

Sun Java System Access Manager Policy Agent 2.2 Release Notes

Copyright © 2010, 2011, Oracle and/or its affiliates. All rights reserved.

License Restrictions Warranty/Consequential Damages Disclaimer

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

Warranty Disclaimer

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

Restricted Rights Notice

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS

Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

Hazardous Applications Notice

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Trademark Notice

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group in the United States and other countries.

Third Party Content, Products, and Services Disclaimer

This software or hardware and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Contents

Preface	5
 Sun Java System Access Manager Policy Agent 2.2 Release Notes 11	
About Access Manager Policy Agent 2.2	12
What's New in This Release	12
What's New About Web Agents in This Release	12
What's New About J2EE Agents in This Release	14
Policy Agent 2.2-05 Update Release	19
Web Agents in the Policy Agent 2.2-05 Update Release	19
Key Fixes and Enhancements in the Policy Agent 2.2-05 Update Release	20
Known Issues in the Policy Agent 2.2-05 Update Release	22
Policy Agent 2.2-04 Update Release	22
Web Agents in the Policy Agent 2.2-04 Update Release	23
Key Fixes and Enhancements in the Policy Agent 2.2-04 Update Release	24
Policy Agent 2.2-03 Update Release	26
Java EE Agents in the Policy Agent 2.2-03 Update Release	26
Web Agents in the Policy Agent 2.2-03 Update Release	27
Policy Agent 2.2-02 Update Release	32
Policy Agent 2.2-02 Update For Web Agents	32
Policy Agent 2.2-02 Update For J2EE Agents	33
Key Fixes and Enhancements in the Policy Agent 2.2-02 Update	34
Policy Agent 2.2-01 Update Release	37
Policy Agent 2.2-01 Web Agents	38
Policy Agent 2.2-01 J2EE Agents	43
Supported Servers in Policy Agent 2.2	50
Understanding Server and Operating System Support for Policy Agent 2.2	50
Supported Servers for Web Agents in Policy Agent 2.2	52
Supported Servers for J2EE Agents in Policy Agent 2.2	57

Compatibility With Access Manager and OpenSSO Enterprise	63
Installation Notes	64
Installation Notes for Web Agents in Policy Agent 2.2	64
Installation Notes for J2EE Agents in Policy Agent 2.2	64
Known Issues and Limitations	66
All Agents in Policy Agent 2.2	66
Web Agents in Policy Agent 2.2	66
J2EE Agents in Policy Agent 2.2	70
Documentation Updates	81
Wrong separator used in web agent guides for com.sun.am.policy.agents.config.local.log.size property (6901494)	81
Policy Agent 2.2 documentation should reference OpenSSO (6857941)	81
Deprecation Notifications and Announcements	82
Redistributable Files	82
How to Report Problems and Provide Feedback	82
Release Notes Revision History	83

Preface

These Sun Java System Access Manager Policy Agent 2.2 Release Notes contain important information about Sun Java System Access Manager Policy Agent 2.2 as it is available at the time of release, including new features, installation notes, known issues and limitations, and how to report problems.

Who Should Use This Book

These *Sun Java System Access Manager Policy Agent 2.2 Release Notes* is intended for use by IT professionals who manage access to their network using Sun Java System servers and software. Administrators should understand the following technologies:

- Directory technologies
- JavaServer Pages (JSP) technology
- HyperText Transfer Protocol (HTTP)
- HyperText Markup Language (HTML)
- eXtensible Markup Language (XML)

Before You Read This Book

Sun Java System Policy Agent software works with Sun Java System Access Manager. Both products work with Sun Java Enterprise System, a software infrastructure that supports enterprise applications distributed across a network or Internet environment. Furthermore, Sun Java System Directory Server is a necessary component in a new Access Manager deployment since it is used as the data store. To understand how these products interact and to understand this book, you should be familiar with the following documentation:

- Sun Java Enterprise System documentation set, which can be accessed online at <http://www.oracle.com/technetwork/indexes/documentation/index.html>. All Sun technical documentation is available online through this web site, including the other documentation sets referred to in this list.

You can browse the documentation archive or search for a specific book title, part number, or subject.

- Sun Java System Directory Server documentation set.

- Sun Java System Access Manager documentation set, which is explained in more detail subsequently in this chapter.
- Sun Java System Access Manager Policy Agent 2.2 documentation set, which is explained in more detail subsequently in this chapter.

How This Book Is Organized

This book is organized in the following manner:

- The Preface provides information about this book to help you use the book to your best advantage.
- [Sun Java System Access Manager Policy Agent 2.2 Release Notes](#) provides the release notes content.

Related Books

Sun Microsystems server documentation sets, some of which are mentioned in this preface, are available at <http://www.oracle.com/technetwork/indexes/documentation/index.html>. These documentation sets provide information that can be helpful for a deployment that includes Policy Agent.

Sun Java System Access Manager Documentation Set

Policy Agent 2.2 was first introduced with Access Manager 7, but now also supports Access Manager 7.1. The Access Manager documentation sets are available at the following locations:

- Sun Java System Access Manager 7.1:
<http://download.oracle.com/docs/cd/E19462-01/index.html>
- Sun Java System Access Manager 7 2005Q4
<http://download.oracle.com/docs/cd/E19461-01/index.html>

Policy Agent 2.2 Documentation Set

These [Sun Java System Access Manager Policy Agent 2.2 Release Notes](#) are available online after an agent or set of agents is released.

- “[Sun Java System Access Manager Policy Agent 2.2 User's Guide](#)” on page 7
- “[Individual Policy Agent Guides](#)” on page 7

Sun Java System Access Manager Policy Agent 2.2 User's Guide

The *Sun Java System Access Manager Policy Agent 2.2 User's Guide* is available in two documentation sets: Access Manager documentation and Policy Agent 2.2 documentation set.

Individual Policy Agent Guides

The individual agents in the Policy Agent 2.2 software set are available on a different schedule than Access Manager itself. Therefore, documentation for Access Manager and Policy Agent are available in separate sets, except for the *Sun Java System Access Manager Policy Agent 2.2 User's Guide*, which is available in both documentation sets.

The documentation for the individual agents is divided into two subsets: a web agent subset and a J2EE agent subset.

Each web agent guide provides general information about web agents and installation, configuration, and uninstallation information for a specific web agent.

Each J2EE agent guide provides general information about J2EE agents and installation, configuration, and uninstallation information for a specific J2EE agent.

The individual agent guides are listed along with supported server information in the following chapters of the *Sun Java System Access Manager Policy Agent 2.2 User's Guide*:

Web Agents	Chapter 2, “Access Manager Policy Agent 2.2 Web Agents: Compatibility, Supported Servers, and Documentation,” in <i>Sun Java System Access Manager Policy Agent 2.2 User's Guide</i>
J2EE Agents	Chapter 3, “Access Manager Policy Agent 2.2 J2EE Agents: Compatibility, Supported Servers, and Documentation,” in <i>Sun Java System Access Manager Policy Agent 2.2 User's Guide</i>

Sun Java Enterprise System Product Documentation

Policy Agent 2.2 was first introduced with Sun Java Enterprise System 2005Q4 and also supports Sun Java Enterprise System 5.

The documentation collections for Sun Java Enterprise System are available at the following location:

[http://www.oracle.com/
technetwork/documentation/legacy-sun-identity-mgmt-193462.html](http://www.oracle.com/technetwork/documentation/legacy-sun-identity-mgmt-193462.html)

Accessing Resources Online

For product downloads, professional services, patches and support, and additional developer information, go to the following:

Oracle Technology Network	http://www.oracle.com/technetwork/index.html
Oracle Software Downloads	http://www.oracle.com/technetwork/indexes/downloads/index.html
Oracle Advanced Customer Services	http://www.oracle.com/us/support/systems/advanced-customer-services/index.html
My Oracle Support	https://support.oracle.com/

Contacting Oracle Technical Support

If you have technical questions about this product that are not answered in the product documentation, go to:

<https://support.oracle.com/>

Related Third-Party Web Site References

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 or alleged to be caused by or in connection with use of or reliance on any such content, goods, or services that are available on or through such sites or resources.

Oracle Welcomes Your Comments

Oracle is interested in improving its documentation and welcomes your comments and suggestions.

To share your comments, go to <http://www.oracle.com/technetwork/indexes/documentation/index.html> and click Send Comments. In the online form, provide the document title and part number. The part number is a seven-digit or nine-digit number that can be found on the title page of the guide or at the top of the document.

For example, the title of this guide is *Sun Java System Access Manager Policy Agent 2.2 Release Notes*, and the part number is 819-2796-38.

Documentation, Support, and Training

See the following web sites for additional resources:

- Documentation (<http://www.oracle.com/technetwork/indexes/documentation/index.html>)
- Support (<http://www.oracle.com/us/support/systems/index.html>)
- Training (http://www.oracle.com/global/us/education/sun_select_country.html) – Choose the country for which you want Training information for former Sun products.

Oracle Software Resources

Oracle Technology Network (<http://www.oracle.com/technetwork/index.html>) offers a range of resources related to Oracle software:

- Discuss technical problems and solutions on the Discussion Forums (<http://forums.oracle.com>).
- Get hands-on step-by-step tutorials with Oracle By Example (<http://www.oracle.com/technetwork/tutorials/index.html>).
- Download Sample Code (http://www.oracle.com/technology/sample_code/index.html).

Typographic Conventions

The following table describes the typographic conventions that are used in this book.

TABLE P-1 Typographic Conventions

Typeface	Meaning	Example
AaBbCc123	The names of commands, files, and directories, and onscreen computer output	Edit your .login file. Use ls -a to list all files. machine_name% you have mail.
AaBbCc123	What you type, contrasted with onscreen computer output	machine_name% su Password:

TABLE P-1 Typographic Conventions *(Continued)*

Typeface	Meaning	Example
<i>aabbcc123</i>	Placeholder: replace with a real name or value	The command to remove a file is <code>rm filename</code> .
<i>AaBbCc123</i>	Book titles, new terms, and terms to be emphasized	Read Chapter 6 in the <i>User's Guide</i> . A <i>cache</i> is a copy that is stored locally. Do <i>not</i> save the file.

Shell Prompts in Command Examples

The following table shows the default UNIX system prompt and superuser prompt for shells that are included in the Oracle Solaris OS. Note that the default system prompt that is displayed in command examples varies, depending on the Oracle Solaris release.

TABLE P-2 Shell Prompts

Shell	Prompt
Bash shell, Korn shell, and Bourne shell	\$
Bash shell, Korn shell, and Bourne shell for superuser	#
C shell	machine_name%
C shell for superuser	machine_name#

Sun Java System Access Manager Policy Agent 2.2 Release Notes

Last updated March 28, 2011

Part number 819-2796-38

These release notes contain important information available at the time of the release of Sun Java System Access Manager Policy Agent 2.2 software. Individual agents comprise the Access Manager Policy Agent software set. These individual agents belong to two distinct categories: web agents and J2EE agents. Web agents protect content on web and proxy servers while J2EE agents protect content on a variety of deployment containers, including application servers and portal servers.

To protect content on a particular server you need to use the specific agent designed for that server. For a list of servers that Policy Agent 2.2 supports, see “[Supported Servers in Policy Agent 2.2](#)” on page 50.

In this document and in related documentation, you might see Sun Java System Access Manager referred to by its previous names: Sun ONE Identity Server or Sun Java System Identity Server.

These release notes contain the following sections:

- “[About Access Manager Policy Agent 2.2](#)” on page 12
- “[What’s New in This Release](#)” on page 12
- “[Policy Agent 2.2–05 Update Release](#)” on page 19
- “[Policy Agent 2.2–04 Update Release](#)” on page 22
- “[Policy Agent 2.2–03 Update Release](#)” on page 26
- “[Policy Agent 2.2–02 Update Release](#)” on page 32
- “[Policy Agent 2.2–01 Update Release](#)” on page 37
- “[Supported Servers in Policy Agent 2.2](#)” on page 50
- “[Compatibility With Access Manager and OpenSSO Enterprise](#)” on page 63
- “[Installation Notes](#)” on page 64
- “[Known Issues and Limitations](#)” on page 66
- “[Documentation Updates](#)” on page 81

- “Deprecation Notifications and Announcements” on page 82
- “Redistributable Files” on page 82
- “How to Report Problems and Provide Feedback” on page 82
- “Release Notes Revision History” on page 83

About Access Manager Policy Agent 2.2

Access Manager Policy Agent 2.2 protects content on supported deployment containers, such as web servers and application servers, from unauthorized intrusions. It controls access to services and web resources based on the policies configured by an administrator.

Other important information about Policy Agent 2.2 can be found in the following sections of these release notes.

What's New in This Release

In Policy Agent 2.2, web agents and J2EE agents offer a variety of new features as described in the following sections:

- “What's New About Web Agents in This Release” on page 12
- “What's New About J2EE Agents in This Release” on page 14

These sections describe the new features available.

What's New About Web Agents in This Release

Several important features have been added to the web agents in the 2.2 release as follows:

- “Support for Fetching User Session Attributes” on page 12
- “Log Rotation” on page 13
- “Policy-Based Response Attributes” on page 13
- “Composite Advice” on page 13
- “Additional Method for Fetching the REMOTE_USER Server Variable” on page 13
- “Malicious Header Attributes Automatically Cleared by Agents” on page 13
- “Load Balancing Enablement” on page 13
- “Support for Heterogeneous Agent Types on the Same Machine” on page 14
- “Support for Turning Off FQDN Mapping” on page 14
- “Web Agents and Backward Compatibility With Access Manager 6.3” on page 14

Support for Fetching User Session Attributes

Before this release of web agents, header and cookie information was retrieved, or *sourced*, solely from user profile properties. Now, header and cookie information can also be sourced from session properties.

Log Rotation

Starting with this release of web agents, when the current log file reaches a specific size, a new log file is created. Log information is then stored in the new log file until it reaches the size limit. This default behavior is configurable. Therefore, log rotation can be turned off and the size limit can be changed.

Policy-Based Response Attributes

Starting with this release of web agents, a new method is available for retrieving header attributes based on Access Manager policy configurations.

Policy-based response attributes take advantage of functionality now available in Access Manager that involves querying policy decisions. In previous versions of Access Manager, header attributes could only be determined by the list of attribute-value pairs in the agent configuration. Now, header attributes can also be determined by Access Manager policy configurations. With policy-based response attributes, you can define attribute-value pairs at each policy definition as opposed to the method used in prior versions of Access Manager, which only allowed policy decisions defined globally in the agent configuration.

Composite Advice

Starting with this release, web agents provide a composite advice feature. This feature allows the policy and authentication services of Access Manager to decouple the advice handling mechanism of the agents. This allows you to introduce and manage custom advices by solely writing Access Manager side plug-ins. Starting with this release, you are not required to make changes on the agent side. Such advices are honored automatically by the composite advice handling mechanism.

Additional Method for Fetching the REMOTE_USER Server Variable

Prior to this release of web agents, the only method for fetching the value of the REMOTE_USER variable set by an agent was from session properties. Starting with the 2.2 release, the value can also be fetched from user profiles. This fetching process uses LDAP.

Malicious Header Attributes Automatically Cleared by Agents

Starting with this release of web agents, malicious header attributes are automatically cleared.

Load Balancing Enablement

Starting with this release of web agents, the default agent hostname, port, and protocol settings can be overridden to enable load balancing.

HTTP requests might pass through an SSL off-loader, load balancer, or proxy server before getting to the web agent. In such cases, the protocol (HTTP scheme), the hostname, or the port

of the web agent might be different than that of the SSL off-loader, load balancer, or proxy server. You can set properties in the web agent `AMAgent.properties` configuration file to ensure that the protocol, hostname, and port of the web agent matches the load balancing mechanism.

Support for Heterogeneous Agent Types on the Same Machine

Starting with this release of web agents, you can install different types of agents on the same machine. Prior to this release, you could not install web agents from different product groups on the same machine. For example, previously, an agent instance for Sun Java System Web Server 6.1 and an agent instance for Apache 2.0.52 could not be installed on the same machine. Now, they can.

Support for Turning Off FQDN Mapping

Starting with this release, fully qualified domain name (FQDN) mapping of HTTP requests can be disabled. In prior web agent releases, the methods employed for checking if a user is using a valid URL could not be turned off.

Web Agents and Backward Compatibility With Access Manager 6.3

Policy Agent 2.2 is backward compatible with Access Manager 6.3 Patch 1 or greater.

Note – Policy Agent 2.2 is only compatible with Access Manager 6.3 when the Access Manager patch has been applied.

Be aware that Policy Agent 2.2 takes advantage of certain features that exist in Access Manager 7 that do not exist in Access Manager 6.3, such as “composite advices,” “policy-based response attributes,” and others.

What's New About J2EE Agents in This Release

Several important features have been added to J2EE agents in release 2.2 as follows:

- “Removal of Dependencies on LDAP and on Administrative Accounts” on page 15
- “Enhanced Installation Process” on page 15
- “Coexistence With Access Manager” on page 16
- “Support for Client Identification Based on Custom HTTP Headers” on page 16
- “Agent Specific Application for Housekeeping Tasks” on page 16
- “URL Policy Enhancements” on page 16
- “Support for Flexible User Mapping Mechanisms” on page 17
- “Support for Fetching User Session Attributes (J2EE Agents)” on page 17
- “Support for Version Checking” on page 17

- “Support for Not-Enforced IP Lists” on page 17
- “Support for Custom Response Headers” on page 17
- “Support for Application Logout Integration” on page 17
- “Support for Application Specific Agent Filter Operation Modes” on page 18
- “Support for Affinity-Based Login URL Selection” on page 18
- “Support for a Sample Application” on page 18
- “J2EE Agents and Backward Compatibility With Access Manager 6.3” on page 18

Removal of Dependencies on LDAP and on Administrative Accounts

Unlike previous releases, J2EE agents in the Policy Agent 2.2 release do not use a direct LDAP connection. Instead, J2EE agents obtain support for their entire functionality by communicating with Access Manager solely with XML over HTTP.

With the authorization of administrators now being handled by an *agent profile* account, the dependence on two administrative accounts, the `amAdmin` account and the `amldapuser` account, has been removed. Now, during installation, the agent installer prompts you for the agent profile account.

Enhanced Installation Process

Starting with this release of J2EE agents, the installation process includes the following features that allow for a smoother, less restrictive, more secure installation process and deployment:

- Support for Installation Using Non-Administrative User Accounts

The requirement in prior agent releases that the installation user have root (or Administrator) privileges has been removed. The agent can now be installed by any user regardless of access privileges.
- Secure Handling of Sensitive Information

All sensitive information, such as passwords, is now read from files. This information is not typed in clear text during interactive session. Therefore, it is never displayed on the command line or in any logs.
- Self-Contained Installation

All agent configuration and log files are generated and maintained within an agent's installation directory. This installation directory is referred to as the Policy Agent base directory. In code examples this directory is listed as such, *PolicyAgent-base*. The distribution files for the 2.2 release of J2EE agents are provided to you in three formats. You can choose the format that best fits your needs: zip format, tar format, or a package format. The files are small in size since the installer for this release uses a simple configuration mechanism. In summary, when you unpack the binaries, the configuration and log files remain within the installation directory.
- Support for Multiple Physical Installations

There is no longer any restriction on using multiple different binaries of the same agent on the same machine.

Coexistence With Access Manager

Starting with this release, you can deploy a J2EE agent on an instance of an application server where Access Manager has already been installed. Note that Access Manager should be installed prior to the agent being installed.

Support for Client Identification Based on Custom HTTP Headers

Starting with this release, J2EE agents can be configured to use custom HTTP headers to identify the remote client IP address and host name. This client IP address is used to validate an Access Manager session or to evaluate applicable policies.

Agent Specific Application for Housekeeping Tasks

Starting with this release of J2EE agents, a bundled application is available to perform housekeeping tasks on the deployment container, such as an application server.

This bundled application, when deployed on an agent-protected application server instance, expands the agent's functionality. For example, this bundled application allows the agent to receive notifications and to support cross-domain single sign-on. In previous releases, this functionality was tied to an application referred to as the *primary application*, which was secured by the agent.

URL Policy Enhancements

Starting with this release of J2EE agents, the following features are available that enhance Uniform Resource Locator (URL) policy:

- Remote Policy Evaluation Failover

J2EE agents can now leverage session failover functionality to ensure that remote policy evaluation failover can occur if an Access Manager instance becomes unavailable.

- Configurable Policy Evaluation Mechanism

Starting with this release, J2EE agents can be configured to use two different mechanisms to remotely evaluate policies as follows:

- The agent remotely requests policy evaluation for all resources applicable to a user within the agent's scope of protection.
- The agent remotely requests policy evaluation for the resource accessed by the user and not any other resources that the user might access later.

- Composite Advice

In the 2.2 release, J2EE agents provide a composite advice feature. This feature allows the policy and authentication services of Access Manager to decouple the advice handling mechanism of the agents. This allows you to introduce and manage custom advices by writing solely Access Manager side plug-ins. Starting with this release, you are not required to make changes on the agent side. Such advices are honored automatically by the composite advice handling mechanism.

- Policy Based Response Attributes

The policy-based response attribute feature allows the policy service to provide static and dynamic attributes based on the resource accessed by the user. These attributes can be made available to the agent protected application as HTTP headers, request attributes, or cookies.

Support for Flexible User Mapping Mechanisms

Starting with this release, J2EE agents provide support for user mapping modes that have flexibility in the user names they choose. In prior releases, a user name had to be an Access Manager user ID. Now, user names can be chosen from a few different sources as long as the names are for authenticated users who have trusted identities. A trusted identity can be established on the agent-protected server for a security principal (or for an equivalent trusted identity of the user). This mechanism allows the agent to choose a user ID for the authenticated user from the user's profile attributes, the user's session properties, or an HTTP header accompanying the user request.

Support for Fetching User Session Attributes (J2EE Agents)

Before this release of J2EE agents, information for HTTP headers, request attributes, or cookies was retrieved, or *sourced*, solely from profile attributes. Now, this information can also be sourced from session properties.

Support for Version Checking

Starting with this release of J2EE agents, you can easily check the exact version of the agent you are using, including build date, build number, and Client SDK version. Prior to this release, administrators could not easily identify the build date of the agent they were using. Since code changes occur between build dates, identifying the exact build can be useful.

Support for Not-Enforced IP Lists

Starting with this release, J2EE agents support *not-enforced IP lists*. With this feature, an agent always grants access to resources when the request comes from a machine with an IP address that appears on a specified list in the agent configuration file.

Support for Custom Response Headers

Starting with this release, J2EE agents provide support for custom response headers. The agent can be configured so that custom response headers are set on every request. Such headers are defined statically in the agent configuration file and are honored on all enforced web resources as identified by the agent.

Support for Application Logout Integration

Starting with this release, J2EE agents can be configured to identify an application logout event and to synchronize the event with the Access Manager logout. The agent can identify the logout of an application based on preconfigured information sent with a request as follows:

- The request URI
- A query parameter sent with the request
- A request parameter sent within the request body

Support for Application Specific Agent Filter Operation Modes

The application-specific filter operation mode mechanism allows different applications to use different levels of protection as necessary. Different filter operation modes provide different levels of functionality, thus enabling the selection of the best mode for each protected application.

Support for Affinity-Based Login URL Selection

Starting with this release, J2EE agents support a prioritized (or an *affinity-based*) selection of login URLs for authenticating users. End users are directed to the URL highest on the list if it is available. If not, the second URL on the list is targeted. If a URL higher on the list becomes available again, the agent switches to that URL.

You can disable this affinity-based selection process if desired, which would allow you to use a round-robin selection scheme.

Support for a Sample Application

Starting with this release, the J2EE agents provide a bundled sample application to demonstrate the key features and functionality of the agent. Some of the features demonstrated are:

- J2EE declarative security
- J2EE programmatic security
- URL policy-based access control deployed on an agent-protected application server

The `sampleapp` directory includes the sample application and a `README.TXT` file explaining how to use the sample application.

J2EE Agents and Backward Compatibility With Access Manager 6.3

Policy Agent 2.2 is backward compatible with Access Manager 6.3 Patch 1 or greater.

Note – Policy Agent 2.2 is only compatible with Access Manager 6.3 when the Access Manager patch has been applied.

Be aware that Policy Agent 2.2 takes advantage of certain features that exist in Access Manager 7 that do not exist in Access Manager 6.3, such as “composite advices,” “policy-based response attributes,” and others.

Policy Agent 2.2-05 Update Release

The Policy Agent 2.2-05 update release currently includes fixes and enhancements for web agents. This section describes the following:

- “[Web Agents in the Policy Agent 2.2-05 Update Release](#)” on page 19
- “[Key Fixes and Enhancements in the Policy Agent 2.2-05 Update Release](#)” on page 20
- “[Known Issues in the Policy Agent 2.2-05 Update Release](#)” on page 22

Web Agents in the Policy Agent 2.2-05 Update Release

TABLE 1 Web Agents in the Policy Agent 2.2-05 Update Release

Version 2.2-05 Policy Agent For	Patch ID
Apache HTTP Server 2.0.x	141243-03
Apache HTTP Server 2.2.x	141244-03
IBM Lotus Domino 6.x, 7.0, 8.0	141245-03
Microsoft IIS 6.0	141247-03
Sun Java System Web Proxy Server 4.0	141248-03
Sun Java System Web Server 6.1	141249-03
Sun Java System Web Server 7.0	141250-03

Note: A version 2.2-05 policy agent for Microsoft IIS 5.0 is not available in this release.

To Download and Install a Version 2.2-05 Web Agent

1. Create a download directory to download the patch. For example: `v2.2-05_agent`
2. In the download directory from Step 1, download the patch for the agent you want to install from My Oracle Support: <https://support.oracle.com/>.
For example, for the Apache HTTP Server 2.2.x agent, download `141244-03.zip`.
3. In the download directory, unzip the patch.

Each patch contains a README file and a separate ZIP file for each supported platform. The README file contains information about the patch, including a list of the bugs fixed in the patch.

For example, files for the Apache HTTP Server 2.2.x agent are:

- `README.141244-03`
- Solaris SPARC 64-bit systems: `apache_v22_solaris_sparc64_agent.zip`
- Solaris SPARC 32-bit systems: `apache_v22_SunOS_agent.zip`
- Linux 32-bit systems: `apache_v22_Linux_agent.zip`

- Linux 64-bit systems: apache_v22_linux64_agent.zip
 - Solaris x86 systems: apache_v22_SunOS_x86_agent.zip
 - Windows: apache_v22_WINNT_agent.zip
4. Unzip the file for your specific platform. For example, for Solaris SPARC 64-bit systems, unzip apache_v22_solaris_sparc64_agent.zip.
The files and directories required by the specific agent are then available in the *zip-root/web_agents/agent-name* directory, where *zip-root* is where you unzipped the file and *agent-name* identifies the specific agent. For example, for the Apache HTTP Server 2.2.x agent:
zip-root/web_agents/apache22_agent
 5. Follow the installation and configuration procedures in the respective Policy Agent 2.2 guide in the following collection:
Policy Agent 2.2 documentation: <http://download.oracle.com/docs/cd/E19534-01/index.html>
Note: Each version 2.2–05 web agent requires a full installation. That is, you must uninstall your existing agent and then re-install the new version 2.2–05 agent.

Key Fixes and Enhancements in the Policy Agent 2.2–05 Update Release

- “Web agent behind load balancer now evaluates request against not-enforced client IP list (6915959)” on page 20
- “Wildcard (*) support is added for not-enforced client IP list (6903850)” on page 21
- “Web agents can map LDAP attributes to more than one HTTP header (6937504)” on page 21
- “NSS libraries are upgraded to version 3.12.3 (6870161)” on page 21
- “New properties for POST data preservation (6891373)” on page 22

Web agent behind load balancer now evaluates request against not-enforced client IP list (6915959)

The Policy Agent Update 2.2–05 release allows you to configure the web agent to evaluate the request against the not-enforced client IP list, when a load balancer is deployed in front of the agent.

The following properties in the `AMAgent.properties` file support this feature:

- `com.sun.agents.load_balancer.enable` enables (`true`) or disables (`false`) the option to evaluate the request against the not-enforced client IP list, if a load balancer is deployed in front of the agent. The default is `false`.

The following two properties are not used unless this property has a value of `true`.

- `com.sun.am.policy.agents.config.client.ip.header` is the name of the HTTP header that contains client IP, which depends on the type of load balancer you are using. If not used, leave this property blank.
- `com.sun.am.policy.agents.config.client.hostname.header` is the name of the HTTP header that contains the hostname of the client. If not used, leave this property blank.

After you set these properties, restart the agent web container instance.

Note – The Policy Agent Update 2.2–04 release implemented this feature for the Microsoft IIS 6.0 agent. The Policy Agent Update 2.2–05 release extends this feature to the other web agents in this release. See also “[IIS 6.0 agent behind a load balancer now evaluates requests against not-enforced client IP list \(6894700, 6864977\)](#)” on page 24.

Wildcard (*) support is added for not-enforced client IP list (6903850)

The Policy Agent 2.2–05 release allows wildcard characters (*) in the not-enforced client IP list for web agents. This list can include both exact IP addresses and IP addresses that contain a asterisk (*) to represent one or more characters.

To specify the not-enforced client IP list, set the `com.sun.identity.agents.config.notenforced.ip` property in the `AMAgent.properties` file, with multiple IP addresses separated by a comma. For example:

```
com.sun.identity.agents.config.notenforced.ip = 192.168.*.*,.10.10.*
```

After you set this property, restart the agent web container instance.

Web agents can map LDAP attributes to more than one HTTP header (6937504)

The Policy Agent 2.2–05 release allows web agents to map the same LDAP attribute to different HTTP headers or cookies. To specify this mapping, set the `com.sun.am.policy.agents.config.profile.attribute.map` property in the `AMAgent.properties` file, using a colon (:) to separate the names. For example:

```
com.sun.am.policy.agents.config.profile.attribute.map = cn|name1:name2:name3
```

After you set this property, restart the agent web container instance.

NSS libraries are upgraded to version 3.12.3 (6870161)

To prevent security issues, the NSS libraries for web agents in the Policy Agent 2.2–05 release are upgraded to version 3.12.3 for all platforms, including Oracle Solaris, Microsoft Windows, HP-UX, Linux, and IBM AIX systems.

New properties for POST data preservation (6891373)

For web agents that support POST data preservation and are deployed behind a load balancer, the Policy Agent 2.2-05 release allows you to send the sticky session information as a parameter in the URL rather than a cookie. Previously, this information was sent as part of a cookie and used the `com.sun.am.policy.agents.config.postdata.preserve.lbcookie` property.

Currently, the Microsoft IIS 6.0, Sun Java System Web Server 6.1, and Sun Java System Web Server 7.0 web agents support POST data preservation.

In the Policy Agent 2.2-05 release, these agents do not use the `com.sun.am.policy.agents.config.postdata.preserve.lbcookie` property for POST data preservation. Instead, these agents use the following new properties:

- `com.sun.am.policy.agents.config.postdata.preserve.stickyession.mode` specifies the sticky session mode. Values can be URL or COOKIE. For example:
`com.sun.am.policy.agents.config.postdata.preserve.stickyession.mode=URL`
- `com.sun.am.policy.agents.config.postdata.preserve.stickyession.value` specifies the name of the sticky cookie or query parameter and its value. For example:
`com.sun.am.policy.agents.config.postdata.preserve.stickyession.value=agentID=01`

After you set these properties, restart the agent web container.

Known Issues in the Policy Agent 2.2-05 Update Release

In cookie hijacking mode, logout request hangs (6894077)

In cookie hijacking mode, logout requests are not handled properly and session invalidation does not happen. This problem is fixed in OpenSSO 8.0 Update 2, Access Manager 7.1 patch 5, and Access Manager 7 2005Q4 patch 12. However, this problem still occurs when version 2.2-05 agents are used with OpenSSO 8.0 Update 1 patch 2 and the older patch releases.

Policy Agent 2.2–04 Update Release

The Policy Agent 2.2-04 update release currently includes fixes and enhancements for web agents:

- “[Web Agents in the Policy Agent 2.2-04 Update Release](#)” on page 23
- “[Key Fixes and Enhancements in the Policy Agent 2.2-04 Update Release](#)” on page 24

Web Agents in the Policy Agent 2.2–04 Update Release

TABLE 2 Web Agents in the Policy Agent 2.2–04 Update Release

Version 2.2–04 Policy Agent For	Patch ID
Apache HTTP Server 2.0.x	141243-02
Apache HTTP Server 2.2.x	141244-02
Microsoft IIS 5.0	141246-02
Microsoft IIS 6.0	141247-02
Sun Java System Web Proxy Server 4.0	141248-02
Sun Java System Web Server 6.1	141249-02
Sun Java System Web Server 7.0	141250-02

Note: A version 2.2–04 policy agent for IBM Lotus Domino 6.x, 7.0, and 8.0 is not currently available.

To Download and Install a Version 2.2–04 Web Agent

1. Create a download directory to download the patch. For example: v2.2-04_agent
2. In the download directory from Step 1, download the patch for the agent you want to install from My Oracle Support: <https://support.oracle.com/>.
For example, for the Apache HTTP Server 2.2.x agent, download 141244-02.zip.
3. In the download directory, unzip the patch.

Each patch contains a README file and a separate ZIP file for each supported platform. The README file contains information about the patch, including a list of the bugs fixed in the patch (and bugs fixed in earlier releases).

For example, files for the Apache HTTP Server 2.2.x agent are:

- README.141244-02
- Solaris SPARC 64-bit systems: apache_v22_solaris_sparc64_agent.zip
- Solaris SPARC 32-bit systems: apache_v22_SunOS_agent.zip
- Linux 32-bit systems: apache_v22_Linux_agent.zip
- Linux 64-bit systems: apache_v22_linux64_agent.zip
- Solaris x86 systems: apache_v22_SunOS_x86_agent.zip
- Windows: apache_v22_WINNT_agent.zip

4. Unzip the file for your specific platform. For example, for Solaris SPARC 64-bit systems, unzip apache_v22_solaris_sparc64_agent.zip.

The files and directories required by the specific agent are then available in the `zip-root/web_agents/agent-name` directory, where `zip-root` is where you unzipped the file and `agent-name` identifies the specific agent. For example, for the Apache HTTP Server 2.2.x agent:

`zip-root/web_agents/apache22_agent`

5. Follow the installation and configuration procedures in the respective Policy Agent 2.2 guide in the following collection:

Policy Agent 2.2 documentation: <http://download.oracle.com/docs/cd/E19534-01/index.html>

Note: Each version 2.2–04 web agent requires a full installation. That is, you must uninstall your existing agent and then re-install the new version 2.2–04 agent.

Key Fixes and Enhancements in the Policy Agent 2.2-04 Update Release

- “IIS 6.0 agent behind a load balancer now evaluates requests against not-enforced client IP list (6894700, 6864977)” on page 24
- “Sticky cookie support added for web agents behind a load balancer with POST data preservation (6836393)” on page 25
- “Apache HTTP Server 2.0.x and 2.2.x agents can encode special characters in cookies by URL encoding (6814694)” on page 25
- “Web agents have changes in the path info related properties (6854806)” on page 25
- “NSS and NSPR libraries are bundled with web agents on Solaris and Linux systems (6794995)” on page 26

IIS 6.0 agent behind a load balancer now evaluates requests against not-enforced client IP list (6894700, 6864977)

Previously, if a load balancer or proxy was configured in front of the Microsoft IIS 6.0 agent and a user attempted to access a protected resource from a machine whose IP was in the not-enforced client IP list, the user would be redirected to the Access Manager or OpenSSO server, since the agent used the IP of the proxy instead of the client machine.

The Policy Agent Update 2.2-04 release includes the following new properties in `AMAgent.properties` that you can set if a load balancer is deployed in front of the IIS 6.0 agent and you want the agent to evaluate the request against the not-enforced client IP list:

- `com.sun.agents.load_balancer.enable` enables (`true`) or disables (`false`) the option to evaluate the request against the not-enforced client IP list, if a load balancer is deployed in front of the IIS 6.0 agent. The default is `false`. The following two properties are not used unless this property has a value of `true`.

- `com.sun.am.policy.agents.config.client.ip.header` is the name of the HTTP header that contains client IP, which depends on the type of load balancer you are using. If not used, leave this property blank.
- `com.sun.am.policy.agents.config.client.hostname.header` is the name of the HTTP header that contains the hostname of the client. If not used, leave this property blank.

After you set these properties, restart the IIS 6.0 instance.

Note. These new properties apply only to the IIS 6.0 agent. CR 6894700 fixes the 32-bit IIS 6.0 agent, and CR 6864977 fixes the 64-bit IIS 6.0 agent and OWA.

Sticky cookie support added for web agents behind a load balancer with POST data preservation (6836393)

For web agents that support POST data preservation and are deployed behind a load balancer, the Policy Agent 2.2-04 update release includes the new `com.sun.am.policy.agents.config.postdata.preserve.lbcookie` property in `AMAgent.properties` to ensure that the POST data are preserved when using the load balancer.

To use this feature, set the following properties in the `AMAgent.properties` file:

```
com.sun.am.policy.agents.config.postdata.preserve.enable = true  
com.sun.am.policy.agents.config.postdata.preserve.lbcookie = palbcookie=01
```

After you set these properties, restart the web agent container.

Note. The new `com.sun.am.policy.agents.config.postdata.preserve.lbcookie` property applies only to the IIS 6.0, Web Server 6.1, and Web Server 7.0 agents, which are the only agents that support POST data preservation.

Apache HTTP Server 2.0.x and 2.2.x agents can encode special characters in cookies by URL encoding (6814694)

The version 2.2-04 Apache HTTP Server 2.0.x and Apache HTTP Server 2.2.x agents can use the new `com.sun.am.policy.agents.config.encode_cookie_special_chars.enable` property in `AMAgent.properties` to enable encoding for special characters in cookies. The default value for this property is `false`.

To enable the encoding, set the property to `true` and restart the Apache HTTP Server web container.

Web agents have changes in the path info related properties (6854806)

The Policy Agent 2.2-04 update release now has two properties related to the path info, allowing you to decouple the possibility to ignore the path info for the policy evaluation from the possibility to ignore the path info when evaluating the URL against the not-enforced list. These properties are:

- The `com.sun.am.policy.agents.config.ignore_path_info` property existed in the previous releases. In the Policy Agent 2.2–04 update release, this property indicates only whether the path information and query should be stripped from the request URL before the URL is evaluated by Access Manager. The default value is `false`.
- The new `com.sun.am.policy.agents.config.ignore_path_info_for_not_enforced_list` property indicates whether the path information and query should be stripped from the request URL before being compared with the URLs of the not-enforced list when those URLs contain a wild-card (*) character. For security reasons, the default value is `true`.

NSS and NSPR libraries are bundled with web agents on Solaris and Linux systems (6794995)

On Solaris and Linux systems, web agents in the Policy Agent 2.2–04 update release now include the following Sun NSS and NSPR libraries:

- NSS 3.11.9
- NSPR 4.7

These libraries are already included on other operating systems.

Policy Agent 2.2–03 Update Release

The Policy Agent 2.2–03 update release includes fixes and enhancements for web agents and Java EE agents (formerly called J2EE agents). Consider updating to a version 2.2–03 web agent if you have not updated an agent with any of the hot patches since the Policy Agent 2.2–02 update, or if you need any of the fixes or enhancements in the 2.2–03 update.

- “Java EE Agents in the Policy Agent 2.2–03 Update Release” on page 26
- “Web Agents in the Policy Agent 2.2–03 Update Release” on page 27

Java EE Agents in the Policy Agent 2.2–03 Update Release

The Java EE agents in the Policy Agent 2.2–03 update release are available as patches on My Oracle Support: <https://support.oracle.com/>. For a list of the problems fixed by each patch, check the README file included with the respective patch.

Patch IDs for Java EE Agents in the Policy Agent 2.2–03 Update Release

These patches are full installations. To install a version 2.2–03 agent, you must first uninstall your existing agent and then reinstall the new 2.2–03 agent.

TABLE 3 Patch IDs for Java EE Agents in the Policy Agent 2.2–03 Update Release

Version 2.2–03 Java EE Agent For	Patch ID
JBoss Application Server 4.0	143085-01
Oracle Application Server 10g	143086-01
Sun Java System Application Server 8.1/8.2/ 9.0/9.1	143089-01
Apache Tomcat 5.5 Servlet/JSP Container	143090-01
Apache Tomcat 6.0	143091-01
Oracle WebLogic Server/Portal 10	143092-01
Oracle WebLogic Server/Portal 8.1 SP4	143093-01
Oracle WebLogic Server 9.0/9.1	143094-01
Oracle WebLogic Server/Portal 9.2	143095-01
IBM WebSphere Application Server 5.1.1	143096-01
IBM WebSphere Application Server 6.0/6.1	143097-01
SAP Enterprise Portal 6.0 and Web Application Server 6.4	143098-01

Web Agents in the Policy Agent 2.2–03 Update Release

- “Patch IDs for Web Agents in the Policy Agent 2.2–03 Update Release” on page 27
- “Web Agents: Key Fixes and Enhancements in the Policy Agent 2.2–03 Update” on page 29
- “Web Agents: Known Issues in the Policy Agent 2.2–03 Update Release” on page 31

Patch IDs for Web Agents in the Policy Agent 2.2–03 Update Release

The web agents in the Policy Agent 2.2–03 update release are available as patches on My Oracle Support: <https://support.oracle.com/>.

TABLE 4 Patch IDs for Web Agents in the Policy Agent 2.2–03 Update Release

Version 2.2–03 Web Agent For	Patch ID
Apache HTTP Server 2.0.x	141243-01
Apache HTTP Server 2.2.x	141244-01
IBM Lotus Domino 6.x, 7.0, 8.0	141245-01
Microsoft IIS 5.0	141246-01

TABLE 4 Patch IDs for Web Agents in the Policy Agent 2.2–03 Update Release *(Continued)*

Version 2.2–03 Web Agent For	Patch ID
Microsoft IIS 6.0	141247-01
Sun Java System Web Proxy Server 4.0	141248-01
Sun Java System Web Server 6.1	141249-01
Sun Java System Web Server 7.0	141250-01

To Download and Install a Version 2.2–03 Web Agent

1. Create a directory to download the patch. For example: `v2.2-03_patch`
2. In the directory from Step 1, download the patch for the agent you want to install from My Oracle Support: <https://support.oracle.com/>. For example, for the Apache HTTP Server 2.2.x agent, download `141244-01.zip`.
3. In the download directory, unzip the patch.

Each patch contains a README file and a separate ZIP file for each supported platform. The README file contains information about the patch, including a list of the bugs fixed in the patch (and bugs fixed in earlier releases).

For example, files for the Apache HTTP Server 2.2.x agent are:

- `README.141244-01`
- Solaris SPARC 64-bit systems: `apache_v22_solaris_sparc64_agent.zip`
- Solaris SPARC 32-bit systems: `apache_v22_SunOS_agent.zip`
- Linux 32-bit systems: `apache_v22_Linux_agent.zip`
- Linux 64-bit systems: `apache_v22_linux64_agent.zip`
- Solaris x86 systems: `apache_v22_SunOS_x86_agent.zip`
- Windows: `apache_v22_WINNT_agent.zip`

4. Unzip the file for your specific platform. For example, for Solaris SPARC 64-bit systems, unzip `apache_v22_solaris_sparc64_agent.zip`.

Some files have the `.tar.gz` extension. For example, to unpack the IBM Domino Server agent for Linux:

```
# gunzip -dc sun-one-policy-agent-2.2-domino6-linux.tar.gz | tar -xvof -
```

The files and directories required by the specific agent are then available in the `zip-root/web_agents/agent-name` directory, where `zip-root` is where you unzipped the file and `agent-name` identifies the specific agent. For example, for the Apache HTTP Server 2.2.x agent:

```
zip-root/web_agents/apache22_agent
```

5. Follow the installation and configuration procedures in the respective Policy Agent 2.2 guide in the following collection:

Policy Agent 2.2 documentation: <http://download.oracle.com/docs/cd/E19534-01/index.html>

Note: Each version 2.2–03 web agent requires a full installation. That is, you must uninstall your existing agent and then re-install the new version 2.2–03 agent.

Web Agents: Key Fixes and Enhancements in the Policy Agent 2.2–03 Update

- “IIS 6.0 agent supports POST data preservation (6735280)” on page 29
- “Web Proxy Server 4.0 agent can send GET request without header (6787007)” on page 29
- “Web agents libxml2.so library is upgraded (6817868)” on page 30
- “Not-enforced POST requests can be accessed in CDSSO mode (6789020)” on page 30
- “Web agent can handle new Access Manager 7.1 policy advices (6785022)” on page 30
- “Log entry added if web agent causes Apache Web Server to hang when the agent's log rotation fails (6804139)” on page 30
- “IIS 6.0 agent supports agent URL override functionality (6829880)” on page 30
- “IIS 6.0 SharePoint agent redirects to access-denied page if user doesn't exist in Active Directory (6854317)” on page 31

IIS 6.0 agent supports POST data preservation (6735280)

The version 2.2–03 agent for Microsoft IIS 6.0 now supports POST data preservation. Users can preserve POST data, which is submitted to IIS 6.0 through HTML forms before the users log in to Access Manager.

To Configure POST Data Preservation for the IIS 6.0 Agent

1. Add the HTML pages containing the forms to the not-enforced URL list, as described in “Configuring the Not-Enforced URL List” in *Sun Java System Access Manager Policy Agent 2.2 Guide for Microsoft Internet Information Services 6.0*.
2. In the `AMAgent.properties` file for the IIS 6.0 agent, set the following properties:
 - `com.sun.am.policy.agents.config.postdata.preserve.enable = true`
Enables POST data preservation. The default is `false`.
 - `com.sun.am.policy.agents.config.postcache.entry.lifetime = interval`
Specifies the *interval* in minutes that the POST data stays valid in the IIS 6.0 agent cache. POST data cache entries that have existed beyond the specified time interval are automatically removed from the cache. The default time is 10 minutes.
3. Restart the IIS 6.0 server instance.

Web Proxy Server 4.0 agent can send GET request without header (6787007)

The version 2.2–03 agent for Sun Java System Web Proxy Server 4.0 can send a GET request without a header. Previously, this type of request caused a dump core, which resulted in a denial of service (DOS) security vulnerability.

For more information, check the security alerts on <https://support.oracle.com/>.

Web agents libxml2.so library is upgraded (6817868)

The libxml2.so library for version 2.2–03 web agents is upgraded from version 2.6.23 to version 2.7.3, in order to prevent a denial of service (DOS) security vulnerability.

For more information, check the security alerts on <https://support.oracle.com/>.

Not-enforced POST requests can be accessed in CDSSO mode (6789020)

For version 2.2–03 web agents in cross-domain single sign-on (CDSSO) mode, if a POST request is added to the not-enforced URL list, the browser now displays the POST data without redirecting to the Access Manager login page.

Web agent can handle new Access Manager 7.1 policy advices (6785022)

Version 2.2–03 web agents can handle the new Access Manager 7.1 policy advices for the AuthenticateToServiceConditionAdvice condition on 64-bit web containers.

Log entry added if web agent causes Apache Web Server to hang when the agent's log rotation fails (6804139)

A web agent can cause the Apache Web Server to hang if the agent's log rotation fails. A log entry to report this condition has been added in the version 2.2–03 release.

Workaround: Make sure that the correct permissions are set for the web agent log directory and that the partition where the logs are stored has enough space. Additional considerations for this issue are:

- To prevent permissions failures for the web agent's log directory, make sure all web server child processes have write permissions to the log directory. For example, consider the agent for Apache HTTP Server. If the initial Apache HTTP Server web agent log file is opened by super user (root) and the log rotation will subsequently be attempted by a child process running as a different user (such as apache user), make sure that apache user has write permissions to the log directory.
- In case of log rotation failures due to write permissions, the logs will be written to the web server's error log file.

IIS 6.0 agent supports agent URL override functionality (6829880)

The version 2.2–03 IIS 6.0 agent now supports the agent URL override functionality, if the following properties are set in the agent's `AMAgent.properties` file:

```
com.sun.am.policy.agents.config.override_protocol = true  
com.sun.am.policy.agents.config.override_host = true  
com.sun.am.policy.agents.config.override_port = true  
com.sun.am.policy.agents.config.agenturi.prefix =
```

```
https://iis-host.example.com:443/amagent  
com.sun.am.policy.agents.config.fqdn.map = agent-host|load-balancer-host
```

These properties are used if the agent-protected web server is behind a load balancer or SSL over-loader and the external URL is different and should be overridden.

IIS 6.0 SharePoint agent redirects to access-denied page if user doesn't exist in Active Directory (6854317)

If a user doesn't exist in Microsoft Active Directory but is authenticated by Access Manager, the version 2.2–03 IIS 6.0 SharePoint agent now redirects the request to the access-denied page. Previously, the agent returned Error 403 (Forbidden) to the user.

Web Agents: Known Issues in the Policy Agent 2.2–03 Update Release

- “Agent for Apache HTTP Server 2.0.x on IBM AIX 5.3 requires `bos.rte.libc fileset upgrade`” on page 31
- “NSPR libraries need to be upgraded to version 4.7.0” on page 31
- “Version 2.2-02 agent for Apache HTTP Server 2.2.3 fails to start on Linux 5.0” on page 31

Agent for Apache HTTP Server 2.0.x on IBM AIX 5.3 requires `bos.rte.libc fileset upgrade`

On IBM AIX 5.3, if you are running the web agent for IBM HTTP Server based on Apache HTTP Server 2.0.x, the server sometimes crashes at startup.

Workaround. Upgrade the AIX `bos.rte.libc` fileset from Service Pack 7 to Service Pack 9 (AIX 5.3.0.68 to 5.3.0.70). For information see:

<http://www-01.ibm.com/support/docview.wss?uid=isglfileset-870201775>

NSPR libraries need to be upgraded to version 4.7.0

For the version 2.2–03 web agents, the NSPR libraries need to be upgraded to version 4.7.0. Make sure that the upgraded NSPR libraries are picked up by the web server.

Version 2.2-02 agent for Apache HTTP Server 2.2.3 fails to start on Linux 5.0

The version 2.2-02 web agent for Apache HTTP Server 2.2.3 fails to start on Red Hat Linux 5.0 because the compatibility libraries are not installed. The OS includes `/usr/lib/libstdc++.so.6` but not `libstdc++.so.5`.

Workaround: Install `libstdc++.so.5` using the `compat-libstdc++-33` RPM.

Policy Agent 2.2–02 Update Release

Policy agent update 2.2–02 includes fixes and enhancements released in hot patches since the Policy Agent 2.2–01 update. Consider updating to a new 2.2–02 agent if you have not updated your agent with any of these recent hot patches, or if you need any of the fixes or enhancements in the update.

- [“Policy Agent 2.2–02 Update For Web Agents” on page 32](#)
 - [“Policy Agent 2.2–02 Update For J2EE Agents” on page 33](#)
 - [“Key Fixes and Enhancements in the Policy Agent 2.2–02 Update” on page 34](#)
-

Note –

- Version 2.2–02 web and J2EE policy agents supersede the respective version 2.2 and 2.2–01 agents.
 - Support for Policy Agent 2.1 is being dropped, as noted in [“Deprecation Notifications and Announcements” on page 82](#).
 - See also [“Compatibility With Access Manager and OpenSSO Enterprise” on page 63](#).
-

Policy Agent 2.2–02 Update For Web Agents

The following Access Manager Policy Agent 2.2–02 web agents are available on My Oracle Support: <https://support.oracle.com/>.

- Policy Agent 2.2–02 for Apache Web Server 2.0.54
- Policy Agent 2.2–02 for Apache 2.2.9
- Policy Agent 2.2–02 for IBM Lotus Domino Server 6.5 / 7.0
- Policy Agent 2.2–02 for Microsoft IIS 5.0
- Policy Agent 2.2–02 for Microsoft IIS 6.0
- Policy Agent 2.2–02 for Sun Java System Web Server 6.1
- Policy Agent 2.2–02 for Sun Java System Web Server 7.0
- Policy Agent 2.2–02 for Web Proxy Server 4.0

New Certifications and Support Added in 2.2–02 Web Agents

- [“Large File Support For Apache 2.0 Agent” on page 32](#)
- [“New Platform Support for 2.2–02 Web Agents” on page 33](#)

Large File Support For Apache 2.0 Agent

Large file support is added for the Apache 2.0 agent. Support for the large file option is specifically needed because the latest versions of the Solaris 10 OS, both SPARC and x86 platforms, include a pre-installed Apache server with large file support enabled.

With update 2.2-02, two shared objects are included with the Apache agent:

- `libamapc2.largefile.so` - The Apache server was built with the large file option enabled.
- `libamapc2.so` - The Apache server was built with the large file option **not** enabled.

Non-large file support is the default. For an Apache 2.0 server with the large file option enabled, you might need to backup `libamapc2.so` and then copy `libamapc2.largefile.so` to the location of `libamapc2.so`.

To check for the large file option, use `apxs -q CFLAGS`. If the large file option is enabled, the command shows `-D_LARGEFILE_SOURCE -D_FILE_OFFSET_BITS=64`. The agent's large file supported library is built using these compiler flags.

Important: If third-party components such as `php` or `mod_perl` are deployed on an Apache server that is built with the large file option set, these components also need to be compiled with the large file options set. Generally, use the Apache server header files during the compilation of these third-party components. Header files that are generated by Apache after enabling the large file support need to be used in these compilations.

New Platform Support for 2.2-02 Web Agents

In addition to the platforms listed in “[Supported Servers for Web Agents in Policy Agent 2.2](#)” on page 52, the following new platforms are added for web agents in the 2.2-02 update.

TABLE 5 New Platform Support for 2.2-02 Web Agents

2.2-02 Web Agent	New Supported Platform
All 2.2-02 web agents	Red Hat Enterprise Linux 5.0, 32-bit and 64-bit systems
Apache Web Server 2.0.54	Solaris 10 OS, SPARC platform, 64-bit systems
Apache 2.2.9	Solaris 10 OS, SPARC platform, 64-bit systems
Sun Java System Web Server 6.1	Solaris 9 and 10 OS, x86 platform, 32-bit systems HP-UX 11i
IBM Domino Server 6.5	IBM AIX 5.3
IBM Domino Server 7.0	
IBM Domino Server 8.0	

Policy Agent 2.2-02 Update For J2EE Agents

The following Access Manager Policy Agent 2.2-02 J2EE agents are available on My Oracle Support: <https://support.oracle.com/>.

- Apache Tomcat 6.0

- Apache Tomcat 5.5 Servlet/JSP container
- JBoss Application Server 4.0
- IBM WebSphere Application Server 5.1.1
- IBM WebSphere Application Server 6.0
- BEA WebLogic Server 8.1 Service Pack 4
- BEA WebLogic Server 9.0/9.1
- BEA WebLogic Server 9.2
- BEA WebLogic Server 10
- IBM Domino Server 6.5/7.0
- Oracle Application Server 10g
- Sun Java System Application Server 8.1/8.2
- Sun Java System Application Server 9.0/9.1

New Platform Support for 2.2–02 J2EE Agents

In addition to the platforms listed in “[Supported Servers for J2EE Agents in Policy Agent 2.2](#)” [on page 57](#), the following new platforms are added for J2EE agents in the 2.2–02 update.

- All version 2.2–02 J2EE agents on Red Hat Enterprise Linux AS 5.0, 32-bit and 64-bit, if the previous version of the agent was supported on Red Hat Enterprise Linux AS 3.0 and 4.0
- Version 2.2–02 Apache Tomcat 6.0 agent on HP-UX 11i

Key Fixes and Enhancements in the Policy Agent 2.2–02 Update

- “[J2EE_POLICY and ALL filter modes do not work on 2.2–02 J2EE Agent on Oracle Application Server 10g \(6790321\)](#)” [on page 35](#)
- “[J2EE policy agent fails to log when the log action is LOG_DENY \(6729386\)](#)” [on page 35](#)
- “[Performance issue resolved for policy agent \(6768406\)](#)” [on page 35](#)
- “[For web agents, sunwMethod parameter is removed from the URL in CDSSO mode \(6725383\)](#)” [on page 35](#)
- “[Domino 7.0 agent redirects client to URL instead of displaying a 500 error if Access Manager server is not responding \(6715064\)](#)” [on page 36](#)
- “[Composite advice can be included in the query instead of through a POST request \(6676032\)](#)” [on page 36](#)
- “[Apache 2.0 agent supports additional HTTP methods for a Subversion repository \(6647805\)](#)” [on page 36](#)
- “[For web agents, support is added to adjust the policy clock skew \(6608463\)](#)” [on page 37](#)

J2EE_POLICY and ALL filter modes do not work on 2.2-02 J2EE Agent on Oracle Application Server 10g (6790321)

If the filter mode (`com.sun.identity.agents.config.filter.mode` property) is set to `J2EE_POLICY` or `ALL` (which is the default value set during the agent installation), the version 2.2-02 Oracle Application Server 10g agent returns an error in the `amFilter` log when a protected resource is accessed.

Workaround. See the additional task in the “Post-Installation Steps Specific to Agent for Oracle Application Server 10g” in *Sun Java System Access Manager Policy Agent 2.2 Guide for Oracle Application Server 10g*.

J2EE policy agent fails to log when the log action is LOG_DENY (6729386)

For a J2EE agent, the Audit Log properties in `AMAgent.properties` are set as:

```
com.sun.identity.agents.config.audit.accesstype = LOG_DENY  
com.sun.identity.agents.config.log.disposition = ALL
```

If a user for whom the access is denied to a J2EE protected resource tries to access a the resource in a deployed application, access to the protected resource is denied, but there is no entry in the logs for the deny action on either the Access Manager or J2EE agent side.

Workaround. None. This is a limitation of the product. For a J2EE policy to be evaluated, the control is given to the web container on which the agent is deployed, to determine the access policies. The web container doesn't send the access decision back to the agent for a resource that is protected with J2EE security policies. The web container just denies the access, and the agent cannot effectively log when the access is denied.

Performance issue resolved for policy agent (6768406)

Previously, a delay occurred for the Microsoft IIS 5.0 agent when a user accessed a protected resource. When the agents were deployed on multiple servers, serious performance degradation occurred.

Workaround. The Policy Agent 2.2-02 update includes the following new property:

```
com.sun.am.policy.agents.config.policy_number_of_tries
```

If this property is set to 0 (the default value), you can prevent the delay for all agents.

For web agents, sunwMethod parameter is removed from the URL in CDSSO mode (6725383)

For web agents, the `sunwMethod` parameter is removed from the URL in cross domain single sign-on (CDSSO) mode, because this parameter can cause problems with AJAX driven applications.

Web agents can use the following new property:

```
com.sun.am.policy.agents.config.use.sunwmethod
```

The default value is `false`, meaning that the `sunwmethod` parameter will not be used in CDSSO mode. For backward compatibility, if this property is set to `true`, CDSSO mode will function as it previously did.

Domino 7.0 agent redirects client to URL instead of displaying a 500 error if Access Manager server is not responding (6715064)

The IBM Lotus Domino 7.0 agent previously displayed an internal server error (HTTP 500) if the Access Manager server was not responding.

Workaround. Set the following new property to the URL where you want the version 2.2–02 Lotus Domino 7.0 agent to redirect the client if the Access Manager server does not respond:

```
com.sun.am.policy.agents.config.errorpage.url
```

This new property also applies to the version 2.2–02 Apache 2.x agent.

Composite advice can be included in the query instead of through a POST request (6676032)

When a web client accesses a resource and that request results in composite advice (`sunamcompositeadvice`) returned, the policy agent produces an auto-submitting HTML form, which can be difficult for a web client to interpret. Now, the following new property determines whether the composite advice is added in the query or through a POST request:

```
com.sun.am.use_redirect_for_advice
```

- `true`: Composite advice will be added to the redirect URL.
- `false`: Composite advice will be sent through a POST request.

The default is `false`.

Apache 2.0 agent supports additional HTTP methods for a Subversion repository (6647805)

The Apache 2.0 agent now recognizes these additional methods: `VERSION_CONTROL`, `CHECKOUT`, `UNCHECKOUT`, `CHECKIN`, `UPDATE`, `LABEL`, `REPORT`, `MKWORKSPACE`, `MKACTIVITY`, `BASELINE_CONTROL`, and `MERGE`. These methods are used for WebDAV versioning (RFC 3253) and specifically for a Subversion repository.

For web agents, support is added to adjust the policy clock skew (6608463)

If the time on the web agent host machine differs from the Access Manager time, you might occasionally see an incorrect policy decision or an infinite re-direction. The following new property in `AMAgent.properties` adjusts the clock skew between the web agent and Access Manager machines:

```
com.sun.am.policy.agents.config.policy_clock_skew
```

This properties specifies the time in seconds used to adjust the time difference between the policy agent machine and the Access Manager machine, as follows:

```
Clock skew in seconds = AgentTime - AccessManagerTime
```

The default is zero (0).

You should also run a time syncing service to keep the time on the agent machine and the Access Manager machine as close as possible.

Policy Agent 2.2-01 Update Release

Policy Agent 2.2 has had a variety of minor updates since its initial release. These updates have been referred to as hot patches. These hot patches include a variety of fixes and enhancements. The changes made in a hot patch can apply to a single agent, several agents, or all agents in an agent type: web agents or J2EE agents. Furthermore, the changes made in hot patches are cumulative, therefore, the changes are carried forward to the next hot patch.

The various agent hot patches have been combined into a single update release called Policy Agent 2.2-01. By combining all the Policy Agent 2.2 hot patches in one release, Policy Agent 2.2-01 addresses a range of issues, from relatively minor to significant.

Consider updating Policy Agent 2.2 to Policy Agent 2.2-01, especially if you have not as of yet updated Policy Agent 2.2 with any of the available hot patches.

As with all Policy Agent releases, the 2.2-01 release is divided into a J2EE agent version and a web agent version. Accordingly, this section has been divided into a web agent subsection and a J2EE agent subsection. Refer to the applicable subsection as follows:

- [“Policy Agent 2.2-01 Web Agents” on page 38](#)
- [“Policy Agent 2.2-01 J2EE Agents” on page 43](#)

Furthermore, as with Policy Agent 2.2, Policy Agent 2.2-01 is compatible with the following Access Manager versions: 6.3 (backward compatible), 7.0, and 7.1.

As you will notice in the J2EE agent and web agent subsections that follow, the 2.2-01 update is more comprehensive for web agents than for J2EE agents. Therefore, more fixes and enhancements were made to web agents for the 2.2-01 update.

Policy Agent 2.2-01 Web Agents

This section on 2.2-01 web agents consists of the following subsections:

- “Determining the Version of a Policy Agent 2.2 Web Agent” on page 38
- “Key Fixes and Enhancements in Policy Agent 2.2-01 Web Agents” on page 39
- “The Key New Properties Added for Policy Agent 2.2-01 Web Agents” on page 40
- “Access Manager and Policy Agent 2.2-01 Web Agents: Allowing Requests Using Non-Standard HTTP Methods” on page 42
- “Supported HTTP Methods of Web Agents in Policy Agent 2.2-01” on page 43

The first subsection that follows explains how to determine the version of a Policy Agent 2.2 web agent. For example, you could determine if a hot patch has been applied or not.

Subsequently in this section is a subsection that describes the important fixes and enhancements introduced during the various Policy Agent 2.2 web agent hot patches and a subsection explaining the important new properties introduced.

For the complete list of known problems fixed and enhancements made, see the README provided in the web agent download. Some of the fixes, enhancements, and properties described in the sections that follow only apply to a single agent. For example, many of the changes are specific to Agent for Microsoft Internet Information Services 6.0.

Determining the Version of a Policy Agent 2.2 Web Agent

The method for determining the specific version of an installed Policy Agent 2.2 web agent is different depending upon if the web agent was developed through the OpenSSO project or not. The documentation specific to each web agent states if it was developed through the OpenSSO project. Most Policy Agent 2.2 agents were not developed through the OpenSSO project.

The following information explains how to determine the version of a web agent; therefore, you can determine if a hot patch has been applied to the web agent using the appropriate method, as follows:

OpenSSO Project Web Agents	For most OpenSSO project web agents, you can use the command line, in the <i>PolicyAgent-base/bin</i> directory, to issue the <code>agentadmin --version</code> command.
----------------------------	--

Where the `agentadmin --version` command does not apply, check the `amAgent` log file as described in the Other Web Agents section that follows.

Other Web Agents	See the <code>amAgent</code> log file. If you are uncertain of the location of the <code>amAgent</code> log file, you can find it in the web agent <code>AMAgent.properties</code> configuration file as the value assigned to the following property:
------------------	--

`com.sun.am.policy.agents.config.local.log.file`

Key Fixes and Enhancements in Policy Agent 2.2-01 Web Agents

This section lists the key fixes and enhancements introduced in the various Policy Agent 2.2 web agent hot patches, which are now rolled into the 2.2-01 update release. The initial issue is described with its associated change request (bug) number. Furthermore, a short summary is provided about how the fix or enhancement resolved the issue.

Policy Agent 2.2 for Microsoft IIS 6.0 does not function properly when Basic Authentication is set (6415948)

This enhancement involved a behavior modification to the Basic Authentication filter. This fix corresponds to specific versions of Access Manager, as follows:

- Access Manager 7.0 series from patch 5 forward
- Access Manager 7.1 series from patch 1 forward

Support is now provided for using Policy Agent and Access Manager in conjunction with Microsoft IIS 6.0 Basic Authentication. For more information on Agent for Microsoft IIS 6.0 see *Sun Java System Access Manager Policy Agent 2.2 Guide for Microsoft Internet Information Services 6.0*.

Request for specific session attributes to be populated in HTTP headers (6409146)

This enhancement allows the following session attributes to be set as headers:

- `maxSessionTime`
- `maxIdleTime`

In Policy Agent 2.2 for Microsoft IIS 6.0, Replay Password Encryption is lacking for Basic Authentication (6475899)

This enhancement improved the security around how user passwords are handled. Furthermore, this enhancement involved adding a new property to the web agent `AMAgent.properties` configuration file as described in “[Property Made Available: com.sun.am.replaypasswd.key](#)” on page 41.

Web agents in the Policy Agent 2.2 release fail with Access Manager 6.3 (6490037)

This fix enabled Policy Agent 2.2 to work properly with Access Manager 6.3.

Disabling Internet Explorer pop up when protocol changes from HTTP to HTTPS (6532260)

This problem only applied to Agent for Microsoft Internet Information Services 6.0 when the agent was deployed to provide protection for Microsoft Outlook Web Access.

While one was able to configure a local redirection page to automatically redirect incoming HTTP connection to HTTPS, when configured with Access Manager, this local redirection invoked a security pop up window in Internet Explorer browsers in certain deployment scenarios.

To fix this issue, a property was made available to convert the HTTP connection to HTTPS automatically, without a local redirection page. See “[Properties Made Available for Microsoft Office SharePoint and Outlook Web Access](#)” on page 42 for info on the following property:

```
com.sun.am.policy.agents.config.iis.owa_enabled_change_protocol
```

Web Distributing Authoring and Versioning (WebDAV) support is necessary to allow for a wider range of HTTP methods (6567164)

WebDAV support has been implemented for web agents. Using the WebDAV protocol with web agents requires additional configuration as described in these release notes. For more information, see “[Access Manager and Policy Agent 2.2–01 Web Agents: Allowing Requests Using Non-Standard HTTP Methods](#)” on page 42.

Program Database (.pdb) files should be part of agent binaries to help in debugging issues (6581272)

For Windows systems, the 2.2–01 web agents come with .pdb files as part of the agent binaries. These .pdb files, which are in the same location as .dll files, can be of assistance in debugging.

Other Additions to Policy Agent 2.2–01 Web Agents

Windows Systems: For web agents on Windows systems, Policy Agent 2.2–01 is compiled with Microsoft Visual Studio 2003. As a result, the Microsoft libraries msrvr71.dll and msvcpr71.dll are bundled with web agents since they are required for the agents to run successfully.

The Key New Properties Added for Policy Agent 2.2–01 Web Agents

This section describes the key properties that were added to the web agent AMAgent.properties configuration file in conjunction with the hot patches bundled in the 2.2–01 web agent release. For each property listed in this section, the following information is provided:

- The associated bug (change request) number
- A description of why the property was added

Property Added: com.sun.am.tcp_nodelay.enable

Change Request: 6425354

This property was added to allow you to disable the Nagle algorithm. When the agent and an associated load balancer both use the Nagle algorithm, buffering of small packets can take place, causing network delays and performance problems.

Property Added: com.sun.am.cookie.secure

Change Request: 6432320

This property was added to Policy Agent to allow all cookies set by the agents to be marked as secure. A cookie marked as secure is only transmitted if the communications channel with the host is secure. Therefore, only secure cookies are sent to HTTPS servers.

Property Made Available: com.sun.am.replaypasswd.key

Change Request: 6475899

This property was made available to both Access Manager and Agent for Microsoft IIS 6.0 to allow Access Manager to send an encrypted password to Agent for Microsoft IIS 6.0.

This property was not specifically added to the configuration file of Access Manager or Policy Agent but simply made available. Therefore, if you want to set this property, you must add both the property name and the corresponding value. For more information, see *Sun Java System Access Manager Policy Agent 2.2 Guide for Microsoft Internet Information Services 6.0*.

Property Added:

com.sun.am.policy.agents.config.encode_url_special_chars.enable

Change Request: 6481331

When set to true, this property enables encoding of special characters, such as Chinese characters in the URL before the request is sent for policy evaluation. Otherwise, the use of special characters in the URL can cause unreliable results, even causing the web server to crash. The default setting is false. Enable this property by setting it as follows:

```
com.sun.am.policy.agents.config.encode_url_special_chars.enable = true
```

Property Made Available:

com.sun.am.policy.agents.config.no_child_thread_activation_delay

Change Request: 6570155

This property is specific to Apache-HTTP-Server related web agents in the Policy Agent 2.2 software set. The default for this property is `false`.

This property was made available to address a delay that occurs when Apache HTTP Server spawns a new process. The parent process goes to sleep for up to one second to allow the child process to get into commission. This one second delay applies to every process that the Apache HTTP Server spawns.

Setting this property to `true`, as shown in the following example, reduces the delay down to a range from ten microseconds to one millisecond.

```
com.sun.am.policy.agents.config.no_child_thread_activation_delay = true
```

This property was not specifically added to the web agent `AMAgent.properties` configuration file, but simply made available. Therefore, to set this property to `true`, you must add both the property name and the value.

Properties Made Available for Microsoft Office SharePoint and Outlook Web Access

Properties Made Available:

Microsoft Office SharePoint: `com.sun.am.sharepoint_login_attr_name = login`

Microsoft Outlook Web Access: `com.sun.am.iis_owa_enabled = true`

Change Request:

6532260

These new properties were added to indicate whether or not Microsoft Office SharePoint or Outlook Web Access is configured.

These properties were not specifically added to the web agent `AMAgent.properties` configuration file, but simply made available. Therefore, to configure these properties, you must add the applicable property name and its corresponding value.

Access Manager and Policy Agent 2.2–01 Web Agents: Allowing Requests Using Non-Standard HTTP Methods

The sections that follow are applicable to web agents starting with Policy Agent 2.2–01 used with Access Manager starting with the 7.0 release.

Supported HTTP Methods of Web Agents in Policy Agent 2.2-01

Prior to Policy Agent 2.2-01, the only HTTP methods supported by web agents were GET, HEAD, PUT, POST, DELETE, TRACE, OPTIONS. Any request received by the agent with a method other than one of these was marked as UNKNOWN and access to the resource was denied.

Policy Agent 2.2-01 Web Agents: Newly Supported HTTP Methods

With Policy Agent 2.2-01, web agents also support the following methods: CONNECT, COPY, INVALID, LOCK, UNLOCK, MOVE, MKCOL, PATCH, PROPFIND, PROPPATCH.

By default, policies in Access Manager only allow control of GET and POST actions. To extend Access Manager control to other actions, see the corresponding Access Manager document. For example, for Access Manager 7.1, see “[Adding a Policy Enabled Service](#)” in *Sun Java System Access Manager 7.1 Administration Guide*.

Policy Agent 2.2-01 Web Agents: Support for INVALID Methods

Typically, a web server marks a request as an INVALID method and denies access to the resource when the request uses a method other than any of the methods listed in the preceding section.

However, in cases where the web server is configured to forward requests to an application that can handle non-standard HTTP methods, the web server does not deny access, but forwards the request to the requested application. You can configure Access Manager to allow or deny such INVALID requests. A typical example is when a web agent is installed on Apache HTTP Server that is configured as a proxy for Microsoft Exchange Server. In this scenario, requests can use methods such as SEARCH or SUBSCRIBE, which are not recognized by Apache HTTP Server and, therefore, marked as INVALID.

To decide if such requests should be allowed or denied, the INVALID method must be loaded in the iPlanetAMWebAgentService service.

Policy Agent 2.2-01 J2EE Agents

This section on 2.2-01 J2EE agents consists of the following subsections:

- “[Determining the Version of a Policy Agent 2.2 J2EE Agent](#)” on page 44
- “[Key Fixes and Enhancements in Policy Agent 2.2-01 J2EE Agents](#)” on page 44
- “[The Key New Properties Added for Policy Agent 2.2-01 J2EE Agents](#)” on page 45
- “[Policy Agent 2.2-01: Enabling Access Manager Identities to Access the IBM WebSphere Administration Console](#)” on page 45

The first subsection that follows explains how to determine the version of a Policy Agent 2.2 J2EE agent. For example, you could determine if a hot patch has been applied or not.

Subsequently in this section is a subsection that describes the important fixes and enhancements introduced during the various Policy Agent 2.2 J2EE agent hot patches and a subsection explaining the important new properties introduced.

For the complete list of known problems fixed and enhancements made, see the README provided in the J2EE agent download.

Determining the Version of a Policy Agent 2.2 J2EE Agent

The method for determining the specific version of an installed Policy Agent 2.2 J2EE agent is by using the command line. With this method, you can find the version info, such as the hot patch version, if applicable.

In the *PolicyAgent-base/bin* directory, issue the `agentadmin --version` command, where *PolicyAgent-base* represents the directory where the J2EE agent is installed.

Key Fixes and Enhancements in Policy Agent 2.2–01 J2EE Agents

This section lists the key fixes and enhancements introduced in the Policy Agent 2.2 J2EE agent hot patches, which are now rolled into the 2.2–01 update release. The initial issue is described with its associated change request (bug) number. Furthermore, a short summary is provided about the fix.

If you restart Access Manager but not the J2EE agent, future attempts to access an agent protected page from a browser result in a 403 Forbidden message (6636155)

This problem was fixed in Access Manager 7.0 patch 7 (CR 6496155), but the problem still exists in Access Manager 7.1.

Workaround: Two workarounds exist:

- Add the following new property to the J2EE agent `AMAgent.properties` configuration:

```
com.sun.identity.enableUniqueSSOTokenCookie=false
```

For more about setting the value for the preceding property, see “[Property Made Available: com.sun.identity.enableUniqueSSOTokenCookie](#)” on page 45.

or

- Always restart agent after restarting Access Manager.

IBM WebSphere Administration Console can not be used to access the users, roles and group identities in the Access Manager identity repository (6462779)

This problem stems from the custom registry that Policy Agent adds for IBM WebSphere Application Server and applies to the following agents:

- Agent for IBM WebSphere Application Server 5.1.1

- Agent for IBM WebSphere Application Server 6.0

In terms of Agent for IBM WebSphere Application Server 6.1, the fix was integrated into the original version of the agent.

In terms of Agent for IBM WebSphere Application Server 5.1.1 and Agent for IBM WebSphere Application Server 6.0, this fix enables you to use the WebSphere Administration Console to map the Access Manager roles, groups, and user identities to local J2EE roles that are specific to IBM WebSphere Application Server for authorization purposes. Furthermore, being able to use the WebSphere Administration Console in this manner eliminates the necessity of manually editing the `admin-authz.xml` file or using the Policy Agent `agentadmin --setGroup` command.

For the fix to work, you must also implement specific tasks as described in these Release Notes. The instructions apply to Agent for IBM WebSphere Application Server 5.1.1 and Agent for IBM WebSphere Application Server 6.0. See “[Policy Agent 2.2-01: Enabling Access Manager Identities to Access the IBM WebSphere Administration Console](#)” on page 45.

The Key New Properties Added for Policy Agent 2.2-01 J2EE Agents

Property Made Available: com.sun.identity.enableUniqueSSOTokenCookie

Change Request: 6636155

The default setting for this property is `true`. This property was not specifically added to the J2EE agent `AMAgent.properties` configuration file, but simply made available. Therefore, to set this property to `false`, which is required to solve the issue described in “[If you restart Access Manager but not the J2EE agent, future attempts to access an agent protected page from a browser result in a 403 Forbidden message \(6636155\)](#)” on page 44, you must add both the property name and the value as follows:

```
com.sun.identity.enableUniqueSSOTokenCookie = false
```

Policy Agent 2.2-01: Enabling Access Manager Identities to Access the IBM WebSphere Administration Console

This section includes instructions necessary to take advantage of a fix implemented in Policy Agent 2.2-01 specific to agents for IBM WebSphere Application Server.

The instructions in this section apply to the following agents:

- Agent for IBM WebSphere Application Server 5.1.1
- Agent for IBM WebSphere Application Server 6.0

The instructions in this section do not apply to Agent for IBM WebSphere Application Server 6.1 since the instructions for that agent are integrated into the following guide: [*Sun Java System Access Manager Policy Agent 2.2 Guide for IBM WebSphere Application Server 6.1*](#).

Policy Agent 2.2: Problem Accessing Identities With IBM WebSphere Administration Console

In Policy Agent 2.2, the custom registry added by the agents for IBM WebSphere Application Server did not allow the IBM WebSphere Administration Console to access the users, roles and group identities in the Access Manager identity repository.

The respective guides, [*Sun Java System Access Manager Policy Agent 2.2 Guide for IBM WebSphere Application Server 5.1.1*](#) and [*Sun Java System Access Manager Policy Agent 2.2 Guide for IBM WebSphere Application Server 6.0*](#) provide tasks that allow you to add J2EE roles for authorization: manually editing `admin-authz.xml` or executing `agentadmin --setGroup` option. However, those tasks do not work in an IBM WebSphere cluster deployment. Furthermore, those tasks are error prone and should be avoided.

After you implement the instructions in “[To Install and Configure Policy Agent 2.2–01 for IBM WebSphere Application Server](#)” on page 48, you can solely use IBM WebSphere Administration Console to map the local users and groups to Access Manager roles, groups and users.

Policy Agent 2.2–01: Overview of Fix for IBM WebSphere Administration Console Access Problem

After you upgrade Agent for IBM WebSphere Application Server Policy Agent 2.2 to Policy Agent 2.2–01, you must implement the instructions, “[To Install and Configure Policy Agent 2.2–01 for IBM WebSphere Application Server](#)” on page 48, to fix the console problem. For more information about the problem this fix addresses, see “[IBM WebSphere Administration Console can not be used to access the users, roles and group identities in the Access Manager identity repository \(6462779\)](#)” on page 44. This fix also removes the constraint that remote node operations must be carried out by logging in as `serverId`, which is supplied in the custom user registry.



Caution – Specific guidelines for case sensitivity must be adhered to, as follows:

- Access Manager group and role identities mapped to an IBM WebSphere Application Server role
For example if you have a role named “WASAdmin” in Access Manager, you must enter “wasadmin” in the IBM WebSphere Administration Console not “WASAdmin” or “WasAdmin.” If you type “WasAdmin,” the console is likely to validate and save the changes. However, a failure will result during access control evaluation because of the mismatch in case. Therefore, always use lower case characters for Access Manager role and group names in the IBM WebSphere Administration Console.
 - An Access Manager user identity mapped to an IBM WebSphere Application Server user identity
For example, if you have created a user in Access Manager named “WasAdminUser,” use the same case in the IBM WebSphere Administration Console.
-

Supplemental Instructions for Installing and Configuring Policy Agent 2.2-01 for IBM WebSphere Application Server

The instructions describe supplemental steps for installing and configuring Policy Agent 2.2-01 for IBM WebSphere Application Server 5.1.1 or 6.0. Use the instructions in conjunction with the appropriate agent guide, *Sun Java System Access Manager Policy Agent 2.2 Guide for IBM WebSphere Application Server 5.1.1* or *Sun Java System Access Manager Policy Agent 2.2 Guide for IBM WebSphere Application Server 6.0* and with the appropriate Access Manager documentation. The instructions include examples that serve to clarify the type of actions you can take. The examples include the following:

Example Identities: **wasagentuser**

WasAgentRole

Example Access Manager Version: **Access Manager 7.1**

While you can use Access Manager 6.3 or Access Manager 7.0 with Policy Agent 2.2-01, the examples provided in the instructions that follow use Access Manager 7.1.

Therefore, links to Access Manager documentation are specifically to Access Manager 7.1 documentation. If you are using a different version of Access Manager, consult the appropriate documentation.

The instructions that follow include supplemental pre-installation, installation, and post-installation steps for Policy Agent 2.2–01.

▼ To Install and Configure Policy Agent 2.2–01 for IBM WebSphere Application Server

1 Create a user in Access Manager.

Example user: wasagentuser

This user is the user ID to use while installing the agents and adding the custom user registry in the Deployment Manager (In this scenario, serverId would be wasagentuser). For more information on creating a user, see “[To Create or Modify a User](#)” in *Sun Java System Access Manager 7.1 Administration Guide*.

Note – When you install the agent for IBM WebSphere Application Server, enter the same name in the agent-profile-name prompt that you have created for the user in this step. For example, wasagentuser. The following example prompt is from the agent installer and illustrates the proper response in this scenario:

```
Enter a valid agent profile name. Before proceeding with the agent
installation, please ensure that a valid Agent profile exists in Access Manager.
[ ? : Help, < : Back, ! : Exit ]
Enter the Agent Profile name: wasagentuser
```

2 Create a role in Access Manager.

Example role: WasAgentRole

For more information on creating a role, see “[To Create or Modify a Role](#)” in *Sun Java System Access Manager 7.1 Administration Guide*.

3 Add the newly created user (wasagentuser) to the newly created role (WasAgentRole).

For more information about adding users to roles, see “[To Add Users to a Role or Group](#)” in *Sun Java System Access Manager 7.1 Administration Guide*.

4 Add the appropriate privilege to the newly created role (WasAgentRole).

The privilege to use varies according to the Access Manager version as follows:

- **Access Manager 7.0:**

Assign the “Read only access to data stores” privilege to the newly created role (WasAgentRole).

- **Access Manager 7.1:**

Assign the “Read and write access only for policy properties” privilege to the newly created role (`WasAgentRole`).

For more information about adding privileges to roles for Access Manager 7.1, see “[Defining Privileges for Access Manager 7.1](#)” in *Sun Java System Access Manager 7.1 Administration Guide* or “[Defining Privileges for an Access Manager 7.0 to 7.1 Upgrade](#)” in *Sun Java System Access Manager 7.1 Administration Guide*.

5 Edit the Access Manager `AMConfig.properties` file to allow the agent to get a non-expiring SSO token to Access Manager

This step is required to get a non-expiring SSO token for the agent's self authentication to Access Manager.

You must edit the following property to include the distinguished name (DN) of the user (`wasagentuser`):

```
com.sun.identity.authentication.special.users
```

If you have a server farm, you must perform this step on all servers.

Use the legacy SDK DN not the universal UID of the user. For the example presented in this task, the appropriate setting is as follows:

```
com.sun.identity.authentication.special.users = cn=dsameuser,  
ou=DSAME Users, ROOT_SUFFIX|cn=amService-UrlAccessAgent, ou=DSAME Users,  
ROOT_SUFFIX|uid=dmgr,ou=people,ROOT_SUFFIX|  
uid=wasagentuser,ou=people,ROOT_SUFFIX
```

Where `ROOT_SUFFIX` is a place holder that represents the root suffix of the directory user management node. For example, `dc=example, dc=com`. Ensure that this suffix exists in the instance of the directory server you are using.

Note – To find the DN of the user, you can issue an `ldapsearch` command with the following base:

```
ou=people,ROOT_SUFFIX
```

And with the following filter:

```
(|(uid=wasagentuser)(cn=wasagentuser))
```

6 Restart Access Manager.

- 7 Add the following properties and corresponding values to the J2EE agent `AMAgent.properties` configuration file:

```
com.sun.identity.agents.config.privileged.attribute.type[1] = Group  
com.sun.identity.agents.config.privileged.attribute.tolowercase[Group] = false
```

This step has to be performed on all instances of Agent for IBM WebSphere Application Server that are participating in an agent farm or cluster.

- 8 Restart WebSphere Deployment Manager.
- 9 Synchronize all the nodes.

Next Steps Now you can log in to the IBM WebSphere Network Deployment Server's Administration Console to allow authorization to Access Manager that would enable access to the applications deployed in an IBM WebSphere cluster.

Supported Servers in Policy Agent 2.2

The next two subsections cover the supported servers for web agents and J2EE agents in the Policy Agent 2.2 release.

Understanding Server and Operating System Support for Policy Agent 2.2

These release notes provide the server and operating system support information for all the agents in the Policy Agent 2.2 software set. For web agents, that information is listed in [Table 6](#). For J2EE agents, that information is listed in [Table 7](#). Generally, information provided about Policy Agent 2.2 support for servers (deployment containers) and operating systems indicates only versions tested. However, each agent provides support beyond the specific versions tested.

Sun Java System Access Manager Policy Agent 2.2 supports all minor versions of both the server and of the operating systems. The term *minor* can include terms such as update, service pack, and patch.

Web Agents and Minor Version Support of Servers and Operating Systems

This section provides examples of minor version support that applies to web agents in the Policy Agent 2.2 software set. Be aware that terms such as service pack or update do not always apply when referring to minor versions. For example, in reference to the deployment container

Apache HTTP Server 2.0.54, the term “minor” refers to the part of the version number after “2.0.” Therefore, 2.1 is not considered a minor version. All versions that exist in the 2.0 series (2.0.x) are considered minor.

The following examples illustrate the type of minor version support provided. For these examples, the agent is Agent for Sun Java System Web Server 6.1. One of the platforms for which this agent was originally tested was Sun Java System Web Server 6.1 on Solaris version 10.

Example Deployment Container

Web Server 6.1

Examples of Supported Minor Versions

- Web Server 6.1 Service Pack 4
- Web Server 6.1 Service Pack 7
- Web Server 6.1 Service Pack 11
- And so on, as service packs become available

Example Operating System

Solaris 10

Examples of Supported Minor Versions

- Solaris 10 1/06 release
- Solaris 10 6/06 release
- Solaris 10 11/06 release
- And so on, as updates become available

For example, you could use Agent for Sun Java System Web Server 6.1 with Sun Java System Web Server 6.1 Service Pack 7 on Solaris 10 6/06 release.

J2EE Agents and Minor Version Support of Servers and Operating Systems

This section provides examples of minor version support that applies to J2EE agents in the Policy Agent 2.2 software set. Be aware that terms such as service pack or update do not always apply when referring to minor versions. For example, in reference to the deployment container IBM WebSphere Application Server 5.1.1, the term “minor” refers to the part of the version number after “5.1.” Therefore, 5.2 is not considered a minor version. All versions that exist in the 5.1.0 series (5.1.x) are considered minor.

The following examples illustrate the type of minor version support provided. For these examples, the agent is Agent for BEA WebLogic Server/Portal 8.1 SP4. One of the platforms for which this agent was originally tested was BEA WebLogic Server/Portal 8.1 SP4 on Windows 2003, Enterprise Edition.

Example Deployment Container	Examples of Supported Minor Versions
BEA WebLogic Server/Portal 8.1 SP4	<ul style="list-style-type: none"> ■ BEA WebLogic Server/Portal 8.1 SP3 ■ BEA WebLogic Server/Portal 8.1 SP5 ■ BEA WebLogic Server/Portal 8.1 SP6 ■ And so on, as service packs become available
Example Operating System	Examples of Supported Minor Versions
Windows 2003, Enterprise Edition	<ul style="list-style-type: none"> ■ Windows 2003, Enterprise Edition, SP1 ■ Windows 2003, Enterprise Edition, SP2 ■ Windows 2003, Enterprise Edition, SP3 ■ And so on, as updates become available

For example, you could use Agent for BEA WebLogic Server/Portal 8.1 SP4 with BEA WebLogic Server/Portal 8.1 SP5 on Windows 2003, Enterprise Edition, SP2.

Supported Servers for Web Agents in Policy Agent 2.2

The following table shows the supported platforms and versions of Access Manager for version 2.2 web agents, including agents in the 2.2–02 update.

See also “[New Platform Support for 2.2–02 Web Agents](#)” on page 33.

TABLE 6 Web Agent Server and Platform Support for Policy Agent 2.2

Agent for	Supported Policy Agent Version	Supported Access Manager Versions	Supported Platforms
Sun Java System Web Server 6.1	Version 2.2	Version 6.3 Patch 1 or greater Version 7 Version 7.1	Solaris OS for SPARC platforms, versions 8, 9, and 10 Solaris (OS) for x86 platforms, versions 8, 9, and 10 Red Hat Enterprise Linux Advanced Server 3.0.4.0, and 5.0, 32-bit only Windows Server 2003, Standard Edition Windows Server 2003, Enterprise Edition HP-UX 11i (2.2–02 agent only)

TABLE 6 Web Agent Server and Platform Support for Policy Agent 2.2 *(Continued)*

Agent for	Supported Policy Agent Version	Supported Access Manager Versions	Supported Platforms
Sun Java System Web Server 7.0	Version 2.2	Version 6.3 Patch 1 or greater Version 7 Version 7.1	Solaris OS for SPARC platforms, versions 9 and 10, 32-bit and 64-bit Solaris OS for x86 platforms, versions 9 and 10, 32-bit only Red Hat Enterprise Linux Advanced Server 3.0 and 5.0 Windows 2003, Enterprise Edition Windows 2008
Apache HTTP Server 1.3.33 Note – The <i>Sun Java System Access Manager Policy Agent 2.2 Guide for Apache HTTP Server 2.0.54</i> applies to both the Apache HTTP Server 1.3.33 and Apache HTTP Server 2.0.54 agents. This agent also supports minor versions of the 1.3 Apache HTTP Server series.	Version 2.2	Version 6.3 Patch 1 or greater Version 7 Version 7.1	Solaris OS for SPARC platforms, versions 8, 9, and 10 Solaris OS for x86 platforms, versions 8, 9, and 10 Red Hat Enterprise Linux Advanced Server 3.0 SUSE Linux Enterprise Server 9

TABLE 6 Web Agent Server and Platform Support for Policy Agent 2.2 *(Continued)*

Agent for	Supported Policy Agent Version	Supported Access Manager Versions	Supported Platforms
<p>Apache HTTP Server 2.0.54</p> <p>Note – Also supports minor versions of the 2.0 Apache HTTP Server series.</p>	Version 2.2	Version 6.3 Patch 1 or greater Version 7 Version 7.1	Solaris OS for SPARC platforms, versions 8, 9, and 10 Solaris 10 OS for SPARC platform, 64-bit systems (2.2–02 agent only) Solaris (OS) for x86 platforms, versions 8, 9, and 10 AIX 5L 5.1, 5.2, and 5.3 Red Hat Enterprise Linux Advanced Server 3.0, 32-bit and 64-bit Red Hat Enterprise Linux Advanced Server 4.0, 32-bit and 64-bit Red Hat Enterprise Linux Advanced Server 5.0, 32-bit and 64-bit Apache HTTP Server bundled with Solaris 10 OS and Red Hat Linux Advanced Server 4.0 and 5.0 SUSE Linux Enterprise Server 9 Debian GNU/Linux 3.0 Windows 2003, Enterprise Edition Windows 2003, Standard Edition
<p>Microsoft Internet Information Services 6.0 (Microsoft IIS 6.0)</p> <p>Note – This agent can be deployed to protect Microsoft Office SharePoint and Outlook Web Access.</p>	Version 2.2	Version 6.3 Patch 1 or greater Version 7 Version 7.1	Windows 2003, Enterprise Edition (includes all service packs, such as SP1, SP2, and so on) Windows 2003, Standard Edition (includes all service packs, such as SP1, SP2, and so on)

TABLE 6 Web Agent Server and Platform Support for Policy Agent 2.2 *(Continued)*

Agent for	Supported Policy Agent Version	Supported Access Manager Versions	Supported Platforms
IBM Lotus Domino 6.5 and 7.0	Version 2.2 and 2.2-02	Version 6.3 Patch 1 or greater Version 7 Version 7.1	Solaris OS for SPARC platforms, versions 8, 9, and 10 Red Hat Enterprise Linux Advanced Server 3.0 Windows 2003, Enterprise Edition Windows 2003, Standard Edition AIX 5L 5.3 (2.2-02 agent only)
Sun Java System Web Proxy Server 4.0	Version 2.2	Version 6.3 Patch 1 or greater Version 7 Version 7.1	Solaris OS for SPARC platforms, versions 8, 9, and 10 Solaris OS for x86 platforms, versions 8, 9, and 10 Red Hat Enterprise Linux Advanced Server 3.0 Windows 2003, Enterprise Edition Windows 2003, Standard Edition
Apache HTTP Server 2.2	Version 2.2	Version 6.3 Patch 1 or greater Version 7 Version 7.1	Solaris OS for the SPARC platform, versions 8, 9, and 10 Solaris OS for x86 platforms, versions 8, 9, and 10 Red Hat Enterprise Linux Advanced Server 3.0, 32-bit and 64-bit Red Hat Enterprise Linux Advanced Server 4.0, 32-bit and 64-bit SUSE Linux 10.1 Windows 2003, Enterprise Edition Windows 2003, Standard Edition

TABLE 6 Web Agent Server and Platform Support for Policy Agent 2.2 (Continued)

Agent for	Supported Policy Agent Version	Supported Access Manager Versions	Supported Platforms
Microsoft Internet Information Services 5.0 (Microsoft IIS 5.0)	Version 2.2	Version 6.3 Patch 1 or greater Version 7 Version 7.1	Windows 2000 Advanced Server Windows 2000 Professional
Microsoft IIS 6.0 With Outlook Web Access 2007/SharePoint 2007 (Microsoft IIS 6.0) Note – This agent can be deployed to protect Microsoft Office SharePoint 2007 and Outlook Web Access 2007. This agent does not apply to Microsoft Exchange 2003 or Microsoft Office SharePoint Portal Server 2003. For information about protecting those resources, see <i>Sun Java System Access Manager Policy Agent 2.2 Guide for Microsoft Internet Information Services 6.0</i> In terms of 32-bit and 64-bit architecture support, the following applies: <ul style="list-style-type: none">■ Agent for Web Server 6.1 64-bit■ Outlook Web Access 2007 64-bit■ SharePoint 2007 32-bit	Version 2.2	Version 6.3 Patch 1 or greater Version 7 Version 7.1 Note – The Access Manager compatibility information listed in this column does not apply when Agent for Microsoft IIS 6.0 is protecting Microsoft Office SharePoint 2007 or Outlook Web Access 2007. For specific details, including patch information on Access Manager compatibility in such a scenario, see the guide, as follows: <i>Sun Java System Access Manager Policy Agent 2.2 Guide for Microsoft IIS 6.0 With Outlook Web Access 2007/SharePoint 2007</i>	Windows 2003, Enterprise Edition (includes all service packs, such as SP1, SP2, and so on), 64-bit Windows 2003, Standard Edition (includes all service packs, such as SP1, SP2, and so on), 64-bit

Many of the individual agent guides from the Policy Agent 2.2 software set have not been updated at this time in terms of indicating that Access Manager 7.1 is a supported version.

Supported Servers for J2EE Agents in Policy Agent 2.2

The following table shows the supported platforms and versions of Access Manager for version 2.2 J2EE agents, including agents in the 2.2–02 update.

See also “[New Platform Support for 2.2–02 J2EE Agents](#)” on page 34.

TABLE 7 J2EE Agent Server and Platform Support for Policy Agent 2.2

Agent for	Supported Policy Agent Version	Supported Access Manager Versions	Supported Platforms
Sun Java System Application Server 8.1	Version 2.2	Version 6.3 Patch 1 or greater Version 7 Version 7.1	Solaris Operating System (OS) for the SPARC platform, versions 8, 9, and 10 Solaris (OS) for x86 platforms, versions 8, 9, and 10 Red Hat Enterprise Linux Advanced Server 3.0 Windows 2003, Enterprise Edition Windows 2003, Standard Edition
BEA WebLogic Server/Portal 8.1 SP4 (also supports BEA WebLogic Express 8.1 SP4)	Version 2.2	Version 6.3 Patch 1 or greater Version 7 Version 7.1*	Solaris Operating System (OS) for the SPARC platform, versions 8, 9, and 10 Solaris (OS) for x86 platforms, versions 8, 9, and 10 Red Hat Enterprise Linux Advanced Server 3.0 Windows 2003, Enterprise Edition Windows 2003, Standard Edition

TABLE 7 J2EE Agent Server and Platform Support for Policy Agent 2.2 (Continued)

Agent for	Supported Policy Agent Version	Supported Access Manager Versions	Supported Platforms
Apache Tomcat 5.5 Servlet/JSP Container (also supports Apache Tomcat 5.0.28 Servlet/JSP Container)	Version 2.2	Version 6.3 Patch 1 or greater Version 7 Version 7.1*	Solaris Operating System (OS) for the SPARC platform, versions 8, 9, and 10 Solaris (OS) for x86 platforms, versions 8, 9, and 10 Red Hat Enterprise Linux Advanced Server 3.0 Windows 2003, Enterprise Edition Windows 2003, Standard Edition
IBM WebSphere Application Server 5.1.1	Version 2.2	Version 6.3 Patch 1 or greater Version 7 Version 7.1*	Solaris Operating System (OS) for the SPARC platform, versions 8, 9, and 10 Red Hat Enterprise Linux Advanced Server 2.1 Red Hat Enterprise Linux Advanced Server 3.0 AIX 5L version 5.2 Windows 2003, Enterprise Edition Windows 2003, Standard Edition
IBM WebSphere Application Server 6.0	Version 2.2	Version 6.3 Patch 1 or greater Version 7 Version 7.1*	Solaris Operating System (OS) for the SPARC platform, versions 8, 9, and 10 Red Hat Enterprise Linux Advanced Server 3.0 AIX 5L version 5.2 Windows 2003, Enterprise Edition Windows 2003, Standard Edition

TABLE 7 J2EE Agent Server and Platform Support for Policy Agent 2.2 (Continued)

Agent for	Supported Policy Agent Version	Supported Access Manager Versions	Supported Platforms
SAP Enterprise Portal 6.0 and Web Application Server 6.40 (SAP Portal 6.0/Server 6.40)	Version 2.2	Version 6.3 Patch 1 or greater Version 7 Version 7.1	Solaris Operating System (OS) for the SPARC platform, versions 8, 9, and 10 AIX 5L Note – With the proper patch, this agent supports the AIX 5L version 5.3 platform. Contact Sun Microsystems support to obtain the correct patch. Windows 2003, Enterprise Edition Windows 2003, Standard Edition
IBM WebSphere Portal Server 5.1.0.2 deployed on: <ul style="list-style-type: none">■ IBM WebSphere Application Server 5.1.1.7■ IBM WebSphere Business Integration-Server Foundation 5.1.1	Version 2.2	Version 6.3 Patch 1 or greater Version 7 Version 7.1*	Solaris Operating System (OS) for the SPARC platform, versions 8, 9, and 10 AIX 5L version 5.2 Windows 2003, Enterprise Edition Windows 2003, Standard Edition
BEA WebLogic Server 9.0/9.1	Version 2.2	Version 6.3 Patch 1 or greater Version 7 Version 7.1	Solaris Operating System (OS) for the SPARC platform, versions 8, 9, and 10 Solaris (OS) for x86 platforms, versions 8, 9, and 10 Red Hat Enterprise Linux Advanced Server 3.0 Red Hat Enterprise Linux Advanced Server 4.0 Windows 2003, Enterprise Edition Windows 2003, Standard Edition

TABLE 7 J2EE Agent Server and Platform Support for Policy Agent 2.2 (Continued)

Agent for	Supported Policy Agent Version	Supported Access Manager Versions	Supported Platforms
Oracle Application Server 10g, which includes the following versions: <ul style="list-style-type: none">■ The 10.1.2 series.■ The 10.1.3 series.	Version 2.2	Version 6.3 Patch 1 or greater Version 7 Version 7.1*	Solaris Operating System (OS) for the SPARC platform, versions 8, 9, and 10 Red Hat Enterprise Linux Advanced Server 3.0 and 4.0 Windows 2003, Enterprise Edition Windows 2003, Standard Edition
BEA WebLogic Server/Portal 9.2 (also supports BEA WebLogic Express 9.2)	Version 2.2	Version 6.3 Patch 1 or greater Version 7 Version 7.1*	Solaris Operating System (OS) for the SPARC platform, versions 8, 9, and 10 Solaris (OS) for x86 platforms, versions 8, 9, and 10 HP-UX 11i Red Hat Enterprise Linux Advanced Server 3.0 Red Hat Enterprise Linux Advanced Server 4.0 Windows 2003, Enterprise Edition Windows 2003, Standard Edition

TABLE 7 J2EE Agent Server and Platform Support for Policy Agent 2.2 (Continued)

Agent for	Supported Policy Agent Version	Supported Access Manager Versions	Supported Platforms
JBoss Application Server 4.0 Note – Besides supporting the JBoss Application Server 4.x series, this agent supports JBoss Application Server from 3.2.5 through the rest of the 3.x series.	Version 2.2	Version 6.3 Patch 1 or greater Version 7 Version 7.1	Solaris Operating System (OS) for the SPARC platform, versions 8, 9, and 10 Solaris (OS) for x86 platforms, versions 8, 9, and 10 Red Hat Enterprise Linux Advanced Server 3.0, 32-bit and 64-bit Red Hat Enterprise Linux Advanced Server 4.0, versions 32-bit and 64 bit Windows 2003, Enterprise Edition Windows 2003, Standard Edition
Sun Java System Application Server 9.0/9.1 Note – Besides supporting Sun Java System Application Server 9.0 and 9.1, this agent supports Sun Java System Application Server 8.2.	Version 2.2	Version 6.3 Patch 1 or greater Version 7 Version 7.1	Solaris Operating System (OS) for the SPARC platform, versions 9, and 10 Solaris (OS) for x86 platforms, versions 9, and 10 Red Hat Enterprise Linux Advanced Server, versions 3.0 and 4.0. Windows 2003, Enterprise Edition
BEA WebLogic Server/Portal 10 Supports: BEA WebLogic Server 10 BEA WebLogic Portal 10	Version 2.2	Version 6.3 Patch 1 or greater Version 7 Version 7.1	Solaris Operating System (OS) for the SPARC platform, versions 9 and 10 Solaris (OS) for x86 platforms, versions 9 and 10 Red Hat Enterprise Linux Advanced Server 3.0 and 4.0 Windows 2003, Enterprise Edition

TABLE 7 J2EE Agent Server and Platform Support for Policy Agent 2.2 *(Continued)*

Agent for	Supported Policy Agent Version	Supported Access Manager Versions	Supported Platforms
IBM WebSphere Application Server 6.1	Version 2.2	Version 6.3 Patch 1 or greater Version 7 Version 7.1	Solaris Operating System (OS) for the SPARC platform, versions 8, 9, and 10 Red Hat Enterprise Linux Advanced Server 3.0 AIX 5L versions 5.2 and 5.3 Windows 2003, Enterprise Edition Windows 2003, Standard Edition
IBM WebSphere Portal Server 6.0 deployed on: ■ IBM WebSphere Application Server 6.0 ■ IBM WebSphere Business Integration-Server Foundation 6.0	Version 2.2	Version 6.3 Patch 1 or greater Version 7 Version 7.1	Solaris Operating System (OS) for the SPARC platform, versions 8, 9, and 10 Red Hat Enterprise Linux Advanced Server 3.0 AIX 5L version 5.3 Windows 2003, Enterprise Edition Windows 2003, Standard Edition
SAP Enterprise Portal 7.0 and Web Application Server 7.0 (SAP Enterprise Portal 7.0/Web Application Server 7.0)	Version 2.2	Version 7 Version 7.1	Solaris Operating System (OS) for the SPARC platform, version 9 and 10 AIX 5L Windows 2003, Enterprise Edition, 32-bit Windows 2003, Standard Edition, 32-bit

TABLE 7 J2EE Agent Server and Platform Support for Policy Agent 2.2 *(Continued)*

Agent for	Supported Policy Agent Version	Supported Access Manager Versions	Supported Platforms
Apache Tomcat 6.0	Version 2.2	Version 6.3 Patch 1 or greater Version 7 Version 7.1	Solaris Operating System (OS) for the SPARC platform, versions 9 and 10 Solaris (OS) for x86 platforms, versions 9, and 10 Red Hat Enterprise Linux Advanced Server 4.0 and 5.0 Windows 2003, Enterprise Edition Windows 2003, Standard Edition

Some of the individual agent guides from the Policy Agent 2.2 software set have not been updated at this time because Access Manager 7.1 is a supported version.

Compatibility With Access Manager and OpenSSO Enterprise

Both web agents and J2EE agents in the Policy Agent 2.2 release are compatible with Sun Java System Access Manager and Sun OpenSSO Enterprise, as follows.

All agents in the Policy Agent 2.2 release are compatible with:

- Access Manager 6 2005Q1 (6.3) patch 1 and later
- Access Manager 7 2005Q4 (both Realm Mode and Legacy Mode)
- Access Manager 7.1 (both Realm Mode and Legacy Mode)
- OpenSSO Enterprise 8.0 (using the 2.2 agent type for the agent profile)

All agents in the Policy Agent 3.0 release are compatible with:

- Access Manager 7 2005Q4 (both Realm Mode and Legacy Mode)
- Access Manager 7.1 (both Realm Mode and Legacy Mode)
- OpenSSO Enterprise 8.0

To ensure that all enhancements and fixes are applied, it is recommended that you install the latest Access Manager 7 2005Q4 or Access Manager 7.1 patch, depending on your platform. Check the respective Access Manager *Release Notes* for information about these patches.

See also “[Policy Agent 2.2 documentation should reference OpenSSO \(6857941\)](#)” on page 81.

Installation Notes

This section describes some of the key points of the installation, configuration, and uninstallation for Sun Java System Access Manager Policy Agent 2.2. Information about installation is divided by agent type as follows:

- “[Installation Notes for Web Agents in Policy Agent 2.2](#)” on page 64
- “[Installation Notes for J2EE Agents in Policy Agent 2.2](#)” on page 64

See also “[Policy Agent 2.2 documentation should reference OpenSSO \(6857941\)](#)” on page 81.

Installation Notes for Web Agents in Policy Agent 2.2

While the functionality of web agents has increased considerably for this release, the installation, post-installation configuration, and uninstallation processes have not changed significantly from the 2.1 release. The following section points out a change in the name of the uninstallation script. Changes in the installation and uninstallation process tend to be along this scale. See the individual web agent guides for detailed information. For a current list of the individual web agent guides, see “[Supported Servers and Documentation of Web Agents in Policy Agent 2.2](#)” in *Sun Java System Access Manager Policy Agent 2.2 User’s Guide*.

Uninstallation Script for Web Agents in Policy Agent 2.2

The uninstallation script name for web agents in the 2.2 release has a different suffix for each web container. The suffix is a short name for the web container. For example, the following is the uninstallation script name for Agent for Sun Java System Web Server 6.1:

`uninstall_agent_es6`

Installation Notes for J2EE Agents in Policy Agent 2.2

The installation and uninstallation processes for this release have changed dramatically. However, the post-installation configuration has not changed as much. For this release, the installation and uninstallation processes rely heavily on the `agentadmin` program. The directory structure of J2EE agents has also changed significantly. This section briefly describes these aspects of J2EE agents. See the individual J2EE agent guides for detailed information. For a current list of individual J2EE agent guides, see “[Supported Servers and Documentation of J2EE Agents in Policy Agent 2.2](#)” in *Sun Java System Access Manager Policy Agent 2.2 User’s Guide*.

Using the `agentadmin` Program with J2EE Agents

The `agentadmin` program is a required tool for the 2.2 release of J2EE agents. The most basic of tasks, such as installation and uninstallation can only be performed with this program.

This section lists the tasks you can perform with this program. Moreover, this section lists the specific options you need to issue with the `agentadmin` command to accomplish each task:

- All agent installation and uninstallation is achieved with the `agentadmin` command.
- All tasks performed by the `agentadmin` program, except those involving uninstallation, require the acceptance of a license agreement. This agreement is only presented the first time you use the program.
- The following table lists options that can be used with the `agentadmin` command and gives a brief description of the specific task initiated by the option.

TABLE 8 The `agentadmin` Command: Supported Options

Option	Task Performed
--install	Installs a new agent instance
--uninstall	Uninstalls an existing Agent instance
--listAgents	Displays details of all the configured agents
--agentInfo	Displays details of the agent corresponding to the specified agent IDs
--version	Displays the version information
--encrypt	Encrypts a given string
--getEncryptKey	Generates an Agent Encryption key
--uninstallAll	Uninstalls all the agent instances
--usage	Displays the usage message
--help	Displays a brief help message

Policy Agent Directories

Agent instance information is stored in its own directory at the following location:

PolicyAgent-base/AgentInstance-Dir

where *PolicyAgent-base* represents the directory where a J2EE agent is installed

and where *AgentInstance-Dir* refers to an agent instance directory and represents the directory for a specific instance of a J2EE agent.

Deploying the Agent Application

The following task is a required post-installation step.

Deploy the URI for the agent application using the deployment container, such as the application server.

The agent application is a housekeeping application used by the agent for notifications and other internal functionality. This application is bundled with the agent binaries.

Combining a J2EE Agent With Access Manager (Conditional)

This is a conditional post-installation step that must be performed when a J2EE agent is installed on an deployment container instance where Access Manager has already been installed. Note that Access Manager should be installed prior to the agent being installed.

Known Issues and Limitations

The known issues concerning Policy Agent 2.2 are separated into subsections as follows:

- “All Agents in Policy Agent 2.2” on page 66
- “Web Agents in Policy Agent 2.2” on page 66
- “J2EE Agents in Policy Agent 2.2” on page 70

All Agents in Policy Agent 2.2

The following known issue exists that affects all agents (both J2EE agents and web agents) in the Policy Agent 2.2 software set.

Individual Policy Agent 2.2 Guides Do Not Describe Precautions Against Cookie Hijacking

Precautions you can take against cookie hijacking in an Access Manager deployment are documented in a separate technical note. Though such a deployment includes the configuration of agents from the Policy Agent 2.2 software set, the information is not currently documented in individual agent guides. The following technical note covers this issue: *Technical Note: Precautions Against Cookie Hijacking in an Access Manager Deployment*.

Web Agents in Policy Agent 2.2

Important known issues concerning web agents are separated in this document into the following categories:

- “All Web Agents in Policy Agent 2.2” on page 66
- “Policy Agent 2.2 for Microsoft Internet Information Services 6.0 (Microsoft IIS 6.0)” on page 69

All Web Agents in Policy Agent 2.2

The following known issues exist that affect all web agents in Policy Agent 2.2.

On UNIX-based machines, all web agents require that the X11 DISPLAY variable be set properly.

To set the X11 DISPLAY variable properly, set the variable to a valid X server before installing or uninstalling the web agent. This condition applies even when the install or uninstall command is performed from the command line using the -nodisplay argument.

A harmless error message appears in the web agent log files (6334519)

An error message appears when many concurrent users access the web agent. The error message is as follows: LogService::process() logRecWrite SAXParseException. This exception occurs in the Access Manager log in the following directory: /var/opt/SUNWam/debug. This problem is due to a bug in the multi-threaded logging mechanism of the web agent. However, no known effect to the web agent or the respective Access Manager instance occurs with this error message.

Workaround: You can ignore this message.

Web agent log entries are written to the wrong files (6301676)

When a large number of logging entries are recorded, log rotation fails and the log entries are redirected from the web agent log files to the error log files of the web container. These redirected log entries get written as stderr. The log files then accumulate on the web container without being automatically deleted.

Workaround: During production, do not use fine-grained logging levels, such as levels 4 or 5. These logging levels are only appropriate for short periods of time, such as for debugging.

Besides Agent for Apache HTTP Server 2.0.54, web agents do not support the 64-bit version of a deployment container (6474344)

For example, Agent for Sun Java System Web Server 6.1 does not support the 64-bit release of Sun Java System Web Server 6.1.

Workaround: Except when using Agent for Apache HTTP Server 2.0.54, do not use a web agent with a 64-bit version of the supported web container.

Web Servers often cannot interpret hyphens used in header names

When you set the following property in the web agent AAgent.properties configuration file, be aware of the web server behavior that typically applies:

`com.sun.am.policy.agents.config.profile.attribute.map`

Most web servers demonstrate the following behavior:

- Prefix the header name by `HTTP_`.

- Replace all lower case letters with upper case letters.
- Replace all hyphens with underscores.

Therefore, use underscores “_” rather than hyphens “-” in the header name mapped to the LDAP attribute name to avoid problems. For example, the following property setting could be problematic:

```
com.sun.am.policy.agents.config.profile.attribute.map = cn|common-name
```

Web servers search for the header `HTTP_COMMON_NAME`, and would not find `HTTP_COMMON-NAME`.

Note – You can use the following property to customize the “`HTTP_`” prefix:

```
com.sun.am.policy.agents.config.profile.attribute.cookie.prefix
```

The following example demonstrates how this property can be set:

```
com.sun.am.policy.agents.config.profile.attribute.cookie.prefix = EXAMPLE
```

Error message issued during installation of Policy Agent 2.2 on Linux systems

When the Linux operating system is installed, specific components can be selected. Occasionally the specific components of the operating system selected lack the libraries necessary for Policy Agent 2.2 to function. When the complete Linux operating system is installed, all the required libraries are available. The libraries that are required for the agent to function are as follows: NSPR, NSS, and libxml2.

Workaround: If the Linux operating system you are using is not complete, install the latest versions of these libraries as described in the steps that follow:

At the time this note was added, the latest version of the NSPR library packages was NSPR 4.6.x, while the latest version of the NSS library package was NSS 3.11.x.

To Install Missing Libraries for Policy Agent 2.2 on Linux Systems

- Install the NSS, and libxml2 libraries. These libraries are usually available as part of Linux installation media. NSPR and NSS are available as part of Mozilla binaries/development packages. You can also check the following sites:
 - **NSPR:** <http://www.mozilla.org/projects/nspr/>
 - **NSS:** <http://www.mozilla.org/projects/security/pki/nss/>

Web agents do not function properly when a load balancer exists in front of an Access Manager 6.3 host (6674827)

Since the `com.sun.am.ignore.naming_service` property is not documented in the individual web agent guides, it is explained in this release note.

Starting with Access Manager 7.0, if a load balancer is deployed in front of an Access Manager host, by default the naming response (for all services) uses the protocol, host, and port number of the load balancer.

However, for Access Manager 6.3, the naming response by default uses the protocol, host and port number of the individual Access Manager Server instances. The web agents must then replace the protocol, host, and port number of the individual Access Manager Server instances with the protocol, host, and port number of the of the load balancer. In this scenario, for Policy Agent 2.2, configure the web agent to use the correct server information by setting the `com.sun.am.ignore.naming_service` property as shown in the workaround that follows.

Workaround: Add the following property to the web agent `AMAgent.properties` configuration file and set the value to `true` as indicated:

```
com.sun.am.ignore.naming_service = true
```

While the `com.sun.am.ignore.naming_service` property is not visible in the web agent `AMAgent.properties` configuration file, it exists in the web agent and is by default set to `false`. Therefore, you must add both the property and the value.

The web agent property `com.sun.am.receive_timeout` is not documented in any of the web agent guides (6523846)

The value for this property is the number of milliseconds the agent waits to receive responses from Access Manager. Once the amount of time that has passed matches the value set for this property, any incomplete transactions are dropped and an error is issued indicating that one of the connections has failed.

The default value is `0`. When set to `0`, the socket remains open indefinitely. In most cases, the value should remain at `0`.

Workaround: Not applicable.

Policy Agent 2.2 for Microsoft Internet Information Services 6.0 (Microsoft IIS 6.0)

The following known problem exists that affects Agent for Microsoft IIS 6.0.

When a specific environment variable is not properly set, the system might fail (6433790)

This problem involves the following global environment variable:

```
NSPR_NATIVE_THREADS_ONLY
```

Workaround: Before you install this agent, set this environment variable as shown:

```
NSPR_NATIVE_THREADS_ONLY = 1
```

J2EE Agents in Policy Agent 2.2

Important known issues concerning J2EE agents are separated in this document into the following categories:

- ["All J2EE Agents in Policy Agent 2.2" on page 70](#)
- ["Policy Agent 2.2 for Sun Java System Application Server 8.1" on page 75](#)
- ["Policy Agent 2.2 for Apache Tomcat 5.5 Servlet/JSP Container" on page 75](#)
- ["Policy Agent 2.2 for IBM WebSphere Application Server" on page 76](#)
- ["Policy Agent 2.2 for Oracle Application Server 10g" on page 79](#)

All J2EE Agents in Policy Agent 2.2

The following known issues exist that affect all J2EE agents in Policy Agent 2.2.

A harmless error message appears in the J2EE agent log files (6301668)

This error message, which appears in certain situations, is as follows: ERROR:
RemoteHandler.getLogHostURL(): 'null' is malformed. null.

Workaround: You can ignore this message.

The agentadmin --install command displays an error message after being issued a second time (6268136)

The error message displayed in this situation is as follows:

```
*** ERROR: Another instance of agentadmin is already running. Please stop that instance and try again.
```

This message appears when the first installation operation is aborted with the CTRL-z keystroke combination. This keystroke combination suspends the process, but does not actually stop the process. If other methods are used to abort the operation, such as the CTRL-c keystroke combination, this problem does not occur.

Workaround: When this problem is encountered, close the terminal window and open a new terminal window.

Resources accessed with Internet Explorer 6.0 SP1 can result in 404 Not Found Error (6362249)

This problem occurs when the following conditions apply:

- The J2EE Agent and Access Manager are on the same machine.
- The agent is running in J2EE_POLICY mode.

- The application being accessed is protected by form-based declarative security.

This specific configuration results in an error message primarily because of a bug in Internet Explorer 6.0 SP1, which cannot properly handle redirection when the HTTP request contains a port number. More specifically, this browser does not update the host header to reflect the new port number when you redirect HTTP requests that contain a port number.

Workaround: If the browser used to access content protected by a J2EE agent is Internet Explorer, at a minimum, the version must be Internet Explorer 6.0 SP2.

Harmless error messages related to JAX-RPC appear in the J2EE agent debug files (6325238)

In the J2EE agent debug files, you might see exceptions related to Java API for XML-based remote procedure calls (JAX-RPC). Such messages are not an indication of any known problem.

Workaround: You can safely ignore these error messages.

Exceptions thrown when Access Manager uses polling with a J2EE agent (6452320)

Errors can occur when you perform both of the following:

1. Deploy `amclientsdk.jar` file on a client machine, such as when deploying a J2EE agent.
2. Enable polling in Access Manager.

The errors that appear are similar to the following:

```
ERROR: Send Polling Error:  
com.iplanet.am.util.ThreadPoolException: amSessionPoller thread pool's task queue  
is full.
```

Workaround: This workaround is specific to J2EE agents. If you deployed Access Manager Client SDK in another manner, such as by deploying the Distributed Authentication UI, the two properties mentioned subsequently would be added to the Access Manager `AMConfig.properties` configuration file instead of to the J2EE agent `AMAgents.properties` configuration file.

If you have only a few hundred concurrent sessions, you can create the following properties in the J2EE agent `AMAgents.properties` configuration file by adding the two following lines to the bottom of the file:

```
com.sun.identity.session.polling.threadpool.size=10  
com.sun.identity.session.polling.threadpool.threshold=10000
```

For thousands or tens of thousands of sessions, the values should be set the same as those for notification in the Access Manager `AMConfig.properties` file after running `amtune -identity`.

For example, for a machine with 4GB of RAM, the Access Manager `amtune-identity` will set the following:

```
com.sun.identity.session.notification.threadpool.size=28  
com.sun.identity.session.notification.threadpool.threshold=76288
```

You can set similar values in the J2EE agent `AMAgents.properties` configuration file when the machine for the J2EE agent has 4GB of RAM:

```
com.sun.identity.session.polling.threadpool.size=28  
com.sun.identity.session.polling.threadpool.threshold=76288
```

Policy Agent 2.2 guides do not explain configuration of J2EE Agents and Access Manager SDK on the Same Deployment Container

Currently, no information is provided in Policy Agent 2.2 documentation for J2EE agents regarding this issue. Therefore, the required task for this scenario is presented at this time in this document.

If you install a J2EE agent instance on the same deployment container (such as an application server) as an Access Manager SDK instance, you must edit a property in the `AMConfig.properties` file of the Access Manager SDK instance.

This task is necessary to ensure proper evaluation of policies. The configuration task described in this section applies to J2EE agents, not web agents, in the Policy Agent 2.2 software set. Therefore, no additional configuration steps are required when an Access Manager SDK instance and a web agent instance are installed on the same deployment container (such as a web server).

Note – The configuration task described in this section applies to situations where Access Manager SDK was installed as a separate component using the Sun Java Enterprise System installer. The configuration task described in this section is not required for the following versions of the SDK:

- The client SDK
 - Access Manager SDK bundled with Access Manager
-

▼ To Install a J2EE Agent Instance With an Access Manager SDK Instance

This task is performed on the deployment container on which the Access Manager SDK is installed. This same deployment container is protected by the J2EE agent.

- 1 Using an editor of your choice access the Access Manager SDK `AMConfig.properties` file.**
- 2 Edit the following property as shown**

```
com.sun.identity.agents.config.location = PolicyAgent-base/AgentInstance-Dir/config/AMAgent.properties
```

- 3 Save and close the `AMConfig.properties` file.
- 4 Restart the deployment container.

J2EE agent installation prompts do not allow responses with leading or trailing spaces (6452708)

The installer for J2EE agents does not ignore leading and trailing spaces when you provide answers to prompts. This situation can cause a variety of problems. For example, if you include a leading or trailing space when pointing to a resource, the resource would not be recognized and an error message such as the following would be issued:

```
ERROR: Invalid Server Instance directory.
```

The preceding error message is one example. Any one of several messages could be issued depending upon the specific scenario.

Workaround: None. However, be aware of the situation and be sure not to include leading or trailing spaces when providing responses to installation prompts.

The `agentadmin --install` command fails to install the J2EE agent because of a previous unsuccessful installation (6443460)

An agent instance directory, for example `agent_001`, is created early in a J2EE agent installation. If that installation is unsuccessful, then the actual agent “`agent_001`” is not created, but the directory `agent_001` might have been created. If the agent instance directory was created, the installer does not remove it in cases where the installation fails. In such a scenario, a subsequent installation attempt of a J2EE agent would fail unless the directory `agent_001` is manually removed first.

In this scenario, the installer does not detect the previously unsuccessful installation of `agent_001`. and, therefore, attempts to create it. At first, the installer only searches for the agent instance, not the agent instance directory. As the installation begins, the installer attempts to create the `agent_001` directory, but at that point the installer finds that this directory already exists. The installer then aborts the installation. In such a scenario, an error message such as the following is issued:

```
ERROR: Installation failed due to the following error - (Failed to  
create directory /export/j2ee_agents/am_websphere_agent/agent_001.)
```

Workaround: Manually remove the agent instance directory of the unsuccessful agent installation before attempting to install the agent again.

The first use of a resource protected by a declarative constraint results in a misdirect

At this time, this behavior affects all J2EE agents except for the various agents for BEA WebLogic and Apache Tomcat.

This situation occurs prior to the user being authenticated by Access Manager and only when web-tier declarative security is set for the specific resource the user is attempting to access. Under these circumstances, when the user attempts to access the resource, she (after authentication) is directed to the welcome page of the application instead of to the exact location requested.

While the user might not expect to be directed to the welcome page, the result does not constitute an access problem. From the welcome page, the user can still access the desired resource based on the policies defined.

Workaround: This behavior is expected. No workaround exists.

The agentadmin --getUuid command fails for amadmin user on Access Manager 7 with various agents (6452713)

When you issue the agentadmin --getUuid command to retrieve the universal ID of the amadmin user, you might see an error message such as the following:

```
agentadmin --getUuid amadmin user example
Failed to create debug directory
10/25/2006 02:22:39:834 PM PDT: Thread[main,5,main]
DataLayer: number of retry = 3
```

The problem occurs under these conditions:

- Install one of the following agents:
 - Agent for IBM WebSphere Application Server 5.1.1
 - Agent for IBM WebSphere Application Server 6.0
 - Agent for BEA WebLogic Server/Portal 8.1 SP4
 - Agent for BEA WebLogic Server 9.0/9.1
 - Agent for BEA WebLogic Server/Portal 10
 - Agent for Sun Java System Application Server 8.1
 - Agent for Sun Java System Application Server 9.0/9.1
- Configure the agent with Access Manager 7 in realm mode.

Workaround: None at this time.

Policy Agent 2.2 for Sun Java System Application Server 8.1

The following known problems exist that affect Agent for Sun Java System Application Server 8.1.

When interacting with Application Server 8.1, the Access Manager SDK cannot initialize admin data and displays an exception message (6284280)

The exception message displayed in this situation is as follows:

```
javax.crypto.BadPaddingException
```

Workaround: None at this time.

Policy Agent 2.2 for Apache Tomcat 5.5 Servlet/JSP Container

The following known problems exist that affect Agent for Apache Tomcat 5.5 Servlet/JSP Container. This agent also supports Agent for Apache Tomcat 5.0.28 Servlet/JSP Container.

Apache Tomcat Servlet/JSP Container bits with the .exe extension do not allow the agent to perform properly (6371980)

The Apache Tomcat Servlet/JSP Container bits with the .exe extension do not contain the Catalina scripts required to plug in the agent realm and filter. Therefore, Apache Tomcat Servlet/JSP Container bits with the .exe extension are not supported by the agent.

Workaround: When installing Apache Tomcat Servlet/JSP Container bits use the .zip extension. For example, for version 5.5.9, the correct compressed file supported by the agent is as follows:

```
jakarta-tomcat-5.5.9.zip
```

Compressed files for Apache Tomcat Servlet/JSP Container are available at the Apache web site. For example, you can attempt to retrieve the compressed file specifically for version 5.5.9 using the following link: <http://archive.apache.org/dist/tomcat/tomcat-5/archive/v5.5.9/bin/jakarta-tomcat-5.5.9.zip>.

Error message issued with certain versions of the deployment container starting with Apache Tomcat 5.5.23 Servlet/JSP Container

This is a classpath issue. After installing Agent for Apache Tomcat 5.5 Servlet/JSP Container on Apache Tomcat 5.5.23, the Apache server does not start. The server log might show an error that includes the following line:

```
java.lang.NoClassDefFoundError: org/apache/commons/modeler/BaseModelMBean
```

This error occurs because a jar file that was named commons-modeler.jar prior to Apache Tomcat 5.5.23 Servlet/JSP Container changed names to commons-modeler-2.0.jar in Apache Tomcat 5.5.23 Servlet/JSP Container.

Workaround: After installing Agent for Apache Tomcat 5.5 Servlet/JSP Container on Apache Tomcat 5.5.23, follow these steps:

1. Open the following platform specific file:

Unix-based systems (includes Linux)	<i>Tomcat-base/bin/setAgentclasspath.sh</i>
Windows Systems	<i>Tomcat-base\bin\setAgentclasspath.bat</i>
2. Change the name of `commons-modeler.jar` file to `commons-modeler-2.0.jar`.
3. Save the file.
4. Restart Apache Tomcat 5.5 Servlet/JSP Container.

Policy Agent 2.2 for IBM WebSphere Application Server

The following known problems exist that can affect the following agents: Agent for IBM WebSphere Application Server 5.1.1, Agent for IBM WebSphere Application Server 6.0, Agent for IBM WebSphere Application Server 6.1.

The `agentadmin --install` command fails on Agent for IBM WebSphere Application Server (6385085)

This issue applies to both Agent for IBM WebSphere Application Server 5.1.1 and Agent for IBM WebSphere Application Server 6.0.

The `--install` option of the `agentadmin` command can fail because of an issue with the IBM Java Development Kit (JDK). The IBM JDK comes with IBM WebSphere Application Server.

To run the `--install` option, the `agentadmin` script searches for a JDK with a Sun Microsystems JCE provider. However, the IBM JDK does not come with this JCE provider.

Therefore, to allow the agent installer to work with the IBM JDK, implement the steps described in the following workaround.

Workaround: The following task involving the editing of the `agentadmin` file makes available a JCE implementation that allows the agent installer to function properly.

▼ To Enable the `agentadmin` Script to Locate the Respective JCE Implementation

1 Change to the directory containing the `agentadmin` file:

PolicyAgent-base/bin

2 Create a backup copy of `agentadmin` file.

This file is either the `agentadmin` script or, for Windows systems, the `agentadmin.bat` file.

3 Edit the `agentadmin` file accordingly.

a. Locate the last line of the `agentadmin` script.

This line starts with the following string: `$JAVA_VM -classpath ...`

b. Add the following two properties between the string `$JAVA_VM` and the string `-classpath`:

`-DamCryptoDescriptor.provider=IBMJCE -DamKeyGenDescriptor.provider=IBMJCE`

For example, after editing the final line of the script, it appears as follows:

```
$JAVA_VM -DamCryptoDescriptor.provider=IBMJCE
-DamKeyGenDescriptor.provider=IBMJCE -classpath $AGENT_CLASSPATH
com.sun.identity.agents.tools.launch.AgentAdminLauncher $*
```

Harmless error message related to the `DirectoryManager` class appears in the debug files of agents for IBM WebSphere Application Server (6403913)

This issue applies to both Agent for IBM WebSphere Application Server 5.1.1 and Agent for IBM WebSphere Application Server 6.0.

An exception message appears in the debug logs for the message mode. The exception message states that the `DirectoryManager` class cannot be found. The message is issued by the software development kit (SDK) as it searches for an indication of the mode in which it is running: remote or server.

Workaround: You can safely ignore this message.

Using the `agentadmin` command fails under specific conditions when Agent for IBM WebSphere Application Server is used with Access Manager 6.3 (6443463)

The problem occurs when spaces are used in the common name (`cn`) in specific scenarios. The following conditions can cause the problem:

- When either of the following agents are used:
 - Agent for IBM WebSphere Application Server 5.1.1
 - Agent for IBM WebSphere Application Server 6.0
- When either of the following `agentadmin` options are used:
 - `agentadmin --setGroup`
 - `agentadmin --removeGroup`
- When Access Manager 6.3 is used, since the problem occurs when the group name includes `cn`, which is specific to Access Manager 6.3.

The following `agentadmin` command illustrates the problem. Notice that the `cn` contains spaces: `was admin role`. The spaces before and after the string `admin` are not allowed:

```
/agentadmin --setGroup administrator "cn=was admin role,dc=example,dc=com"  
/opt/WebSphere/AppServer/config/cells/
```

Workaround: Use a text editor of your choice to directly map the groups in the `admin-authz.xml` file.

The sample application of Agent for IBM WebSphere Application Server provides incorrect information about the role required (6452733)

This issue applies to both Agent for IBM WebSphere Application Server 5.1.1 and Agent for IBM WebSphere Application Server 6.0.

The sample application issues a message that erroneously states that you must be logged in with the role “employee” in order to be granted access.

The following specific conditions apply:

- Install and configure Agent for IBM WebSphere Application Server
- Deploy the sample application.
- Invoke the declarative J2EE security test sample.

At this point, a message appears saying that access to this servlet requires you to belong to the “employee” role.

- Log in with the role “employee.”
- Access is denied.
- Log in with the role “manager.”
- Access is allowed.

Workaround: None. However, be aware of the situation and be sure to log in as a user who belongs to the “manager” role.

The `agentadmin --install` command fails to install a second instance of Agent for IBM WebSphere Application Server when using the same bits on the same host (6452719)

This issue applies to both Agent for IBM WebSphere Application Server 5.1.1 and Agent for IBM WebSphere Application Server 6.0.

If two instances of Agent for IBM WebSphere Application Server are required on the same host, you cannot use the same agent bits to install each instance.

Workaround: Download a second set of bits to install the second instance of Agent for IBM WebSphere Application Server.

During the installation of Agent for IBM WebSphere Application Server on a Windows system, the IBM JVM returns an empty encryption key (6461210)

This issue applies to both Agent for IBM WebSphere Application Server 5.1.1 and Agent for IBM WebSphere Application Server 6.0.

Be aware that this issue only occurs on Windows systems. During the installation of the agent, you are prompted for the encryption key, as such:

```
Enter a valid Encryption Key.  
[ ? : Help, < : Back, ! : Exit ]  
Enter the Encryption Key []:
```

Usually, a default encryption key is provided in the prompt. However, depending upon the configuration of the IBM WebSphere Application Server instance, the IBM Java Virtual Machine (JVM) might return an empty encryption key. In such a case, the agent installer presents the prompt without a default encryption key included, as illustrated by the preceding example prompt.

Workaround: Manually enter a random value in response to this prompt.

Settings for CLASPATH variable are lost after agentadmin command is issued (6653936)

This behavior has been observed with Agent for IBM WebSphere Application Server 6.0. Though rare, CLASPATH variable settings can be cleared after the `agentadmin` command is executed.

Workaround: Manually add the following entries to the CLASPATH variable of the IBM WebSphere Application Server 6.0 instance (where `agent_001` is an example of the agent instance. It might be another instance, such as a `agent_002` or `agent_003`):

- `PolicyAgent-base/agent_00x/config`
- `PolicyAgent-base/locale`

Policy Agent 2.2 for Oracle Application Server 10g

The following known problem exists that affects Agent for Oracle Application Server 10g.

The sample application requires editing to work properly (6486895)

The sample application of Agent for Oracle Application Server 10g requires minor editing of XML files to work properly. The following task explains the editing required.

▼ To Configure XML Files of the Sample Application

1 Using a text editor of your choice, access the *PolicyAgent-base/sampleapp/build.xml* file.

2 Change line 69 as shown:

Change From <pathelement location="\${appserv.lib.dir}/ejb.jar"/>

Change To <pathelement location="\${appserv.lib.dir}/ejb.jar"/>

3 At line 95, add the following snippet:

```
<pathelement location="${appserv.lib.dir}/servlet.jar"/>
<pathelement location="${appserv.lib.dir}/ejb.jar"/>
```

4 Save and close the *build.xml* file.

5 Using a text editor of your choice, access the *META-INF/orion-application.xml* file.

6 Add the following attribute as indicated:

"location=../../jazn-data.xml"

The following shows how the element appears before and after you have added the required attribute:

Change From <jazn provider="XML">

Change To <jazn provider="XML" "location=../../jazn-data.xml">

7 (Conditional) If the *jazn-data.xml* file does not exist in the *META-INF* directory, create one as demonstrated in the following example:

```
<?xml version="1.0" encoding="UTF-8" standalone='yes'?>
<!DOCTYPE jazn-data PUBLIC "JAZN-XML Data"
  "http://xmlns.oracle.com/ias/dtds/jazn-data.dtd">
<jazn-data>
  <!-- JAZN Realm Data -->
  <jazn-realm>
    <realm>
      <name>jazn.com</name>
      <users>
        </users>
      <roles>
        </roles>
      </realm>
    </jazn-realm>

    <!-- JAZN Policy Data -->
    <jazn-policy>
      </jazn-policy>
    <!-- Permission Class Data -->
    <jazn-permission-classes>
      </jazn-permission-classes>
```

```
<!-- Principal Class Data -->
<jazn-principal-classes>
</jazn-principal-classes>
<!-- Login Module Data -->
<jazn-loginconfig>
</jazn-loginconfig>
</jazn-data>
```

- Next Steps** After you have performed the preceding steps, rebuild the sample application as described in the sample application `readme.txt` file, which is in the following location:

PolicyAgent-base/sampleapp/readme.txt

Documentation Updates

- “[Wrong separator used in web agent guides for com.sun.am.policy.agents.config.local.log.size property \(6901494\)](#)” on page 81
- “[Policy Agent 2.2 documentation should reference OpenSSO \(6857941\)](#)” on page 81

Wrong separator used in web agent guides for com.sun.am.policy.agents.config.local.log.size property (6901494)

Some web agent guides show a colon rather than an equal sign (=) as the separator to set the `com.sun.am.policy.agents.config.local.log.size` property. To set this property, always use the equal sign. For example:

`com.sun.am.policy.agents.config.local.log.size = n`

Where *n* represents the size of a file in bytes. The file size should be a minimum of 3000 bytes. The default size is 10 megabytes.

Policy Agent 2.2 documentation should reference OpenSSO (6857941)

The Policy Agent 2.2 guides refer to Sun Java System Access Manager. The version 2.2 policy agents, however, are also compatible with Sun OpenSSO Enterprise and Sun OpenSSO Express releases.

Considerations for using a version 2.2 policy agent with OpenSSO Enterprise or OpenSSO Express include:

- A version 2.2 policy agent must continue to store its configuration data locally in its `AMAgent.properties` file. Therefore, because the version 2.2 policy agent configuration data is local to the agent, the OpenSSO centralized agent configuration option is not supported for version 2.2 agents. To configure a version 2.2 policy agent, you must continue to edit the agent's `AMAgent.properties` file.
- When you are configuring a version 2.2 policy agent with OpenSSO, the default Primary Server Deployment URI (and Failover Server Deployment URI, if required by the agent) is `/opensso` rather than `/amserver`.
- You can create a version 2.2 Java EE (formerly J2EE) or web agent profile in the OpenSSO Administration Console under Access Control, *realm-name*, Agents, and 2.2 Agents. However, you must configure the agent by editing its `AMAgent.properties` file.
- OpenSSO Enterprise supports both version 3.0 and version 2.2 policy agents in the same deployment.

For more information about policy agents, see the following documentation collections:

- Policy Agent 3.0: <http://download.oracle.com/docs/cd/E19681-01/index.html>
- Policy Agent 2.2: <http://download.oracle.com/docs/cd/E19534-01/index.html>

Deprecation Notifications and Announcements

With the release of Policy Agent 3.0, support for Policy Agent 2.1 will be dropped. You should migrate Policy Agent 2.1 environments to Policy Agent 2.2 or Policy Agent 3.0 (if a version 3.0 agent is available) to be in a supported configuration.

Redistributable Files

Sun Java System Access Manager Policy Agent 2.2 does not contain any files which you can redistribute.

How to Report Problems and Provide Feedback

If you have problems with Sun Java System Access Manager Policy Agent 2.2, contact Oracle customer support using one of the following mechanisms:

- My Oracle Support: <https://support.oracle.com/>

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

- The telephone dispatch number associated with your maintenance contract

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

- 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

Release Notes Revision History

TABLE 9 Revision History

Date	Description of Changes
June 20, 2005	Early access release.
October 5, 2005	The first release of Sun Java System Access Manager Policy Agent 2.2 includes Policy Agent for Sun Java System Web Server 6.1 and Policy Agent for Sun Java System Application Server 8.1.
November 29, 2005	This release of Sun Java System Access Manager Policy Agent 2.2 includes Policy Agent for Apache HTTP Server 2.0.54. This agent also supports Apache HTTP Server 1.3.33.
January 10, 2006	This release of Sun Java System Access Manager Policy Agent 2.2 includes Policy Agent for BEA WebLogic Server/Portal 8.1 SP4. This agent also supports BEA WebLogic Express 8.1 SP4.
January 18, 2006	This release of Sun Java System Access Manager Policy Agent 2.2 includes Policy Agent for Apache Tomcat 5.5 Servlet/JSP Container. This agent also supports Apache Tomcat 5.0.28 Servlet/JSP Container.
February 4, 2006	This release of Sun Java System Access Manager Policy Agent 2.2 includes Policy Agent for Microsoft Internet Information Services 6.0 (Microsoft IIS 6.0).
March 31, 2006	This release of Sun Java System Access Manager Policy Agent 2.2 includes Policy Agent for IBM WebSphere Application Server 5.1.1 and Policy Agent for IBM WebSphere Application Server 6.0.

TABLE 9 Revision History *(Continued)*

Date	Description of Changes
May 11, 2006	<p>This release of Sun Java System Access Manager Policy Agent 2.2 includes the following agents:</p> <ul style="list-style-type: none"> ■ Policy Agent for IBM Lotus Domino 6.5.4 ■ Policy Agent for SAP Enterprise Portal 6.0 and Web Application Server 6.40
June 16, 2006	<p>This release of Sun Java System Access Manager Policy Agent 2.2 includes Policy Agent for IBM WebSphere Portal Server 5.1.0.2.</p>
August 8, 2006	<p>This release of Sun Java System Access Manager Policy Agent 2.2 includes the following agents:</p> <ul style="list-style-type: none"> ■ Policy Agent for Sun Java System Web Proxy Server 4.0 ■ Policy Agent for BEA WebLogic Server 9.0/9.1
September 30, 2006	<p>This release of Sun Java System Access Manager Policy Agent 2.2 includes minor changes, such as an addition to “Known Issues and Limitations” on page 66.</p>
October 30, 2006	<p>This release of Sun Java System Access Manager Policy Agent 2.2 includes Policy Agent for Oracle Application Server 10g.</p>
December 22, 2006	<p>This release of Sun Java System Access Manager Policy Agent 2.2 includes Policy Agent for BEA WebLogic Server/Portal 9.2.</p>
March 12, 2007	<p>This update of <i>Sun Java System Access Manager Policy Agent 2.2 Release Notes</i> is being made to specify that Policy Agent 2.2 supports Access Manager 7.1.</p>
April 19, 2007	<p>This release of Sun Java System Access Manager Policy Agent 2.2 includes Policy Agent for IBM Lotus Domino 7.0.</p>
May 11, 2007	<p>This release of Sun Java System Access Manager Policy Agent 2.2 includes updated operating system support of Policy Agent for Apache HTTP Server. This update of the Release Notes also includes an explanation of Policy Agent 2.2 minor version support for deployment containers and operating systems.</p>
June 20, 2007	<p>This release of Sun Java System Access Manager Policy Agent 2.2 includes Policy Agent for JBoss Application Server 4.0. Also the web agent guides were updated at this time to correct various typographical and informational errors.</p>
August 20, 2007	<p>This release of Sun Java System Access Manager Policy Agent 2.2 includes Policy Agent for Sun Java System Application Server 9.0/9.1 and Policy Agent for Sun Java System Web Server 7.0.</p>

TABLE 9 Revision History *(Continued)*

Date	Description of Changes
October 3, 2007	<p>This release of Sun Java System Access Manager Policy Agent 2.2 includes Policy Agent for BEA WebLogic Server/Portal 10.</p> <p>Furthermore, this release includes an update to Policy Agent for Microsoft Internet Information Services (IIS) 6.0, enabling the agent to protect Microsoft Office SharePoint and Outlook Web Access.</p>
November 1, 2007	<p>This release of Sun Java System Access Manager Policy Agent 2.2 includes Policy Agent for Apache HTTP Server 2.2.</p> <p>Furthermore, this release includes an update to Policy Agent for Apache HTTP Server 2.0.54 to include support for Windows Systems and AIX systems.</p>
December 11, 2007	<p>This release of Sun Java System Access Manager Policy Agent 2.2 involves the following agents:</p> <ul style="list-style-type: none"> ■ New Agent: Policy Agent for IBM WebSphere Application Server 6.1 ■ Update of Agent: Policy Agent for SAP Enterprise Portal 6.0 and Web Application Server 6.40 to include support for AIX systems <p>This update of the Release Notes also includes an addition to the “Known Issues and Limitations” section. For more information, see “Web Servers often cannot interpret hyphens used in header names” on page 67.</p>
June 02, 2008	This release of Sun Java System Access Manager Policy Agent 2.2 includes Policy Agent for SAP Enterprise Portal 7.0 and Web Application Server 7.0.
June 21, 2008	<p>This release of Sun Java System Access Manager Policy Agent 2.2 includes the following agents:</p> <ul style="list-style-type: none"> ■ Policy Agent for Apache Tomcat 6.0 ■ Policy Agent for Microsoft IIS 6.0 With Outlook Web Access 2007/ SharePoint 2007
September 14, 2008	This update of <i>Sun Java System Access Manager Policy Agent 2.2 Release Notes</i> is being made to indicate that the supported platforms for Policy Agent 2.2 for Apache HTTP Server 2.2 has increased to include SUSE Linux 10.1.
March 2, 2009	<p>The Release Notes are updated as follows:</p> <ul style="list-style-type: none"> ■ Added the “Policy Agent 2.2–02 Update Release” on page 32 section. ■ Added drop of support statement for Policy Agent 2.1 in “Deprecation Notifications and Announcements” on page 82.
July 21, 2009	<p>The Release Notes are updated as follows:</p> <ul style="list-style-type: none"> ■ Added the “Policy Agent 2.2–03 Update Release” on page 26 section. ■ Documented CR 6857941 in “Documentation Updates” on page 81.

TABLE 9 Revision History *(Continued)*

Date	Description of Changes
December 7, 2009	The Release Notes are updated as follows: <ul style="list-style-type: none">■ Added the “Policy Agent 2.2–04 Update Release” on page 22 section.■ Documented CR 6901494 in “Documentation Updates” on page 81.
April 9, 2010	Updated “Policy Agent 2.2–03 Update Release” on page 26 for Java EE (formerly J2EE) agents.
March 28, 2011	The Release Notes are updated as follows: <ul style="list-style-type: none">■ Added the “Policy Agent 2.2–05 Update Release” on page 19 section.■ Revised outdated URLs.