Technical Note: Installing Access Manager to Run as a Non-Root User

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

Part No: 819–5574–10
February 2006

060201@13215

Technical Note: Installing Access Manager to Run as a Non-root User

Overview

This document describes how to install and configure Sun Java™ System Access Manager to run as a non-root user with either Sun Java System Web Server 6.1 or Sun Java System Application Server Enterprise Edition (EE) 8.1 as the web container. The supported versions of these components include:

- For Access Manager 7 2005Q4:
  - Web Server 6.1 2005Q4 SP5
  - Application Server EE 8.1 2005Q2
- For Access Manager 6 2005Q1:
  - Web Server 6.1 2005Q1 SP4
  - Application Server EE 8.1 2005Q1

This document is intended for system administrators and software technicians who are deploying Access Manager and other Sun Java Enterprise System (Java ES) components. You should be familiar with the administrative commands for your deployment platform (Solaris™ system or Linux system) and the following tasks.

Task	Where to Find More Information
Understanding Access Manager technical concepts	*Sun Java System Access Manager 7 2005Q4 Technical Overview*

Running the Java ES installer to install Java ES components, including:
■ Sun Java System Access Manager
■ Sun Java System Directory Server
■ Sun Java System Message Queue
■ Access Manager web container:
  ■ Sun Java System Web Server
  ■ Sun Java System Application Server
	Sun Java Enterprise System 2005Q4 Installation Guide for UNIX

Running the Access Manager `amconfig` script to deploy and configure Access Manager instances.	Chapter 1, "Access Manager 7 2005Q4 Configuration Scripts," in *Sun Java System Access Manager 7 2005Q4 Administration Guide*
Administering Java ES components, including starting and stopping Directory Server and the web container (Web Server or Application Server)	Java ES collection: `http://docs.sun.com/prod/entsys.05q4` Java ES component documentation: ■ Directory Server: `http://docs.sun.com/coll/1316.1` ■ Web Server: `http://docs.sun.com/coll/1308.1` ■ Application Server: `http://docs.sun.com/coll/1310.1` ■ Message Queue: `http://docs.sun.com/coll/1307.1`

Installing Access Manager With Web Server to Run as a Non-root User

To install and configure Access Manager with Web Server 6.1 as the web container, follow these steps.

1. As superuser (`root`), create a non-root user and group, if they do not already exist. Examples in this document use `amuser` and `amgroup` as the non-root user and group. For example:

```
# groupadd amgroup
# mkdir /export/home
# useradd -d /export/home/amuser -g amgroup -m
```

2. As superuser (`root`), install Directory Server and Administration Server by running the Java ES installer. Specific values that you must set are:

- On the Common Server Settings page, enter the non-root user (`amuser`) for System User and non-root group (`amgroup`) for System Group.
- Select port numbers for Directory Server and Administration Server that are greater than 1024. Do not use port number 389 or 390.

3. As the non-root user, start Administration Server and Directory Server. For example:

   DirectoryServer-base`/start-admin`
   `...`
   DirectoryServer-base`/slapd-host.example.com/start-slapd`

   All processes should be owned by the non-root user (`amuser` in `amgroup`). For example:

   ```
   amuser 2474 1 0 01:32:08 ? 0:00 ./uxwdog -e -d /javaes/ds/admin-serv/config
   amuser 2485 1 0 01:32:16 ? 0:01 ./ns-slapd -D /javaes/ds/slapd-host -i /javaes/ds/slapd-h
   amuser 2475 2474 0 01:32:08 ? 0:00 ns-httpd -d /javaes/ds/admin-serv/config
   amuser 2477 2475 0 01:32:08 ? 0:01 ns-httpd -d /javaes/ds/admin-serv/config
   ```

4. As superuser (`root`), install Web Server 6.1 by running the Java ES installer. Specific values that you must set are:

   - On the Common Server Settings page, enter the non-root user for System User and non-root group for System Group.
   - On the Web Server: Administration (1 of 2) page, change the Administration Runtime User ID to the non-root user.
   - On the Web Server: Default Web Server Instance (2 of 2) page, change the Runtime User ID to the non-root user and the Runtime Group to the non-root group. Specify a value for HTTP Port that is greater than 1024.

5. As the non-root user, start the Web Server administration instance and Web Server instance. All processes should be owned by the non-root user (`amuser` in `amgroup`). For example:

   ```
   amuser 4200 1 0 02:00:44 ? 0:00 ./webservd-wdog -r  /javaes/ws -d /javaes/ws/https-admser
   amuser 2474 1 0 01:32:08 ? 0:00 ./uxwdog -e -d /javaes/ds/admin-serv/config
   amuser 4202 4201 1 02:00:44 ? 0:02 webservd -r /javaes/ws -d /javaes/ws/https-admserv/con
   amuser 4220 4219 1 02:00:54 ? 0:03 webservd -r /javaes/ws -d /javaes/ws/https-amhost.exam
   amuser 4219 4218 0 02:00:54 ? 0:00 webservd -r /javaes/ws -d /javaes/ws/https-amhost.exam
   amuser 4201 4200 0 02:00:44 ? 0:00 webservd -r /javaes/ws -d /javaes/ws/https-admserv/con
   ```

6. As superuser (`root`), install Access Manager by running the Java ES installer. On the Configuration Type page, select the Configure Later option.

7. Depending on your platform, change the ownership of the following directories from `root` and `other` to the non-root user and non-root group:

   - Solaris systems: `/opt/SUNWma` and `/etc/opt/SUNWma`
   - Linux systems: `/opt/sun/mobileaccess` and `/etc/opt/sun/mobileaccess`

   For example, on Solaris systems:

   ```
   # chown -R amuser:amgroup /opt/SUNWma /etc/opt/SUNWma
   ```

8. As superuser (root), change to the Access Manager /bin directory, depending on your platform. For example:
   - Solaris systems: cd /opt/SUNWam/bin
   - Linux systems: cd /opt/sun/identity/bin
9. As superuser (root), make a copy of the amsamplesilent file. For example:

   ```
   # cp -p amsamplesilent am.non_root_install
   ```

10. As superuser (root), edit the am.non_root_install file as follows:
    - Set BASEDIR to the same value that you selected for the Access Manager installation directory when you ran the Java ES installer.
    - Set NEW_OWNER to the non-root user and NEW_GROUP to the non-root group.
    - Update the following variables: SERVER_HOST, SERVER_PORT, DS_HOST, DS_PORT, ROOT_SUFFIX, COOKIE_DOMAIN, WS61_ADMINPORT and all related password fields, including DS_DIRMGRPASSWD, ADMINPASSWD, and AMLDAPUSERPASSWD.
11. As superuser (root), run the amconfig script with the edited am.non_root_install file to deploy Access Manager. For example:

    ```
    # ./amconfig -s ./am.non_root_install
    ```

12. As the non-root user, stop the Web Server Administration Server instance and Web Server instance.
13. As superuser (root), change the ownership of the Web Server installation directory to the non-root user and group. For example:

    ```
    # chown -R amuser:amgroup /opt/SUNWwbsvr
    ```

14. As the non-root user, start the Web Server Administration Server instance and the Web Server instance.
15. Access the Web Server Administration Console in a browser and login as the Web Server administrator.
16. Select the instance on which you deployed Access Manager and click Manage.
17. Click Apply and then Apply Changes.

Installing Access Manager With Application Server to Run as a Non-root User

To install and configure Access Manager with Application Server 8.1 as the web container, follow these steps.

1. As superuser (root), create a non-root user and group, if they do not already exist. Examples in this document use amuser and amgroup as the non-root user and group. For example:

```
# groupadd amgroup
# mkdir /export/home
# useradd -d /export/home/amuser -g amgroup -m
```

2. As superuser (root), install Directory Server and Administration Server by running the Java ES installer. Specific values that you must set are:
   - On the Common Server Settings page, enter the non-root user (amuser) for System User and non-root group (amgroup) for System Group.
   - Select port numbers for Directory Server and Administration Server that are greater than 1024. Do not use port number 389 or 390.
3. As the non-root user, start Directory Server and Administration Server. For example:

```
DirectoryServer-base/start-admin
...
DirectoryServer-base/slapd-host.example.com/start-slapd
```

   All processes should be owned by the non-root user (amuser in amgroup). For example:

```
amuser 2474 1 0 01:32:08 ? 0:00 ./uxwdog -e -d /javaes/ds/admin-serv/config
amuser 2485 1 0 01:32:16 ? 0:01 ./ns-slapd -D /javaes/ds/slapd-host -i /javaes/ds/slapd-h
amuser 2475 2474 0 01:32:08 ? 0:00 ns-httpd -d /javaes/ds/admin-serv/config
amuser 2477 2475 0 01:32:08 ? 0:01 ns-httpd -d /javaes/ds/admin-serv/config
```

4. As superuser (root), install Application Server 8.1 and Message Queue by running the Java ES installer. Specific values that you must set are:
   - On the Installation Directories page, for the Application Server and Application Server Data and Configuration directories, enter values that are beneath the non-root user's home directory. For example, if the non-root user's home directory is /export/home/amuser, the Application Server installation directory could be /export/home/amuser/as.
   - On the Common Server Settings page, enter the non-root user for System User and non-root group for System Group.
   - On the Application Server Domain Administration Server (1 of 1) page, select port numbers that are greater than 1024 for the Application Server Administration Port, JMX Port, HTTP Port, and HTTPS Port.
5. As superuser (root), delete the Application Server domain created by the Java ES installer in the following location, depending on your platform:
   - Solaris systems: *ApplicationServer-base*/appserver/bin
   - Linux systems: *ApplicationServer-base*/bin

   For example, to delete the Application Server domain:

```
#./asadmin delete-domain --domaindir /asdomains domain1
```

6. As superuser (root), change the ownership of the Application Server installation directory and the Application Server data and configuration directory to the non-root user and group. For example:

   ```
   # chown -R amuser:amgroup /export/home/amuser/as /export/home/amuser/as_var/
   ```

7. As superuser (root), create an administration password file as follows:

   ```
   # echo "AS_ADMIN_PASSWORD=application-server-admin-password" > /tmp/asAdminPassFile
   ```

8. Recreate the Application Server domain as the non-root user:

   a. Change to the non-root user. For example:

      ```
      # su - amuser
      ```

   b. Change to the /bin directory. For example, on Solaris systems:

      ```
      cd ApplicationServer-base/appserver/bin
      ```

      Or, on Linux systems:

      ```
      cd ApplicationServer-base/bin
      ```

   c. Invoke the asadmin create-domain command to recreate the deleted domain. You will be prompted to enter and confirm the domain's administration password and the master password. For example:

      ```
      ./asadmin create-domain --domaindir /export/home/amuser/as_var/domains --adminport 4849
      --adminuser admin --passwordfile /tmp/asAdminPassFile --instanceport 8080
      --domainproperties domain.jmxPort=8686:http.ssl.port=8181 --savemasterpassword=true domain1
      Please enter adminpassword> adminpassword
      Please enter adminpassword again> adminpassword
      Please enter the master password> masterpassword
      Please enter the master password again> masterpassword
      Using default port 7,676 for JMS.
      Using default port 3,700 for IIOP.
      Using default port 3,820 for IIOP_SSL.
      Using default port 3,920 for IIOP_MUTUALAUTH.
      Domain domain1 created.
      ```

9. As superuser (root), remove the Application Server administration password file. For example:

   ```
   # rm -rf /tmp/asAdminPassFile
   ```

10. As the non-root user, use the asadmin start-domain command to start the Application Server domain that you just created. You will be prompted for the administration password. For example:

    ```
    ./asadmin start-domain --user admin domain1
    ```

    The Application Server and Message Queue processes should be owned by the non-root user (amuser in amgroup). For example:

    ```
    amuser 15009 15007 0 12:26:20 pts/4 0:00 /bin/sh /usr/bin/imqbrokerd -javahome /usr/jdk/entsys-
    amuser 15007 582 0 12:26:09 pts/4 2:20 /export/home/amuser/as/appserver/lib/appservDAS domain1
    amuser 15017 15009 0 12:26:20 pts/4 0:05 /usr/jdk/entsys-j2se/bin/java -server -cp /usr/bin/../
    ```

11. Verify that the Application Server administration instance is accessible by entering the following URL in a browser:

`https://`*fqdn*`:`*as-admin-port*`/`

Where *fqdn* and *as-admin-port* are the fully qualified domain name and port.

12. Verify that the Application Server HTTP port is accessible by entering the following URL in a browser:

    `http://`*fqdn*`:8080/`

    Where *fqdn* is the fully qualified domain name.

13. Install Access Manager by running the Java ES installer. For the Configuration Type, select the Configure Later option.
14. As superuser (`root`), change the ownership of the following directories from `root` and `other` to the non-root user and non-root group, depending on your platform:

    - Solaris systems: `/opt/SUNWma` and `/etc/opt/SUNWma`
    - Linux systems: `/opt/sun/mobileaccess` and `/etc/opt/sun/mobileaccess`

    For example:

    ```
    # chown -R amuser:amgroup /opt/SUNWma /etc/opt/SUNWma
    ```

15. As superuser (`root`), change to the Access Manager `/bin` directory, depending on your platform:

    - Solaris systems: `cd /opt/SUNWam/bin`
    - Linux systems: `cd /opt/sun/identity/bin`

16. As superuser (`root`), make a copy of the `amsamplesilent` file. For example:

    ```
    # cp -p amsamplesilent am.non_root_install
    ```

17. As superuser (`root`), edit the `am.non_root_install` file as follows:

    - Set `BASEDIR` to the same value that you selected for the installation directory of Access Manager in the Java ES installer.
    - Set `NEW_OWNER` to the non-root user and `NEW_GROUP` to the non-root group.
    - Update the following variables: `SERVER_HOST`, `SERVER_PORT`, `DS_HOST`, `DS_PORT`, `ROOT_SUFFIX`, `COOKIE_DOMAIN`, `WEB_CONTAINER`, `AS81_HOME`, `AS81_ADMINPASSWD`, `AS81_INSTANCE_DIR`, `AS81_DOCS_DIR` and all related password fields, including `DS_DIRMGRPASSWD`, `ADMINPASSWD`, and `AMLDAPUSERPASSWD`.

    Important: Set the `AS81_HOME` variable to the parent directory of the Application Server `/bin` directory.

    See Example 1for a sample edited `amsamplesilent` file.

18. As superuser (`root`), run the `amconfig` script with the edited `am.non_root_install` file to deploy Access Manager. For example:

    ```
    # ./amconfig -s ./am.non_root_install
    ```

If you encounter the question "`Do you trust the above certificate [y|n]`" during the deployment of the Access Manager Web applications, specify "`y`" and press Enter.

19. As the non-root user, stop the Application Server domain and then restart it. First change to the`/bin` directory. For example, on Solaris systems:

    Change to the `/bin` directory. For example, on Solaris systems:

    `cd` *ApplicationServer-base*`/appserver/bin`

    Or, on Linux systems:

    `cd` *ApplicationServer-base*`/bin`

    Then, stop and restart the Application Server domain. For example:

    ```
    ./asadmin stop-domain domain1
    ./asadmin start-domain --user admin domain1
    ```

    The `asadmin start-domain` command will prompt you for the Application Server administration password.

20. Use a browser with the following URL to verify that the Access Manager Administrator Console is accessible.

    `http://`*fqdn*`:8080/amserver/`

    Where *fqdn* is the fully qualified domain name.

EXAMPLE 1 Sample `amsamplesilent` File With Application Server as the Web Container

The following example shows a sample edited `amsamplesilent` file. For a description of these variables, see Chapter 1, "Access Manager 7 2005Q4 Configuration Scripts," in *Sun Java System Access Manager 7 2005Q4 Administration Guide*.

```
DEPLOY_LEVEL=1
BASEDIR=/export/home/amuser/am
SERVER_HOST=host.example.com
SERVER_PORT=8080
SERVER_PROTOCOL=http
CONSOLE_HOST=$SERVER_HOST
CONSOLE_PORT=$SERVER_PORT
CONSOLE_PROTOCOL=$SERVER_PROTOCOL
CONSOLE_REMOTE=false
DS_HOST=host.example.com
DS_PORT=8389
DS_DIRMGRDN="cn=Directory Manager"
DS_DIRMGRPASSWD=password
ROOT_SUFFIX="dc=host,dc=example,dc=com"
# ADMINPASSWD, the amadmin password, and AMLDAPUSERPASSWD, the amldapuser password, must be set to
ADMINPASSWD=password
AMLDAPUSERPASSWD=password
CONSOLE_DEPLOY_URI=/amconsole
SERVER_DEPLOY_URI=/amserver
PASSWORD_DEPLOY_URI=/ampassword
```

EXAMPLE 1 Sample `amsamplesilent` File With Application Server as the Web Container *(Continued)*

```
COMMON_DEPLOY_URI=/amcommon
COOKIE_DOMAIN=.iplanet.com
JAVA_HOME=/usr/jdk/entsys-j2se
AM_ENC_PWD=""
PLATFORM_LOCALE=en_US
# Non-root user and group
NEW_OWNER=amuser
NEW_GROUP=amgroup
####
XML_ENCODING=ISO-8859-1
NEW_INSTANCE=false
WEB_CONTAINER=AS8
AS81_HOME=/export/home/amuser/as/appserver
AS81_PROTOCOL=$SERVER_PROTOCOL
AS81_HOST=$SERVER_HOST
AS81_PORT=$SERVER_PORT
AS81_ADMINPORT=4849
AS81_ADMIN=admin
AS81_ADMINPASSWD="password"
AS81_INSTANCE=server
AS81_DOMAIN=domain1
AS81_INSTANCE_DIR=/export/home/amuser/as_var/domains/${AS81_DOMAIN:-domain1}
AS81_DOCS_DIR=/export/home/amuser/as_var/domains/${AS81_DOMAIN:-domain1}/docroot
# true if container is SSL enabled, installer will use SSL_PASSWORD to start server without
AS81_IS_SECURE=false
AS81_ADMIN_IS_SECURE=true
SSL_PASSWORD="sample"
DIRECTORY_MODE=1
USER_NAMING_ATTR=uid
ORG_NAMING_ATTR=o
ORG_OBJECT_CLASS=sunismanagedorganization
USER_OBJECT_CLASS=inetorgperson
DEFAULT_ORGANIZATION=
```

Accessing Sun Resources Online

The docs.sun.com^{SM} 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 819-5574.

Revision History

Release Date	Description of Changes
February 1, 2006	Review draft