Sun OpenSSO Enterprise Policy Agent 3.0 Guide for Microsoft Internet Information Services (IIS) 7.0

Part No: 821–0267–11
July 8, 2011

110713@25097

Sun OpenSSO Enterprise Policy Agent 3.0 Guide for Microsoft Internet Information Services (IIS) 7.0

The IIS 7.0 policy agent is a version 3.0 web agent that functions with Oracle OpenSSO to protect resources deployed on Microsoft Internet Information Services (IIS) 7.0.

Contents

For general information about web policy agents, including the new features for version 3.0 agents, see the *OpenSSO Enterprise Policy Agent 3.0 User's Guide for Web Agents* in `http://download.oracle.com/docs/cd/E19681-01/index.html`.

Supported Platforms, Compatibility, and Coexistence for the IIS 7.0 Agent

Supported Platforms for the IIS 7.0 Agent

TABLE 1 Supported Platforms for the IIS 7.0 Agent

Agent For	Support Platforms
Microsoft IIS 7.0	Microsoft Windows Server 2008, 32–bit and 64–bit systems
Microsoft IIS 7.0 with Microsoft Office SharePoint Server 2010	Microsoft Windows Server 2008, 64–bit systems Microsoft Windows Server 2008 R2, 64–bit systems **Note**. The agent for IIS 7.0 with Microsoft Office SharePoint Server 2010 is supported with OpenSSO Enterprise 8.0 and later releases.

- Minor versions of Microsoft IIS 7.0 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

Oracle OpenSSO 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 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://download.oracle.com/docs/cd/E19534-01/index.html`.

Unsupported OpenSSO Features

The IIS 7.0 agent does not support POST data preservation.

Pre-Installation Tasks for the IIS 7.0 Agent

- "Meeting the Requirements for the IIS 7.0 Agent" on page 5
- "Downloading and Unzipping the IIS 7.0 Agent Distribution File" on page 5
- "Creating an Agent Profile" on page 6
- "Creating a Password File" on page 7
- "Creating an Agent Administrator (Optional)" on page 8

Meeting the Requirements for the IIS 7.0 Agent

Before you install the IIS 7.0 agent, your deployment must meet these requirements:

- Microsoft IIS 7.0 must be installed and configured on the Windows Server 2008 host.
- An OpenSSO server instance must be installed and accessible to Microsoft IIS 7.0 and the Windows Server 2008 host.

Downloading and Unzipping the IIS 7.0 Agent Distribution File

▼ To Download and Unzip the IIS 7.0 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	Agent Distribution File
Windows Server 2008, 32-bit systems	`iis_v7_WINNT_agent_3.zip`
Windows Server 2008, 64-bit systems	`iis_v7_WINNT_x64_agent_3.zip`
Windows Server 2008, 64-bit systems running IIS 7.0 with Office SharePoint Server 2010	`iis_v7_WINNT_x64_agent_3.zip` **Note**. To deploy the IIS 7.0 agent with Windows Server 2008 running IIS 7.x with Office SharePoint Server 2010, you must obtain the latest 64–bit agent distribution file.

The distribution files are available on the following site: https://edelivery.oracle.com/.

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\iis7_agent`

where *AgentHome* is where you unzipped the agent distribution file. For example: `C:\Agents\web_agents\iis7_agent`

File or Directory	Description
`README` and `license.txt`	Readme and license files
`\bin`	■ `IIS7CreateConfig.vbs` and `IIS7Admin.vbs` scripts ■ `IIS7Resource.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 7.0 agent uses an agent profile to communicate with Oracle OpenSSO server.

To create an agent profile use either of these methods:

- Use the Oracle OpenSSO Administration 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 *OpenSSO Enterprise 8.0 Administration Reference* in http://download.oracle.com/docs/cd/E19681-01/index.html.

▼ To Create an Agent Profile in the Oracle OpenSSO Console

1. **Login into the Oracle OpenSSO 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: `IIS7Agent`**

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 server central configuration data repository.

7 **In the `Server URL` field, enter the OpenSSO 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:8090`

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 *OpenSSO Enterprise 8.0 Administration Reference* in `http://download.oracle.com/docs/cd/E19681-01/index.html`.

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 7.0 agent configuration file using the `IIS7CreateConfig.vbs` script, you will be prompted to specify the path to the IIS 7.0 agent profile password file.

If you plan to use the `ssoadm` utility to manage the IIS 7.0 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\IIS7Agentpw.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 Oracle OpenSSO, using either the OpenSSO Console or by executing the `ssoadm` utility.

▼ To Create an Agent Administrator in the OpenSSO Console

1 **Login to OpenSSO Administration 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 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 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 7.0 Agent

- "Gathering Information to Install and Configure the IIS 7.0 Agent" on page 9
- "Installing and Configuring the IIS 7.0 Agent" on page 10
- "Considering Specific Deployment Scenarios for the IIS 7.0 Agent" on page 13
- "Installing and Configuring the IIS 7.0 Agent With Office SharePoint Server 2010 on Windows Server 2008" on page 14

Gathering Information to Install and Configure the IIS 7.0 Agent

The following table describes the information you will need to provide when you install and configure the IIS 7.0 agent.

TABLE 2 Information Required to Install and Configure the IIS 7.0 Agent

Script	Prompt
`IIS7CreateConfig.vbs`	IIS 7.0 agent prompts: ■ Agent Resource File Name: Default is `IIS7Resource.en` (English version) ■ Agent URL: For example `http://agenthost.example.com:80` ■ Web Site Identifier: Accept value from the displayed list. Oracle OpenSSO prompts: ■ OpenSSO server URL, including the deployment URI: For example `http://ssohost.example.com:8080/opensso` ■ Agent Profile name: For example `IIS7Agent` ■ Path to password file: For example `C:\tmp\IIS7Agentpw.txt`

TABLE 2 Information Required to Install and Configure the IIS 7.0 Agent *(Continued)*

Script	Prompt
`IIS7Admin.vbs`	Agent Resource File Name: Default is `IIS7Resource.en` (English version)

Installing and Configuring the IIS 7.0 Agent

- "Creating a Configuration File for the IIS 7.0 Agent" on page 10
- "Configuring the IIS 7.0 Agent for a Web Site " on page 12
- "Verfiying an IIS 7.0 Agent Installation" on page 13

Creating a Configuration File for the IIS 7.0 Agent

The `IIS7CreateConfig.vbs` script creates the IIS 7.0 agent configuration file. The `IIS7CreateConfig.vbs` script prompts you for information and then creates a configuration file that you can use later to configure the IIS 7.0 agent.

You must have Administrator privileges to run the `IIS7CreateConfig.vbs` script.

Note: If you are deploying the IIS 7.0 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 7.0 Agent

1 **On the Windows Server 2008 instance, open a command window as administrator. For example, click Start, All Programs, Accessories, and right click on "Command Prompt" to select "Run as administrator".**

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

where *PolicyAgent-base* depends where you unzipped the IIS 7.0 agent distribution file. For example:

For example: `C:\Agents\web_agents\iis7_agent\bin`

The `\bin` directory contains the `IIS7CreateConfig.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 IIS7CreateConfig.vbs` *ConfigFile*

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

For example: `cscript IIS7CreateConfig.vbs IIS7Config.txt`

The `IIS7CreateConfig.vbs` script creates this file and then saves your responses to prompts about the agent host and the OpenSSO server in the file.

4 **When prompted, provide the following information about the IIS 7.0 server that this agent will protect:**

- **Agent Resource File Name**: Accept the default value `IIS7Resource.en` (English version).
- **Agent URL:** : Specify the URL for the IIS 7.0 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 host:**

- **OpenSSO server URL, including the deployment URI:** For example: `http://ssohost.example.com:8080/opensso`
- **Agent Profile name**: For example: `IIS7Agent`.
- **Agent Profile password File**: Path to the file that contains the agent profile password. For example: `C:\tmp\IIS7Agentpw.txt`

Example 1 Sample `IIS7CreateConfig.vbs` Script Run

```
Microsoft (R) Windows Script Host Version 5.7
Copyright (C) Microsoft Corporation. All rights reserved.

Copyright c 2011 Oracle Corporation, All rights reserved
Use is subject to license terms
---------------------------------------------------------
    Microsoft (TM) Internet Information Server (7.0)
---------------------------------------------------------
Enter the Agent Resource File Name [IIS7Resource.en] :

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

Displaying the list of Web Sites and its corresponding Identifiers (id)

SITE "Default Web Site" (id:1,bindings:http/*:80:,state:Started)

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

Please enter the Agent Profile name :
IIS7Agent

Enter the Agent profile password file :
c:\tmp\IIS7Agentpw.txt

-----------------------------------------------------
```

```
Agent Configuration file created : IIS7Config.txt
----------------------------------------------------
```

Configuring the IIS 7.0 Agent for a Web Site

The `IIS7Admin.vbs` script configures the IIS 7.0 agent for a specific Web site, based on an agent configuration file created by the `IIS7CreateConfig.vbs` script.

You must have Administrator privileges to run the `IIS7Admin.vbs` script.

The `IIS7Admin.vbs` script performs these functions:

- Creates a subdirectory named `Identifier_`*id* under the `web_agents\iis7_agent` directory, where *id* is the Web site identifier. This directory contains the IIS 7.0 agent's `\config` and `\logs` directories.
- Creates the `OpenSSOAgentBootstrap.properties` and `OpenSSOAgentConfiguration.properties` files for the IIS 7.0 agent using the agent configuration file created by the `IIS7CreateConfig.vbs` script.
- Updates the Windows registry with the location of properties file.
- Adds the IIS 7.0 HTTP module to the Web site for which the agent is configured.

Note: To configure the IIS 7.0 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 7.0 Agent for a Web Site

1 **On the Windows Server 2008 instance, open a command window as administrator. For example, click Start, All Programs, Accessories, and right click on "Command Prompt" to select "Run as administrator".**

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

where *PolicyAgent-base* depends where you unzipped the IIS 7.0 agent distribution file. For example:

For example: `C:\Agents\web_agents\iis7_agent\bin`

3 **Configure the Web site for the IIS 7.0 agent by running the `IIS7Admin.vbs` script with the `-config` option.**

For example: `cscript IIS7Admin.vbs -config IIS7Config.txt`

where `IIS7Config.txt` is the agent configuration file that you created in "Creating a Configuration File for the IIS 7.0 Agent" on page 10.

Notes:

- The script name and options are case-sensitive.

- For the Agent Resource File Name prompt, accept the default value (`IIS7Resource.en`).

The `IIS7Admin.vbs` script displays the progress of the configuration, as shown in the following sample:

```
Microsoft (R) Windows Script Host Version 5.7
Copyright (C) Microsoft Corporation. All rights reserved.

Copyright c 2011 Oracle Corporation, Inc. All rights reserved
Use is subject to license terms

Enter the Agent Resource File Name [IIS7Resource.en] :

Creating the Agent Config Directory
Creating the OpenSSOAgentBootstrap.properties
    and OpenSSOAgentConfiguration.properties File
Updating the Windows Product Registry
Completed Configuring the IIS 7.0 Agent
```

4 **Ensure that the IIS 7.0 authentication method is set to Anonymous.**

5 **Restart IIS 7.0 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 7.0 agent is being configured.

Verfiying an IIS 7.0 Agent Installation

▼ To Verify an IIS 7.0 Agent Installation

1 **Attempt to access a resource protected by the IIS 7.0 agent.**

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

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

After a successful authentication, you should be able to access the protected resource, if the agent is correctly defined.

Considering Specific Deployment Scenarios for the IIS 7.0 Agent

- "Installing the IIS 7.0 Agent on Multiple IIS 7.0 Servers" on page 14
- "Installing the IIS 7.0 Agent on the OpenSSO Host Server" on page 14

Installing the IIS 7.0 Agent on Multiple IIS 7.0 Servers

After you install the IIS 7.0 agent on a specific IIS 7.0 server, you can install the agent on another IIS 7.0 server instance by running the `IIS7CreateConfig.vbs` and `IIS7Admin.vbs` scripts again for the new server instance.

You can also just copy and edit an existing IIS 7.0 agent configuration file, providing new values for the new IIS 7.0 server instance. Then, run the `IIS7Admin.vbs` script using the edited agent configuration file.

The `IIS7Admin.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 7.0 Agent on the OpenSSO Host Server

Oracle OpenSSO server is not supported on the web container. Therefore, installing the IIS 7.0 agent and OpenSSO server on the same server instance is not supported.

Installing and Configuring the IIS 7.0 Agent With Office SharePoint Server 2010 on Windows Server 2008

To protect Microsoft Office with SharePoint Server 2010 on Windows Server 2008, 64–bit systems, the IIS 7.0 agent is deployed as an ISAPI filter.

To configure the IIS 7.0 agent, you run the `IIS7CreateConfig.vbs` and `IIS7Admin.vbs` scripts and then configure the agent in OpenSSO server. To run these scripts using `cscript`, you must be logged in as a Windows Server 2008 Administrator who owns the execution (`cmd`) environment.

Note – The IIS 7.0 agent with SharePoint Server 2010 is supported with OpenSSO Enterprise 8.0 and later releases.

▼ To Install and Configure the IIS 7.0 Agent With Office SharePoint Server 2010

1 **If necessary, download and unzip the agent distribution file (`iis_v7_WINNT_x64_agent_3.zip`), as described in “Downloading and Unzipping the IIS 7.0 Agent Distribution File” on page 5.**

2 On the Windows Server 2008 instance, open a command window while logged in as an Administrator. For example, click Start, All Programs, Accessories, and right click on "Command Prompt" to select "Run as administrator".

3 Run the `IIS7CreateConfig.vbs` script to generate the agent configuration file.

The `IIS7CreateConfig.vbs` script is in the *PolicyAgent-base*`\bin directory`. For example:

```
cscript IIS7CreateConfig.vbs agent-config.txt
```

When the script prompts you, provide values for your deployment or accept the default values:

```
Microsoft (R) Windows Script Host Version 5.8
Copyright (C) Microsoft Corporation. All rights reserved.

Copyright c 2009, 2011, Oracle and/or its affiliates. All rights reserved.
-----------------------------------------------------------
   Microsoft (TM) Internet Information Server (7.0)
-----------------------------------------------------------
Enter the Agent Resource File Name [IIS7Resource.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 (id)

SITE "Default Web Site" (id:1,bindings:http/*:80:,net.tcp/808:*,net.pipe/*,net.m
smq/localhost,msmq.formatname/localhost,state:Stopped)

SITE "SharePoint Web Services" (id:2,bindings:http/*:32843:,https/*:32844:,net.t
cp/32845:*,net.pipe/*,state:Stopped)

SITE "SharePoint Central Administration v4" (id:155768732,bindings:http/:48923:,
state:Started)

SITE "SharePoint - 80" (id:766968230,bindings:http/:80:,state:Started)

Web Site Identifier :
766968230
--------------------------------------------------
Oracle OpenSSO Enterprise 8.0
--------------------------------------------------
Enter the URL where the OpenSSO server is running. Please include the deployment
URI also as shown in the example (Example: http://opensso.example.com:58080/opensso):
http://opensso.example.com:58080/opensso

Please enter the Agent Profile name :
IIS7SharePoint2010Agent

Enter the Agent profile password file :
C:\sharepointagent\password.txt

-------------------------------------------------------
Agent Configuration file created : agent-config.txt
-------------------------------------------------------------------------------
```

4 **Run the `IIS7Admin.vbs` script using the configuration file you generated in Step 2 as input to install the SharePoint Server 2010 filter.**

The `IIS7Admin.vbs` script is also in the *PolicyAgent-base*`\bin` directory. For example:

```
cscript IIS7Admin.vbs -config agent-config.txt
```

5 **Generate the replay password key using `DESgenKey.class` on the OpenSSO server side. For example:**

`java -classpath` *amserver.jarPath*`/amserver.jar com.sun.identity.common.DESGenKey`

In this example, *amserver.jarPath* is the complete path to the `amserver.jar` file.

Executing the `DESgenKey.class` returns a string as output. For example: `c1QBAWv7vHk=`

6 **Add the replay password key to the `OpenSSOAgentConfiguration.properties` file. For example:**

```
com.sun.identity.agents.config.replaypasswd.key = c1QBAWv7vHk=
```

7 **Add the replay password key in the OpenSSO Administration console:**

a. **In the OpenSSO Administration console, click Configuration, Servers and Sites, and then the** *OpenSSO-server-name***.**

b. **Click Advanced and add the following properties and values:**

- `com.sun.am.replaypasswd.key` with the replay password key value. For example: `c1QBAWv7vHk=`
- `com.sun.am.sharepoint_login_attr_name` with an attribute name in the user repository used by SharePoint Server 2010 to authenticate. For example: `displayName`

c. **Click Save.**

Note: Ignore any warnings after you add these keys.

8 **Add the replay password to the Agent profile in the OpenSSO Administration console:**

a. **In the OpenSSO Administration console, click Access Control, Top Level Realm, Agents, Web,** *IIS7SharePointAgentProfile***, and then Advanced.**

b. **In the Microsoft IIS Server section, set the following fields:**

- Authentication Type to Basic (from the default value dsame).
- Replay Password Key to the generated key (`c1QBAWv7vHk=` in the example).

c. **Click Save.**

9 **Configure the post-authentication plug-in in the OpenSSO Administration console:**

a. **In the OpenSSO Administration console, click Access Control, Top Level Realm, Authentication, Advanced Properties, and then scroll down to Authentication Post Processing Classes.**

b. **Add `com.sun.identity.authentication.spi.ReplayPasswd` to the Authentication Post Processing Classes.**

c. **Click Save and then log out of the Console**

10 **Restart the OpenSSO server.**

11 **For IIS 7.x web sites where the filter is configured, set the authentication method as Basic Authentication by running `inetmgr`:**

a. **Select the local computer, Web Sites, SharePoint – 80. Then, right click and select Properties.**

b. **Select the Directory Security tab and edit Authentication and Access Control.**

c. **Check the Basic Authentication box and accept the warning.**

d. **Close all property windows**

12 **Restart the IIS 7.x server using `iisreset`.**

Post-Installation Tasks for the IIS 7.0 Agent

- "Creating and Adding Logout URLS in a CDSSO Deployment" on page 17
- "Using SSL With the IIS 7.0 Agent (Optional)" on page 18
- "Changing the Password for an Agent Profile (Optional)" on page 20

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 7.0 resources.

▼ To Create the Logout URL Pages

1 **Create two logout URL pages as IIS 7.0 resources. For example: `logout.html` and `logout2.html`**

2 **Store the logout URL pages in the `doc` directory of the IIS 7.0 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 7.0 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 7.0 instance should invoke the logout URL used in this procedure.

Using SSL With the IIS 7.0 Agent (Optional)

If you specify the `https` protocol for the OpenSSO server URL during the IIS 7.0 agent installation, the agent is automatically configured and ready to communicate to the OpenSSO server over Secure Sockets Layer (SSL). However, to ensure that the IIS 7.0 agent is configured for SSL communication to the server, follow these tasks:

- "Installing the OpenSSO Root CA Certificate on the IIS 7.0 Agent" on page 19
- "Disabling the Trust Behavior for the IIS 7.0 Agent " on page 20

Installing the OpenSSO Root CA Certificate on the IIS 7.0 Agent

The root CA certificate that you install on the IIS 7.0 agent must be the same certificate that is installed on the OpenSSO host server.

Oracle provides the Certificate Database Tool, `certutil.exe`, in the IIS 7.0 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 Root CA Certificate on the IIS 7.0 Agent

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

2. **On the IIS 7.0 server, locate the `certutil.exe` utility.**

   After you unzip the IIS 7.0 agent distribution file, `certutil.exe` is available in the *PolicyAgent-base*`\bin` directory.

   For example: `C:\Agents\web_agents\iis7_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\iis7_agent\cert
   C:\Agents\web_agents\iis7_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 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 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\iis7_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 7.0 Agent

By default, the IIS 7.0 agent installed on a remote IIS 7.0 server trusts any server certificate presented over SSL by the OpenSSO server host. For the IIS 7.0 agent to perform certificate checking, you must disable this trust behavior.

▼ To Disable the Trust Behavior for the IIS 7.0 Agent

1. **Find the IIS 7.0 agent's `OpenSSOAgentBootstrap.properties` file in the agent's `\config` directory. For example:**

   ```
   C:\Agents\web_agents\iis7_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 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/iis7_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 server.

4. **Restart IIS 7.0 using the `iisreset` command.**

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 Oracle OpenSSO 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 7.0 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\iis7_agent\bin
```

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

```
cryptit.exe C:\tmp\IIS7Agentpw.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 7.0 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 7.0 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 7.0 server.

Managing the IIS 7.0 Agent

Managing a Version 3.0 Agent With a Centralized Configuration

OpenSSO 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 Administration Console

  You can manage both version 3.0 J2EE and web agents from the OpenSSO 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 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 *OpenSSO Enterprise 8.0 Administration Reference* in `http://download.oracle.com/docs/cd/E19681-01/index.html`.

Managing a Version 3.0 Agent With a Local Configuration

In some scenarios, you might need to deploy the IIS 7.0 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 7.0 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 7.0 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 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 7.0 Agent

You uninstall the IIS 7.0 agent for a specific IIS 7.0 server instance by running the `IIS7Admin.vbs` script with the `-unconfig` option.

You must have Administrator privileges to run the `IIS7Admin.vbs` script.

▼ To Uninstall the IIS 7.0 Agent

1 **On the Windows Server 2008 instance, open a command window as administrator. For example, click Start, All Programs, Accessories, and right click on "Command Prompt" to select "Run as administrator".**

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

where *PolicyAgent-base* depends where you unzipped the IIS 7.0 agent distribution file. For example:

For example: `C:\Agents\web_agents\iis7_agent\bin`

3 **Run the `IIS7Admin.vbs` script with the `-unconfig` option. Both the script name and `-unconfig` option are case-sensitive.**

For example: `cscript IIS7Admin.vbs -unconfig IIS7Config.txt`

where `IIS7Config.txt` is the agent configuration file for the IIS 7.0 agent on the specific IIS 7.0 server instance.

4 **Restart IIS 7.0 using the `iisreset` command.**

Related Information

Additional Resources

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

- Oracle Advanced Customer Services:

  `http://www.oracle.com/us/support/systems/advanced-customer-services/index.html`
- Oracle Technology Network:

  `http://www.oracle.com/technetwork/index.html`
- Sun Software Product Map:

  `http://www.oracle.com/us/sun/sun-products-map-075562.html`

Oracle's Accessibility Program

For information about Oracle's commitment to accessibility, see the following site:

`http://www.oracle.com/us/corporate/accessibility/index.html`

Related Third-Party Web Sites

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

Note – Oracle is not responsible for the availability of third-party Web sites mentioned in this document. Oracle 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. Oracle 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, contact Oracle as follows:

http://www.oracle.com/us/support/systems/advanced-customer-services/index.html

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 version, including any patches or other software that might be affecting the problem
- Steps to reproduce the problem
- Any error logs or core dumps

Revision History

Part Number	Date	Description
821–0267–11	July 8, 2011	■ Added support for the IIS 7.0 agent with Microsoft Office SharePoint Server 2010 on Windows Server 2008. ■ Revised outdated URLs.
821–0267–10	September 9, 2009	Initial release.