Oracle® OpenSSO

Policy Agent 3.0 Guide for IBM Lotus Domino 8.5.2

Release 3.0

E23265-01

September 2012

This guide describes how to install and configure the version 3.0 policy agent for IBM Lotus Domino 8.5.2.

ORACLE

Oracle OpenSSO Policy Agent 3.0 Guide for IBM Lotus Domino 8.5.2, Release 3.0

E23265-01

Primary Author: John Spencer

Contents

Preface ix

Audience ix
Documentation Accessibility ix
Related Documents ix
Conventions x
Additional Resources x
How to Report Problems and Provide Feedback x

1 Policy Agent 3.0 Guide for IBM Lotus Domino 8.5.2

1.1 Supported Platforms, Compatibility, and Coexistence for the Lotus Domino 8.5.2 Agent 1-1
1.1.1 Supported Platforms for the Lotus Domino 8.5.2 Agent 1-2
1.1.2 Compatibility with Access Manager 7.1 and Access Manager 7 2005Q4 1-2
1.1.3 Coexistence with Version 2.2 Policy Agents 1-2
1.1.4 No Support for CDSSO with the Lotus Domino 8.5.2 Agent 1-3
1.2 Pre-Installation Tasks for the Lotus Domino 8.5.2 Agent 1-3
1.2.1 Setting the IBM JDK/JRE on IBM AIX Systems 1-3
1.2.2 Setting Your `JAVA_HOME` Environment Variable 1-3
1.2.3 Downloading the Lotus Domino 8.5.2 Agent 1-4
1.2.4 Creating an Agent Profile 1-5
1.2.5 Creating a Password File 1-5
1.2.6 Creating an Agent Administrator (Optional) 1-6
1.3 Installing the Lotus Domino 8.5.2 Agent 1-7
1.3.1 Gathering Information to Install the Lotus Domino 8.5.2 Agent 1-7
1.3.2 Installing the Lotus Domino 8.5.2 Agent Using the `agentadmin` Program 1-8
1.3.3 Considering Specific Deployment Scenarios for the Lotus Domino 8.5.2 Agent 1-10
1.4 Post-Installation Tasks for the Lotus Domino 8.5.2 Agent 1-10
1.4.1 Setting File Ownership and Permissions for the Lotus Domino 8.5.2 Agent (Required) 1-11
1.4.2 Setting the `LIBPATH` to Include Libraries Specific to the Lotus Domino 8.5.2 Agent (Required on AIX Systems) 1-11
1.4.3 Configuring the DSAPI Filter for the Lotus Domino 8.5.2 Agent (Required) 1-12
1.4.4 Adding Policies to the Oracle OpenSSO Server (Required) 1-12
1.4.5 Adding the Lotus Domino 8.5.2 `notes` User to the OpenSSO Console (Required) .. 1-13
1.4.6 Adding the Logout URL to the Lotus Domino 8.5.2 Agent Profile (Optional) 1-13

1.4.7 Configuring the Lotus Domino 8.5.2 Agent on Multiple Web Server Instances (Optional) 1-13
1.4.8 Using the Lotus Domino Database for the Lotus Domino 8.5.2 Agent (Optional) ... 1-14
1.4.9 Using SSL with the Lotus Domino 8.5.2 Agent (Optional) 1-14
1.4.10 Changing the Password for an Agent Profile (Optional) 1-16
1.5 Managing the Lotus Domino 8.5.2 Agent 1-17
1.5.1 Managing a Version 3.0 Agent with a Local Configuration 1-17
1.6 Uninstalling the Lotus Domino 8.5.2 Agent 1-18
1.6.1 Preparing to Uninstall the Lotus Domino 8.5.2 Agent 1-18
1.6.2 Uninstalling the Lotus Domino 8.5.2 Agent Using the `agentadmin` Program 1-18
1.6.3 Removing the DSAPI Filter for the Lotus Domino 8.5.2 Agent 1-20

List of Examples

1–1 Lotus Domino 8.5.2 Agent Uninstall Sample Run 1-19

List of Tables

1–1 Supported Platforms for the Lotus Domino 8.5.2 Agent 1-2
1–2 Information Required to Install the Lotus Domino 8.5.2 Agent 1-7

Preface

This preface provides the following information about the Lotus Domino 8.5.2 policy agent, a version 3.0 web agent that functions with Oracle OpenSSO to protect resources on IBM Lotus Domino 8.5.2:

- Audience
- Documentation Accessibility
- Related Documents
- Conventions
- Additional Resources
- How to Report Problems and Provide Feedback

Audience

This guide is intended for system administrators, deployment specialists, and other IT professionals who are installing and configuring the Lotus Domino 8.5.2 policy agent.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` or visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` if you are hearing impaired.

Related Documents

For more information, see the documents in the Oracle OpenSSO documentation library:

`http://docs.oracle.com/cd/E19681-01/index.html`

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

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`

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

1

Policy Agent 3.0 Guide for IBM Lotus Domino 8.5.2

The Lotus Domino 8.5.2 policy agent is a version 3.0 web agent that functions with Oracle OpenSSO to protect resources on IBM Lotus Domino 8.5.2 server.

This chapter describes these topics:

- Section 1.1, "Supported Platforms, Compatibility, and Coexistence for the Lotus Domino 8.5.2 Agent"
- Section 1.2, "Pre-Installation Tasks for the Lotus Domino 8.5.2 Agent"
- Section 1.3, "Installing the Lotus Domino 8.5.2 Agent"
- Section 1.4, "Post-Installation Tasks for the Lotus Domino 8.5.2 Agent"
- Section 1.5, "Managing the Lotus Domino 8.5.2 Agent"
- Section 1.6, "Uninstalling the Lotus Domino 8.5.2 Agent"

For more information about version 3.0 policy agents, see the *Oracle OpenSSO Policy Agent 3.0 Release Notes* in the following documentation library:

`http://docs.oracle.com/cd/E19681-01/index.html`

1.1 Supported Platforms, Compatibility, and Coexistence for the Lotus Domino 8.5.2 Agent

- Section 1.1.1, "Supported Platforms for the Lotus Domino 8.5.2 Agent"
- Section 1.1.2, "Compatibility with Access Manager 7.1 and Access Manager 7 2005Q4"
- Section 1.1.3, "Coexistence with Version 2.2 Policy Agents"
- Section 1.1.4, "No Support for CDSSO with the Lotus Domino 8.5.2 Agent"

1.1.1 Supported Platforms for the Lotus Domino 8.5.2 Agent

Table 1–1 Supported Platforms for the Lotus Domino 8.5.2 Agent

Agent For	Supported Platforms
IBM Lotus Domino 8.5.2 server	▪ Oracle Solaris 10 OS on SPARC 32-bit platforms ▪ Microsoft Windows 2003 and Windows 2008, both 32-bit and 64-bit platforms ▪ IBM AIX version 6.1 ▪ Red Hat Enterprise Linux (RHEL) 5.5, 32-bit agent on 32-bit Domino Server running on both 32-bit and 64-bit RHEL 5.5

Note: Considerations:

- Minor updates to IBM Lotus Domino 8.5.2 server are supported.
- Minor versions of the supported platforms, including updates, service packs, and patches, are also supported.
- To avoid an exception when you start the Lotus Domino server on AIX, first check that the base file set `bos.iocp.rte` (for I/O completion ports) is installed. If necessary, install this file set from the AIX installation media.

  For information, see http://www-01.ibm.com/support/docview.wss?uid=swg21086556.

1.1.2 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.

1.1.3 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, Oracle 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://docs.oracle.com/cd/E19534-01/index.html.

1.1.4 No Support for CDSSO with the Lotus Domino 8.5.2 Agent

The Lotus Domino 8.5.2 agent does not support cross domain single sign-on (CDSSO). The Lotus Domino 8.5.2 deployment container does not allow the agent to change the method type from `POST` to `GET`, which is necessary for cross domain single sign-on.

1.2 Pre-Installation Tasks for the Lotus Domino 8.5.2 Agent

- Section 1.2.1, "Setting the IBM JDK/JRE on IBM AIX Systems"
- Section 1.2.2, "Setting Your `JAVA_HOME` Environment Variable"
- Section 1.2.3, "Downloading the Lotus Domino 8.5.2 Agent"
- Section 1.2.4, "Creating an Agent Profile"
- Section 1.2.5, "Creating a Password File"
- Section 1.2.6, "Creating an Agent Administrator (Optional)"

1.2.1 Setting the IBM JDK/JRE on IBM AIX Systems

Perform this task only if you are installing the Lotus Domino 8.5.2 agent on an IBM AIX system and you are using the IBM JDK/JRE.

1.2.1.1 To Set the IBM JDK/JRE on IBM AIX Systems

1. After you download and unzip the Lotus Domino 8.5.2 agent distribution file for AIX, locate the `agentadmin` script in the following directory:

   `AgentHome``/web_agents/domino_agent/bin`

   where *`AgentHome`* is where you unzipped the agent distribution file.

2. In the `agentadmin` script, comment out the following line, which sets the regular JDK/JRE classpath:

   ```
   $JAVA_VM -classpath "$AGENT_CLASSPATH"
   com.sun.identity.install.tools.launch.AdminToolLauncher $*
   ```

3. In the `agentadmin` script, uncomment the following line at the end of the file, which sets the IBM JDK/JRE `classpath`:

   ```
   #$JAVA_VM -DamKeyGenDescriptor.provider=IBMJCE
   -DamCryptoDescriptor.provider=IBMJCE
   -DamRandomGenProvider=IBMJCE -classpath "$AGENT_CLASSPATH"
   com.sun.identity.install.tools.launch.AdminToolLauncher $*
   ```

4. Save your changes.

1.2.2 Setting Your `JAVA_HOME` Environment Variable

The agent installation program requires the Java Runtime Environment (JRE) 1.5 or later. Before you install the agent, set your `JAVA_HOME` environment variable to point to the JDK installation directory for the JDK version you are using. If you have not set this variable (or if you set it incorrectly), the program will prompt you for the correct path.

1.2.3 Downloading the Lotus Domino 8.5.2 Agent

The Lotus Domino 8.5.2 agent is available as patch ID **149027-01** on My Oracle Support:

https://support.oracle.com/

1.2.3.1 To Download the Lotus Domino 8.5.2 Agent

1. Login to the IBM Lotus Domino 8.5.2 server where you want to install the agent.
2. Download and unzip the Lotus Domino 8.5.2 agent patch file from My Oracle Support.

   Separate README and ZIP files are available for each platform supported by the agent, as shown in the following table.

Platform	Lotus Domino 8.5.2 Agent Distribution File Name
Solaris 10 SPARC systems	`domino_SunOS_sparc_agent_3.zip`
Linux systems	`domino_Linux_agent_3.zip`
Windows systems, 32-bit	`domino_WINNT_agent_3.zip`
Windows systems, 64-bit	`domino_WINNT_64_agent_3.zip`
IBM AIX systems	`domino_AIX_agent_3.zip`

3. Unzip the agent distribution file for your specific platform.

   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/domino_agent`

   where *AgentHome* is where you unzipped the agent distribution file.

   For example: `/opt/web_agents/domino_agent`

File or Directory	Description
`README.txt`	Readme file
`/bin`	▪ Solaris, Linux, and AIX systems: `agentadmin`, `certutil`, and `crypt_util` ▪ Windows systems: `agentadmin.bat`, `certutil.exe`, and `cryptit.exe`
`/config`	Template, properties, and XML files
`/etc`	`dsame.config.template` file
`/lib`	Library and JAR files
`/locale`	Properties files
`/installer-logs`	Log files after you install the agent
`/data`	Agent specific data

1.2.4 Creating an Agent Profile

The Lotus Domino 8.5.2 agent uses an agent profile to communicate with Oracle OpenSSO server. You can create an agent profile using any of these methods:

- Use the Oracle OpenSSO Console, as described in Creating an Agent Profile.
- 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*.
- Choose the "Option to create the agent profile in the server during installation" when you run the `agentadmin` program.

1.2.4.1 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.
5. Enter and confirm the `Password`.

   Important: This password must be the same password that you enter in the agent profile password file that you specify when you run the `agentadmin` program to install the agent.
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`: In the Oracle OpenSSO server central configuration data repository.
7. In the `Server URL` field, enter the Oracle 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: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 this link to display the `Edit` agent page. For information about the agent configuration fields, refer to the Console online Help.

1.2.5 Creating a Password File

A password file is an ASCII text file with only one line specifying the password in clear text. By using a password file, you are not forced to expose a password at the command line during the agent installation. When you install the Lotus Domino 8.5.2 agent using the `agentadmin` program, you are prompted to specify paths to following password files:

- An **agent profile password file** is required for both the `agentadmin` default and custom installation options.

- An **agent administrator password file** is required if you use the custom installation option and have the `agentadmin` program automatically create the agent profile in Oracle OpenSSO server during the installation. If you prefer, you can use `amadmin` as the agent administrator

1.2.5.1 To Create a Password File

1. Create an ASCII text file for the password file. For example: `/tmp/domino8agentpw`
2. If you want the `agentadmin` program to automatically create the agent profile in Oracle OpenSSO server during the installation, create another password file for the agent administrator. For example: `/tmp/agentadminpw`
3. Using a text editor, enter the appropriate password in clear text on the first line in each file.
4. Secure each password file appropriately, depending on the requirements for your deployment.

1.2.6 Creating an Agent Administrator (Optional)

Creating an agent administrator is optional. An agent administrator can manage agents in Oracle OpenSSO, including:

- **Agent management**: Use the agent administrator to manage agents either in the Oracle OpenSSO Console or by executing the `ssoadm` utility.
- **Agent installation**: If you install the agent using the custom installation option (`agentadmin --custom-install`) and want to have the installation program create the agent profile, specify the agent administrator (and password file) when you are prompted.

1.2.6.1 To Create an Agent Administrator

1. Login to Oracle OpenSSO 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: `agentadmingroup`
   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: `agentadminuser`

        This is the name you will use to login to the Oracle OpenSSO Console.
      – **First Name** (optional), **Last Name**, and **Full Name**.

        For simplicity, use the same name for each of these values that you specified 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 Oracle 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.

1.3 Installing the Lotus Domino 8.5.2 Agent

- Section 1.3.1, "Gathering Information to Install the Lotus Domino 8.5.2 Agent"
- Section 1.3.2, "Installing the Lotus Domino 8.5.2 Agent Using the agentadmin Program"
- Section 1.3.3, "Considering Specific Deployment Scenarios for the Lotus Domino 8.5.2 Agent"

1.3.1 Gathering Information to Install the Lotus Domino 8.5.2 Agent

The following table describes the information you will need to provide when you run the agentadmin program to install Lotus Domino 8.5.2 agent. For some agentadmin prompts, you can accept the default value displayed by the program, if you prefer.

Table 1–2 Information Required to Install the Lotus Domino 8.5.2 Agent

Prompt Request	Description
IBM Lotus Domino Data Directory	Path to the data directory used by the Lotus Domino 8.5.2 server instance. Default: /opt/ibm/notesdata
OpenSSO server URL	URL for Oracle OpenSSO server. For example: http://openssohost.example.com:8080/opensso
Agent URL	URL for the Lotus Domino 8.5.2 agent. For example: http://agenthost.example.com:80
Encryption Key	Key used to encrypt passwords.
Agent Profile Name	Name of the agent profile. For example: Domino8Agent For information, see Creating an Agent Profile.

Table 1–2 (Cont.) Information Required to Install the Lotus Domino 8.5.2 Agent

Prompt Request	Description
Agent Profile Password File	Path to the agent profile password file. For example: `/tmp/domino8agentpw` For information, see Creating a Password File.
Option for the installer to create the agent profile The `agentadmin` program displays the following prompt if the agent profile previously specified for the Agent Profile Name prompt does not already exist in Oracle OpenSSO: `Enter true if the Agent Profile is being created into OpenSSO server by the installer. Enter false if it will be not be created by installer.`	To have the installation program create the agent profile, enter `true`. The program then prompts you for: ▪ Agent administrator who can create, update, or delete the agent profile. For example: `agentadmin` **Important**: To use this option, the agent administrator must already exist in Oracle OpenSSO server and must have agent administrative privileges. If you prefer, you can specify `amadmin` as this user. For information see, Creating an Agent Administrator (Optional). ▪ Path to the agent administrator password file. For example: `/tmp/agentadminpw` For information, see Creating a Password File.

1.3.2 Installing the Lotus Domino 8.5.2 Agent Using the `agentadmin` Program

Before you install the Lotus Domino 8.5.2 agent, your deployment must meet these requirements:

- A Lotus Domino 8.5.2 server instance must be installed and configured on the agent host server where you plan to install the agent.
- An Oracle OpenSSO server instance must be installed and accessible to the Lotus Domino 8.5.2 instance.
- You must have downloaded and unzipped the agent distribution file, as described in Downloading the Lotus Domino 8.5.2 Agent.

1.3.2.1 To Install the Lotus Domino 8.5.2 Agent Using the `agentadmin` Program

1. Login into the server where you want to install the agent.

   Important: To install the agent, you must have write permission to the files and directories for the Lotus Domino 8.5.2 instance.

   On Linux systems, run the `agentadmin` program as `root`.

2. Stop the Lotus Domino 8.5.2 instance.
3. Change to the *`PolicyAgent-base`*`/bin` directory. For example:

   ```
   # cd /opt/web_agents/domino_agent/bin
   ```

4. Start the agent installation. For example:

   ```
   # ./agentadmin --custom-install
   ```

   On Windows systems, run the `agentadmin.bat` program.

5. Enter information as requested by the `agentadmin` program, or accept the default values displayed by the program.

   After you have made your choices, the `agentadmin` program displays a summary of your responses. For example:

```
-------------------------------------------
SUMMARY OF YOUR RESPONSES
-------------------------------------------
IBM Lotus Domino Data Directory : /opt/domino/notesdata
OpenSSO server URL : http://openssohost.example.com:8080/opensso
Agent URL : http://agenthost.example.com:80
Encryption Key : u7hsteKDD+L9cp5P+sAxzdiwuq6XxJRH
Agent Profile name : domino8agent
Agent Profile Password file name : /tmp/domino8agentpw
Agent Profile will be created right now by agent installer : true
Agent Administrator : amadmin
Agent Administrator's password file name : /tmp/amadminpw

Verify your settings above and decide from the choices below.
1. Continue with Installation
2. Back to the last interaction
3. Start Over
4. Exit
Please make your selection [1]:
```

6. Verify your choices and either continue with the installation (selection 1, the default), or make any necessary changes.

   If you continue, the program installs the agent and displays a summary of the installation. For example:

```
SUMMARY OF AGENT INSTALLATION
-----------------------------
Agent instance name: Agent_001
Agent Bootstrap file location:
/opt/domino/agent/web_agents/domino_agent/Agent_001/config/
  OpenSSOAgentBootstrap.properties
Agent Configuration Tag file location
/opt/domino/agent/web_agents/domino_agent/Agent_001/config/
  OpenSSOAgentConfiguration.properties
Agent Audit directory location:
/opt/domino/agent/web_agents/domino_agent/Agent_001/logs/audit
Agent Debug directory location:
/opt/domino/agent/web_agents/domino_agent/Agent_001/logs/debug

Install log file location:
/opt/domino/agent/web_agents/domino_agent/installer-logs/audit/custom.log
```

7. After the installation finishes successfully, if you wish, check the installation log file in the `/installer-logs/audit` directory
8. Restart the Lotus Domino 8.5.2 instance where you installed the agent.

1.3.2.2 Agent Installation Program Functions

The agent installation program performs these functions:

- Creates the `OpenSSOAgentBootstrap.properties` and `OpenSSOAgentConfiguration.properties` configuration files from the respective template files.
- Creates the `dsame.conf` file under `/opt/domino/notesdata` from the template file.
- Creates the **agent instance directory** as *`PolicyAgent-base`*`/Agent_`*`nnn`*, where *`nnn`* identifies the agent instance as `Agent_001`, `Agent_002`, and so on for each additional agent instance.

For example: `/opt/web_agents/domino_agent/Agent_001`

Each agent instance directory contains the following subdirectories:

- `/config` contains the configuration files for the agent instance, including `OpenSSOAgentBootstrap.properties` and `OpenSSOAgentConfiguration.properties`.
- `/logs` contains the following subdirectories
  - `/audit` contains local audit trail for the agent instance.
  - `/debug` contains the debug files for the agent instance when the agent runs in debug mode.

1.3.3 Considering Specific Deployment Scenarios for the Lotus Domino 8.5.2 Agent

- Section 1.3.3.1, "Installing the Lotus Domino 8.5.2 Agent on Multiple Lotus Domino 8.5.2 Instances"
- Section 1.3.3.2, "Installing Lotus Domino 8.5.2 Agent on the Oracle OpenSSO Host Server"

1.3.3.1 Installing the Lotus Domino 8.5.2 Agent on Multiple Lotus Domino 8.5.2 Instances

After you install the Lotus Domino 8.5.2 agent on a specific Lotus Domino 8.5.2 instance, you can install the agent on another Lotus Domino 8.5.2 instance by executing the `agentadmin` program again for that instance.

1.3.3.2 Installing Lotus Domino 8.5.2 Agent on the Oracle OpenSSO Host Server

Oracle OpenSSO is not supported on IBM Lotus Domino 8.5.2. Therefore, installing the Lotus Domino 8.5.2 agent and Oracle OpenSSO on the same server instance is not supported.

1.4 Post-Installation Tasks for the Lotus Domino 8.5.2 Agent

- Section 1.4.1, "Setting File Ownership and Permissions for the Lotus Domino 8.5.2 Agent (Required)"
- Section 1.4.2, "Setting the `LIBPATH` to Include Libraries Specific to the Lotus Domino 8.5.2 Agent (Required on AIX Systems)"
- Section 1.4.3, "Configuring the DSAPI Filter for the Lotus Domino 8.5.2 Agent (Required)"
- Section 1.4.4, "Adding Policies to the Oracle OpenSSO Server (Required)"
- Section 1.4.5, "Adding the Lotus Domino 8.5.2 `notes` User to the OpenSSO Console (Required)"
- Section 1.4.6, "Adding the Logout URL to the Lotus Domino 8.5.2 Agent Profile (Optional)"
- Section 1.4.7, "Configuring the Lotus Domino 8.5.2 Agent on Multiple Web Server Instances (Optional)"
- Section 1.4.8, "Using the Lotus Domino Database for the Lotus Domino 8.5.2 Agent (Optional)"
- Section 1.4.9, "Using SSL with the Lotus Domino 8.5.2 Agent (Optional)"

- Section 1.4.10, "Changing the Password for an Agent Profile (Optional)"

1.4.1 Setting File Ownership and Permissions for the Lotus Domino 8.5.2 Agent (Required)

On Solaris, Linux, and AIX systems, the Lotus Domino 8.5.2 must run as a non-root user. During the server installation, the `notes` user in the `notes` group is created as the default user to run the Lotus Domino 8.5.2 server. You can, however, specify another user name if you prefer, but this guide uses `notes` as the default user name in examples.

The `notes` user must have read and write permission to the files in the Lotus Domino 8.5.2 agent instance directory, which is created by the `agentadmin` program when you install the agent:

`PolicyAgent-base``/Agent_`*`nnn`*, where *`nnn`* identifies the agent instance as `Agent_001`, `Agent_002`, and so on for each additional agent instance.

For example: `/opt/web_agents/domino_agent/Agent_001`

Note: This task is not required for Windows systems because the Lotus Domino 8.5.2 can run as a Windows Administrator user. Therefore, on Windows you do not need to set any special permissions for the files in the Lotus Domino 8.5.2 agent instance directory.

1.4.1.1 To Set File Ownership and Permissions for the Lotus Domino 8.5.2 Agent

1. Log in to the Lotus Domino 8.5.2 server as superuser (`root`).
2. Change ownership of all files in the agent instance directory and subdirectories. For example:

   ```
   chown -R notes:notes /opt/web_agents/domino_agent/Agent_001
   ```

3. If the Lotus Domino 8.5.2 agent is using SSL, change ownership of the certificate and key databases. For example:

   ```
   chown -R notes:notes /opt/certdb/cert8.db /opt/certdb/key3.db
   ```

1.4.2 Setting the `LIBPATH` to Include Libraries Specific to the Lotus Domino 8.5.2 Agent (Required on AIX Systems)

Setting the `LIBPATH` environment variable is required on IBM AIX systems before you start the Lotus Domino 8.5.2 server instance.

1.4.2.1 To Set the `LIBPATH` to Include Libraries Specific to the Lotus Domino 8.5.2 Agent

1. Before you start the Lotus Domino 8.5.2 server instance, set the `LIBPATH` environment variable to include the directory that contains the `libamsdk.so` library:
   - C shell, including `csh` and `tcsh`:

     `setenv LIBPATH` *`PolicyAgent-base`*`/lib:/usr/mps:/lib:/usr/lib`

     For example:

```
setenv LIBPATH /opt/web_agents/domino_
agent/lib:/usr/mps:/lib:/usr/lib
```

- Bourne shell, including `ksh` and `bash`:

  ```
  export LIBPATH=PolicyAgent-base/lib:/usr/mps:/lib:/usr/lib
  ```

  For example:

  ```
  export LIBPATH=/opt/web_agents/domino_
  agent/lib:/usr/mps:/lib:/usr/lib
  ```

1.4.3 Configuring the DSAPI Filter for the Lotus Domino 8.5.2 Agent (Required)

Configuring the Domino Web Server API (DSAPI) filter is a required task for all platforms. The DSAPI filter authenticates users and passes their information to the Lotus Domino 8.5.2 server. If the DSAPI filter is not configured properly, users will not be able to access resources.

1.4.3.1 To Configure the DSAPI Filter for the Lotus Domino 8.5.2 Agent

1. In the Lotus Domino 8.5.2 Administrator web console, select the Configuration tab.
2. In the left pane, under Server, click All Server Documents A window appears, displaying a list of servers.
3. From the list of servers, select the Lotus Domino 8.5.2 server instance that you want to configure.
4. Click Internet Protocols.
5. Select the HTTP tab.
6. Click Edit Server.
7. In the DSAPI Filter File Names field, add the following DSAPI filter file name. For example:
   - Solaris and Linux systems: `/opt/web_agents/domino_agent/lib/libamdomino.so`
   - AIX systems: `/opt/web_agents/domino_agent/lib/libamdomino.a`
   - Windows: `c:\web_agents\domino_agent\lib\amdomino.dll`
8. Click Save and then Close to save the changes.
9. Restart the Lotus Domino 8.5.2 or HTTP server.

Next Steps

Multiple Instances. To configure the DSAPI filter for multiple Lotus Domino 8.5.2 server instances, perform this task for each instance.

1.4.4 Adding Policies to the Oracle OpenSSO Server (Required)

1.4.4.1 To Add Policies to the Oracle OpenSSO Server (Required)

1. In the OpenSSO Administration Console, click Access Control, *realm-name*, then Policies.

2. Under New Policy... and add the new policies for the Lotus Domino 8.5.2 URLs that you want to protect.

   For information about adding a policy, click the online Help.

1.4.5 Adding the Lotus Domino 8.5.2 `notes` User to the OpenSSO Console (Required)

1.4.5.1 To Add the Lotus Domino 8.5.2 `notes` User to the OpenSSO Console

1. In the OpenSSO Administration Console, click Access Control, *`realm-name`*, Subjects, and then User.
2. Click New and provide the following values:
   - **ID**. Name of the user: `notes`
   - **First Name** (optional), **Last Name**, and **Full Name**. For simplicity, use the same name for each of these values that you specified for ID.
   - **Password** (and confirmation). This password can be different from the `notes` user password in Lotus Domino 8.5.2.
   - **User Status**: Active
3. Click OK.

Next Steps

You can use the `notes` user to test the configuration. Restart the Lotus Domino 8.5.2 after you finish the configuration and then log in using the following URL as the `notes` user with the password you specified in the OpenSSO Console.

`http://`*`dominoHost`*`.`*`domain`*`:`*`dominoPort`*`/webadmin.nsf`

1.4.6 Adding the Logout URL to the Lotus Domino 8.5.2 Agent Profile (Optional)

1.4.6.1 To Add the Logout URL to the Lotus Domino 8.5.2 Agent Profile

1. In the OpenSSO Administration Console, click Access Control, *`realm-name`*, Agents, and then the Lotus Domino 8.5.2 agent profile name.
2. On the Lotus Domino 8.5.2 agent Edit page, click OpenSSO Services.
3. Under Agent Logout URL, add the logout URL. For example:

   `http://`*`dominoHost`*`.`*`domain`*`:`*`dominoPort`*`/webadmin.nsf/pgSignout?Logout`

4. Click Save.

1.4.7 Configuring the Lotus Domino 8.5.2 Agent on Multiple Web Server Instances (Optional)

After you install the Lotus Domino 8.5.2 agent on a specific Lotus Domino 8.5.2 instance, you can install the agent on another Lotus Domino 8.5.2 instance by running the `agentadmin` program again for that instance.

However, if you install the same Lotus Domino 8.5.2 agent on multiple Lotus Domino 8.5.2 instances, all configuration directories, which include the `notes.ini` file, should have the same parent directory.

1.4.8 Using the Lotus Domino Database for the Lotus Domino 8.5.2 Agent (Optional)

You can configure the Lotus Domino 8.5.2 agent to check the Lotus Domino database for each user name after the agent authenticates the user. This optional task applies to all platforms.

1.4.8.1 To Use the Lotus Domino Database for the Lotus Domino 8.5.2 Agent

1. Log in to the OpenSSO Administration Console.
2. Click Access Control, *realm-name*, Agents, Web, and then the name of the Lotus Domino 8.5.2 agent profile. The Console displays the Edit page for the agent profile.
3. Click Advanced.
4. Click the IBM Lotus Domino Server link.
5. For Check User in Domino Database, check Enabled.

   The corresponding property is com.sun.identity.agents.config.domino.check.name.database.
6. Click Save.

1.4.9 Using SSL with the Lotus Domino 8.5.2 Agent (Optional)

If you specify the `HTTPS` protocol during the Lotus Domino 8.5.2 agent installation, the agent is automatically configured and ready to communicate over Secure Sockets Layer (SSL). Before continuing with the tasks in this section, however, ensure that the Lotus Domino 8.5.2 instance is configured for SSL. For information, see the Lotus Domino 8.5.2 documentation: `https://www.ibm.com/developerworks/lotus/documentation/domino/`.

- Section 1.4.9.1, "Disabling the Trust Behavior of the Lotus Domino 8.5.2 Agent"
- Section 1.4.9.2, "Installing the Oracle OpenSSO Root CA Certificate on the Lotus Domino 8.5.2 Instance"

1.4.9.1 Disabling the Trust Behavior of the Lotus Domino 8.5.2 Agent

By default, the Lotus Domino 8.5.2 agent installed on a remote Lotus Domino 8.5.2 instance trusts any server certificate presented over SSL by the Oracle OpenSSO host server. For the Lotus Domino 8.5.2 agent to perform certificate checking, you must disable this behavior.

1.4.9.1.1 To Disable the Trust Behavior of the Lotus Domino 8.5.2 Agent

1. Find the Lotus Domino 8.5.2 agent's `OpenSSOAgentBootstrap.properties` file in the agent's `/config` directory. For example:

   ```
   /opt/web_agents/domino_agent/Agent_
   001/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 Oracle OpenSSO host server:

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

- Specify the certificate database directory. For example:

  ```
  com.sun.identity.agents.config.sslcert.dir = /opt/certdb
  ```

- 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 Oracle OpenSSO server.

1.4.9.2 Installing the Oracle OpenSSO Root CA Certificate on the Lotus Domino 8.5.2 Instance

The root CA certificate that you install on the Lotus Domino 8.5.2 instance must be the same certificate that is installed on the Oracle OpenSSO host server.

Oracle provides the Certificate Database Tool, `certutil`, in the Lotus Domino 8.5.2 agent distribution file, to manage the root CA certificate and the certificate database.

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

1.4.9.2.1 To Install the Oracle OpenSSO Root CA Certificate on the Lotus Domino 8.5.2 Instance

1. Obtain the root CA certificate file that is installed on the Oracle OpenSSO host server.
2. On the Lotus Domino 8.5.2 instance, locate the `certutil` utility.

   After you unzip the Lotus Domino 8.5.2 agent distribution file, `certutil` is available in the *`PolicyAgent-base`*`/bin` directory.

   For example: `/opt/web_agents/domino_agent/bin/certutil`
3. Before you use `certutil`, set the `LD_LIBRARY_PATH` environment variable to the location of the `certutil` library files.

   After you unzip the Lotus Domino 8.5.2 agent distribution file, these library files are available in the *`PolicyAgent-base`*`/lib` directory.

   For example: `/opt/web_agents/domino_agent/lib`
4. If necessary, create the certificate database using `certutil`. For example:

   ```
   # cd /opt/web_agents/domino_agent/bin
   # mkdir /opt/domino_agent/certdb
   # ./certutil -N -d /opt/domino_agent/certdb
   ```

5. Install the Oracle OpenSSO root CA certificate using `certutil`. For example:

   ```
   # ./certutil -A -n cert-name -t "C,C,C" -d /opt/domino_agent/certdb -i
   cert-file
   ```

where:

- *cert-name* is the name of the Oracle OpenSSO root CA certificate.
- *cert-file* is the base-64 encoded root CA certificate file.

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

```
# ./certutil -L -d /opt/certdb
```

You should see the name of the root CA certificate.

7. Restart the Lotus Domino 8.5.2 instance.

1.4.10 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.

1.4.10.1 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 Lotus Domino 8.5.2 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 /opt/web_agents/domino_agent/bin
      ```
   c. Encrypt the new password using the `agentadmin` program. For example:

      ```
      #./agentadmin --encrypt Agent_001 /tmp/domino8agentpw
      ```

      `Agent_001` is the agent instance whose password you want to encrypt.

      `domino8agentpw` is the password file in the `/tmp` directory.

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

      ```
      The encrypted value is: /54GwN432q+MEnfh/AHLMA==
      ```
   d. In the *agent-instance*`/config/OpenSSOAgentBootstrap.properties` file, set the following property to the new encrypted password from the previous step. For example:

      ```
      com.sun.identity.agents.config.password=/54GwN432q+MEnfh/AHLMA==
      ```
   e. Restart the Lotus Domino 8.5.2 instance that is being protected by the policy agent.

1.5 Managing the Lotus Domino 8.5.2 Agent

Oracle 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:

- Oracle OpenSSO Administration Console

  You can manage both version 3.0 J2EE and web agents from the Oracle 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 Oracle 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*.

1.5.1 Managing a Version 3.0 Agent with a Local Configuration

In some scenarios, you might need to deploy a version 3.0 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, the local configuration is used by default.

The following property in the Oracle OpenSSO server Agent Service schema (`AgentService.xml` file) indicates that the configuration is local:

```
com.sun.identity.agents.config.repository.location=local
```

In this scenario, you must manage the version 3.0 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).

> **Caution:** A version 3.0 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 Oracle OpenSSO server. In most cases, you won't need to edit the bootstrap file; however, if you do edit the file, be very careful, or the agent might not function properly.

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

1.5.1.1 Changing an Existing Centralized Configuration to a Local Configuration

If you have an existing agent profile with a centralized configuration and you want to change the configuration to local, edit the agent profile in the Oracle OpenSSO Console, as follows:

1. Log in to the Oracle OpenSSO Console as `amadmin`.
2. Click Access Control, *realm-name*, Agents, Web, and then the name of the version 3.0 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.

You can now manage the agent by editing the properties in the agent's local `OpenSSOAgentConfiguration.properties` file.

1.6 Uninstalling the Lotus Domino 8.5.2 Agent

This section provides the following information about unintalling the agent:

- Section 1.6.1, "Preparing to Uninstall the Lotus Domino 8.5.2 Agent"
- Section 1.6.2, "Uninstalling the Lotus Domino 8.5.2 Agent Using the `agentadmin` Program"
- Section 1.6.3, "Removing the DSAPI Filter for the Lotus Domino 8.5.2 Agent"

1.6.1 Preparing to Uninstall the Lotus Domino 8.5.2 Agent

1.6.1.1 To Prepare to Uninstall Lotus Domino 8.5.2 Agent

1. Undeploy any applications protected by the Lotus Domino 8.5.2 agent.
2. Stop the Lotus Domino 8.5.2 instance, if it is running.

1.6.2 Uninstalling the Lotus Domino 8.5.2 Agent Using the `agentadmin` Program

1.6.2.1 To Uninstall the Lotus Domino 8.5.2 Agent

1. Change to the *`PolicyAgent-base`*`/bin` directory. For example:

   For example: `cd /opt/web_agents/domino_agent/bin`
2. Issue one of the following commands:

   ```
   # ./agentadmin --uninstall
   ```

   or

   ```
   # ./agentadmin --uninstallAll
   ```

   The `--uninstall` option removes only one instance of the agent, while the `--uninstallAll` option prompts you to remove all configured instances of the agent.
3. The `uninstall` program prompts you for the complete path to the Lotus Domino 8.5.2 data or configuration files.

For example: `/opt/domino/notesdata`

4. The `uninstall` program displays the path and then asks if you want to continue:

   To continue with the uninstallation, select 1 (the default).

   The `uninstall` program uninstalls the agent (or all configured instances, if specified).

   ```
   /opt/web_agents/domino_
   agent/installer-logs/audit/uninstall.log
   ```

Example 1–1 Lotus Domino 8.5.2 Agent Uninstall Sample Run

```
**************************************************************************
Welcome to the OpenSSO Policy Agent for IBM Lotus Domino Server.
**************************************************************************

Removing Agent Instance ...

Enter the complete path to the directory which is used by IBM Lotus Domino
Server to store its data or configuration files. This directory uniquely
identifies the IBM Lotus Domino Server instance that is secured by this
Agent.
[ ? : Help, ! : Exit ]
Enter the IBM Lotus Domino Data Directory [/opt/domino/notesdata]:

---------------------------------------------
SUMMARY OF YOUR RESPONSES
---------------------------------------------
IBM Lotus Domino Data Directory : /opt/domino/notesdata

Verify your settings above and decide from the choices below.
1. Continue with Uninstallation
2. Back to the last interaction
3. Start Over
4. Exit
Please make your selection [1]:

Deleting the config directory
/opt/domino/agent/web_agents/domino_agent/Agent_001/config ...DONE.


Uninstall log file location:
/opt/domino/agent/web_agents/domino_agent/installer-logs/audit/uninstall.log

Thank you for using OpenSSO Policy Agent for IBM Lotus Domino Server.
```

1.6.2.2 After You Finish the Uninstall

- The `/config` directory is removed from the agent instance directory, but the `/installer-logs` directory still exists.
- The `uninstall` program creates the `uninstall.log` file in the *`PolicyAgent-base`*`/installer-logs/audit` directory. For example:

  ```
  /opt/web_agents/domino_
  agent/installer-logs/audit/uninstall.log
  ```

- The agent instance directory is not automatically removed. For example, if you uninstall the agent for `Agent_001`, a subsequent agent installation creates the

`Agent_002` instance directory. To remove an agent instance directory, you must manually remove the directory.

You must also remove the Domino Web Server API (DSAPI) filter as described in Removing the DSAPI Filter for the Lotus Domino 8.5.2 Agent.

1.6.3 Removing the DSAPI Filter for the Lotus Domino 8.5.2 Agent

After you run the uninstall program, you must manually remove the Domino Web Server API (DSAPI) filter that was added as a post-installation step.

1.6.3.1 To Remove the DSAPI Filter for the Lotus Domino 8.5.2 Agent

1. In the Lotus Domino 8.5.2 Administrator web console, select the Configuration tab.
2. In the left pane, under Server, click All Server Documents.

   A window appears, displaying a list of servers.
3. From the list of servers, select the Lotus Domino 8.5.2 server instance that you want to configure.
4. Click Internet Protocols.
5. Select the HTTP tab.
6. Click Edit Server.
7. In the DSAPI Filter File Names field, remove the DSAPI filter file. For example:
   - Solaris and Linux systems: `/opt/web_agents/domino_agent/lib/libamdomino.so`
   - AIX systems: `/opt/web_agents/domino_agent/lib/libamdomino.a`
   - Windows: `c:\web_agents\domino_agent\lib\amdomino.dll`
8. Click Save and then Close to save the changes.
9. Restart the Lotus Domino 8.5.2 or HTTP server.