AMAgent.properties` file. And because the version 2.2 agent configuration data is local to the agent, OpenSSO Enterprise centralized agent configuration is not supported for version 2.2 agents. To configure a version 2.2 agent, you must continue to edit the agent's `AMAgent.properties` file.

For documentation about version 2.2 agents, see `http://docs.sun.com/coll/1322.1`.

Pre-Installation Tasks for the IIS 6.0 Agent

Meeting the Requirements for the IIS 6.0 Agent

Before you install the IIS 6.0 agent, your deployment must meet these requirements:

- Microsoft IIS 6.0 must be installed and configured on the Windows Server 2003 host.
- An OpenSSO Enterprise server instance must be installed and accessible to Microsoft IIS 6.0 and the Windows Server 2003 host.

Downloading and Unzipping the IIS 6.0 Agent Distribution File

▼ To Download and Unzip the IIS 6.0 Agent Distribution File

1. **Login into the server where you want to install the agent.**
2. **Create a directory to unzip the agent distribution file.**
3. **Download and unzip the agent distribution file, depending on your platform:**

Platform	Distribution File
Windows 2003 Server, 32-bit systems	`iis_v6_WINNT_agent_3.zip`
Windows 2003 Server, 64-bit systems	`iis_v6_WINNT_x64_agent_3.zip`

These distribution files are available from the following sites:

- Sun Downloads under View by Category, Identity Management, and Policy Agents: `http://www.sun.com/download/index.jsp`
- OpenSSO project: `https://opensso.dev.java.net/public/use/index.html`

The following table shows the files and directories after you unzip the agent distribution file. These files are in the following directory:

AgentHome`\web_agents\iis6_agent`

where *AgentHome* is where you unzipped the agent distribution file. For example: `C:\Agents\web_agents\iis6_agent`

File or Directory	Description
`README` and `license.txt`	Readme and license files
`\bin`	■ `IIS6CreateConfig.vbs` and `IIS6Admin.vbs` scripts ■ `IIS6Resource.en` resource file (English version) ■ `certutil.exe` and `cryptit.exe` utilities ■ `dll` and other supporting files
`\config`	Template and properties files

Creating an Agent Profile

The IIS 6.0 agent uses an agent profile to communicate with OpenSSO Enterprise server.

To create an agent profile use either of these methods:

- Use the OpenSSO Enterprise Console, as described in this section.
- Use the `ssoadm` command-line utility with the `create-agent` subcommand. For more information about the `ssoadm` command, see the *Sun OpenSSO Enterprise 8.0 Administration Reference*.

▼ To Create an Agent Profile in the OpenSSO Enterprise Console

1. **Login into the OpenSSO Enterprise Administration Console as `amadmin`.**
2. **Click `Access Control`, *realm-name*, `Agents`, and `Web`.**
3. **Under `Agent`, click `New`.**
4. **In the `Name` field, enter the name for the new agent profile. For Example: `IIS6AgentProfile`**
5. **Enter and confirm the `Password`.**
6. **In the `Configuration` field, check the location where the agent configuration properties are stored:**
   - `Local`: In the `OpenSSOAgentConfiguration.properties` file on the server where the agent is installed.
   - `Centralized` (default): In the OpenSSO Enterprise server central configuration data repository.

7. **In the `Server URL` field, enter the OpenSSO Enterprise server URL.**

   For example: `http://openssohost.example.com:8080/opensso`

8. **In the `Agent URL` field, enter the URL for the agent.**

   For example: `http://agenthost.example.com:80`

9. **Click `Create`.**

   The console creates the agent profile and displays the Web agent page again with a link to the new agent profile.

   To do additional configuration for the agent, click the specific link to display the `Edit` agent page. For information about the agent configuration fields, see the Console online Help.

   If you prefer, you can also use the `ssoadm` command-line utility to edit the agent profile. For more information, see the *Sun OpenSSO Enterprise 8.0 Administration Reference*.

Creating a Password File

A password file is an ASCII text file with only one line specifying a password in clear text. By using a password file, you are not forced to expose a password at the command line.

When you create the IIS 6.0 agent configuration file using the `IIS6CreateConfig.vbs` script, you will be prompted to specify the path to the IIS 6.0 agent profile password file.

If you plan to use the `ssoadm` utility to manage the IIS 6.0 agent, you will also need a password file to store the password for the agent administrator (which can be `amadmin`, if you prefer).

▼ To Create a Password File

1. **Create an ASCII text file for the password file. For example, for an agent profile:**
   `C:\tmp\IIS6Agentpw.txt`

2. **Using a text editor, enter the appropriate password in clear text on the first line of the password file.**

3. **Secure the password file appropriately, depending on the requirements for your deployment.**

Creating an Agent Administrator (Optional)

Creating an agent administrator is optional. An agent administrator can manage agents in OpenSSO Enterprise, using either the OpenSSO Enterprise Console or by executing the `ssoadm` utility.

▼ To Create an Agent Administrator in the OpenSSO Console

1. **Login to OpenSSO Enterprise Console as** `amadmin`**.**
2. **Create a new agents administrator group:**
   a. **Click** `Access Control`**,** *realm-name*`, Subjects`**, and then** `Group`**.**
   b. **Click** `New`**.**
   c. **In** `ID`**, enter the name of the group. For example:** `AgentAdministrators`
   d. **Click** `OK`**.**
3. **Create a new agent administrator user and add the agent administrator user to the agents administrator group:**
   a. **Click** `Access Control`**,** *realm-name*`, Subjects`**, and then** `User`**.**
   b. **Click** `New` **and provide the following values:**
      - **ID**: Name of the agent administrator. For example: `AgentAdmin`
        This is the name you will use to login to the OpenSSO Enterprise Console .
      - **First Name** (optional), **Last Name**, and **Full Name**.
        For simplicity, use the same name for each of these values that you specified in the previous step for ID.
      - **Password** (and confirmation)
      - **User Status**: Active
   c. **Click** `OK`**.**
   d. **Click the new agent administrator name.**
   e. **On the** `Edit User` **page, click** `Group`**.**
   f. **Add the agents administrator group from** `Available` **to** `Selected`**.**
   g. **Click** `Save`**.**
4. **Assign read and write access to the agents administrator group:**
   a. **Click** `Access Control`**,** *realm-name*`, Privileges` **and then on the new agents administrator group link.**

b. **Check** `Read and write access to all configured Agents`.

c. **Click** `Save`.

Next Steps Login into the OpenSSO Enterprise Console as the new agent administrator. The only available top-level tab is `Access Control`. Under *realm-name*, you will see only the `Agents` tab and sub tabs.

Installing the IIS 6.0 Agent

Gathering Information to Install and Configure the IIS 6.0 Agent

The following table describes the information you will need to provide when you install and configure the IIS 6.0 agent.

TABLE 2 Information Required to Install and Configure the IIS 6.0 Agent

Script	Prompt
`IIS6CreateConfig.vbs`	IIS 6.0 agent prompts: ■ Agent Resource File Name: Default is `IIS6Resource.en` (English version) ■ Agent URL: For example `http://agenthost.example.com:80` ■ Web Site Identifier: Accept value from the displayed list. Sun OpenSSO Enterprise prompts: ■ OpenSSO server URL, including the deployment URI: For example `http://openssohost.example.com:8080/opensso` ■ Agent Profile name: For example `IIS6AgentProfile` ■ Path to password file: For example `C:\tmp\IIS6Agentpw.txt`
`IIS6Admin.vbs`	Agent Resource File Name: Default is `IIS6Resource.en` (English version)

Installing and Configuring the IIS 6.0 Agent

Creating a Configuration File for the IIS 6.0 Agent

The `IIS6CreateConfig.vbs` script creates the IIS 6.0 agent configuration file. The `IIS6CreateConfig.vbs` script prompts you for information and then creates a configuration file that you can use later to configure the IIS 6.0 agent.

You must have Administrator privileges to run the `IIS6CreateConfig.vbs` script.

Note: If you are deploying the IIS 6.0 agent on multiple Web sites, you must create a unique agent configuration file for each of the Web sites.

▼ To Create a Configuration File for the IIS 6.0 Agent

1. **On the Windows 2003 Server instance, open a command window. For example, click Start, Run, and then type `cmd`.**

2. **Change to the *PolicyAgent-base*`\bin` directory.**

   where *PolicyAgent-base* depends where you unzipped the IIS 6.0 agent distribution file. For example:

   For example: `C:\Agents\web_agents\iis6_agent\bin`

   The `\bin` directory contains the `IIS6CreateConfig.vbs` script, which you run to create the agent configuration file.

3. **Create the agent configuration file by issuing the following case-sensitive command:**

   `cscript IIS6CreateConfig.vbs` *ConfigFile*

   where *ConfigFile* is the unique name for agent configuration file.

   For example: `cscript IIS6CreateConfig.vbs IIS6Config.txt`

   The `IIS6CreateConfig.vbs` script creates this file and then saves your responses to prompts about the agent host and the OpenSSO Enterprise server in the file.

4. **When prompted, provide the following information about the IIS 6.0 server that this agent will protect:**

   - **Agent Resource File Name**: Accept the default value `IIS6Resource.en` (English version).
   - **Agent URL:** : Specify the URL for the IIS 6.0 agent including the port number. For example: `http://agenthost.example.com:80`
   - **Web Site Identifier**: Specify the unique identifier associated with the Web site for which you are creating a configuration file. Accept a value from the displayed list.

5. **When prompted, provide the following information about the OpenSSO Enterprise host:**

- **OpenSSO server URL, including the deployment URI:** For example: `http://openssohost.example.com:8080/opensso`
- **Agent Profile name**: For example: `IIS6AgentProfile`.
- **Agent Profile password File**: Path to the file that contains the agent profile password. For example: `C:\tmp\IIS6Agentpw.txt`

Example 1 Sample `IIS6CreateConfig.vbs` Script Run

```
Microsoft (R) Windows Script Host Version 5.6
Copyright (C) Microsoft Corporation 1996-2001. All rights reserved.


Copyright c 2009 Sun Microsystems, Inc. All rights reserved
Use is subject to license terms
-----------------------------------------------------------
    Microsoft (TM) Internet Information Server (6.0)
-----------------------------------------------------------
Enter the Agent Resource File Name [IIS6Resource.en] :

Enter the Agent URL (Example: http://agent.example.com:80) :
http://agent.example.com:80

Displaying the list of Web Sites and its corresponding Identifiers
Site Name (Site Id)
Default Web Site (1)
testPolicy (204642793)
Test2 (223085047)

Web Site Identifier :
1
-----------------------------------------------
Sun OpenSSO Enterprise 8.0
-----------------------------------------------
Enter the URL where the OpenSSO server is running.
Please include the deploymentURI also as shown in the example
(Example: http://opensso.example.com:58080/opensso):
http://openssohost.example.com:8080/opensso

Please enter the Agent Profile name :
IIS6AgentProfile

Enter the Agent profile password file :
c:\tmp\IIS6Agentpw.txt

-----------------------------------------------------
Agent Configuration file created : IIS6AgentConfig.txt
-----------------------------------------------------
```

Configuring the IIS 6.0 Agent for a Web Site

The `IIS6Admin.vbs` script configures the IIS 6.0 agent for a specific Web site, based on an agent configuration file created by the `IIS6CreateConfig.vbs` script.

You must have Administrator privileges to run the `IIS6Admin.vbs` script.

The `IIS6Admin.vbs` script performs these functions:

- Creates a subdirectory named `Identifier_`*id* under the `web_agents\iis6_agent` directory, where *id* is the Web site identifier. This directory contains the IIS 6.0 agent's `\config` and `\logs` directories.
- Creates the `OpenSSOAgentBootstrap.properties` and `OpenSSOAgentConfiguration.properties` files for the IIS 6.0 agent using the agent configuration file created by the `IIS6CreateConfig.vbs` script.
- Updates the Windows registry with the location of properties file.
- Adds the wildcard ISAPI extension to the Web site for which the agent is configured.

Note: To configure the IIS 6.0 agent for multiple Web sites, follow this procedure for each Web site, using a unique agent configuration file for each site.

▼ To Configure the IIS 6.0 Agent for a Web Site

1. **On the Windows 2003 Server instance, open a command window. For example, click Start, Run, and then type** `cmd`**.**

2. **Change to the** *PolicyAgent-base*`\bin` **directory.**

   where *PolicyAgent-base* depends where you unzipped the IIS 6.0 agent distribution file. For example:

   For example: `C:\Agents\web_agents\iis6_agent\bin`

3. **Configure the Web site for the IIS 6.0 agent by running the** `IIS6Admin.vbs` **script with the** `-config` **option.**

   For example: `cscript IIS6Admin.vbs -config IIS6AgentConfig.txt`

   where `IIS6Config.txt` is the agent configuration file that you created in "Creating a Configuration File for the IIS 6.0 Agent" on page 10.

   Notes:

   - The script name and options are case-sensitive.
   - For the Agent Resource File Name prompt, accept the default value (`IIS6Resource.en`).

The `IIS6Admin.vbs` script displays the progress of the configuration, as shown in the following sample:

```
Microsoft (R) Windows Script Host Version 5.6
Copyright (C) Microsoft Corporation 1996-2001. All rights reserved.

Copyright c 2009 Sun Microsystems, Inc. All rights reserved
Use is subject to license terms

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

Creating the Agent Config Directory
Creating the OpenSSOAgentBootstrap.properties
    and OpenSSOAgentConfiguration.properties File
Updating the Windows Product Registry
Loading the IIS 6.0 Agent
Completed Configuring the IIS 6.0 Agent
```

4. **Ensure that the IIS 6.0 authentication method is set to Anonymous.**

5. **Restart IIS 6.0 using the `iisreset` command. For example, in a command prompt, type `iisreset`.**

Next Steps To view the agent log file (`amAgent`), see *PolicyAgent-base*`\debug\Identifier_`*site-identifier*`\logs\debug`, where *site-identifier* is a number such as 1 that identifies the Web site where the IIS 6.0 agent is being configured.

Verifying an IIS 6.0 Agent Installation

▼ To Verify an IIS 6.0 Agent Installation

1. **Attempt to access a resource protected by the IIS 6.0 agent.**

   If the agent is installed correctly, accessing the protected resource will redirect you to the OpenSSO Enterprise server login page.

2. **Log in to the OpenSSO Enterprise server.**

   After a successful authentication, you should be able to access the protected resource, if the agent is correctly defined and an Allow policy is set for you for that resource.

Considering Specific Deployment Scenarios for the IIS 6.0 Agent

Installing the IIS 6.0 Agent on Multiple IIS 6.0 Servers

After you install the IIS 6.0 agent on a specific IIS 6.0 server, you can install the agent on another IIS 6.0 server instance by running the `IIS6CreateConfig.vbs` and `IIS6Admin.vbs` scripts again for the new server instance.

You can also just copy and edit an existing IIS 6.0 agent configuration file, providing new values for the new IIS 6.0 server instance. Then, run the `IIS6Admin.vbs` script using the edited agent configuration file.

The `IIS6Admin.vbs` script creates the `OpenSSOAgentBootstrap.properties` and `OpenSSOAgentConfiguration.properties` files for the new server instance, so you do not need to copy and edit these files manually for the new instance.

Installing the IIS 6.0 Agent on the OpenSSO Enterprise Host Server

OpenSSO Enterprise is not supported on the web container. Therefore, installing the IIS 6.0 agent and OpenSSO Enterprise on the same server instance is not supported.

Post-Installation Tasks for the IIS 6.0 Agent

Creating and Adding Logout URLs in a CDSSO Deployment

If Cross-Domain Single Sign-On (CDSSO) is enabled for the agent, the OpenSSO logout URL cannot clear the cookies in the agent domain, and you must create two logout pages as IIS 6.0 resources.

▼ To Create the Logout URL Pages

1 **Create two logout URL pages as IIS 6.0 resources. For example:** `logout.html` **and** `logout2.html`

2. **Store the logout URL pages in the `doc` directory of the IIS 6.0 instance. The default directory is `C:\inetpub\wwwroot`.**

3. **Make sure you can access the logout URLs from a browser. For example:**
   - `http://agenthost.example.com:port/logout.html`
   - `http://agenthost.example.com:port/logout2.html`

▼ To Add the Logout URLs in the OpenSSO Console

1. **Login to the OpenSSO console as `amadmin`.**
2. **Click Access Control, *realm-name*, Agents, and then the profile name for the IIS 6.0 agent.**
3. **On the agent Edit page, click OpenSSO Services.**
4. **Under Agent Logout URL, add the logout URLs. For example:**
   - **Logout URL**: `http://agenthost.example.com:port/logout.html`
   - **Logout Redirect URL**: `http://agenthost.example.com:port/logout2.html`
5. **Click Save.**
6. **On the agent Edit page, click Application.**
7. **Add the same URLs as Not Enforced URLs:**
   - `http://agenthost.example.com:port/logout.html`
   - `http://agenthost.example.com:port/logout2.html`
8. **Click Save.**

Next Steps The logout links in an application deployed on the IIS 6.0 instance should invoke the logout URL used in this procedure.

Using SSL With the IIS 6.0 Agent (Optional)

If you specify the `https` protocol for the OpenSSO Enterprise server URL during the IIS 6.0 agent installation, the agent is automatically configured and ready to communicate to the OpenSSO Enterprise server over Secure Sockets Layer (SSL). However, to ensure that the IIS 6.0 agent is configured for SSL communication to the server, follow these tasks:

- "Installing the OpenSSO Enterprise Root CA Certificate on the IIS 6.0 Agent" on page 16
- "Disabling the Trust Behavior for the IIS 6.0 Agent " on page 17

Installing the OpenSSO Enterprise Root CA Certificate on the IIS 6.0 Agent

The root CA certificate that you install on the IIS 6.0 agent must be the same certificate that is installed on the OpenSSO Enterprise host server.

Sun provides the Certificate Database Tool, `certutil.exe`, in the IIS 6.0 agent distribution file, to manage the root CA certificate and the certificate database.

For information about using `certutil.exe`, see `http://www.mozilla.org/projects/security/pki/nss/tools/certutil.html`.

▼ To Install the OpenSSO Enterprise Root CA Certificate on the IIS 6.0 Agent

1. **Obtain the root CA certificate file that is installed on the OpenSSO Enterprise host server. The following examples use `root_ca.crt` as the name for the root CA certificate file.**

2. **On the IIS 6.0 server, locate the `certutil.exe` utility.**

   After you unzip the IIS 6.0 agent distribution file, `certutil.exe` is available in the *PolicyAgent-base*`\bin` directory.

   For example: `C:\Agents\web_agents\iis6_agent\bin\certutil.exe`

3. **If necessary, create the certificate database directory and the certificate database in the *PolicyAgent-base* directory. For example:**

   ```
   mkdir C:\Agents\web_agents\iis6_agent\cert
   C:\Agents\web_agents\iis6_agent\bin certutil.exe -N -d ..\cert
   ```

   where `cert` is the name of the certificate database directory.

   When prompted, enter and confirm the password that will be used to encrypt your keys.

4. **Install the OpenSSO Enterprise root CA certificate in the database. For example:**

   ```
   certutil.exe -A -n am_root_ca_cert -t "C,C,C" -d ..\cert -i ..\cert\root_ca.crt
   ```

   where:

   - `am_root_ca_cert` is the name of the OpenSSO Enterprise root CA certificate.
   - `root_ca.crt` is the binary root CA certificate request file.

5. **To verify that the root CA certificate is installed correctly, use `certutil.exe` with the `-L` option. For example:**

   ```
   C:\Agents\web_agents\iis6_agent\bin certutil.exe -L -d ..\cert am_root_ca_cert
   ```

You should see the name of the root CA certificate. For example:

```
am_root_ca_cert                                                C,C,C
```

Disabling the Trust Behavior for the IIS 6.0 Agent

By default, the IIS 6.0 agent installed on a remote IIS 6.0 server trusts any server certificate presented over SSL by the OpenSSO Enterprise host. For the IIS 6.0 agent to perform certificate checking, you must disable this trust behavior.

▼ To Disable the Trust Behavior for the IIS 6.0 Agent

1. **Find the IIS 6.0 agent's `OpenSSOAgentBootstrap.properties` file in the agent's `\config` directory. For example:**

   ```
   C:\Agents\web_agents\iis6_agent\config\OpenSSOAgentBootstrap.properties
   ```

2. **In the `OpenSSOAgentBootstrap.properties` file, set the SSL-related properties, depending on your specific deployment.**

   Note: These properties have new names for version 3.0 web agents.

   - Disable the option to trust the server certificate sent over SSL by the OpenSSO Enterprise host server:

     ```
     com.sun.identity.agents.config.trust.server.certs = false
     ```

   - Specify the certificate database directory.

     ```
     com.sun.identity.agents.config.sslcert.dir = path-to-cert-database
     ```

     For example:

     ```
     com.sun.identity.agents.config.sslcert.dir = C:/Agents/web_agents/iis6_agent/cert
     ```

   - If the certificate database directory has multiple certificate databases, set the following property to the prefix of the database you want to use. For example:

     ```
     com.sun.identity.agents.config.certdb.prefix = prefix-
     ```

   - Specify the certificate database password:

     ```
     com.sun.identity.agents.config.certdb.password = password
     ```

   - Specify the certificate database alias:

     ```
     com.sun.identity.agents.config.certificate.alias = alias-name
     ```

3. **Save the changes to the `OpenSSOAgentBootstrap.properties` file.**

   The agent uses information in the `OpenSSOAgentBootstrap.properties` file to start and initialize itself and to communicate with OpenSSO Enterprise server.

4. **Restart IIS 6.0 using the `iisreset` command.**

Setting the Post Data Preservation Load Balancer Cookie (Optional)

If a load balancer is configured in front of multiple agent instances and post data preservation is enabled in these agent instances, you must specify the post data preservation load balancer cookie by setting the following property in the OpenSSO Console:

`com.sun.identity.agents.config.postdata.preserve.lbcookie`

This property specifies the name and value of the sticky cookie used by the load balancer to route the incoming request.

▼ To Set the Post Data Preservation Load Balancer Cookie

1. **Login to the OpenSSO Console as** `amadmin`**.**
2. **Click Access Control,** *realm-name*, **Agents, and then the profile name for the IIS 6.0 agent.**
3. **Click Advanced.**
4. **Scroll down to Custom Properties and add the** `com.sun.identity.agents.config.postdata.preserve.lbcookie` **property. For example:**

   ```
   com.sun.identity.agents.config.postdata.preserve.lbcookie = palbcookie=01
   ```

5. **Click Save.**

Ignoring the Path for Not Enforced URLs (Optional)

The `com.sun.identity.agents.config.ignore.path.info.for.not.enforced.list` property indicates whether the path information and query should be removed from the request URL before it is compared with not-enforced URLs, when those URLs have a wildcard (*) character.

For security reasons, this property should be set to `true`, to avoid certain situations. For example, if a not-enforced URL such as `http://host/*.gif` exists, someone can access `http://host/index.html` by using the request URL `http://host/index.html/hack.gif`.

The default value for `com.sun.identity.agents.config.ignore.path.info.for.not.enforced.list` is `true`. If necessary, you can set is property in the OpenSSO Console.

▼ To Ignore the Path for Not Enforced URLs

1. **Login to the OpenSSO Console as** `amadmin`**.**
2. **Click Access Control,** *realm-name*, **Agents, and then the profile name for the IIS 6.0 agent.**
3. **Click Advanced.**
4. **Scroll down to Custom Properties and add the following property:**

   ```
   com.sun.identity.agents.config.ignore.path.info.for.not.enforced.list=true
   ```

5. **Click Save.**

Changing the Password for an Agent Profile (Optional)

This task is optional. After you install the agent, you can change the agent profile password, if required for your deployment.

▼ To Change the Password for an Agent Profile

1. **On the OpenSSO Enterprise server:**
   a. **Login into the Administration Console.**
   b. **Click Access Control,** *realm-name*, **Agents, Web, and then the name of the agent you want to configure.**

      The Console displays the Edit page for the agent profile.

   c. **Enter and confirm the new unencrypted password.**
   d. **Click** `Save`**.**
2. **On the server where the IIS 6.0 agent is installed:**
   a. **In the agent profile password file, replace the old password with the new unencrypted password.**
   b. **Change to the** *PolicyAgent-base*`\bin` **directory. For example:**

      ```
      cd C:\Agents\web_agents\iis6_agent\bin
      ```

   c. **Encrypt the new password using** `cryptit.exe`**.**

      ```
      cryptit.exe C:\tmp\IIS6Agentpw.txt encryption-key
      ```

where *encryption-key* can be either the existing key value from the `com.sun.identity.agents.config.key` property in the IIS 6.0 agent's `OpenSSOAgentBootstrap.properties` file or a new encryption key value. A new key value must be a minimum of eight alphanumeric characters.

The `cryptit.exe` program returns the new encrypted password. For example:

```
/54GwN432q+MEnfh/AHLMA==
```

d. In the IIS 6.0 agent's `OpenSSOAgentBootstrap.properties` file, set the following properties, as needed:

- Set the following property to the new encrypted password from the previous step. For example:

  ```
  com.sun.identity.agents.config.password=/54GwN432q+MEnfh/AHLMA==
  ```

- If you specified a new encryption key value in the previous step, set the following property to this new key value:

  ```
  com.sun.identity.agents.config.key=new-key-value
  ```

e. Restart the IIS 6.0 server.

Managing the IIS 6.0 Agent

Managing a Version 3.0 Agent With a Centralized Configuration

OpenSSO Enterprise stores version 3.0 policy agent configuration data (as well as server configuration data) in a centralized data repository. You manage this configuration data using these options:

- OpenSSO Enterprise Administration Console

  You can manage both version 3.0 J2EE and web agents from the OpenSSO Enterprise Console. Tasks that you can perform include creating, deleting, updating, listing, and displaying agent configurations. Using the Console, you can set properties for an agent that you previously set by editing the agent's `AMAgent.properties` file.

  For more information, refer to the Administration Console online Help.

- `ssoadm` command-line utility

The `ssoadm` utility is the command-line interface to OpenSSO Enterprise server and is available after you install the tools and utilities in the `openssoAdminTools.zip` file. The `ssoadm` utility includes subcommands to manage policy agents, including:

- Creating, deleting, updating, listing, and displaying agent configurations
- Creating deleting, listing, and displaying agent groups
- Adding and removing an agent to and from a group

For information about the `ssoadm` utility, including the syntax for each subcommand, see the *Sun OpenSSO Enterprise 8.0 Administration Reference*.

Managing a Version 3.0 Agent With a Local Configuration

In some scenarios, you might need to deploy the IIS 6.0 agent using a local configuration. For example, if you deploy the agent with Access Manager 7.1 or Access Manager 7 2005Q4, which do not support centralized agent configuration, local configuration is used by default.

If you are creating a new agent profile in the OpenSSO Console, set Configuration to Local.

To specify a local configuration for an existing agent profile, edit the agent profile in the OpenSSO Console:

1. Log in to the Console as `amadmin`.
2. Click Access Control, *realm-name*, Agents, Web, and then the name of the agent profile you want to edit.

   The Console displays the Edit page for the agent profile.
3. On the Edit page, check Local for Location of Agent Configuration Repository.
4. Click Save.

For a local configuration, you manage the IIS 6.0 agent by editing properties in the agent's local `OpenSSOAgentConfiguration.properties` file (in the same manner that you edit the `AMAgent.properties` file for version 2.2 agents).

The IIS 6.0 agent also stores configuration information in the local `OpenSSOAgentBootstrap.properties` file. The agent uses information in the bootstrap file to start and initialize itself and to communicate with OpenSSO Enterprise server. In most cases, you won't need to edit the bootstrap file; however, if you do edit the file, be careful, or the agent might not function properly.

Uninstalling the IIS 6.0 Agent

You uninstall the IIS 6.0 agent for a specific IIS 6.0 server instance by running the `IIS6Admin.vbs` script with the `-unconfig` option.

You must have Administrator privileges to run the `IIS6Admin.vbs` script.

▼ To Uninstall the IIS 6.0 Agent

1. **On the Windows 2003 Server instance, open a command window. For example, click Start, Run, and then type `cmd`.**

2. **Change to the *PolicyAgent-base*`\bin` directory.**

   where *PolicyAgent-base* depends where you unzipped the IIS 6.0 agent distribution file. For example:

   For example: `C:\Agents\web_agents\iis6_agent\bin`

3. **Run the `IIS6Admin.vbs` script with the `-unconfig` option. Both the script name and `-unconfig` option are case-sensitive.**

   For example: `cscript IIS6Admin.vbs -unconfig IIS6AgentConfig.txt`

   where `IIS6Config.txt` is the agent configuration file for the IIS 6.0 agent on the specific IIS 6.0 server instance.

   For example:

   ```
   Microsoft (R) Windows Script Host Version 5.6
   Copyright (C) Microsoft Corporation 1996-2001. All rights reserved.

   Copyright c 2009 Sun Microsystems, Inc. All rights reserved
   Use is subject to license terms

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

   Removing the Agent Bootstrap file
   Removing the Agent Config file
   Removing the Agent Config Directory
   C:\Agents\web_agents\iis6_agent\Identifier_1\config
   Removing the entries from Windows Product Registry
   Unloading the IIS6 Agent
   Completed Unconfiguring the IIS 6.0 Agent
   ```

4. **Restart IIS 6.0 using the `iisreset` command.**

Sun Microsystems Related Information

Additional Sun Resources

You can find additional useful information and resources at the following locations:

- Sun Services: `http://www.sun.com/service/consulting/`
- Sun Software Products: `http://wwws.sun.com/software/`
- Sun Support Resources `http://sunsolve.sun.com/`
- Sun Developer Network (SDN): `http://developers.sun.com/`
- Sun Developer Services: `http://www.sun.com/developers/support/`

Accessibility Features for People With Disabilities

To obtain accessibility features that have been released since the publishing of this media, consult Section 508 product assessments available from Sun upon request to determine which versions are best suited for deploying accessible solutions.

For information about Sun's commitment to accessibility, visit `http://sun.com/access`.

Related Third-Party Web Sites

Third-party URLs are referenced in this document and provide additional, related information.

Note – Sun is not responsible for the availability of third-party Web sites mentioned in this document. Sun does not endorse and is not responsible or liable for any content, advertising, products, or other materials that are available on or through such sites or resources. Sun will not be responsible or liable for any actual or alleged damage or loss caused by or in connection with the use of or reliance on any such content, goods, or services that are available on or through such sites or resources.

How to Report Problems and Provide Feedback

If you have questions or issues with OpenSSO Enterprise, contact Sun as follows:

- Sun Support Resources (SunSolve) services at `http://sunsolve.sun.com/`.

This site has links to the Knowledge Base, Online Support Center, and ProductTracker, as well as to maintenance programs and support contact numbers.

- The telephone dispatch number associated with your maintenance contract

So that we can best assist you in resolving problems, please have the following information available when you contact support:

If you are requesting help for a problem, please include the following information:

- Description of the problem, including when the problem occurs and its impact on your operation
- Machine type, operating system version, web container and version, JDK version, and OpenSSO Enterprise version, including any patches or other software that might be affecting the problem
- Steps to reproduce the problem
- Any error logs or core dumps

Sun Welcomes Your Comments

Sun is interested in improving its documentation and welcomes your comments and suggestions. To share your comments, go to `http://docs.sun.com/` and click `Feedback`. In the online form, provide the full document title and part number. The part number is a 7-digit or 9-digit number that can be found on the title page or in the document's URL. For example, the title of this guide is *Sun OpenSSO Enterprise Policy Agent 3.0 Guide for Microsoft IIS 6.0*, and the part number is 821-0334.

Revision History

Part Number	Date	Description
821-0334–10	December 8, 2009	Initial release.