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

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

Part No: 819–2143–20
December 22, 2006

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

CETTE PUBLICATION EST FOURNIE "EN L'ETAT" ET AUCUNE GARANTIE, EXPRESSE OU IMPLICITE, N'EST ACCORDEE, Y COMPRIS DES GARANTIES CONCERNANT LA VALEUR MARCHANDE, L'APTITUDE DE LA PUBLICATION A REPONDRE A UNE UTILISATION PARTICULIERE, OU LE FAIT QU'ELLE NE SOIT PAS CONTREFAISANTE DE PRODUIT DE TIERS. CE DENI DE GARANTIE NE S'APPLIQUERAIT PAS, DANS LA MESURE OU IL SERAIT TENU JURIDIQUEMENT NUL ET NON AVENU.

070215@16599

Contents

Preface

The Sun Java™ System Policy Agent software consists of J2EE (Java 2 Platform Enterprise Edition) agents and web agents. This Access Manager Policy Agent 2.2 User's Guide provides an overview of how Sun Java System Policy Agent 2.2 works, detailing features and processes of Policy Agent that are the same for all J2EE and web agents. The J2EE and web agents have many similarities, but the two types of agents also have some differences. This book covers the similarities in detail while summarizing the differences. This book is designed to help you identify topics relevant to your enterprise needs so that you can explore those topics more fully in other Access Manager and Policy Agent documentation.

Within the Policy Agent documentation set, each agent has its own guide. Each book specific to a J2EE agent covers what all J2EE agents have in common as well as covering aspects that are unique to that particular J2EE agent. Similarly, each book specific to a web agent covers what all web agents have in common as well as covering aspects that are unique to that particular web agent.

Who Should Use This Book

This *Access Manager Policy Agent 2.2 User's Guide* 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)
- Web technologies or J2EE technologies

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://docs.sun.com`. 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.

Related Books

Sun Microsystems server documentation sets, some of which are mentioned in this preface, are available at `http://docs.sun.com`. These documentation sets provide information that can be helpful for a deployment that includes Policy Agent:

Access Manager Documentation Set

TABLE P–1 Access Manager 7 2005Q4 Documentation Set

Title	Description
Sun Java System Access Manager 7 2005Q4 Release Notes	Available after the product is released. Contains last-minute information, including a description of what is new in this current release, known problems and limitations, installation notes, and how to report issues with the software or the documentation.
Sun Java System Access Manager 7 2005Q4 Technical Overview	Provides an overview of how Access Manager components work together to consolidate identity management and to protect enterprise assets and web-based applications. Explains basic Access Manager concepts and terminology.

TABLE P–1 Access Manager 7 2005Q4 Documentation Set *(Continued)*

Title	Description
Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide	Provides information about planning a deployment within an existing information technology infrastructure.
Sun Java System Access Manager 7 2005Q4 Performance Tuning Guide	Describes how to tune Access Manager and its related components.
Sun Java System Access Manager 7 2005Q4 Administration Guide	Describes how to use the Access Manager Console as well as how to manage user and service data via the command line.
Sun Java System Access Manager 7 2005Q4 Federation and SAML Administration Guide	Provides information about the features in Access Manager that are based on the Liberty Alliance Project and SAML specifications. It includes information on the integrated services based on these specifications, instructions for enabling a Liberty-based environment, and summaries of the application programming interface (API) for extending the framework.
Sun Java System Access Manager 7 2005Q4 Developer's Guide	Offers information on how to customize Access Manager and integrate its functionality into an organization's current technical infrastructure. Contains details about the programmatic aspects of the product and its API.
Sun Java System Access Manager 7 2005Q4 C API Reference	Provides summaries of data types, structures, and functions that make up the Access Manager public C APIs.
Sun Java System Access Manager 7 2005Q4 Java API Reference	Are generated from Java code using the JavaDoc tool. The pages provide information on the implementation of the Java packages in Access Manager.
Sun Java System Access Manager Policy Agent 2.2 User's Guide (this guide)	Provides an overview of Policy Agent software, introducing web agents and J2EE agents. Also provides a list of web agents and J2EE agents currently available.

Updates to the *Release Notes* and links to modifications of the core documentation can be found on the Access Manager page at the Sun Java System 2005Q4 documentation web site. Updated documents are marked with a revision date.

Policy Agent 2.2 Documentation Set

This *Sun Java System Access Manager Policy Agent 2.2 User's Guide* is available in two documentation sets: the Access Manager documentation set as described in Table P–1 and in the Policy Agent 2.2 documentation set as described in this section. The other guides in the Policy Agent 2.2 documentation set are described in the following sections:

- "Individual Agent Guides" on page 8 (each agent has its own guide)
- "Release Notes" on page 8

Individual 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 this 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 and configuration information for a specific web agent.

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

The individual agent guides are listed along with supported server information in this guide in the following chapters:

Web Agents	Chapter 2
J2EE Agents	Chapter 3

Release Notes

The *Sun Java System Access Manager Policy Agent 2.2 Release Notes* are available online after an agent or set of agents is released. The release notes include a description of what is new in the current release, known problems and limitations, installation notes, and how to report issues with the software or the documentation.

Sun Java Enterprise System Product Documentation

For useful information for related products, see the following documentation collections on the Sun Java Enterprise System documentation web site (`http://docs.sun.com/prod/entsys.05q4`)

- Sun Java System Directory Server:

  `http://docs.sun.com/coll/1316.1`
- Sun Java System Web Server:

  `http://docs.sun.com/coll/1308.1`
- Sun Java System Application Server:

  `http://docs.sun.com/coll/1310.1`
- Sun Java System Message Queue:

  `http://docs.sun.com/coll/1307.1`
- Sun Java System Web Proxy Server:

  `http://docs.sun.com/coll/1311.1`

Accessing Sun Resources Online

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

Download Center
`http://wwws.sun.com/software/download`

Sun Java System Services Suite
`http://www.sun.com/service/sunps/sunone/index.html`

Sun Enterprise Services, Solaris Patches, and Support
`http://sunsolve.sun.com/`

Developer Information
`http://developers.sun.com/prodtech/index.html`

Contacting Sun Technical Support

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

`http://www.sun.com/service/contacting`

Related Third-Party Web Site References

Sun is not responsible for the availability of third-party web sites mentioned in this document. Sun does not endorse and is not responsible or liable for any content, advertising, products, or other materials that are available on or through such sites or resources. Sun will not be responsible or liable for any actual or alleged damage or loss caused 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.

Sun Welcomes Your Comments

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

To share your comments, go to (`http://docs.sun.com`) and click 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 *Access Manager Policy Agent 2.2 User's Guide*, and the part number is 819-2143.

Documentation, Support, and Training

Sun Function	URL	Description
Documentation	`http://www.sun.com/documentation/`	Download PDF and HTML documents, and order printed documents
Support and Training	`http://www.sun.com/training/`	Obtain technical support, download patches, and learn about Sun courses

Typographic Conventions

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

TABLE P–2 Typographic Conventions

Typeface or Symbol	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:`

aabbcc123	Placeholder: replace with a real name or value	The command to remove a file is `rm` *filename*.
AaBbCc123	Book titles, new terms, and terms to be emphasized	Read Chapter 6 in the *User's Guide*. Perform a *patch analysis*. Do *not* save the file. [Note that some emphasized items appear bold online.]

Shell Prompts in Command Examples

The following table shows the default system prompt and superuser prompt for the C shell, Bourne shell, and Korn shell.

TABLE P–3 Shell Prompts

Shell	Prompt
C shell prompt	`machine_name%`
C shell superuser prompt	`machine_name#`
Bourne shell and Korn shell prompt	`$`
Bourne shell and Korn shell superuser prompt	`#`

CHAPTER 1

Role of Policy Agent Software

Sun Java™ SystemPolicy Agent 2.2 software consists of web agents and J2EE agents. This chapter explains the similarities and differences of these two types of agents.

An Overview of Policy Agent

Access control in Sun Java System Access Manager is enforced using agents. Agents protect content on designated deployment containers, such as web servers and application servers, from unauthorized intrusions. Agents are separate from Access Manager.

Note – The most current agents in the Policy Agent software set can be downloaded from the Identity Management page of the Sun Microsystems Download Center: `http://www.sun.com/software/download`

Web agents and J2EE agents differ in a few ways. One significant way the two agent types differ is in the resources that the two agent types protect. Web agents protect resources on web and proxy servers while J2EE agents protect resources on application and portal servers. However, the most basic tasks that the two agent types perform in order to protect resources are similar.

This chapter does the following:

Explains what agents do.

Describes briefly what a web agent is.

Describes briefly what a J2EE agent is.

Explains how these two types of agents are similar to each other and yet different.

All agents do the following:

- Enable cross-domain single sign-on (CDSSO).
- Determine whether a user is authenticated.

- Determine whether a resource is protected.
- For an authenticated user attempting to access a protected resource, determine whether the user is authorized to access that resource.
- Allow or deny a user access to a protected resource according to the results of the authentication and authorization processes.
- Log access information and diagnostic information.

The preceding task descriptions provide a simplified explanation of what agents do. Agents perform these tasks in conjunction with Access Manager. More specifically, agents work with various Access Manager services, such as Authentication Service, Naming Service, Session Service, Logging Service, and Policy Service to perform these tasks.

For example, user authentication is handled by Access Manager Authentication Service. After authentication, users still cannot access a protected resource until the defined policies regarding user privileges are approved. The agent and Access Manager continue to interact, performing several small tasks back and forth, until the agent finally enforces a policy decision to either allow or deny access. The interactions that take place between Policy Agent and Access Manager are not covered in detail in Policy Agent documentation. For a more detailed explanation of these interactions, see Chapter 2, “User Session Management and Single Sign-On,” in *Sun Java System Access Manager 7 2005Q4 Technical Overview*

Example of Policy Decision Process

When a user attempts to access content on a protected resource, many deployment variables are involved. For example, a firewall might or might not be present. Another example of a deployment variable concerns authentication levels. In a real-world deployment, different resources on a deployment container (such as an application or web server) might require different levels of authentication. These two examples hint at the complexity involved in providing an example of a policy decision process: the process varies greatly depending on the specifics of the deployment. Many other factors can affect the policy decision process, such as the IP address, time zone, and policy expiration time.

Each deployment variable can add a layer of complexity, which might affect how an agent reacts and how Access Manager reacts. This section provides a simple example of a policy decision process that highlights the role of an agent. Therefore, many of the detailed tasks and interactions, especially those processes that occur in Access Manager are left out. Do not expect the deployment represented in this example to match the deployment at your site. This is a generalized example that is applicable to both web and J2EE agents. Some of the basic steps in the policy decision process are depicted in Figure 1–1. The figure is followed by a written description of the process.

For this example, in order to focus on stages of the process most relevant to Policy Agent, certain conditions are assumed as follows:

The user is attempting to access a protected resource after having already accessed a protected resource on the same Domain Name Server (DNS) domain. When the user accessed the first protected resource, Access Manager started a session. The user's attempt to access a second resource, makes this user's session a single sign-on (SSO) session. Therefore, at this point, the following already occurred:

- The user attempted to access a protected resource through a browser (the first resource that the user attempts to access during this session).
- The browser request was intercepted by the agent.
- The browser was redirected to a login uniform resource locator (URL), which is the interface to Access Manager Authentication Service.
- After the user entered valid credentials, the service authenticated the credentials.

The following figure and the corresponding step descriptions demonstrate what occurs after a previously authenticated user attempts to access a second protected resource through a browser. This figure depicts user profiles and policy stored together. Note that these data types are often stored separately.

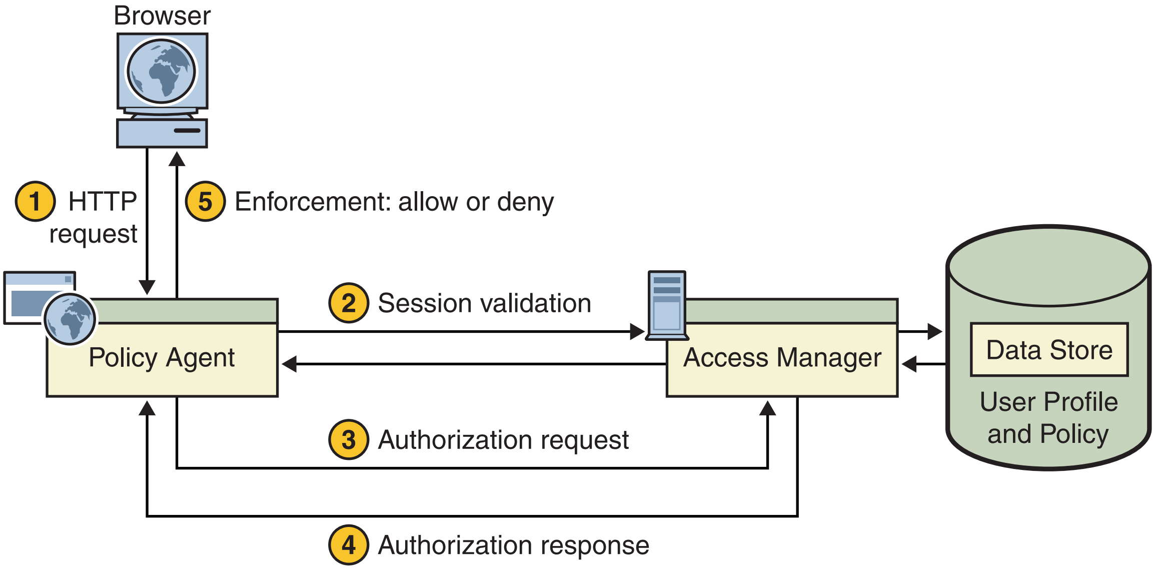

FIGURE 1–1 Policy Agent and the Policy Decision Process

1. The browser sends a request for the protected resource to the deployment container (such as a web or application server) protected by the agent.
2. The agent intercepts the request, checks for a session token embedded in a cookie, and validates the SSO token.

As explained in preceding text, this example assumes that the user's credentials have already been authenticated. Though an SSO session such as this often would *not* require Policy Agent and Access Manager to contact each other during session validation, such contact is sometimes necessary and, therefore, is depicted in Figure 1–1.

3. The agent sends a request to Access Manager Policy Service for user access to the protected resource.
4. Access Manager replies with the policy decision.
5. The agent interprets the policy decision and allows or denies access.

Web and J2EE Agents: Similarities and Differences

Both web agents and J2EE agents protect resources hosted on deployment containers (such as web and application servers) or enforce single sign-on with systems that use deployment containers as the front-end in an environment secured by Access Manager. The two types of agents are similar in some ways and yet different in others as outlined in this section.

Web Agents

Web agents control access to content on web servers and proxy servers. The content that web agents can protect include a multitude of services and web resources based on policies configured by an administrator. When a user points a browser to a URL deployed on a protected web or proxy server, the agent intercepts the request and validates the user’s session token, if any exists. If the token’s authentication level is insufficient (or none exists), the appropriate Authentication Service is called for a login page, prompting the user for (further) authentication. The Authentication Service verifies that the user credentials are valid. For example, the LDAP service verifies that the user name and password are stored in an LDAP v3 compliant directory server, such as Sun Java System Directory Server. After the user’s credentials are properly authenticated, the agent examines all the roles and groups (which contain the policies) assigned to the user. Based on the aggregate of all policies assigned to the user, the individual is either allowed or denied access to the URL.

J2EE Agents

Access Manager provides agents for protecting J2EE applications in a variety of deployment containers, such as application and portal servers.

A J2EE policy agent can be installed for protecting a variety of hosted J2EE applications, which might require a varying set of security policy implementation. The security infrastructure of J2EE provides declarative as well as programmatic security that are platform-independent and are supported by all the J2EE-compliant servers. For details on how to use J2EE platform declarative as well as programmatic security, refer to J2EE documentation at `http://java.sun.com/j2ee`.

The agent helps enable role-to-principal mapping for protected J2EE applications with Access Manager principals. Therefore, at runtime, when a J2EE policy is evaluated, the evaluation is against the information available in Access Manager. Using this functionality, you can configure hosted J2EE applications so that they are protected by the J2EE agent, which provides real security services and other key features such as single sign-on. Apart from enabling J2EE security for hosted applications, J2EE agents also provide complete support for Access Manager based URL policies for enforcing access control over web resources hosted in deployment containers, such as an application servers.

While web agents and J2EE agents both work with Access Manager to implement authentication and authorization processes, the design of the J2EE agents allows them to also enforce J2EE security. The J2EE agents are generally comprised of two components (although this is partially subject to the interfaces exposed and supported by the deployment container): an agent filter for authentication and an agent realm for authorization.

Agent Filter and Authentication

In J2EE agents, the agent filter component manages authentication. The agent filter is a servlet filter, which is supported starting with J2EE 1.3. The agent filter intercepts an inbound request to the server. It checks the request to see if it contains a session token. If one is available, the agent filter validates the token using the Access Manager Session Service. If no token is available, the browser is redirected to the Authentication Service as in a typical SSO exchange. Once the user credentials are authenticated, the request is directed back to the server where the agent filter once again intercepts it, and then validates the newly acquired token. After the user's credentials are validated, the filter enforces J2EE policies or fine-grained URL policies on the resource the user is trying to access. Through this mechanism, the agent filter ensures that only requests with a valid Access Manager token are allowed to access a protected application.

Agent Realm and Authorization

In J2EE agents, the agent realm component manages authorization. A *realm* is a means for a J2EE-compliant application server to provide information about users, groups, and access control to applications deployed on it. It is a scope over which security policy is defined and enforced.

The server is configured to use a specific realm for validation of users and their roles, when attempts are made to access resources. By default, many application servers ship with a number of realm implementations, including the default File Based as well as LDAP, NT, UNIX, and Relational Database Management System (RDBMS). The agent realm component implements the server’s realm interface, and allows user and role information to be managed by the Access Manager deployment. The agent realm component makes it possible to provide granular role-based authorization of J2EE resources to users who have been authenticated by the agent filter component.

Key Similarities of the Two Agent Types

The section "Example of Policy Decision Process" on page 14 describes a deployment that emphasizes the similar tasks performed by web agents and J2EE agents. The two agent types share various other features and tasks that are *not* described in that section. Though this section describes similarities of the two agent types, the features and tasks that they have in common tend to have some differences. However, those differences are often subtle. The details about agent features and tasks are not provided in this guide. For details about the features and tasks for each agent type (web agent or J2EE agent), see any of the individual agent guides for that agent type: see Chapter 2 for information about the individual web agent guides and see Chapter 3 for information about the individual J2EE agent guides. A list of key features and tasks that web agents and J2EE agents have in common follows along with an explanation of each item:

- "Configuration Properties" on page 18
- "Policy Agent Log Files" on page 18
- "Not-Enforced Lists" on page 18
- "Personal Profile Attributes and Session Attributes" on page 19

Configuration Properties

Both agent types use a single text file named `AMAgent.properties` to configure agent properties. Agent configuration is controlled to a great extent by the properties in this file.

The configuration properties file used for web agents is very similar to the configuration properties file used for J2EE agents. The biggest difference between the two files is that the `AMAgent.properties` file for J2EE agents has extra constructs such as map constructs and list constructs. Configuration properties that are present in the `AMAgent.properties` files for both agent types tend to be very similar in terms of functionality.

Policy Agent Log Files

Web agents and J2EE agents can log access information and diagnostic information to an agent log file. Each agent has its own log file, a flat file located on the same host system as the agent. The log file size is configurable. When the active log file reaches the size limit, the log is rotated, which means that the older log information is moved and stored in another log file.

Furthermore, both agent types are capable of logging access information to an Access Manager log file or database table.

Not-Enforced Lists

Both agent types support not-enforced lists. These lists allow for the regular authentication and authorization processes to be bypassed. These lists are set in the `AMAgent.properties` file. Two types of not-enforced lists exist: a not-enforced URL list and a not-enforced IP Address list.

A not-enforced URL list is a list of URLs that are not protected by an agent. A resource represented by a URL on a not-enforced URL list is widely available, without restrictions. This list can be set to have a reverse meaning. With a reverse meaning, only URLs on the list are protected. All other URLs are not protected.

A not-enforced IP Address list is a list of IP addresses that are automatically allowed access to resources. When a user is using a computer that has an IP address on the not-enforced IP address list, that user is allowed access to all the resources protected by the respective agent.

Personal Profile Attributes and Session Attributes

Both agent types can fetch and pass along personal profile attributes and session attributes. Client applications protected by an agent can then use information from these attributes to personalize content for the user.

Key Differences Between the Two Agent Types

Many differences exist between J2EE agents and web agents in the way they perform tasks. However, the basic tasks they perform are similar. While the primary purpose of both types of agents is to enforce authentication and authorization before a user can access a protected resource, the two agent types differ in the kind of resources that they can protect and in the way they enforce such policy decisions.

Differences in Protected Resources

Web agents are capable of protecting resources that can be hosted on the web or proxy servers on which they are installed. This protection includes any resource that can be represented as a uniform resource identifier (URI) available on the protected server. Such a protected URI can be resolved by the server to static content files such as HTML files or dynamic content generation programs such as CGI scripts or servlets hosted by an embedded servlet engine. In other words, before a request is evaluated by the web or proxy server, the web agent can evaluate the necessary credentials of a user and can allow or deny access for the requested resource. Once the request is granted access to the resource, it can be processed internally by the web or proxy server as applicable. In other words, the web agent uses the request URL to enforce all policy decisions regardless of what that URL maps to internally in the web server. In cases where the request URL maps to a servlet which in turn invokes other servlets or JSPs, the web agent will not intercept these subsequent resource requests unless such invocation involves a client-side redirect.

A J2EE agent is capable of protecting web and enterprise applications hosted by the application or portal server on which it is installed. These applications may include resources such as HTML pages, servlets, JSP, and Enterprise JavaBeans (EJB). Apart from these resources, any resource that can be accessed as a URI within a protected web application can also be secured by such agents. For example, images that are packaged within a web application can also be protected by the J2EE Policy Agent. These agents allow the evaluation of J2EE policies and can also enforce Access Manager based URL policies like a web agent on the resources being requested by the user. Minimally the enforcement is done at the outermost requested URL, but can also be done on any intermediate URLs being chained to this resource on most application servers.

Default Scope of Protection

When installed, a web agent automatically protects the entire set of resources available on the web server. However, in order to protect resources within a web application hosted on an application server, the web application must be configured to use the J2EE agent. Thus if multiple web applications are hosted on an application server on which a J2EE agent has been installed, only the web applications that have been specifically configured to use the J2EE agent will be protected by the agent. Other applications will remain unprotected and can potentially malfunction if they depend upon any J2EE security mechanism.

Further, the J2EE agent can only protect resources that are packaged within a web or enterprise application. Certain application servers provide an embedded web server that can be used to host non-packaged web content such as HTML files and images. Such content cannot be protected by a J2EE agent unless it is redeployed as a part of a web application.

Modes of Operation

J2EE agents provide more modes of operation than do web agents. These modes are basically methods for evaluating and enforcing access to resources. You can set the mode according to your site's security requirements. For example, the SSO_ONLY mode is a relatively non-restrictive mode. This mode uses only Access Manager Authentication Service to authenticate users who attempt to access a protected resource.

Some of the modes such as SSO_ONLY and URL_POLICY are also achievable with web agents, whereas other modes of operation such as J2EE_POLICY and ALL modes do not apply to web agents.

For both J2EE agents and web agents, the modes are set in the `AMAgent.properties` file.

In the J2EE_POLICY and ALL modes of operation, J2EE agents enforce J2EE declarative policies as applicable for the protected application and also provide support for evaluation of programmatic security APIs available within J2EE specifications.

◆ ◆ ◆ CHAPTER 2

Access Manager Policy Agent 2.2 Web Agents: Compatibility, Supported Servers, and Documentation

This chapter consists of information about the compatibility of the web agents in Sun Java™ System Policy Agent 2.2 with Sun Java System Access Manager, the supported servers for each of the web agents currently available for Policy Agent 2.2, and the guide available for each web agent. For similar information about J2EE agents see Chapter 3.

Compatibility of Policy Agent 2.2 Web Agents with Access Manager

Web agents in the Policy Agent 2.2 release are compatible with versions of Sun Java System Access Manager as described in this section.

Compatibility of Web Agents With Access Manager 7

All agents in the Policy Agent 2.2 release are compatible with Access Manager 7. Compatibility applies to both of the available modes of Access Manager: Realm Mode and Legacy Mode.

Install the latest Access Manager 7 patches to ensure that all enhancements and fixes are applied. For information about the latest Access Manager 7 patches, see the compatibility information discussed in *Sun Java System Access Manager Policy Agent 2.2 Release Notes*.

Compatibility of Web Agents With Access Manager 6.3

All agents in Policy Agent 2.2 are also compatible with Access Manager 6.3 Patch 1 or greater. However, certain limitations apply. For more information, refer to the section on backward compatibility available in any of the individual web agent guides as listed in Table 2–1.

Supported Servers and Documentation of Web Agents in Policy Agent 2.2

The following table lists the deployment containers, such as web servers, currently supported by web agents in the Policy Agent 2.2 software set and the platforms supported by each agent. The table also lists the corresponding guide that describes each agent. Each individual web agent guide provides detailed information about features and tasks that all web agents have in common as well as providing detailed information about the specific web agent.

TABLE 2–1 Web Agent Platform Support and Documentation for Policy Agent 2.2

Agent for	Supported Access Manager Versions	Corresponding Web Agent Guide	Supported Platforms
Sun Java System Web Server 6.1	Version 6.3 Patch 1 or greater Version 7	*Sun Java System Access Manager Policy Agent 2.2 Guide for Sun Java System Web Server 6.1*	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
Apache HTTP Server 2.0.54 and Apache HTTP Server 1.3.33. **Note –** Also supports minor versions of the 2.0 and 1.3 Apache HTTP Server series when these minor versions do not introduce any interface changes on which the agent relies.	Version 6.3 Patch 1 or greater Version 7	*Sun Java System Access Manager Policy Agent 2.2 Guide for Apache HTTP Server 2.0.54*	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
Microsoft Internet Information Services 6.0 (Microsoft IIS 6.0)	Version 6.3 Patch 1 or greater Version 7	*Sun Java System Access Manager Policy Agent 2.2 Guide for Microsoft Internet Information Services 6.0*	Windows 2003, Enterprise Edition Windows 2003, Standard Edition

TABLE 2–1 Web Agent Platform Support and Documentation for Policy Agent 2.2 *(Continued)*

Agent for	Supported Access Manager Versions	Corresponding Web Agent Guide	Supported Platforms
IBM Lotus Domino 6.5.4	Version 6.3 Patch 1 or greater Version 7	*Sun Java System Access Manager Policy Agent 2.2 Guide for IBM Lotus Domino 6.5.4*	Solaris Operating System (OS) for the SPARC platform , versions 8, 9, and 10 Red Hat Enterprise Linux Advanced Server 3.0 Windows 2003, Enterprise Edition Windows 2003, Standard Edition
Sun Java System Web Proxy Server 4.0	Version 6.3 Patch 1 or greater Version 7	*Sun Java System Access Manager Policy Agent 2.2 Guide for Sun Java System Web Proxy Server 4.0*	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

◆ ◆ ◆ CHAPTER 3

Access Manager Policy Agent 2.2 J2EE Agents: Compatibility, Supported Servers, and Documentation

This chapter consists of information about the compatibility of the J2EE agents in Sun Java System Policy Agent 2.2 with Sun Java System Access Manager, the supported servers for each of the J2EE agents currently available for Policy Agent 2.2, and the guide available for each J2EE agent. For similar information about web agents see Chapter 2

Compatibility of Policy Agent 2.2 J2EE Agents with Access Manager

J2EE agents in the Policy Agent 2.2 release are compatible with versions of Sun Java System Access Manager as described in this section.

Compatibility of J2EE Agents With Access Manager 7

All agents in the Policy Agent 2.2 release are compatible with Access Manager 7. Compatibility applies to both of the available modes of Access Manager: Realm Mode and Legacy Mode.

Install the latest Access Manager 7 patches to ensure that all enhancements and fixes are applied. For information about the latest Access Manager 7 patches, see the compatibility information discussed in *Sun Java System Access Manager Policy Agent 2.2 Release Notes*.

Compatibility of J2EE Agents With Access Manager 6.3

All agents in Policy Agent 2.2 are also compatible with Access Manager 6.3 Patch 1 or greater. However, certain limitations apply. For more information, refer to the section on backward compatibility available in any of the individual J2EE agent guides as listed in Table 3–1.

Supported Servers and Documentation of J2EE Agents in Policy Agent 2.2

The following table lists the deployment containers, such as application servers, currently supported by J2EE agents in the Policy Agent 2.2 software set and the platforms supported by each agent. The table also lists the corresponding guide that describes each agent. Each individual J2EE agent guide provides detailed information about features and tasks that all J2EE agents have in common as well as providing detailed information about the specific J2EE agent.

TABLE 3–1 J2EE Agent Platform Support and Documentation for Policy Agent 2.2

Agent for	Supported Access Manager Versions	Corresponding J2EE Agent Guide	Supported Platforms
Sun Java™ System Application Server 8.1	Version 6.3 Patch 1 or greater Version 7	*Sun Java System Access Manager Policy Agent 2.2 Guide for Sun Java System Application Server 8.1*	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 6.3 Patch 1 or greater Version 7	*Sun Java System Access Manager Policy Agent 2.2 Guide for BEA WebLogic Server/Portal 8.1 SP4*	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 3–1 J2EE Agent Platform Support and Documentation for Policy Agent 2.2 *(Continued)*

Agent for	Supported Access Manager Versions	Corresponding J2EE Agent Guide	Supported Platforms
Apache Tomcat 5.5 Servlet/JSP Container (also supports Apache Tomcat 5.0.28 Servlet/JSP Container)	Version 6.3 Patch 1 or greater Version 7	*Sun Java System Access Manager Policy Agent 2.2 Guide for Apache Tomcat 5.5 Servlet/JSP Container*	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 6.3 Patch 1 or greater Version 7	*Sun Java System Access Manager Policy Agent 2.2 Guide for IBM WebSphere Application Server 5.1.1*	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
IBM WebSphere Application Server 6.0	Version 6.3 Patch 1 or greater Version 7	*Sun Java System Access Manager Policy Agent 2.2 Guide for IBM WebSphere Application Server 6.0*	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 3–1 J2EE Agent Platform Support and Documentation for Policy Agent 2.2 *(Continued)*

Agent for	Supported Access Manager Versions	Corresponding J2EE Agent Guide	Supported Platforms
SAP Enterprise Portal 6.0 and Web Application Server 6.40 (SAP Portal 6.0/Server 6.40)	Version 6.3 Patch 1 or greater Version 7	*Sun Java System Access Manager Policy Agent 2.2 Guide for SAP Enterprise Portal 6.0 and Web Application Server 6.40*	Solaris Operating System (OS) for the SPARC platform, versions 8, 9, and 10 Windows 2003, Enterprise Edition Windows 2003, Standard Edition
IBM WebSphere Portal Server 5.1.0.2 deployed on: ■ IBM WebSphere Application Server 5.1.1.7 ■ IBM WebSphere Business Integration-Server Foundation 5.1.1	Version 6.3 Patch 1 or greater Version 7	*Sun Java System Access Manager Policy Agent 2.2 Guide for IBM WebSphere Portal Server 5.1.0.2*	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 6.3 Patch 1 or greater Version 7	*Sun Java System Access Manager Policy Agent 2.2 Guide for BEA WebLogic Server 9.0/9.1*	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
Oracle Application Server 10g, which includes the following versions: ■ The 10.1.2 series. ■ The 10.1.3 series.	Version 6.3 Patch 1 or greater Version 7	*Sun Java System Access Manager Policy Agent 2.2 Guide for Oracle Application Server 10g*	Solaris Operating System (OS) for the SPARC platform, versions 8, 9, and 10 Red Hat Enterprise Linux Advanced Server 3.0 Windows 2003, Enterprise Edition Windows 2003, Standard Edition

TABLE 3–1 J2EE Agent Platform Support and Documentation for Policy Agent 2.2 *(Continued)*

Agent for	Supported Access Manager Versions	Corresponding J2EE Agent Guide	Supported Platforms
BEA WebLogic Server/Portal 9.2 (also supports BEA WebLogic Express 9.2)	Version 6.3 Patch 1 or greater Version 7	*Sun Java System Access Manager Policy Agent 2.2 Guide for BEA WebLogic Server/Portal 9.2*	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

Index