Technical Note: Deploying Access Manager With Application Server 9.1

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

Part No: 820–3043–11
September 22, 2009

090923@22749

Technical Note: Deploying Access Manager With Application Server 9.1

September 22, 2009

This technical note describes how to deploy Sun Java™ System Access Manager 7.1 (full server) and the Access Manager 7.1 SDK with Sun Java System Application Server 9.1 as the web container, including:

Requirements and Where to Find More Information

Requirement	Where to Find More Information
Sun Java System Application Server 9.1 (or Application Server 9.0) must be installed and running on the server where you plan to deploy Access Manager 7.1 or the Access Manager 7.1 SDK. You should be familiar with using the Application Server 9.1 Administration Console or command-line interface (CLI) to perform administrative tasks such as: ■ Verifying, starting, and stopping an Application Server 9.1 instance ■ Deploying a web application from a WAR file If the Java Security Manager is enabled, you must add the Access Manager 7.1 permissions to the Application Server 9.1 `server.policy` file. See "Adding Access Manager Permissions to the Application Server 9.1 `server.policy` File" on page 14.	Application Server 9.1 documentation collection: `http://docs.sun.com/coll/1343.4`
The Access Manager 7.1 SDK requires access to an Access Manager 7.1 full server installation that is configured and running. This Access Manager 7.1 server installation can be on a remote server or on another instance on the same server where you plan to deploy the Access Manager 7.1 SDK. To install Access Manager 7.1 server, use either of these methods, depending on the requirements of your deployment: ■ If your deployment requires Legacy Mode (including the Legacy Mode Console) or the `ampassword` application (which is used for the password reset of users), you **must** use the Sun Java Enterprise System (Java ES) 5 Update 1 installer. ■ If your deployment requires Realm Mode but not the `ampassword` application, you can deploy Access Manager 7.1 from a WAR file.	**Running the Java ES 5 Update 1 Installer**: "Installing Access Manager 7.1 Using the Java ES 5 Update 1 Installer" on page 5 **Deploying a WAR File**: "Deploying an Access Manager 7.1 WAR File With Application Server 9.1" on page 6
Sun Java System Directory Server must be installed and running, usually on a remote server.	Directory Server Enterprise Edition 6.0 documentation collection: `http://docs.sun.com/coll/1224.1`

Deploying Access Manager 7.1 With Application Server 9.1

Deploy Access Manager 7.1 server using either of these methods, depending on your site requirements:

Use the following table to determine the method you should use.

Site Requirement	Method
Access Manager Legacy Mode, including the Legacy Mode Console	Run the Java ES 5 Update 1 installer either, using the Configure Now or Configure Later option
Access Manager Realm Mode	Run the Java ES 5 Update 1 installer or Deploy the Access Manager 7.1 WAR file
`ampassword` application, which is used to reset user passwords	Run the Java ES 5 Update 1 installer

Installing Access Manager 7.1 Using the Java ES 5 Update 1 Installer

Installing Access Manager 7.1 server with the Java ES 5 Update 1 installer on Application Server 9.1 involves these general steps:

1. Get the Java ES 5 Update 1 installer. The installer is available in a media kit containing CDs or a DVD, as web download, on a pre-installed system, or from a file server on your network.
2. Determine the installation mode:
   - Graphical mode: An interactive wizard guides you through a series of choices on installation pages on a graphical workstation.
   - Text-based mode: An interactive command-line installer prompts you for responses in a terminal window.
   - Silent mode: The installer reads input from a state file, which is a text file containing name-value pairs of configuration information. You create a state file by running the installer with the `-no` and `-saveState` options. Then, you edit the state file for the specific host server where you plan to install the various Java ES components.
3. Determine the installer configuration option you plan to use. You can use either of these options to install Access Manager 7.1 when you run the Java ES 5 Update 1 installer.

- **Configure Now**: During installation, fully configure Access Manager 7.1 by either choosing configuration values or accepting the default values.
- **Configure Later**: During installation, specify only minimal configuration values. Then, configure Access Manager 7.1 by running the `amconfig` script using configuration values in the `amsamplesilent` input file (or a copy of the file).

  On Windows systems, the corresponding files are `amconfig.bat` and `AMConfigurator.properties`. These files are installed in the *javaes-install-dir*`\identity\setup` directory, where *javaes-install-dir* is the Java ES 5 installation directory. The default value is `C:\Program Files\Sun\JavaES5`.

  Note: When you run the `amconfig` script or `amconfig.bat` to configure Access Manager 7.1 (either the full server or SDK), the Application Server 9.1 web container variables begin with `AS81`.

4. Run the installer. For more information, including the detailed steps, see the following documents, depending on your platform:
   - **Solaris, Linux, and HP-UX Systems**: *Sun Java Enterprise System 5 Update 1 Installation Guide for UNIX*
   - **Windows Systems**: *Sun Java Enterprise System 5 Installation Guide for Microsoft Windows*
5. If you ran the installer with the Configure Later option, run the configuration script (`amconfig` or `amconfig.bat`) to configure Access manager 7.1.

   For more information about running these scripts, see Chapter 2, "Running the Access Manager amconfig Script," in *Sun Java System Access Manager 7.1 Postinstallation Guide*.

Deploying an Access Manager 7.1 WAR File With Application Server 9.1

Deploying an Access Manager 7.1 WAR file on Application Server 9.1 involves these steps:

Downloading the Access Manager 7.1 WAR File

The Access Manager 7.1 WAR file (`amserver.war`) is available as part of the Access Manager 7.1 ZIP file under `Identity Management > Access Manager` on the following web site:

`http://www.sun.com/download/index.jsp`

The ZIP file name is `AccessManager7_1`*release*`.zip`, where *release* specifies the Access Manager release. For example, `AccessManager7_1RTM.zip` is the initial release of Access Manager 7.1.

The following table describes the files in the Access Manager 7.1 ZIP file. The directory where you unzip the file is represented by *zip_root*.

Directory	Description
zip_root	`README` describes the contents of the ZIP file. `Software_License_Agt_SLA.txt` is the Software License Agreement.
zip_root`/applications`	`README` is a brief explanation of the web applications. `amDistAuth.zip` contains the files to deploy and configure a Distributed Authentication UI server WAR file (`amauthdistui.war`).
zip_root`/applications/jdk14`	Contains the Access Manager 7.1 WAR file (`amserver.war`) for web containers running under JDK 1.4.x.
zip_root`/applications/jdk14/jarFix`	Contains the following JAR files required for specific deployments: `commons-logging.jar`, `dom.jar`, `jaxrpc-api.jar`, `jaxrpc-ri.jar`, `xalan.jar`, and `xercesImpl.jar`.
zip_root`/applications/jdk15`	Contains the Access Manager 7.1 WAR file (`amserver.war`) for web containers running under JDK 1.5.x. Use this file to deploy Access Manager 7.1 on Application Server 9.1.
zip_root`/samples`	`README` provides instructions about the Access Manager samples.
zip_root`/tools`	`README` describes the contents of the tools ZIP files. `amAdminTools.zip` contains: ■ Files to run the Access Manager CLI utilities and scripts such as `amadmin`, `ampassword`, `amtune` and `amsfoconfig`. ■ Properties files for various locales, including English, French, German, Spanish, Japanese, Korean, Simplified Chinese, and Traditional Chinese. `amSessionTools.zip` contains the files to install Sun Java System Message Queue and the Berkeley DB, which then allows you to configure Access Manager session failover.
zip_root`/legal`	Contains locale specific legal files

Deploying an Access Manager 7.1 WAR File With Application Server 9.1

▼ To Deploy the Access Manager 7.1 WAR File With Application Server 9.1

Before You Begin

- You must have downloaded and unzipped the Access Manager 7.1 ZIP file, as described in "Downloading the Access Manager 7.1 WAR File" on page 6.
- Application Server 9.1 must be installed and running on the host server.
- To execute the `asadmin deploy` command or login to the Application Server 9.1 Administration Console, you must know the administrator password for the domain.

1 If necessary, create a staging directory for the WAR file. For example:

```
# mkdir opt/AccessManagerWAR
```

Create a staging directory for these situations:

- You downloaded and unzipped the Access Manager 7.1 ZIP file on a server other than the server where you plan to deploy Access Manager 7.1
- You want to customize Access Manager 7.1

2 If you created a staging directory in Step 1, copy the `amserver.war` file to that directory.

Important: For Application Server 9.1. copy the `amserver.war` file from the *zip_root*`/applications/jdk15` directory.

3 If you want to customize Access Manager:

a. Explode the `amserver.war` file in the staging area. For example:

```
# cd opt/AccessManagerWAR
# jar -xvf amserver.war
```

b. Modify the exploded files as required for your deployment.

For example, the files that you can customize include `web.xml` and related XML files, Java Server Pages (`.jsp` files), images (`.gif` files), and style sheets (`.css` files).

For more information, see Chapter 10, "Updating and Redeploying Access Manager WAR Files," in *Sun Java System Access Manager 7.1 Developer's Guide*.

c. Recreate a new `amserver.war` file. For example:

```
# cd opt/AccessManagerWAR
# jar -cvf amserver.war *
```

4 **Deploy the `amserver.war` file using either the Application Server 9.1 Administration Console or the `asadmin deploy` command.**

For example, the following `asadmin deploy` command deploys the `amserver.war` file on a Solaris system:

```
# cd opt/SUNWappserver/appserver/bin
# ./asadmin deploy --user admin --port 4848
--passwordfile /tmp/pwdfile /opt/AccessManagerWAR/amserver.war
```

where:

`/opt/AccessManagerWAR` is the directory where the `amserver.war` file exists.

`/tmp/pwdfile` is a password file that contains the administrator password in ASCII text format:

`AS_ADMIN_PASSWORD=`*password*

For more information, see the `deploy` command in the *Sun Java System Application Server 9.1 Reference Manual*. For example, to deploy the WAR file to a different server instance or to a cluster, also include the `--target` option in the command.

For information about the Application Server 9.1 Administration Console, see Chapter 3, Deploying an Application, in the *Sun Java System Application Server 9.1 Quick Start Guide*.

Next Steps Continue with the Access Manager 7.1 configuration in the following sections.

Configuring Access Manager 7.1 Using the Configurator

The Configurator (`configurator.jsp`) allows you to configure Access Manager 7.1 after you deploy the `amserver.war` file.

▼ To Configure Access Manager 7.1 Using the Configurator

Before You Begin **Important**: Before you run the Configurator, make sure that the code set in the `LANG` environment variable is set to `ISO8859-1`. For example, to set the code set for U.S. English when you are using the `sh` or `ksh` shell:

```
# LANG=en_US.ISO8859-1
```

1 **Launch the Configurator by specifying the following URL in your browser:**

protocol`://`*host.domain*`:`*port*`/amserver`

For example:

```
http://amhost1.example.com:8080/amserver
```

Note: If the Access Manager 7.1 instance is already configured successfully, you will be directed to the Access Manager Console login page.

2 Enter the following values for the Access Manager Settings (or accept the default values).

The **Server Settings** are independent of the datastore that you select (File System or Directory Server) to store the Access Manager configuration data.

Server Settings	
Server URL	Host server where you plan to deploy Access Manager. Can be one of the following: ■ Host name. For example: `amhost1` ■ Fully qualified domain name (FQDN). For example: `http://amhost1.example.com` If you plan to use the Access Manager client SDK or a policy agent, you must specify the FQDN. ■ `localhost` Default: Host where you are deploying Access Manager.
Cookie Domain	Name of the trusted DNS domain that Access Manager returns to a browser when it grants a SSO token to a user. Specify a value only if the FQDN is used as the Server URL. For example, if the FQDN for Server URL is `http://amhost1.example.com`, the default value is `.example.com`. If you selected only the host name or `localhost` for the Server URL, Cookie Domain is set to blank, and any value you enter is ignored.
Administrator	
Name	`amAdmin` (read-only)
Password	Access Manager administrator (`amAdmin`) password. Enter and then retype to confirm the password. The password must be at least 8 characters long.
General Settings	

Configuration Directory	Base directory where the Access Manager configuration data is stored. The base directory applies to either File System or Directory Server, which you select under **Configuration Store Settings**. For example: `/am_configuration_data` Access Manager creates the following files and directories under the Configuration Directory: ■ `AMConfig.properties` file ■ `serverconfig.xml` file ■ `LDIF` files (if you select Directory Server to store the service configuration data) ■ *deploy-uri* directory ■ *deploy-uri*`/log` directory ■ *deploy-uri*`/stats` directory ■ *deploy-uri*`/debug` directory ■ *deploy-uri*`/idRepo` directory: All users are created under this directory, even if you select Directory Server to store the service configuration data, since it is the default data store. ■ *deploy-uri*`/sms/` directory: Directories for the service configuration schema XML files *deploy-uri* is the Access Manager server deployment URI. The default is `/amserver`. The Access Manager 7.1 instance determines the location of the Configuration Directory using a "Bootstrap File" on page 13.
Platform Locale	Default language subtype for Access Manager. Default: `en_US` (US English)
Encryption Key	Random number that is used to encrypt passwords. Either accept the default encryption key value or specify a new value. The encryption key should be at least 12 characters long. **Access Manager SDK**: Use the same password encryption key value for the `AM_ENC_PWD` variable when you run the `amconfig` script to configure the Access Manager SDK. **Multiple server deployment**: If you are using the same WAR file to deploy multiple Access Manager instances in a multiple server deployment, you must use the same password encryption key value for each instance.

3 Select either of the following options to store the Access Manager configuration data:

Configuration Store Settings	
File System	Access Manager stores the service configuration data in directories under the *ConfigurationDirectory*`/amserver/sms` directory. For example: `/am_configuration_data/amserver/sms` Default is File System. **Note**: If you use an Access Manager server deployment URI other than `amserver`, that value is used instead of `amserver` for the directory name.
Directory Server	Access Manager stores the service configuration data in Sun Java System Directory Server. Directory Server must be installed and running before you deploy the Access Manager 7.1 WAR file. **Note**: All administrator users are created under the `idRepo` directory, even if you select Directory Server to store the service configuration data.

4 If you selected Directory Server in the previous step, provide values for the following settings:

Server Settings	
Name	Fully qualified host name of Directory Server. For example: `ds.example.com`
Port	Port at which Directory Server is running. Default: `389`
Suffix to store configuration data	Initial or root suffix in the directory where Access Manager configuration data will be stored. This value must exist in the Directory Server you are using. For example: `dc=ds,dc=example,dc=com`
Directory Server Administrator	
Directory Administrator DN	Distinguished Name (DN) of the Directory Server Administrator. Default: `cn=Directory Manager`
Password	Directory Server administrator password. Enter and then retype to confirm the password. The password must be at least eight characters long.

Load User Management Schema	Load Access Manager SDK Schema If checked, the Configurator loads the Access Manager SDK schema object classes and attributes from `sunone_schema2.ldif`, `ds_remote_schema.ldif`, `plugin.ldif`, `index.ldif` and `install.ldif` into Directory Server. Otherwise, the Configurator loads only the Access Manager service management services (SMS) object classes and attributes from the `am_sm_ds_schema.ldif` file into Directory Server.

5 **Click Configure.**

(To reset all values, click Reset.)

Next Steps The Configurator configures Access Manager 7.1 and then displays the configuration status:

- **Succeeded**: The Configurator displays a link to redirect you to the Access Manager Console login page. Login as `amAdmin` and the password you specified during the configuration.
- **Failed**: The Configurator displays an error message that describes the failure. If a configuration error occurred (such as an invalid password or host name), Access Manager returns to the Configurator page. Correct the error and continue. For some errors, the message will point to the Access Manager log files to help you to determine the error.

  Depending on when a failure occurs, the debug logs might not be created in their default locations. In this situation, check the logs for the following directory under the Access Manager web container:

  ```
  @BASE_DIR@@SERVER_URI@/@DEBUG_SUBDIR@
  ```

Note – If configuration was successful, you cannot reconfigure Access Manager using the Configurator. If you subsequently invoke the Configurator, Access Manager displays either the login page or the Console. If you are already logged in and have a valid session, you are redirected to the console. If you do not have a valid session, Access Manager displays the login page.

Bootstrap File

The bootstrap file is an ASCII text file containing a single entry that specifies the location of the configuration directory for the specific Access Manager 7.1 instance. Each configured Access Manager 7.1 instance on a host server has a unique bootstrap file. When you run the Configurator, a bootstrap file is created with the following name for the specific Access Manager 7.1 instance:

user-home-directory/AccessManager/AMConfig_*deployed-instance-server-path*_*deploy-uri*

Where:

- *user-home-directory* is the home directory of the user who deployed the Access Manager instance from the WAR file.
- *deployed-instance-server-path* is the path of the deployed Access Manager instance.
- *deploy-uri* is the Access Manager server deployment URI.

Each time the Access Manager web container is restarted, the Access Manager instance accesses the single WAR bootstrap file to determine the location of its configuration data. If the single WAR bootstrap file is deleted, Access Manager displays the Configurator page instead of the login page, which allows you to reconfigure the Access Manager instance. The value in the bootstrap file is determined from the value you enter in the Configurator Configuration Directory field.

Adding Access Manager Permissions to the Application Server 9.1 server.policy File

If the Java Security Manager is enabled, add the following Access Manager 7.1 permissions to the Application Server 9.1 server.policy file:

```
// Additions for Access Manager
grant codeBase "file:\${com.sun.aas.instanceRoot}/applications/j2ee-modules/amserver/-" {
      permission java.net.SocketPermission "*", "connect,accept,resolve";
      permission java.util.PropertyPermission "*", "read, write";
      permission java.lang.RuntimePermission "modifyThreadGroup";
      permission java.lang.RuntimePermission "setFactory";
      permission java.lang.RuntimePermission "accessClassInPackage.*";
      permission java.util.logging.LoggingPermission "control";
      permission java.lang.RuntimePermission "shutdownHooks";
      permission javax.security.auth.AuthPermission "insertProvider.Mozilla-JSS";
      permission java.security.SecurityPermission "putProviderProperty.Mozilla-JSS";
      permission javax.security.auth.AuthPermission "getLoginConfiguration";
      permission javax.security.auth.AuthPermission "setLoginConfiguration";
      permission javax.security.auth.AuthPermission "modifyPrincipals";
      permission javax.security.auth.AuthPermission "createLoginContext.*";
      permission java.security.SecurityPermission "insertProvider.Mozilla-JSS";
      permission javax.security.auth.AuthPermission "putProviderProperty.Mozilla-JSS";
      permission java.io.FilePermission "<<ALL FILES>>", "execute,delete";
      permission java.util.PropertyPermission "java.util.logging.config.class", "write";
      permission java.security.SecurityPermission "removeProvider.SUN";
      permission java.security.SecurityPermission "insertProvider.SUN";
      permission java.security.SecurityPermission "removeProvider.Mozilla-JSS";
      permission javax.security.auth.AuthPermission "doAs";
```

```
      permission java.util.PropertyPermission "java.security.krb5.realm", "write";
      permission java.util.PropertyPermission "java.security.krb5.kdc", "write";
      permission java.util.PropertyPermission "java.security.auth.login.config", "write";
      permission java.util.PropertyPermission "user.language", "write";
      permission javax.security.auth.kerberos.ServicePermission "*", "accept";
      permission javax.net.ssl.SSLPermission "setHostnameVerifier";
      permission java.security.SecurityPermission "putProviderProperty.IAIK";
      permission java.security.SecurityPermission "removeProvider.IAIK";
      permission java.security.SecurityPermission "insertProvider.IAIK";
};
// End of additions for Access Manager
```

Note – If you deploy Access Manager 7.1 using a name other than `amserver`, change that name in the `grant` statement.

Deploying the Access Manager 7.1 SDK With Application Server 9.1

The Sun Java System Access Manager SDK implements APIs that allow an application such as Sun Java System Portal Server to manage users and related information in the user branch of the identity repository. Deploying the Access Manager 7.1 SDK requires these steps:

- "Installing the Access Manager 7.1 SDK Using the Java Enterprise System 5 Update 1 Installer" on page 15
- "Configuring the Access Manager 7.1 SDK" on page 19

Installing the Access Manager 7.1 SDK Using the Java Enterprise System 5 Update 1 Installer

Install the Access Manager 7.1 SDK by running the Java ES 5 Update 1 installer with the Configure Later option.

▼ To Install the Access Manager 7.1 SDK

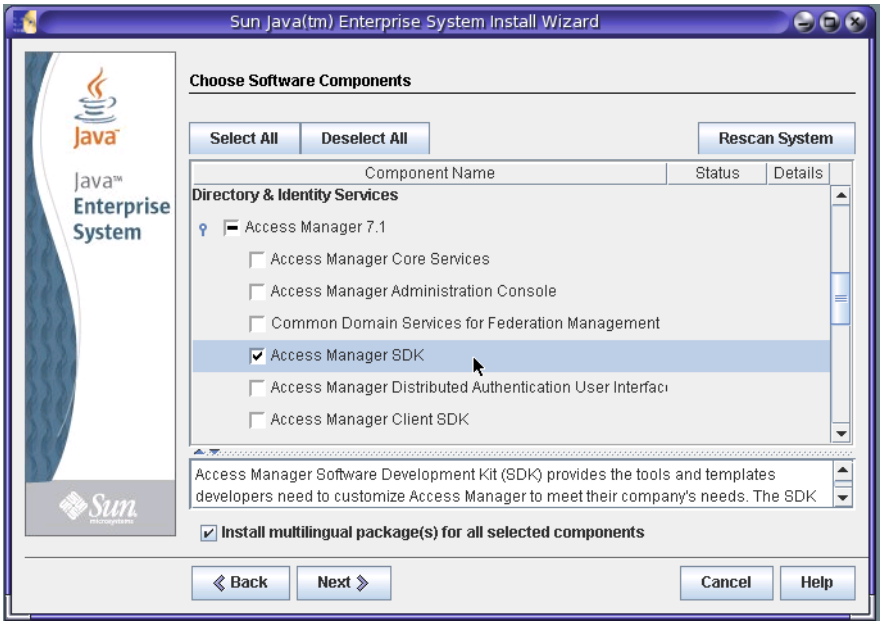
Before You Begin

- Verify that Application Server 9.1 is installed and running on the server.
- Verify that the full Access Manager 7.1 server is running and accessible, either on a remote server or on another instance on the same server where you plan to install the Access Manager SDK.

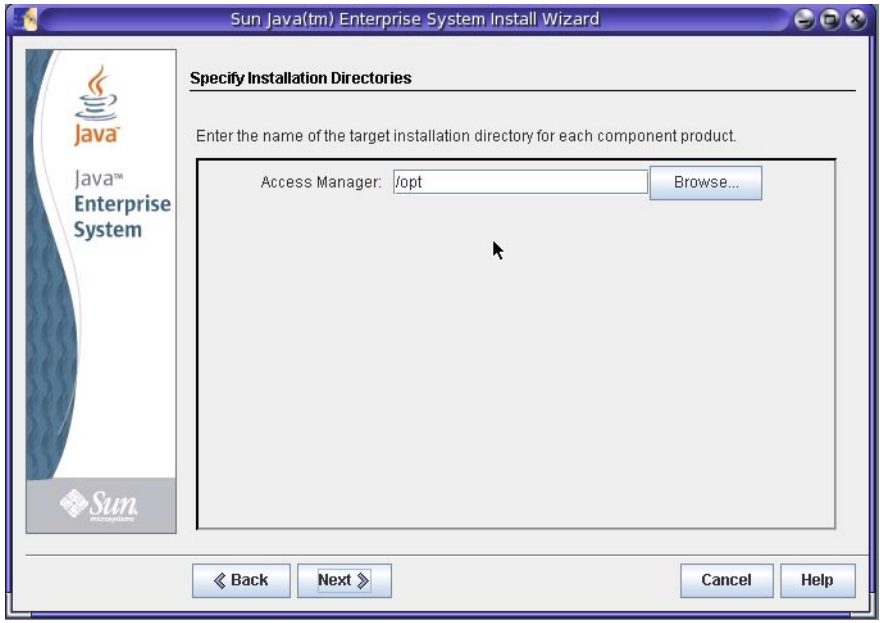
1 On the server where you plan to install the Access Manager SDK, log in as or become superuser (`root`).

2 **Start the Java ES 5 Update 1 installer and accept the Software License Agreement.**

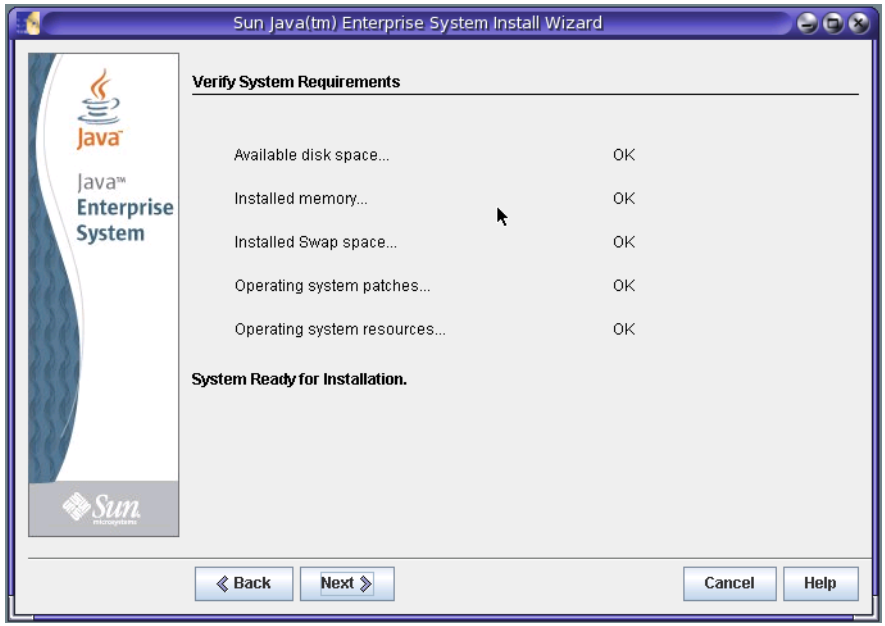
3 **On the Choose Software Components page, under Access Manager 7.1, select only the Access Manager SDK. For example:**



4 **On the Specify Installation Directories page, accept either the Access Manager default installation directory (`/opt`) or specify a different directory, if you prefer. For example:**



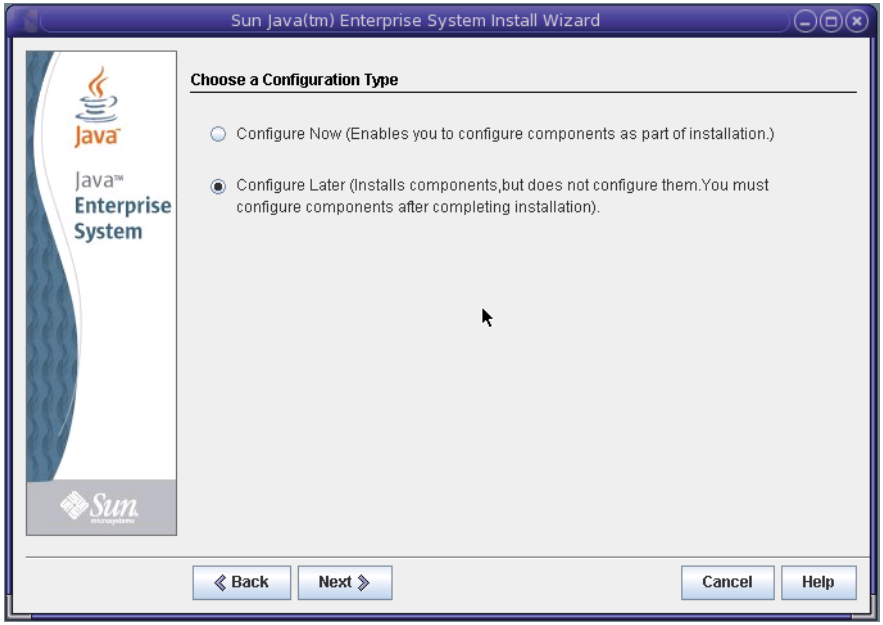
5 The installer then displays the Verify System Requirements page. For example:



The installer checks the system resources based on the components you have selected and the installation directories you provided:

- If the installer displays System Ready for Installation, click Next and continue with the next step.
- If the installer displays System Not Ready for Installation, click View Report for information about the problems that the installer found. If your system does not meet the minimum system requirements, in most cases, the installer cannot continue. For example, the system might be missing one or more required patches, which you must install before continuing with the installation.

6 On the Choose a Configuration Type page, specify Configure Later. For example:



7 On the Ready to Install page, click Install to finish the installation.

Next Steps The installer writes installation summary and log files in the following directory, depending on your platform:

- Solaris systems: `/var/sadm/install/logs`
- Linux and HP-UX systems: `/var/opt/sun/install/logs`
- Windows systems: *temp-directory*`\SunJavaES.log`

  where *temp-directory* is the user-defined temporary directory for the system.

For more information about these log files, see:

- "Examining Installation Log Files" in *Sun Java Enterprise System 5 Installation Guide for UNIX*
- "Examine the Installation Log Files" in *Sun Java Enterprise System 5 Installation Guide for Microsoft Windows*

Configuring the Access Manager 7.1 SDK

Because you specified the Configure Later option when you ran the Java ES 5 Update 1 installer, you must now configure the Access Manager 7.1 SDK by editing variables in the `amsamplesilent` file (or a copy of the file) and then running the `amconfig` script.

On Windows systems, the corresponding files are `amconfig.bat` and `AMConfigurator.properties`. These files are installed in the *javaes-install-dir*`\identity\setup` directory, where *javaes-install-dir* is the Java ES 5 installation directory. The default value is `C:\Program Files\Sun\JavaES5`.

▼ To Configure the Access Manager 7.1 SDK

1. **On the server where you installed the Access Manager 7.1 SDK, change to the `/bin` directory, depending on your platform:**

   - Solaris systems: `/opt/SUNWam/bin`
   - Linux and HP-UX systems: `/opt/sun/identity/bin`
   - Windows systems: *javaes-install-dir*`\identity\setup`

     Where *javaes-install-dir* is the Java ES 5 installation directory. The default value is `C:\Program Files\Sun\JavaES5`.

2. **Make a copy of the `amsamplesilent` file. The following examples use the `amsdk_configure` file.**

3. **In the `amsdk_configure` file, set the following Access Manager configuration variables.**

   If a variable is commented out, also remove the comment character (`#`) when you set the value.

Variable	Description
`DEPLOY_LEVEL`	Action performed by the `amconfig` script. To install the Access Manager 7.1 SDK and configure the Application Server 9.1 web container, set as: `DEPLOY_LEVEL=4`

Variable	Description
AM_REALM	Access Manager mode: AM_REALM=enabled for Realm Mode or AM_REALM=disabled for Legacy Mode. **Note**: Portal Server 7.1 supports either Realm Mode or Legacy Mode if user data is stored in Sun Java System Directory Server. However, if your deployment also includes a Sun Java System Communications Suite product, You must specify Legacy Mode.
BASEDIR	Base installation directory. Set BASEDIR to the installation directory that you specified during the Access Manager 7.1 SDK installation. By default, BASEDIR is set to PLATFORM_DEFAULT, which is /opt on Solaris systems and /opt/sun on Linux systems. On Windows systems, the base installation directory is the Java ES installation directory. The default value is C:\Program Files\Sun\JavaES5.
SERVER_NAME	Host name of the server where the full Access Manager 7.1 installation is running. For example: amhost
SERVER_HOST	Fully qualified name of the host server where the full Access Manager 7.1 installation is running. For example: amhost.example.com
SERVER_PORT	Port number of the host server where the full Access Manager 7.1 installation is running.
ADMIN_PORT	Port on which the administration instance will listen for connections. Default for Application Server 9.1 is 4848.
ADMINPASSWD	Password for the Access Manager administrator (amadmin) for the full Access Manager 7.1 server installation.
COOKIE_DOMAIN	Names of the trusted DNS domains that Access Manager returns to a browser when it grants a session ID to a user. Specify at least one value. The format is the server's domain name preceded with a period. For example: COOKIE_DOMAIN=.example.com
AM_ENC_PWD	Password encryption key value. **Important**: Set AM_ENC_PWD to the same password encryption key value used for the full Access Manager 7.1 server installation.
NEW_OWNER and NEW_GROUP	Owner and group, respectively, of the Application Server 9.1 instance on which the Access Manager SDK is being configured.
PAM_SERVICE_NAME	Name of the PAM service from the PAM configuration or stack that comes with the operating system and is used for the UNIX authentication module. Usually, other for Solaris or password for Linux. Default: other

Variable	Description
WEB_CONTAINER	Web container for the Access Manager 7.1 SDK. **Note**: Although you are deploying the Access Manager SDK on Application Server 9.1, set the variable as follows: WEB_CONTAINER=AS8

Set any other variables in the amsdk_configure file as required for your deployment.

4 **In the amsdk_configure file, set the following Application Server 9.1 web container variables:**

Note: Although you are deploying the Access Manager SDK on Application Server 9.1, the web container variables begin with AS81.

Variable	Description
AS81_HOME	Path to the directory where Application Server 9.1 is installed. Default values: ■ Solaris systems: /opt/SUNWappserver/appserver ■ Linux and HP-UX systems: /opt/sun/appserver ■ Windows systems: *javaes-install-dir*/appserver *javaes-install-dir* represents the Java ES 5 installation directory. The default value is C:\Program Files\Sun\JavaES5.
AS81_PROTOCOL	Protocol used by the Application Server 9.1 instance: http or https. Default: Access Manager protocol variable (SERVER_PROTOCOL).
AS81_HOST	Fully qualified domain name (FQDN) on which the Application Server 9.1 instance listens for connections. Default: Access Manager host variable (SERVER_HOST)
AS81_PORT	Port on which Application Server 9.1 instance listens for connections. Default: Access Manager port number variable (SERVER_PORT).
AS81_ADMINPORT	Port on which the Application Server 9.1 administration server listens for connections. Default: 4848
AS81_ADMIN	User ID of the Application Server 9.1 administrator. Default: admin
AS81_ADMINPASSWD	Password for the Application Server 9.1 administrator. Default: Access Manager administrator password (ADMINPASSWD).

Variable	Description
AS81_INSTANCE	Name of the Application Server 9.1 instance on which the Access Manager SDK will be deployed. Default: server
AS81_DOMAIN	Name of the Application Server 9.1 domain in which the Application Server instance exists. Default: domain1
AS81_INSTANCE_DIR	Path to the directory where Application Server 9.1 stores its files for the instance. Default: ■ Solaris systems: /opt/SUNWappserver/domains/domain1 ■ Linux and HP-UX systems: /opt/sun/appserver/domains/domain1 ■ Windows systems: *javaes-install-dir*/appserver/domains/domain1 *javaes-install-dir* represents the Java ES 5 installation directory. The default value is C:\Program Files\Sun\JavaES5.
AS81_DOCS_DIR	Path to the directory where the Application Server 9.1 instance stores its files. Default: ■ Solaris systems: /opt/SUNWappserver/domains/domain1/docroot ■ Linux and HP-UX systems: /opt/sun/appserver/domains/domain1/docroot ■ Windows systems: *javaes-install-dir*/appserver/domains/domain1/docroot *javaes-install-dir* represents the Java ES 5 installation directory. The default value is C:\Program Files\Sun\JavaES5.
AS81_ADMIN_IS_SECURE	Specifies whether the Application Server 9.1 administration instance is using SSL: ■ true: Secure port is enabled (HTTPS protocol). ■ false: Secure port is not enabled (HTTP protocol). Default: true (enabled)

5 In the amsdk_configure file, set the following Directory Server variables:

Variable	Description
DIRECTORY_MODE	Directory Server mode. For example, specify DIRECTORY_MODE=4 for an existing multiple-server installation. For more information, see "Directory Server Configuration Variables" in *Sun Java System Access Manager 7.1 Postinstallation Guide*.
DS_HOST	Fully qualified server name where Directory Server is running.

Variable	Description
DS_PORT	Directory Server port. Default: 389.
DS_DIRMGRDN	Directory manager DN: user who has unrestricted access to Directory Server. Default: "cn=Directory Manager"
DS_DIRMGRPASSWD	Password for the directory manager.
AMLDAPUSERPASSWD	Password for amldapuser used for the full Access Manager 7.1 server installation. The AMLDAPUSERPASSWD value must be different from the amadmin password.
ROOT_SUFFIX	Root suffix of Directory Server.

6 **While running as `root`, run the `amconfig` script using the edited `amsdk_configure` file. For example, on Solaris systems with the Access Manager SDK installed in the default directory:**

```
# cd /opt/SUNWam/bin
# ./amconfig -s ./amsdk_configure
```

Note – On Windows systems, to configure Access Manager, run `amconfig.bat` with the `AMConfigurator.properties` file. These files are installed in the *javaes-install-dir*`\identity\setup` directory, where *javaes-install-dir* is the Java ES 5 installation directory. The default value is `C:\Program Files\Sun\JavaES5`.

7 **Stop and then restart the Application Server 9.1 instance.**

Next Steps After you have installed and configured the Access Manager 7.1 SDK, an application such as Portal Server can use the Access Manager SDK APIs to manage users and related information in the user branch of the identity repository. If you want to install and configure Portal Server 7.1, refer to the following documentation collection for more information:

`http://docs.sun.com/coll/1552.1`

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 820-3043.

Revision History

Version	Date	Description
820–3043–11	September 22, 2009	Revised for CR 6659499.
820–3043–10	September 18, 2007	Initial publication of this technical note.