



Technical Note: Using Access Manager Distributed Authentication



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

Part No: 819-4566-11

Copyright 2005 Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 U.S.A. All rights reserved.

Sun Microsystems, Inc. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more U.S. patents or pending patent applications in the U.S. and in other countries.

U.S. Government Rights – Commercial software. Government users are subject to the Sun Microsystems, Inc. standard license agreement and applicable provisions of the FAR and its supplements.

This distribution may include materials developed by third parties.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California. UNIX is a registered trademark in the U.S. and other countries, exclusively licensed through X/Open Company, Ltd.

Sun, Sun Microsystems, the Sun logo, the Solaris logo, the Java Coffee Cup logo, docs.sun.com, Java, and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

The OPEN LOOK and Sun™ Graphical User Interface was developed by Sun Microsystems, Inc. for its users and licensees. Sun acknowledges the pioneering efforts of Xerox in researching and developing the concept of visual or graphical user interfaces for the computer industry. Sun holds a non-exclusive license from Xerox to the Xerox Graphical User Interface, which license also covers Sun's licensees who implement OPEN LOOK GUIs and otherwise comply with Sun's written license agreements.

Products covered by and information contained in this publication are controlled by U.S. Export Control laws and may be subject to the export or import laws in other countries. Nuclear, missile, chemical or biological weapons or nuclear maritime end uses or end users, whether direct or indirect, are strictly prohibited. Export or reexport to countries subject to U.S. embargo or to entities identified on U.S. export exclusion lists, including, but not limited to, the denied persons and specially designated nationals lists is strictly prohibited.

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.

Copyright 2005 Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 U.S.A. Tous droits réservés.

Sun Microsystems, Inc. détient les droits de propriété intellectuelle relatifs à la technologie incorporée dans le produit qui est décrit dans ce document. En particulier, et ce sans limitation, ces droits de propriété intellectuelle peuvent inclure un ou plusieurs brevets américains ou des applications de brevet en attente aux Etats-Unis et dans d'autres pays.

Cette distribution peut comprendre des composants développés par des tierces personnes.

Certains composants de ce produit peuvent être dérivées du logiciel Berkeley BSD, licenciés par l'Université de Californie. UNIX est une marque déposée aux Etats-Unis et dans d'autres pays; elle est licenciée exclusivement par X/Open Company, Ltd.

Sun, Sun Microsystems, le logo Sun, le logo Solaris, le logo Java Coffee Cup, docs.sun.com, Java et Solaris sont des marques de fabrique ou des marques déposées de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays. Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux Etats-Unis et dans d'autres pays. Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc.

L'interface d'utilisation graphique OPEN LOOK et Sun a été développée par Sun Microsystems, Inc. pour ses utilisateurs et licenciés. Sun reconnaît les efforts de pionniers de Xerox pour la recherche et le développement du concept des interfaces d'utilisation visuelle ou graphique pour l'industrie de l'informatique. Sun détient une licence non exclusive de Xerox sur l'interface d'utilisation graphique Xerox, cette licence couvrant également les licenciés de Sun qui mettent en place l'interface d'utilisation graphique OPEN LOOK et qui, en outre, se conforment aux licences écrites de Sun.

Les produits qui font l'objet de cette publication et les informations qu'il contient sont régis par la législation américaine en matière de contrôle des exportations et peuvent être soumis au droit d'autres pays dans le domaine des exportations et importations. Les utilisations finales, ou utilisateurs finaux, pour des armes nucléaires, des missiles, des armes chimiques ou biologiques ou pour le nucléaire maritime, directement ou indirectement, sont strictement interdites. Les exportations ou réexportations vers des pays sous embargo des Etats-Unis, ou vers des entités figurant sur les listes d'exclusion d'exportation américaines, y compris, mais de manière non exclusive, la liste de personnes qui font objet d'un ordre de ne pas participer, d'une façon directe ou indirecte, aux exportations des produits ou des services qui sont régis par la législation américaine en matière de contrôle des exportations et la liste de ressortissants spécifiquement désignés, sont rigoureusement interdites.

LA DOCUMENTATION EST FOURNIE "EN L'ETAT" ET TOUTES AUTRES CONDITIONS, DECLARATIONS ET GARANTIES EXPRESSES OU TACITES SONT FORMELLEMENT EXCLUES, DANS LA MESURE AUTORISEE PAR LA LOI APPLICABLE, Y COMPRIS NOTAMMENT TOUTE GARANTIE IMPLICITE RELATIVE A LA QUALITE MARCHANDE, A L'APTITUDE A UNE UTILISATION PARTICULIERE OU A L'ABSENCE DE CONTREFACON.

Sun Java™ System Access Manager 7 2005Q4

Technical Note: Using Access Manager

Distributed Authentication

This document contains the following sections:

- “Revision History” on page 4
- “Overview” on page 4
- “Installing and Customizing the Distributed Authentication Interface” on page 6
- “Building the Distributed Authentication Web Application” on page 7
- “Initializing the Distributed Authentication Web Application” on page 8
- “Accessing the Distributed Authentication User Interface” on page 9
- “Accessing Sun Resources Online” on page 9

Revision History

Release Date	Description of Changes
Oct. 19, 2005	Initial publication of this technical note.
Nov. 14, 2005	Added distributed authentication package information to the Building the Distributed Authentication Web Application section.
Feb. 5, 2006	Updated with fixes and maintenance.

Overview

In order for authentication to occur, Access Manager must be able to send HTTP or HTTPS packets with the authentication interface directly to the web browser. This deployment architecture requires opening holes in any firewalls between the end user and Access Manager.

In order to do this securely, Access Manager 7 supports a distributed authentication user interface web application. With distributed authentication, an additional server provides the authentication UI web application. The authentication UI servers exist solely for the purpose of serving up the authentication interface to web browsers. They let users eliminate the need for opening holes in firewalls between the end user and Access Manager. The following figure outlines the components and runtime flow of a basic distributed authentication deployment scenario.

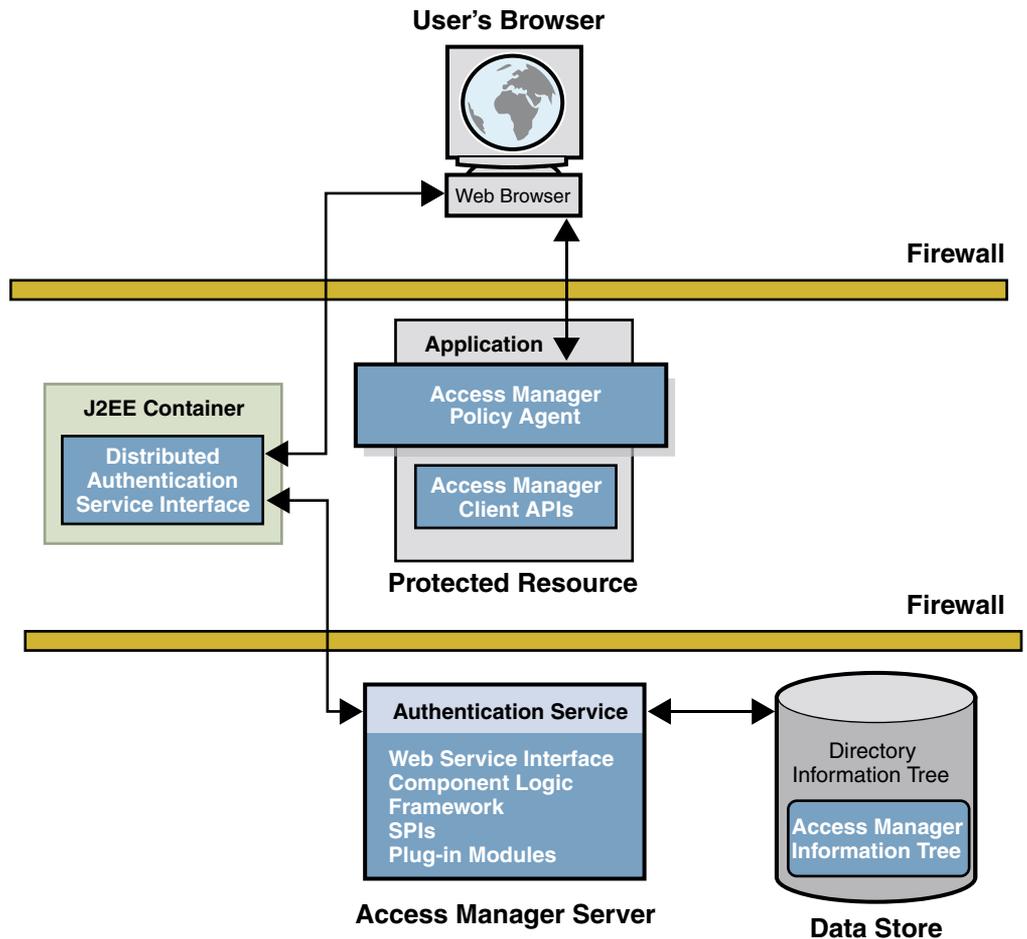


FIGURE 1 Distributed Authentication Overview

The Distributed Authentication UI service has the following dependencies:

- The SUNWamclnt (Access Manager Client SDK package) is installed.
- The SUNWjato (JATO package) is installed.
- Access Manager Server is available (remotely).
- The Client SDK will be able to communicate with Access Manager Server using http(s).

The Certificate, HTTP Basic, and MSISDN authentication modules are not supported through the distributed authentication interface.

The following service flow outlines how distributed authentication works in a typical scenario:

1. The web browser makes a request to the resource protected by a policy agent.
2. If there is no cookie containing an SSO token, the policy agent issues a redirect to its authentication URL. With the distributed authentication interface, the authentication URL is the URL of the distributed authentication service.
3. The browser follows the redirect and makes a request
4. The distributed authentication service recognizes the inbound request. Using the parameters in the request, it communicates with the authentication server (Access Manager) on the back end to determine the appropriate authentication instance, and gets the necessary callbacks to use in the presentation framework/layer. It also determines which presentation to use.
5. The distributed authentication service, using the information from the server, returns a presentation extraction page back to the web browser with the appropriate callbacks info from the server.
6. The browser replies with the credentials in a POST operation.
7. The distributed authentication service gets the credentials and passes them to Access Manager.
8. Access Manager authenticates using the appropriate authentication instance. If successful, it passes back the SSOToken, or it passes back the appropriate error information.
9. If successful, the distributed authentication service, replies with a 302 redirect back to the originally requested resource, which includes the SSOToken in a set-cookie header.

Installing and Customizing the Distributed Authentication Interface

You can install the remote authentication user interface component on any servlet-compliant web container within the non-secure layer of an Access Manager deployment. The remote component works with Authentication client APIs and authentication utility classes to authenticate web users. The remote component is customizable and uses a JATO presentation framework.

If you are deploying multiple Distributed Authentication servers behind a load balancer, stickiness is not required for the load balancer to talk to only one Distributed Authentication server for authentication process completion.

Supported JDK Versions

Supported JDK versions are J2SE 1.4.1, or higher. In order to run using JDK 1.3.1, the following additional jar files would be needed in the CLASSPATH:

- Java Authentication and Authorization Service (JAAS) located at <http://java.sun.com/products/jaas/>
- Java Secure Socket Extension (JSSE) for SSL located at <http://java.sun.com/products/jsse/>
- JDK Logging (jdk_logging.jar). Can be obtained from SUNWamsdk package for Solaris and sun-identity-sdk RPM for Linux

Building the Distributed Authentication Web Application

The JES 4 Installation Utility installs the distributed authentication package in the *AccessManager-base/SUNWcomm/SUNWam*, however in order for distributed authentication to function properly, the packages must be located in *AccessManager-base/SUNWam*. Copy the following files to the *AccessManager-base/SUNWam* directory and proceed with the steps described in this document:

<code>README.distAuthUI</code>	Contains installation and package instructions.
<code>amauthdistui.war</code>	The distributed authentication Web application.
<code>Makefile.distAuthUI</code>	The <code>Makefile.distAuthUI</code> is used to generate and build required web application. The makefile defines targets to build configuration properties and web application and jars

▼ To Build the Distributed Authentication Web Application

1 Edit the `Makefile.distAuthUI` to provide the following required parameters:

- `JAVA_HOME`
- `SERVER_PROTOCOL`
- `SERVER_HOSTNAME`
- `SERVER_PORT`
- `SERVER_DEPLOY_URI`
- `APPLICATION_USERNAME`
- `APPLICATION_PASSWORD`
- `DISTAUTH_DEPLOY_URI`
- `DISTAUTH_PROTOCOL`
- `DISTAUTH_HOSTNAME`
- `DISTAUTH_PORT`

2 Enter the following command to run the makefile:

```
make -f Makefile.distAuthUI
```

This command generates a deployable war file (`amauthdistui_deploy.war`) that can be deployed in any Servlet 2.3 compliant container. The targets defined in the `Makefile.distAuthUI` are:

<code>properties</code>	Generates <code>AMConfig.properties</code> in the temporary directory. This file is used as a template for setting Access Manager Distributed Authentication Web Application's properties
<code>webapp</code>	Generates <code>amauthdistui_deploy.war</code> that can be deployed on any Servlet 2.3-compliant web container

Initializing the Distributed Authentication Web Application

In order for the Access Manager Client SDK to communicate with Access Manager Server, you must initialize several properties. These properties can be set in one of the following methods:

1. Through the properties file – Set the properties in a file and provide a path to it at runtime using the `-Damconfig=filename` command. The properties files should be in the CLASSPATH. The default properties file name is `AMConfig.properties` and is always read at start-up. A sample `AMConfig.properties` can be generated using the `make -f Makefile.distAuthUI properties` command. The `AMConfig.properties` will be present in the `/temp` directory.

2. Through the Java API —

```
com.iplanet.am.util.SystemProperties.initializeProperties
```

(where the `java.util.Properties` file contains the properties).

3. Individual properties can be set at runtime using the `-D` flag. For example, `-DpropertyName=propertyValue`.

The properties expected by Distributed Authentication web application are:

Naming URL property	<code>com.iplanet.am.naming.url</code> and <code>com.iplanet.am.naming.failover.url</code> . This is a mandatory property and it specifies the Access Manager Server's Naming URL. For example: <code>com.iplanet.am.naming.url=http://is.example.com/amserver/namingservice</code>
Debug Level and Directory	The <code>com.iplanet.services.debug.level</code> and <code>com.iplanet.services.debug.directoryproperties</code> specify the debug level and directory. The possible values for debug levels are <code>off</code> , <code>error</code> , <code>warning</code> , and <code>message</code> .
Notification URL property:	The web application can register for changes to server attributes. The <code>com.iplanet.am.notification.url</code> property must be set to receive such notifications.

Security Properties

Some of the Access Manager components such as Service Management, User Management, and so forth, require an identity for the client (application) to read configuration data and to identify the client. The identity for the client can be set up by providing either a username and password that can be authenticated, or by providing an implementation for the interface `com.sun.identity.security.AppSSOTokenProvider` that returns a single-sign-on (SSO) token.

1. The properties to set the username, password and shared secret are:

```
com.sun.identity.agents.app.username
```

```
com.iplanet.am.service.password
```

```
com.iplanet.am.service.secret
```

2. The property to set the SSO Token provider:

```
com.sun.identity.security.AdminToken
```

3. Some of the configuration attributes (such as password) are encrypted and stored in the data store. If such attributes have to be decrypted by the client, the following property must be set, and must be the same as that of the Access Manager Server:

```
am.encryption.pwd
```

Accessing the Distributed Authentication User Interface

Once you have the distributed authentication deployed and configured, you can access it by entering the following access URL syntax into your browser:

```
http://dist_auth_server_host.dist_auth_server_domain:  
dist_auth_server_port/DISTAUTH_DEPLOY_URI/UI/Login
```

This URL should always be an absolute URL, ideally would be used as *goto=absolute successful redirect URL* query parameter with the above Access URL since this web application would be normally deployed in a DMZ layer in production.

For testing purpose, if you happen to use the server's returned default successful redirect URL (the server's Administration Console URL), make sure that you change the URL from its relative value (*SERVER_DEPLOY_URI/console*) to the absolute value in the authentication properties in the Administration Console. For example:

```
SERVER_PROTOCOL://SERVER_HOSTNAME:  
SERVER_PORT/SERVER_DEPLOY_URI/console
```

Accessing Sun Resources Online

The docs.sun.comSM web site enables you to access Sun technical documentation online. You can browse the docs.sun.com archive or search for a specific book title or subject. Books are available as online files in PDF and HTML formats. Both formats are readable by assistive technologies for users with disabilities.

To access the following Sun resources, go to <http://www.sun.com>:

- Downloads of Sun products
- Services and solutions
- Support (including patches and updates)
- Training
- Research

- Communities (for example, Sun Developer Network)

Third-Party Web Site References

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

Note – 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 full document title and part number. The part number is a 7-digit or 9-digit number that can be found on the book's title page or in the document's URL. For example, the part number of this book is 819-4566-11.