

Sun™ ONE Identity Server Policy Agents Release Notes

Version 2.1

Part Number 816-6900-10

April 2005

These release notes contain important information available at the time of the release of Sun™ Open Net Environment (Sun ONE) Identity Server Policy Agents, version 2.1. Sun ONE Identity Server Policy Agents comprise Web Policy Agents for web and proxy servers and J2EE Policy Agents for application servers.

In this document and in related documentation, you might see Sun ONE Identity Server referred to as Sun Java™ System Identity Server and Sun Java™ System Access Manager. These three names refer to the same product, but different versions.

J2EE Agents are also being released as version 2.1.1, with CDSSO support. This feature enables the J2EE agents to successfully achieve Single Sign-On in a multi-domain deployment scenario.

The most up-to-date version of these release notes and the Sun ONE Identity Server Policy Agents guides can be found at the Sun ONE documentation web site:

http://docs.sun.com/db/coll/S1_IdServPolicyAgent_21. Check the web site prior to installing and setting up your software and then periodically thereafter to view the most up-to-date release notes and manuals.

These release notes contain the following sections:

- [Revision History](#)
- [About Sun ONE Identity Server Policy Agents](#)
- [Installation Notes](#)
- [Known Issues](#)
- [How to Report Problems and Provide Feedback](#)
- [Additional Sun Resources](#)

Revision History

Table 1 Revision History

Date	Description of Changes
March 2005	<p>Release notes for the J2EE Policy Agent for IBM WebSphere Application Server 5.0/5.1 and for Sun Java™ System Application Server 8.1.</p> <p>Release notes for the Web Policy Agent for Apache 1.3.29 and for Apache 2.0.52.</p> <p>Added info about load balancing</p>
December 2004	<p>Release notes for the J2EE Policy Agent for BEA WebLogic 8.1 SP3 Server/Portal</p> <p>Release notes for the Web Policy Agent for Apache 2.0.50</p>
November 2004	<p>Release notes for the J2EE Policy Agent for SAP Enterprise Portal 6.0 SP2 and Web Application Server 6.20 SP1 and for the J2EE Policy Agent for BEA WebLogic 8.1 SP2 Server/Portal.</p>
September 2004	<p>Release notes for the J2EE Policy Agent for Macromedia JRun 4 Application Server and a new platform support for the policy agent for BEA WebLogic Server 7.0 SP2.</p>
August 2004	<p>Release notes for the Web Policy Agent for IBM Lotus Domino 6.5/6.5.1.</p>
July 2004	<p>Release notes for the Web Policy Agents for Microsoft IIS 6.0, Oracle Application Server 10g, Sun Java System Web Server 6.1.</p>
June 2004	<p>Release notes for the Web Policy Agent for Apache 2.0.48.</p>
April 2004	<p>Release notes for the J2EE Policy Agents for Tomcat Server 4.1.27, Oracle9i Application Server Release 2 and SAP Enterprise Portal 6.0 SP2.</p> <p>Release notes for the Web Policy Agent for SAP Internet Transaction Server 2.0 and J2EE Policy Agents, version 2.1.1.</p>
March 2004	<p>Release notes for the Web Policy Agent for Oracle9iAS R1 1.3.29</p>
February 2004	<p>Release notes for the Web Policy Agent for IBM HTTP Server 1.3.26.</p>
January 2004	<p>Release notes for the J2EE Policy Agent for BEA WebLogic Server 8.1. This agent is certified to work with Sun ONE Identity Server 6.1.</p>
November 2003	<p>Release notes for the Web Policy Agents for Sun ONE Web Server 6.1 and Apache 2.0.47, and the J2EE Policy Agent for BEA WebLogic Server 8.1.</p>
September 2003	<p>Release notes for the J2EE Policy Agent for PeopleSoft 8.3/8.4/8.8 and Web Policy Agents for Lotus Domino 5.0.11, IBM HTTP Server 1.3.19, and Microsoft IIS 5.0.</p>
August 2003	<p>Release notes for the J2EE Policy Agent for BEA WebLogic Server 7.0 SP2</p>
June 2003	<p>First release of Sun ONE Identity Server J2EE Policy Agents, version 2.1. Includes the policy agents for Sun ONE Application Server 7.0, BEA WebLogic Server 6.1 SP2, IBM WebSphere Application Server 5.0.</p>

Table 1 Revision History (*Continued*)

Date	Description of Changes
June 06, 2003	Added Web Policy Agents for Apache 1.3.27, Sun ONE Web Proxy Server 3.6 and Lotus Domino 6.0.1
May 27, 2003	First release of the Sun ONE Identity Server Web Policy Agents, version 2.1. Includes Sun ONE Web Server 6.0 SPx policy agent.

About Sun ONE Identity Server Policy Agents

Sun ONE Identity Server Policy Agents, version 2.1 protect content on supported web, proxy, and application servers from unauthorized intrusions. They control access to services and web resources based on the policies configured by an administrator. For a list of supported servers, see the following sections:

- [Web Policy Agents](#)
- [J2EE Policy Agents](#)

Web Policy Agents

The following table presents the Web Policy Agents, version 2.1 and the platforms they support. This version of agents works with Sun ONE Identity Server, versions 6.0 SP1, 6.1 and 6.2. Note that the agent supported on Solaris 8 is generally also supported on Solaris 9 and vice versa.

Table 2 Web Policy Agents (*1 of 3*)

Agent	Platforms
Sun ONE Web Server 6.0 SPx	Solaris 8
	Solaris 9
	Microsoft Windows 2000 Server
	HP-UX 11.11
Sun ONE Web Proxy Server 3.6 (in reverse proxy mode)	Solaris 8
Apache 1.3.27	Solaris 8
	Solaris 9

Table 2 Web Policy Agents (2 of 3) (Continued)

	Red Hat Linux 7.2
Lotus Domino 6.0.1	Microsoft Windows 2000 Server
Lotus Domino 5.0.11	Solaris 8
	Microsoft Windows 2000 Server
IBM HTTP Server 1.3.19	Solaris 8
Microsoft IIS 5.0	Microsoft Windows 2000 Server
Apache 2.0.47	Red Hat Linux 9.0
IBM HTTP Server 1.3.26	Solaris 8
	Solaris 9
Sun ONE Web Server 4.1	Solaris 8
Oracle9iAS R1 Apache 1.3.29	Solaris 8
SAP Internet Transaction Server 2.0	Microsoft Windows 2000 Advanced Server
Apache 2.0.48	Solaris 8
	Solaris 9
	Red Hat Advanced Server 2.1
Microsoft IIS 6.0	Microsoft Windows Server 2003
Sun Java System Web Server 6.1	Solaris 8
	Solaris 9 x86
	Microsoft Windows 2000 Server
	Microsoft Windows Server 2003
Oracle 10g Apache Server	Solaris 9
IBM Lotus Domino 6.5	Solaris 9
	Microsoft Windows 2000
	Microsoft Windows Server 2003 EE
IBM Lotus Domino 6.5.1	Red Hat Advanced Server 2.1
Apache 2.0.50	Microsoft Windows Server 2003 EE
Apache 1.3.29	SuSE Linux 8.2

Table 2 Web Policy Agents (3 of 3) (Continued)

Apache 2.0.52	Debian Linux 3.0
	SuSE Linux 8.2

J2EE Policy Agents

The following table presents the J2EE Policy Agents, versions 2.1 and 2.1.1 and the platforms they support. These versions of the agents support Sun ONE Identity Server 6.0 SP1, 6.1 and 6.2. Note that the agent supported on Solaris 8 platform is generally also supported on Solaris 9 platform and vice versa.

Table 3 J2EE Policy Agents (1 of 3)

Policy Agent for	Platforms Supported by the Agent	Agent Version Available
Sun ONE Application Server 7.0	Solaris 8	2.1, 2.1.1
	Solaris 9	2.1, 2.1.1
	Windows 2000 Server	2.1, 2.1.1
	Red Hat Advanced Server 2.1	2.1, 2.1.1
BEA WebLogic Server 6.1 SP2	Solaris 8	2.1, 2.1.1
	Solaris 9	2.1
	Windows 2000	2.1
	HP-UX 11	2.1
IBM WebSphere Application Server 5.0	Solaris 8	2.1, 2.1.1
	Windows 2000	2.1, 2.1.1
	AIX 5.1	2.1, 2.1.1
	AIX 5.2	2.1.1
	Red Hat Advanced Server 2.1	2.1.1
BEA WebLogic Server 7.0 SP2	Solaris 8	2.1
	Solaris 9	2.1
	Red Hat Advanced Server 2.1	2.1

Table 3 J2EE Policy Agents (2 of 3)

	HP-UX 11.11	2.1
PeopleSoft 8.3/8.4/8.8	Solaris 8	2.1
	HP-UX 11	2.1
BEA WebLogic Server 8.1	Solaris 8	2.1
	Solaris 9	2.1
	Red Hat Advanced Server 2.1	2.1
	HP-UX 11.11	2.1
Tomcat Server 4.1.27	Solaris 8	2.1
	Solaris 9	2.1
	Red Hat Advanced Server 2.1	2.1
Oracle9i Application Server Release 2 (version 9.0.3)	Solaris 8	2.1
SAP Enterprise Portal 6.0 SP2	Solaris 8	2.1
	Solaris 9	2.1
	AIX 5.2	2.1
Oracle Application Server 10g (versions 9.0.3 and 9.0.4)	Solaris 8	2.1
Macromedia JRun 4 Application Server	Solaris 8	2.1, 2.1.1
	Solaris 9	2.1, 2.1.1
	Red Hat Enterprise Linux 3.0	2.1, 2.1.1
SAP Enterprise Portal 6.0 SP2 and Web Application Server 6.20 SP1	Windows Server 2003 Enterprise Edition	2.1
BEA Weblogic 8.1 SP2 Server/Portal	Solaris 8	2.1
	Solaris 9	2.1
BEA Weblogic 8.1 SP3 Server/Portal	Red Hat Enterprise Linux AS 3.0	2.1
	Solaris 8	2.1
	Solaris 9	2.1
IBM WebSphere Application Server 5.1	Solaris 8	2.1.1
Sun Java System Application Server 8.1	Solaris 8	2.1

Table 3 J2EE Policy Agents (3 of 3)

	Solaris 9	2.1
	Solaris 10	2.1
	Solaris 9 x86	2.1
	Red Hat Advanced Server 2.1	2.1

Installation Notes

Detailed steps to install and configure Sun ONE Identity Server Policy Agents, version 2.1 on the supported web, proxy and application servers are provided in the Web Policy Agents Guide and the J2EE Policy Agents Guide.

Known Issues

For a list of issues known at the time of release of the agents, see the following sections:

- [All Policy Agents](#)
- [Web Policy Agents](#)
- [J2EE Policy Agents](#)

All Policy Agents

If your deployment uses load balancing, contact your Sun Microsystems representative about obtaining the proper patch for your specific needs.

Web Policy Agents

This section contains a list of the important known issues at the time of the release of Web Policy Agents. Click from the following links to go to the appropriate section.

- [All Web Policy Agents](#)
- [Policy Agent for SAP ITS 2.0](#)
- [Policy Agent for Microsoft IIS 6.0](#)
- [Policy Agent for Oracle9iAS R1 and Oracle Application Server 10g](#)
- [Policy Agent for IBM Lotus Domino 6.5](#)
- [Policy Agent for Sun Java System Web Server 6.1](#)

All Web Policy Agents

The browser would behave erratically if a user accesses a resource where the `loginURL` (in the non-CDSSO mode) or the `cdcservlet` (in the CDSSO mode) property includes the module parameter, and the resource is protected by a policy with condition `auth level` or `auth scheme`. (#4983865)

Workaround

Follow these guidelines:

- Do not use a query parameter for the `loginURL` or the `cdcservlet` property in the `AmAgent.properties` file. Define a policy with `auth conditions`.
- When a module query parameter is set for `loginURL` or the `cdcservlet` property, do not add `auth conditions` to the policies.
- If you have authentication methods other than LDAP as a standard mechanism, it can be configured as a default `auth module` on a per `org/role` basis from Sun ONE Identity Server. Policy `auth conditions` can then be safely used.

When a user tries to access a URL path on a web server that does not result in a physical resource (file, image, JSP, servlet, etc.), the agent will redirect the user to the Sun ONE Identity Server authentication page. (#4979826)

The policy agent considers a URL path on a web server that does not result in a physical resource (file, image, JSP, servlet, etc.) as `path info`. For security reasons, the agent excludes the `path info` from pattern matching in the Not Enforced URL List. In these cases, the agent will redirect the user to the Sun ONE Identity Server authentication page.

Workaround

Make sure the resources on the web server that you are accessing do exist.

If the “module=” parameter is specified in the loginURL property, the agent denies access to resources. (#4983859)

If there is no value specified for the property `com.sun.am.policy.am.library.loginURL`, the agent uses the value of `com.sun.am.policy.am.loginURL` to log onto Sun ONE Identity Server as an agent. Yet, if the user adds a module parameter in the login URL, the agent login to Sun ONE Identity Server will fail because the agent does not know to take the module parameter out before identifying itself to Sun ONE Identity Server.

Workaround

Modify the value of `com.sun.am.policy.am.loginURL`, and set a valid value for `com.sun.am.policy.am.library.loginURL`. By default this is empty.

If a web server host has more than one host name, the agent will allow the user to access only the host URL that he logs in first. The agent will display an error when the user tries to access the second host URL. (#4981755).

Workaround

None exists at this time.

The cookie-hijacking workaround for Sun Java System Identity Server does not work with agents on Windows platforms. The workaround for preventing cookie hijacking is explained in the Identity Server release notes. (#6190422)

Workaround

None exists at this time

Policy Agent for SAP ITS 2.0

When you have an SSO environment with two SAP ITS systems (that is two back-end R/3 systems) and any number of other web applications, the Internet Explorer browser may behave erratically. If, however, there is only one SAP ITS system in the SSO environment, the Internet Explorer works properly.

Workaround

Use Netscape 7 or Mozilla as the browser if the SSO environment involves two back-end SAP ITS systems.

Using Internet Explorer, log on to Identity Server and access a protected SAP application page. If you try to reload this page now, the browser hangs. (#4989653)

Workaround

Use Netscape 7 or Mozilla as the browser.

You are accessing a protected SAP page using Internet Explorer and the session is timed out. Now, if you try to access this page again, the browser hangs. (#4989659)

Workaround

Use Netscape 7 or Mozilla as the browser.

On Solaris 8 and 9, the Apache agent disallows directory browsing if the `index.html` page is not included in the `notEnforcedList`. (#4865950)

Workaround

Add the `index.html` page to the `notEnforcedList` in the `AMAgent.properties` file.

Policy Agent for Microsoft IIS 6.0

The policy agent displays the error “Service Unavailable” when a user tries to access a URL in the Not Enforced List. (#5043366)

Workaround

In the URLs listed in the Not Enforced List in `AMAgent.properties`, make sure that wildcard characters are not used for a protocol, a hostname, or a port number. Wildcard characters can be used to define only a pattern of URLs.

When the agent for Microsoft IIS 6.0 is configured for CDSSO, if a user tries to access a protected resource and refreshes the browser multiple times, it is possible that the browser hangs. (#5051486)

Workaround

Make sure the system time of the machines hosting the application and Sun ONE Identity Server are in sync. Close the browser and open a new browser session.

When the agent for Microsoft IIS 6.0 is configured for CDSSO, if a policy is modified and the resources protected by this policy are simultaneously accessed by a user, the user might be denied access. The `amAgent` log would record the error “Invalid application secret.” (#5051486)

Workaround

User should wait for policy notifications to be sent to the agent before accessing protected resources. A restart of the agent web server is required when the error “Invalid application secret” is encountered.

Policy Agent for Oracle9iAS R1 and Oracle Application Server 10g

After installing the Oracle 9iAS Apache agent, when you run the `config` script to configure the server instance, it does not take the correct Apache Server binary directory. (#4993833)

Workaround

When using the `config` script to configure a second instance of Apache Web Server, you should always give a full path for the Apache Server binary directory.

The Unconfig script fails to remove the debug directory. (#4999369)

Workaround

Remove the debug directory manually.

When the Oracle 9iAS R1 Apache 1.3.29 agent is configured in the SSO_ONLY mode and if a policy is created with a session condition that specifies Terminate User Session as true, the policy terminates the user session. If the value of Terminate User Session is false, the user will be denied access to resources. (#5004246)

Workaround

Do not create a policy with session condition when Oracle 9i AS Apache agent is configured in the SSO_ONLY mode.

After installing the agent, the installation program for Oracle9iAS R1 or Oracle Application Server 10g changes the ownership of the file httpd.conf from the user oracle to the user root. This may cause Oracle startup problems. (#5052932)

Workaround

Change the permissions to the user oracle manually.

The integration of Sun Java System Identity Server and Oracle Application Server 10g does not work well when Identity Server is installed on a different domain. When the agent is enabled for Cross Domain Single Sign On (CDSSO), a user accessing SSO Server or Portal Server sees the 500 Internal Server Error. (#5069515)

Workaround

Make sure that the Sun ONE Identity Server host is on the same domain as Oracle Application Server 10g. CDSSO is not supported for the current Oracle Single Sign On solution with Sun ONE Identity Server policy agent.

In the integrated setup of Sun Java System Identity Server and Oracle Application Server 10g, if, using Internet Explorer 6, a user clicks Login on the Oracle Portal page, the application shows an error page. However, this error does not appear when the Mozilla or the Netscape browser is used. The problem possibly happens due to the way Internet Explorer handles multiple redirections. Since Oracle Portal and Oracle SSO Servers are on the same machine, the Login link on the Portal actually points to Oracle Portal, which redirects the request back to Oracle SSO Server, which is protected by the agent. When the agent gets the URL, the port number is set to 7778 when it should be 7777, and the URL is allowed without redirect/authentication since only the Login URL with port 7777 is enforced. (#5069541)

Workaround

- This problem occurs only if you are using Internet Explorer. Hence, use Mozilla or Netscape instead.
- Alternatively, install Oracle Portal Server and Oracle SSO Server on different systems.
- If both the above options are not possible, always login through Oracle SSO Server first, and then access Oracle Portal Server.

- Use the `config` script to configure a second instance of the agent to protect the port 7778. In the `AMAgent.properties` file of this agent instance, set the value of the property `com.sun.am.policy.agents.reverse_the_meaning_of_notenforcedList` to `true` and set the value of `not-enforced list` as shown in the following sample:

```
com.sun.am.policy.agents.notenforcedList =
http://sb1000-29-09.sfbay.example.com:7778/sso/auth*
http://sb1000-29-09.sfbay.example.com:7778/pls/portal/PORTAL.wwsec_app_priv.login?p_re
quested_url=http%3A%2F%
2Fsb1000-29-09.sfbay.example.com%3A7778%2Fpls%2Fportal%2FPORTAL.home&p_cancel_url=http
%3A%2F%2Fsb1000-29-09.sfbay.example.com%3A7778%2Fpls%2Fportal%2FPORTAL.home
```

Policy Agent for IBM Lotus Domino 6.5

The property `com.sun.am.policy.agents.notenforcedList` does not support URLs with wildcards (the character “*”). If a wildcard is used, only the root URL is recognized. (#5055809)

Workaround

None exists at this time. This behavior is caused by a bug with the PATH-INFO server variable in the IBM Lotus Domino Server.

If access to a resource is allowed by the agent but denied by Domino ACL, another HTTP basic authentication login prompt will appear. (#5062773)

Workaround

None exists at this time. This prompt is displayed by Domino Server and there is no workaround in Domino to return the error HTTP 403 Forbidden instead of the login prompt.

Policy Agent for Sun Java System Web Server 6.1

The uninstallation program does not remove a file (#4868706)

When you run the agent uninstallation program on Windows 2000, it does not remove the following file from the directory `Agent_Install_Dir\es6\bin`:

```
ames6.dll
```

Workaround

Delete the file manually.

Adding a query parameter to `com.sun.am.policy.agents.cdcservletURL` fails to redirect when the agent is CDSSO enabled (#6196728).

Workaround

Do not use query parameters when running in CDSSO mode.

J2EE Policy Agents

This section contains a list of the known issues at the time of the release of J2EE Policy Agents. Click from the following links to go to the appropriate section.

- [All J2EE Policy Agents](#)
- [Policy Agent for IBM WebSphere 5.0/5.1](#)
- [Policy Agent for Sun ONE Application Server 7.0](#)
- [Policy Agent for PeopleSoft 8.3/8.4/8.8](#)
- [Policy Agents for BEA WebLogic Server 6.1 SP2/7.0 SP2/8.1](#)
- [Policy Agents for Oracle9i Application Server Release 2 and Oracle Application Server 10g](#)
- [Policy Agent for SAP Enterprise Portal 6.0 SP2](#)
- [Agent for SAP Enterprise Portal 6.0 SP2 and Web Application Server 6.20 SP1](#)
- [Agent for BEA WebLogic 8.1 SP2 Server/Portal](#)

All J2EE Policy Agents

In the failover environment, the agent will work properly only when the Agent Filter mode is set to either SSO_ONLY or J2EE_POLICY. (#4869458)

Workaround

None exists at this time.

During the command-line installation, from the Identity Server Details prompt, if you return to the Select Installation Directory prompt, the installation program throws an exception. (#4882901)

Workaround

Make sure that you enter the correct installation directory before you proceed to the Sun ONE Identity Server Details prompt. Alternatively, use the GUI-based installation program instead of the command-line program.

Re-installation in silent mode prints the following message: “Incompatible or corrupted state file provided. Cannot continue.” (#4857531)

Workaround

Re-installation of the same agent on the same system is not supported. Instead, use the agent tools to configure the agent for a new instance of the application server. In the case of IBM WebSphere Application Server 5.0/5.1, follow the manual steps provided in the user guide to configure the agent for the new instance of the application server.

No installation status is displayed for any J2EE Agent during silent installation. (#4857532)

Workaround

The user must ensure that the proper environment exists before performing the silent installation/uninstallation. User should check the installation/uninstallation logs to confirm the actual status.

The agent debug log, namely the `amAuthContext` file, displays the `amldapuser` password in the plain text format instead of the encrypted format. (#4873117)

Workaround

This happens only if the `debug` level is set to `message`. Manually change the permission of this file so that only the `root/superuser` has read access. Alternatively, set the debug level to `off` to prevent any sensitive information from appearing in the agent debug logs.

If an invalid FQDN Map is specified and both the login-attempt limit and the redirect-attempt limit are set to 0, then any user who is already authenticated is denied access to the resource. (#4899847)

Workaround

Make sure that you specify a valid FQDN Map.

On Red Hat Advanced Server 2.1, all agent scripts including installation, uninstallation and `agentadmin` require the Korn Shell to be present in the system (#4948025)

Workaround

You may use JDK 1.3.1 or a higher version of Java Virtual Machine to launch the various programs.

The agent does not generate the audit logs, if you have set an invalid value for the property `com.sun.am.policy.amFilter.audit.level` in the `AMAgent.properties` file. (#4966704)

Workaround

Audit logs will not be generated if the value of `com.sun.am.policy.amFilter.audit.level` is invalid. Please ensure that the property has a valid value. Audit logs will be generated when the time specified in the configuration reload interval property elapses or the application server is restarted, if hot-swap is not enabled.

When you have configured a primary server and a failover server for the agent, the agent correctly switches over to the failover server if the primary server is not available. However, even after the primary server is restarted, the agent does not switch back and continues to use the failover server. (#4971291)

Workaround

Stop the failover server and then start the primary server again. The agent automatically returns to the primary server.

If the `agentadmin` script is not run as user `root`, it throws a null pointer exception. (#5020827)

Workaround

This is not a supported usage. Run the tool as user `root`.

All the property names and values in the `AMAgent.properties` file are not case-sensitive even though the description says that they are case-sensitive. (#5018554)

Workaround

For detailed instructions about the properties and their usage, refer the J2EE Policy Agents Guide.

Policy Agent for IBM WebSphere 5.0/5.1

Once the agent is installed and security is enabled, only the “`amldapuser`” can log into the IBM WebSphere 5.0/5.1 Application Server Administrative Console. (#4868888)

Workaround

None exists at this time

Policy Agent for Sun ONE Application Server 7.0

The command-line uninstallation program for the agent for Sun ONE Application Server 7.0 will not work properly if the Administration Server port of Sun ONE Application Server 7.0 is changed after the installation. (#4879650)

Workaround

Make sure the Administration Server port is not changed after the agent is installed. Alternatively, use the GUI-based uninstallation program instead of the command-line program.

The command-line uninstallation program for the agent for Sun ONE Application Server 7.0, will not work properly if the Administration Server user of Sun ONE Application Server 7.0, is changed after the installation. (#4880299)

Workaround

Make sure the Administration Server user is not changed after the agent is installed. Alternatively, use the GUI-based uninstallation program instead of the command-line program.

When running the uninstallation script for Sun ONE Application Server 7.0 agent from the agent’s installation directory, on Red Hat Advanced Server 2.1, the script reports an error that `/bin/dirname` is not found. (#4976473)

Workaround

Create a soft link from `/usr/bin` to `/bin`. For example, `ln -s /usr/bin/dirname /bin/dirname`

When uninstalling the policy agent for Sun ONE Application Server 7.0 using the GUI uninstallation program, if you enter an invalid administrator password, a message pops up saying “Please check if the server is up and running and the admin username, password provided are correct.” (#4964600)

Workaround

Make sure that the Administration Server is running and the application server instance is shut down before you start the uninstallation program.

After the installation of the policy agent for Sun ONE Application Server 7.0, the console displays a few messages. (#4966358)

The following are the messages displayed.

```
CORE1116: Sun ONE Application Server 7.0.0_01
INFO: CORE3016: daemon is running as super-user
WARNING: CORE3283: stderr: Bad level value for property:
com.iplanet.services.debug.level
WARNING: CORE3283: stderr: Bad level value for property:
com.sun.identity.agents.logging.level
WARNING: CORE3283: stderr: Bad level value for property:
com.sun.am.policy.amFilter.audit.level
```

Workaround

Users can ignore these messages. These warning messages do not disable any core functionality of the agent (like audit and agent logs).

Policy Agent for PeopleSoft 8.3/8.4/8.8

When using the PeopleSoft 8.3 agent, if the value of the property `com.sun.am.policy.amAgentLog.disposition` is set to Remote or ALL, the agent will malfunction. (#4919377)

Workaround

By default the value of this property is set to LOCAL during the agent installation. It is recommended that you retain this value. Remote logging is not supported with PeopleSoft 8.3.

PeopleSoft fails to do a normal shutdown after the agent is installed. (#4899838)

Workaround

Some of the application server processes will fail to shut down when you do a normal shutdown from the PeopleSoft Domain Shutdown Menu. You can, instead, do a complete shutdown by choosing Forced shutdown.

Policy Agents for BEA WebLogic Server 6.1 SP2/7.0 SP2/8.1

The uninstallation program of the policy agent for BEA WebLogic Server 8.1 may not remove the agent configuration information from the startup script. (#4968311)

Workaround

You may remove the configuration information manually from the startup script. Restart WebLogic Server.

The error “Logger.log(): ssoToken is null, will not log” is displayed by `amLog` several times even after the successful installation of the agent for WebLogic Server 8.1. (#4968313)

Workaround

Edit the WebLogic Server startup script and remove the following property from the `JAVA_OPTIONS` variable:

```
-Djava.util.logging.manager=com.sun.identity.log.LogManager
```

Also, append the following property at the end of the `JAVA_OPTIONS` variable:

```
-DLOG_COMPATMODE=Off
```

Policy Agents for Oracle9i Application Server Release 2 and Oracle Application Server 10g

The policy agents for Oracle9i Application Server Release 2 and Oracle Application Server 10g do not support fine grained `java2.policy` in this release. (#5026805)

Workaround

None exists at this time.

The policy agents for Oracle 9i Application Server Release 2 and Oracle Application Server 10g do not support Session notifications. By default polling is switched on to keep the agent cache updated. Default polling time is set to three minutes. (#5011227)

Workaround

None exists at this time.

After installing the policy agent for Oracle9i Application Server Release 2, if you try to stop the Enterprise Manager web site using `emctl` command, the Enterprise Manager does not stop completely, instead exits with an exception. (#5019117)

Workaround

You should terminate the `emctl` process manually through the following steps:

1. From `ORACLE_HOME/bin`, execute the following command:

```
cat emctl.pid
```

2. Take the process id of `emctl` and execute the command:

```
ps -ef | grep 2458
```

You will notice an output as follows:

```
orcl 2459 2458 0 13:02:49 pts/4 1:08 ....
```

3. Now, execute the following command:

```
kill -9 2459 2458
```

For more information on stopping the Enterprise Manager web site, refer to Oracle docs at the URL http://download-west.oracle.com/docs/cd/A97329_03/core.902/a92171/tools.htm

Once the agent for Oracle 10g Application Server is installed, users will observe that the OC4J process for the application server is being forcefully shut down after two minutes when stopped through Enterprise Manager, OPMN or `emctl`. (#5057125)

Workaround

Users can decrease the waiting time before OC4J is forcefully shut down by changing the attribute `<stop timeout="" />` in `opmn.xml` for the OC4J component to a timeout value lower than 120 seconds.

For example, to set it to 30 seconds, set the attribute as `<stop timeout="30" />`

The Fully Qualified Domain name (FQDN) feature for the agent for Oracle Application Server 10g does not function properly in a Cross Domain Single Sign On (CDSSO) scenario. (#5060012)

Workaround

None exists at this time.

Policy Agent for SAP Enterprise Portal 6.0 SP2

Remote logging does not work in the policy agent for SAP Enterprise Portal 6.0 SP2. (#5027988)

Workaround

Do the following to set up the remote logging feature:

1. Open the following file:

```
/usr/sap/system-name/j2ee/j2ee_instance_number/additionalsystemproperties
```

2. Set the value of the following property to the full path to the `AMAgent.properties` file for this instance of SAP Enterprise Portal 6.0 SP2:

```
java.util.logging.config.file=
```

You can find the property located between the following comments in the file:

```
# AGENT SETTINGS: BEGIN and # AGENT SETTINGS: OVER
```

Once this property is set and the SAP Enterprise Portal 6.0 SP2 system is restarted, the remote logging feature works properly.

While using the policy agent for SAP Enterprise Portal 6.0 SP2 on AIX 5.2, even if an invalid value is set for the property audit log level (`com.sun.am.policy.amFilter.audit.level`) in the `AMAgent.properties` file, the agent does not default to `LOG_BOTH` as expected. Instead the agent defaults to the value `NONE`. (#5031811)

Workaround

None exists at this time.

Agent for SAP Enterprise Portal 6.0 SP2 and Web Application Server 6.20 SP1

For SAP Enterprise Portal 6.0 SP2 on the Windows 2003 Enterprise Edition platform, the audit log rotation sometimes fails to rotate when the rotate size is changed in `AMAgent.properties`. (#6178114)

Workaround

Restart SAP Enterprise Portal 6.0 SP2.

When the `agentadmin` tool is used to configure or unconfigure a second agent instance, the last question is “Enter the path to SAP Enterprise Portal Server Directory?” The question should be “Enter the path to SAP Server Directory?” (#6182298)

Workaround

None exists at this time.

Agent for BEA WebLogic 8.1 SP2 Server/Portal

Public API `public java.lang.String getSSOTokenForUser (javax.ejb.EJBContext context)` works for `USE_DN` user mapping mode only. For LDAP and `HTTP_HEADER` mode, users get a message that clearly states that the API is not supported for LDAP and `HTTP_HEADER` user mapping modes. (#6182716)

Workaround

None exists at this time.

How to Report Problems and Provide Feedback

If you have problems with Sun ONE Identity Server, contact Sun customer support using one of the following mechanisms:

- Sun Software Support services online at <http://www.sun.com/service/sunone/software>

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:

- Description of the problem, including the situation where the problem occurs and its impact on your operation
- Machine type, operating system version, and product version, including any patches and other software that might be affecting the problem
- Detailed steps on the methods you have used 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. Email your comments to Sun at this address:

docfeedback@sun.com

Please include the part number (816-6900-10) of the document in the subject line and the book title (*Sun ONE Identity Server Policy Agents Release Notes*) in the body of your email.

Additional Sun Resources

Useful Sun ONE information can be found at the following Internet locations:

- **Documentation for Sun ONE Identity Server**
http://docs.sun.com/db/coll/S1_IdServ_60
- **Sun Java Enterprise System Documentation**
<http://docs.sun.com/db/prod/entsys#hic>
- **Sun ONE Documentation**
<http://docs.sun.com/prod/sunone>
- **Sun ONE Professional Services**
<http://www.sun.com/service/sunps/sunone>
- **Sun ONE Software Products and Service**
<http://www.sun.com/software>
- **Sun ONE Software Support Services**
<http://www.sun.com/service/sunone/software>
- **Sun ONE Support and Knowledge Base**
<http://www.sun.com/service/support/software>
- **Sun Support and Training Services**
<http://www.sun.com/supporttraining>
- **Sun ONE Consulting and Professional Services**
<http://www.sun.com/service/sunps/sunone>
- **Sun ONE Developer Information**
<http://sunonedev.sun.com>
- **Sun Developer Support Services**
<http://www.sun.com/developers/support>
- **Sun ONE Software Training**
<http://www.sun.com/software/training>
- **Sun Software Data Sheets**
<http://www.sun.com/software>

Copyright © 2004 Sun Microsystems, Inc. All rights reserved.

Sun, Sun Microsystems, the Sun logo, Solaris, Java and the Java Coffee Cup logo are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries. Use of Identity Server is subject to the terms described in the license agreement accompanying it.