



Technical Note: Host Name Changes in a Sun Java System Access Manager 7.1 WAR Deployment



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

Part No: 820-4196-10
January 2008

Copyright 2008 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 2008 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 États-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 États-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 États-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 États-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 États-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.

Contents

Technical Note: Host Name Changes in a Sun Java™ System Access Manager 7.1 WAR Deployment	5
Software Requirements	5
Changing the Host Machine Name or Domain in an Access Manager Deployment	5
▼ To Change the Host Machine Name in an Access Manager Deployment	6
▼ To Change the Domain in an Access Manager Deployment	8
▼ To Change the Host Machine Name or Domain in the Access Manager Configuration Data Store	9
▼ To Change the Host Machine Name or Domain in the Access Manager Session Data Store	9
▼ To Change the Host Machine Name or Domain in the Access Manager Authentication Data Store	10
▼ To Change the Host Machine Name or Domain in the Access Manager User Data Store ..	10
▼ To Change the Host Machine Name or Domain in the Access Manager Policy Data Store	11
Changing the Host Machine Name or Domain in Access Manager Deployed in a Federation Environment	11
▼ To Make Changes for SAML v2	12
▼ To Make Changes for the Liberty Alliance Project Identity Federation Framework	13
▼ To Make Changes for SAML v1	15

Technical Note: Host Name Changes in a Sun Java™ System Access Manager 7.1 WAR Deployment

Technical Note: Host Name Changes in a Sun Java™ System Access Manager 7.1 WAR Deployment describes the configuration changes that need to be made to an Access Manager system when there are changes to host or domain names of the core servers.

It contains the following sections:

- [“Software Requirements” on page 5](#)
- [“Changing the Host Machine Name or Domain in an Access Manager Deployment” on page 5](#)
- [“Changing the Host Machine Name or Domain in Access Manager Deployed in a Federation Environment” on page 11](#)

Software Requirements

This document is relevant only when using the software specified below as the mechanism for making changes or the properties to be changed may be different between versions of the software.

- Sun Java System Access Manager 7.1 (WAR Download Only)
- Sun Java System Web Server 7.0
- Sun Java System Directory Server 6.0

Changing the Host Machine Name or Domain in an Access Manager Deployment

The following procedures explain the modifications you need to make to an Access Manager configuration when the host machine name or domain changes.

- [“To Change the Host Machine Name in an Access Manager Deployment” on page 6](#)

- “To Change the Domain in an Access Manager Deployment” on page 8
- “To Change the Host Machine Name or Domain in the Access Manager Configuration Data Store” on page 9
- “To Change the Host Machine Name or Domain in the Access Manager Session Data Store” on page 9
- “To Change the Host Machine Name or Domain in the Access Manager Authentication Data Store” on page 10
- “To Change the Host Machine Name or Domain in the Access Manager User Data Store” on page 10
- “To Change the Host Machine Name or Domain in the Access Manager Policy Data Store” on page 11

▼ To Change the Host Machine Name in an Access Manager Deployment

The following procedure explains what you need to modify in an Access Manager deployment when the name of the machine on which Access Manager is hosted changes.

1 Stop Access Manager.

2 Delete the bootstrap file.

```
# rm user_home/AccessManager/*
```

where *user_home* is the home directory of the UNIX user under which the Access Manager web container is running.

3 Copy the value of the `am. encryption. pwd` property from `AMConfig.properties`.

```
am. encryption. pwd=eza2p5sYo+19hlzeZPynfOk+g89JUuRS
```

4 Delete the sample identities created by the Identity Repository Service when Access Manager is deployed.

By default, *context-root* is `amserver`.

a. Change to the `agent` directory.

```
# cd AM-Config-Dir/context-root/idRepo/agent/
```

b. Remove the following.

```
# rm LibertyBearerTokenWSP LibertySAMLTokenWSP  
LibertyX509TokenWSP LocalDiscoDiscovery SAML-HolderOfKeyWSP  
SAML-SenderVouchesWSP UserNameTokenWSP wscWSC wspWSP X509TokenWSP
```

c. Change to the `realm` directory.

```
cd AM-Config-Dir/context-root/idRepo/realm/
```

d. Remove the following.

```
# rm ContainerDefaultTemplateRole
```

e. Change to the user directory.

```
cd AM-Config-Dir/context-root/idRepo/user/
```

f. Remove the following.

```
# rm jondoe jsmith
```

5 Start Access Manager.

6 Using a browser, go to the Access Manager URL using the new host machine name:

```
http://new_FQDN_AM_host:port/amserver.
```

You will be redirected to the Access Manager configuration page. After redirection, verify that the URL in the Location bar reflects the new host name.

7 Fill in the details on the configuration page displayed.

Be sure of the following:

- Verify that the value of the Server URL correctly reflects the new host name.
- Paste the encryption password you previously copied as the value of the Encryption Key.

8 Click Configure to submit the form.

A message confirming a successful configuration will be displayed and you will be redirected to the Access Manager console to login.

9 Login to the Access Manager console as amadmin.

If configuration has failed or you are unable to login, troubleshoot the issue by looking at the logs from the web container that hosts Access Manager and the debug logs from Access Manager itself.

10 Make the following changes to the Access Manager Platform Service.

a. Click the Configuration tab.

b. Click System Properties.

c. Click Platform.

d. Delete the Instance Name entry referring to the old host name.

e. Update the Site Name to include the instance-ID pertaining to the new host name.

- f. Click **Save** to save the changes.
- 11 Make the following changes to the top-level realm.
 - a. From the console home page, click the **Access Control** tab.
 - b. Click the name of the top-level realm.
 - c. Click **Realm Attributes**.
 - d. Under **Realm/DNS Aliases**, delete the entry referring to the old host name.
 - e. Click **Save** to save the changes.
- 12 Follow the instructions in [“To Change the Domain in an Access Manager Deployment” on page 8](#), if applicable.
- 13 Log out of the Access Manager console.

▼ **To Change the Domain in an Access Manager Deployment**

The following procedure explains what you need to modify in an Access Manager deployment when the domain in which the machine on which Access Manager is hosted changes.

- 1 **Login to the Access Manager console** as `amadmin`.
- 2 **Click the Configuration tab.**
- 3 **Click System Properties.**
- 4 **Click Platform.**
- 5 **Add the new Access Manager domain name as a new value to the Cookie Domains attribute.**
- 6 **Click Save** to save the changes.
- 7 Follow the instructions in [“To Change the Host Machine Name in an Access Manager Deployment” on page 6](#), if applicable.
- 8 **Log out of the Access Manager console.**

▼ To Change the Host Machine Name or Domain in the Access Manager Configuration Data Store

The following procedure explains what you need to modify in the Access Manager configuration data store when the host machine name or domain in which the machine on which Access Manager is hosted changes.

- 1 To change the host machine name in the configuration data store, follow steps 1 through 7 in [“To Change the Host Machine Name in an Access Manager Deployment” on page 6](#).
- 2 Enter the domain in which the configuration data store is installed as the value in the Directory Server Settings field on the new Access Manager configuration page.
- 3 Click **Configure** to submit the form.

A message confirming a successful configuration will be displayed and you will be redirected to the Access Manager console to login.

▼ To Change the Host Machine Name or Domain in the Access Manager Session Data Store

Sun Java System Message Queue is used by Access Manager to implement session failover. Part of the installation process includes installing the Berkeley DB as a session data store. The following procedure explains what you need to modify in this session data store when the host machine name or domain in which the machine on which Access Manager is hosted changes.

- 1 Login to the Access Manager console as `amadmin`.
- 2 Click the **Configuration** tab.
- 3 Click **Global Properties**.
- 4 Click **Session**.
- 5 Change the host name of the session data store under **Secondary Configuration Instance**.
- 6 Click **Save** to save the changes.
- 7 Log out of the Access Manager console.

▼ **To Change the Host Machine Name or Domain in the Access Manager Authentication Data Store**

The following procedure explains what you need to modify in a configured Access Manager authentication data store when the host machine name or domain in which the machine on which Access Manager is hosted changes.

- 1 **Login to the Access Manager console as `amadmin`.**
- 2 **Click the Access Control tab.**
- 3 **Click the name of the top-level realm.**
- 4 **Click Authentication.**
- 5 **Click Module Instances.**
- 6 **Click the name of the relevant instance(s) and make the appropriate changes to the configured host machine name and domain.**
- 7 **Click Save to save the changes.**
- 8 **Log out of the Access Manager console.**

▼ **To Change the Host Machine Name or Domain in the Access Manager User Data Store**

- 1 **Login to the Access Manager console as `amadmin`.**
- 2 **Click the Access Control tab.**
- 3 **Click the name of the top-level realm.**
- 4 **Click Data Stores.**
- 5 **Click the name of the relevant data store(s) and make the appropriate changes to the configured host machine name and domain.**
- 6 **Click Save to save the changes.**
- 7 **Log out of the Access Manager console.**

▼ To Change the Host Machine Name or Domain in the Access Manager Policy Data Store

- 1 Login to the Access Manager console as `amadmin`.
- 2 Click the Access Control tab.
- 3 Click the name of the top-level realm.
- 4 Click Services.
- 5 Click Policy Configuration.
- 6 Make changes to the host machine name and domain configured in the appropriate attributes.
- 7 Click Save to save the changes.
- 8 Log out of the Access Manager console.

Changing the Host Machine Name or Domain in Access Manager Deployed in a Federation Environment

If the host machine name or domain is configured in an instance of Access Manager that acts as an identity provider or service provider in a federation environment, the following changes also need to be made, depending upon the federation protocol used.

- [“To Make Changes for SAML v2” on page 12](#)
- [“To Make Changes for the Liberty Alliance Project Identity Federation Framework” on page 13](#)
- [“To Make Changes for SAML v1” on page 15](#)

You only need to change the hosted or remote entities that contain a host machine name or domain that has changed. For example, if the host name of machine A has changed, you need to change the metadata for all entities hosted on machine A. If the metadata for those entities hosted on machine A was imported to machine B, you also need to change the remote metadata (for A) on machine B.

Tip – By default, `saml2meta`, the command line utility used in this section, uses the top-level realm as input when the `--realm` option is not defined. If you are making changes to a sub-realm, use the `--realm` option with a value of `/sub-realm-name`.

▼ To Make Changes for SAML v2

If the host machine name or domain is configured in an instance of Access Manager that acts as an identity provider or service provider in a SAML v2 environment, use this procedure. As Access Manager has no console support for SAML v2, changes to the URLs configured in the metadata files need to be made on the command-line on both the identity provider and the service provider sides.

- 1 **Run the following command to export the standard and extended metadata from the identity provider machine.**

```
# /opt/SUNWam/saml2/bin/saml2meta export
--runasdn amadmin --password passwd-for-amadmin
--realm realm-name --entityid "IDP-OLD-FQDN"
--metadata /tmp/metadata.xml --extended /tmp/ext_metadata.xml
```

Tip – If you receive the following exception:

```
com.ipplanet.sso.SSOException: Invalid sessionid
formatjava.lang.IllegalArgumentException:
Invalid server id in session id com.ipplanet.services.naming.
ServerEntryNotFoundException: Cannot find server.
at com.ipplanet.sso.providers.dpro.SSOProviderImpl.
createSSOToken(SSOProviderImpl.java:177)
at com.ipplanet.sso.SSOTokenManager.createSSOToken(SSOTokenManager.java:305)
at com.sun.identity.authentication.AuthContext.getSSOToken(AuthContext.java:1070)
```

append the following line to `AMConfig.properties`, restart Access Manager, and run the `saml2meta export` again.

```
com.ipplanet.am.naming.ignoreNamingService=true
```

- 2 **Run the following command to delete the standard and extended metadata just exported from the identity provider machine.**

```
# /opt/SUNWam/saml2/bin/saml2meta delete
--runasdn amadmin --password passwd-for-amadmin
--realm realm-name --entityid "IDP-OLD-FQDN"
```

Descriptor and config for entity "IDP-OLD-FQDN" was deleted successfully.

- 3 **Change all occurrences of "IDP-OLD-FQDN" to "IDP-NEW-FQDN" in the exported files, /tmp/metadata.xml and /tmp/ext_metadata.xml.**
- 4 **Run the following command to import the modified metadata files to the identity provider.**

```
# /opt/SUNWam/saml2/bin/saml2meta import
--runasdn amadmin --password passwd-for-amadmin
```

```
--realm realm-name --entityid "IDP-OLD-FQDN"
--metadata /tmp/metadata.xml --extended /tmp/ext_metadata.xml
```

File "/tmp/metadata.xml" was imported successfully.

File "/tmp/ext_metadata.xml" was imported successfully.

5 Run the following command to export the standard and extended metadata from the service provider machine.

```
# /opt/SUNWam/saml2/bin/saml2meta -i /var/opt/SUNWam/fm/war_staging export
--runasdn amadmin --password passwd-for-amadmin
--entityid "IDP-OLD-FQDN"
--metadata /tmp/metadata.xml --extended /tmp/ext_metadata.xml
```

Entity descriptor was exported to file "/tmp/metadata.xml" successfully.

Entity config was exported to file "/tmp/ext_metadata.xml" successfully.

6 Run the following command to delete the standard and extended metadata from the service provider machine.

```
# /opt/SUNWam/saml2/bin/saml2meta -i /var/opt/SUNWam/fm/war_staging delete
--runasdn amadmin --password passwd-for-amadmin
--entityid "IDP-OLD-FQDN"
```

Descriptor and config for entity "IDP-OLD-FQDN" was deleted successfully.

7 Change all occurrences of "IDP-OLD-FQDN" to "IDP-NEW-FQDN" in the files exported from the service provider machine, /tmp/metadata.xml and /tmp/ext_metadata.xml.

8 Run the following command to import the modified metadata files to the service provider.

```
# /opt/SUNWam/saml2/bin/saml2meta -i /var/opt/SUNWam/fm/war_staging import
--runasdn amadmin --password passwd-for-amadmin
--metadata /tmp/metadata.xml --extended /tmp/ext_metadata.xml
```

File "/tmp/metadata.xml" was imported successfully.

File "/tmp/ext_metadata.xml" was imported successfully.

▼ To Make Changes for the Liberty Alliance Project Identity Federation Framework

If the host machine name or domain is configured in an instance of Access Manager that acts as an identity provider or service provider in a Liberty Alliance Project Identity Federation Framework (Liberty ID-FF) environment, use this procedure to make changes to the following:

- Entity descriptors on the identity provider and service provider sides
- Discovery Service

- Liberty Personal Profile Service on the Access Manager system where the Discovery Service is hosted
- 1 Login to the Access Manager console as amadmin.**
 - 2 Change the entity descriptor files.**
 - a. Click the Federation tab.
 - b. Click the Entities tab.
 - c. Change the host machine name in the appropriate General, Identity Provider and Service Provider attributes for entries in the Entities table.
 - d. Click Save to save the changes.
 - 3 Make changes to the Discovery Service.**
 - a. From the Access Manager console home page, click the Web Services tab.
 - b. Click Discovery Service.
 - c. Change the host name in the Provider ID URL.
 - d. Click the Provider ID under Classes for ResourceID Mapper Plug-in.
 - e. Change the host machine name in the Provider ID attribute and click Save.
 - f. Click the configured Service Type entry name under Resource Offerings for Bootstrapping.
 - g. Change the host machine name in the Provider ID attribute and click Save.
 - h. Click Edit for the entry under Service Description.
 - i. Change the host machine name in the value of the End Point URL attribute.
 - j. Click Save to save the changes.
 - 4 Make changes to the Liberty Personal Profile Service.**
 - a. Under Web Services, click Personal Profile.
 - b. Change the host machine name in the value of the Provider ID attribute.

- c. Click **Save** to save the changes.
- 5 Log out of the Access Manager console.

▼ **To Make Changes for SAML v1**

If the host machine name or domain is configured in an instance of Access Manager that acts as an identity provider or service provider in a SAML v1 environment, use this procedure to make the appropriate changes.

- 1 **Login to the Access Manager console as `amadmin`.**
- 2 **Click the Federation tab.**
- 3 **Click the SAML tab.**
- 4 **Click the Instance ID of the relevant entry under Site Identifier.**
- 5 **Change the host machine name in the value of the Instance ID and Issuer Name attributes.**
- 6 **Click **Save** to save the changes.**
- 7 **Click **Save** on the SAML Profile page.**
- 8 **Click the Instance ID of the relevant entry under Trusted Partners, if applicable.**
- 9 **Change the host machine name in the URL endpoints of the relevant entries in the list of Trusted Partners.**
- 10 **Click **Save** to save the changes.**
- 11 **Click **Save** on the SAML Profile page.**
- 12 **Log out of the Access Manager console.**

