Sun™ ONE Identity Server Service Pack 1 Release Notes

Version 6.0

Part Number 816-6844-10

June 2003

These release notes contain important information available at the time of release of Sun Open Network Environment (Sun ONE) Identity Server 6.0 Service Pack 1. New features and enhancements, known limitations and problems, technical notes, and other information are addressed here. Read this document before you begin using Identity Server 6.0 Service Pack 1.

The most up-to-date version of these release notes can be found at the Sun ONE documentation web site:

`http://docs.sun.com/db/coll/S1_IdServ_60`

Check the web site prior to installing and setting up your software and then periodically thereafter to view the most up-to-date release notes and manuals.

These release notes contain the following sections:

- Revision History
- What's New in Identity Server 6.0 Service Pack 1
- Hardware and Software Requirements
- Installation Notes
- Identity Server Documentation Updates
- Known Issues
- How to Report Problems and Provide Feedback
- Additional Sun Resources

Revision History

Table 1 Revision History

Date	Description of Changes
June 2, 2003	Initial release of these release notes.

What's New in Identity Server 6.0 Service Pack 1

The following sections lists the new features and the bugs that have been fixed in Service Pack 1. Additional information on some of the items listed in this section can be found in the Identity Server Documentation Updates section.

Federation Management

- Liberty 1.1 Support - The Liberty specification group published the final Liberty 1.1 specifications in January 2003. Identity Server 6.0 SP1 is fully compliant to the Liberty 1.1 specification and supports all of the defined profiles, such as Browser Artifact, WML Post, LECP, and so forth. SP1 also supports all of the profiles, as required by the "Static Confirmance Requirements," to act as a service provider as well as an identity provider. The primary change in Liberty 1.1 is Name Registration. Other minor changes include AuthContext, AuthnRequest, and the Logout Protocol.

Policy

- Support for includeType in policy definition
- Performance enhancements

SAML

- Support for DNS names in SAML circle of trust
- Improved load balancing feature
- Timeouts can be set for artifacts and assertions

Naming Service

- Failover support

Identity Server Console

- New option to disable automatic search for users
- New option to dynamically create the cn from the givenname and surname

Logging

- Support for Remote Logging

Bugs Fixed in Identity Server 6.0 Service Pack 1

Below is a short description of the most important bugs fixed in Identity Server 6.0 Service Pack 1. For complete list and detailed descriptions on known problems with Identity Server 6.0, please see the Identity Server 6.0 release notes at the following location:

```
http://docs.sun.com/source/816-6684-10/index.html
```

Table 2 Fixed Bugs in Identity Server 6.0 Service Pack 1

Bug Number	Description
4788486	smtp server port property incorrect in `AMConfig.properties`.
4785477	Changes to the policy configuration service are not dynamically applied to existing policies.
4787204	The password was stored in cleartext in Directory Server if basic authentication was used for the SAML trust relationship.
4789637	Certificates not published to the proper attribute in Directory Server
4702556	User search used different scope for simple and advanced searches.
4784279	Error received when creating a normal policy in a suborganization.
4787748	Unable to define referral policies for services with no defined resources.
4786584	Logout does not work with multiple Identity Server instances.
4816388	Port 80 issue in Federation Management code.
4825448	Prelogin service missing URL encoding of LRURL.
4837673	Authentication unable to create users with attributes from an external Directory Server.

Hardware and Software Requirements

The following hardware and software are required for Identity Server 6.0, which must be installed prior to installing Service Pack 1.

Table 3 Hardware and Software Requirements

Component	Solaris Requirement
Operating system	Solaris 8 or Solaris 9 (SPARC® platforms)
CPU	Sun Ultra™ 1 (or compatible) workstation
RAM	256 Mbytes
Disk space	200 Mbytes for Identity Server and associated applications

Installation Notes

This section provides installation instructions for Identity Server Service Pack 1. This service pack is available on Solaris only, and it is in the same format of a regular Solaris patch.

Make sure that you have installed Sun ONE Identity Server version 6.0. Installation instructions are available here:

`http://docs.sun.com/db/coll/S1_IdServ_60`

To install Identity Server SP1:

1. Download the patch, 114772-01.tar.Z from the following location:

   `http://www.sun.com/software/download/inter_ecom.html`

2. Use the following command to decompress and untar the file:

   ```
   uncompress -c 114772-01.tar.Z | tar xf -
   ```

3. Use the following command to install the file:

   ```
   patchadd 114772-01
   ```

4. You will prompted to read the License Agreement. Enter Yes

5. Enter the Directory Manager DN and the password.
6. Change the permissions for the following files:

   `AMConfig.properties` should have read / write permission

   `LogConfig.properties` should have read permission

   Use the following command:

   ```
   chmod 600 AMConfig.properties
   chmod 400 LogConfig.properties
   ```

   Additionally, the ownership of these files might have to be changed to the original owner if Identity Server was not installed as root. To ensure that the ownership of these files match the original Identity Server 6.0 ownership, search for `NEW_OWNER` and `NEW_GROUP` in the following location:

   ```
   /var/sadm/pkg/SUNWamsdk/pkginfo
   ```

   Restart the server.

Identity Server Documentation Updates

This section describes information pertaining to new features in the Identity Server 6.0 SP1 release for the following functional areas:

- Authentication
- Policy
- SAML
- Naming Service
- Undocumented Parameters in the AMConfig.Properties File
- Remote Logging Capabilities

Authentication

"No such domain" Error When Logging Into Orgs With No Configured Authentication Modules (#4845832)

If a user tries to login to an organization with no authentication modules configured, the "No such domain" error message is displayed in the login page. This is the expected behavior. Services must be configured under the organization for the authentication module to be able to recognize the organization to which the user is attempting a login.

"Authentication Failed" Error Expected Behavior (#4842579)

During authentication, when you get an error and then click on the Return To Login link in the error page, you may see that the error page is generated in repetition. This indicates that the Return To Login link contains the originally accessed login URL with the original query parameters. This is expected behavior.

In such a case, the user must remove the query parameters from the Login URL and login to the default organization with the following URL:

```
http://serverhost:port/amserver/UI/login
```

Policy

Policy Supports includeType In policy Definition

When you define a policy with a subject, the policy applies members of that subject. For example, if you define a policy with a manager role subject, it would apply to each one that has manager role defined. This is called inclusion; members of the subject are included for policy evaluation.

In 6.0 SP1, a new feature has been added so that you can define it in such a way that the policy would apply if it is not a member of a subject. This is called subject exclusion. You can select, `exclude` for each subject you add in the console while adding the subject. By default, the exclude is set to false, meaning that the policy applies to those that belong to the subject.

Similarly, you can specify the `inlcudeType` flag, while importing the policies through the `amadmin` command line utility. `inclusive` and `exclusive` are the possible values for this flag. By default, `inclusive` is selected for this value. For the exact syntax and type of this flag, refer to `amAdmin.dtd` after you install Service Pack 1.

When multiple subjects are defined in a policy, there is an OR relationship among multiple subjects. The policy applies to those that are members of one of the subjects defined in the policy. This is true even when one of the subjects defines exclusion. In such a case, the policy applies to those that are members of one of the include type subjects, or that are not a member of one of the exclude type subjects.

SAML

DNS Name Support In SAML Circle Of Trust

The hostlist in the SAML Trusted Partner Sites can now support both IP addresses and DNS hostnames. When a DNS hostname is used, the host to IP resolution can be cached using JVM inetaddress' caching mechanism.

Specifically, for JDK1.3, there is a new JVM option, `sun.net.inetaddr.ttl`. If the value is set to -1, then it means that it will always cache (default). If the value is 0, it means that no caching will occur. Any positive value, such as 10, means that the cache will be kept for 10 seconds.

For JDK1.4, set the key `networkaddress.cache.ttl` key in `java.security` instead.

Improved Load Balancing Feature

Identity Server 6.0 SP1 allows the same host (IP address or hostname) to exist in different entries of an Identity Sever Trusted Partner Site. Each entry must have a unique sourceid. The first found siteid is no longer retrieved. The matching siteid is retrieved.

Timeouts Can Be Set For Artifacts And Assertions

In Identity Server 6.0SP1, both artifacts and assertions have their own timeouts which can be configured through the SAML service in the Service Configuration module in the Identity Server console.

A new flag, `com.sun.identity.saml.removeassersion`, located in `AMConfig.properties` can be used to optionally delete an assertion when the related artifact is dereferenced. The default value is false, which means that the assertion is not deleted when its related artifact is dereferenced. The assertion stays in the memory until it times out. It will be removed when the next assertion / artifact clean up thread runs.

When an artifact times out, it will be removed from memory when the next cleanup thread runs. If the `removeassertion` flag is set to true, then its related assertion will also be removed.

When an artifact is dereferenced, it will be removed from memory. If the `removeassertion` flag is set to true, then its related assertion will be removed as well. This flag is used only when an assertion is associated with an artifact. When an assertion is created from a query, it will be removed from memory when it times out.

Naming Service

Naming Service Supports Failover

The Naming service now supports failover using multiple naming service URLs specified in the `AMConfig.properties` file, under the `com.iplanet.am.naming.url` key. This feature is designed for use in the client installations of the Identity Server SDK, where the naming failover support may be necessary. More than one naming service URLs may be specified for this property as a space-separated list.

The newly introduced `com.iplanet.am.naming.polling.interval` property specifies the polling interval in which the naming service client will poll to test the availability of the specified naming service URLs. This property does not take effect unless there are more than one naming service URLs specified in the `com.iplanet.am.naming.url` property.

The `com.iplanet.am.naming.failover.url` property has been removed from the `AMConfig.properties` file and is no longer needed, as the same functionality is available using the multiple URLs specified for the `com.iplanet.am.naming.url` property.

Undocumented Parameters in the AMConfig.Properties File

The following `AMConfig.properties` file parameters were not exposed, nor were they documented in the Identity Server 6.0 version of the *Programmer's Guide*:

Web Container Cookie Processing (#476144)

com.iplanet.am.cookie.encode

This parameter enables Identity Server to perform URL encoding and decoding before a cookie is sent to a browser and after the cookie is received from a browser, respectively. Web containers have different methods for processing cookies. For example, Sun ONE Web Server performs URL encoding before sending a cookie to a browser, but Weblogic and Webshpere do not perform any URL encoding. When set to `true` (the default is `false`), this parameter makes cookie processing consistent.

NOTE This parameter must be set to `true` for Webshpere and Weblogic. This parameter must be set to `false` for Sun One Webserver and Sun One Application Server.

ApprovalCallback (#4836401)

The following parameters have to be configured when Directory Server is installed with a certificate that has a `cn` of a different Directory Server hostname:

com.iplanet.am.jssproxy.checkSubjectAltName

If set to `true` (default), this parameter enables ApprovalCallback to check for any alternative names in `SunjectAlNamesExtension` that match the configured Directory Server name. If a matched name is found, SSL handshaking continues.

com.iplanet.am.jssproxy.resolveIPAddress

If set to `true` (default), this parameter enables ApprovalCallback to check that the matching names found from the `com.iplanet.jssproxy.checkSubjectAltName` parameter are pointing to the same IP Address. If the names are pointing to the same address, SSL handshaking continues.

Notification Handling

com.iplanet.am.notification.threadpool.size

This parameter is used for the session thread pool for notification handling. It specifies the size of the pool and total number of threads in the pool.

com.iplanet.am.notification.threadpool.threshold

This parameter is used for the session thread pool for notification handling. It specifies the maximum task queue length of the pool. The purpose of this parameter is to prevent the system from being over-loaded by notifications. If the number of unprocessed notification tasks reaches the value specified in this parameter, no additional notification tasks will be accepted until there are vacancies in the task queue.

Console Parameters

The following parameters are new to Identity Server Service Pack 1 and apply to the functionality of the Identity Server console:

com.iplanet.am.console.display.off

If you specify this attribute in `AMconfig.properties`, Identity Server will not perform the initial search, at the time of login, for a given identity object. For example, if you have a large number of users, setting this option for users will drastically reduce the time it takes to load the Identity Server interface. You can disable the search for users, organizations, roles, groups, policies, organizational units, people containers and group containers with the following syntax:

```
com.iplanet.am.console.display.off=orgs,users,groups,...
```

com.iplanet.am.console.set.cn

If you specify this attribute in `AMconfig.properties`, Identity Server will automatically generate a user CN based on the information entered in the First Name, Initial and Last Name fields in the user profile page. The default is set to false, which will not dynamically create the user CN. To enable this feature, add the following parameter:

```
com.iplanet.am.console.set.cn=true
```

Remote Logging Capabilities

Identity Server 6.0 SP1 supports remote logging. This enables a client using the Identity Server SDK to create log records on an Identity Server instance executing on a remote machine. This section contains information on enabling this feature.

Enabling Remote Logging

To enable remote logging, see the following steps:

1. Specify the properties file as a new environment variable to the JVM (Java Virtual Machine).

   ```
   -Djava.util.logging.manager=com.sun.identity.log.LogManager
   ```

   ```
   -Djava.util.logging.config.file=/<IS-Root>/SUNwam/lib/LogConfig.properties
   ```

2. Make sure that the following parameters are configured in the properties file:

   ```
   iplanet-am-logging-remote-handler=com.sun.identity.log.handlers.RemoteHandler
   ```

   ```
   iplanet-am-logging-remote-formatter=com.sun.identity.log.handlers.RemoteFormatter
   ```

   ```
   iplanet-am-logging-remote-buffer-size=1
   ```

3. The SSO Token is needed for the `logrec` and `log` interfaces. The SSO Token passed in to the `logRecord` constructor is used to populate following log fields.

   - Domain
   - IPAddr
   - HostName
   - LoginID

   The SSO Token passed during log request (`logger.log(logRecord, ssoToken)`) is used to authorize the user.The user can only log with a valid SSO Token.

logrec Buffering and Flushing

Remote Logging supports buffering on the basis of the number of log records. Once the buffer is full with the specified number of records, all records will be flushed to the server.

Logging Javadocs

The following section provides sample Java invocation and properties files for the Logging Javadocs.

If the JDK 1.4, or later, version is used and `SUNWamsdk` installation location is `/opt`:

```
java -cp

/opt/SUNWam/lib/am_logging.jar:/opt/SUNWam/lib/xercesImpl.jar:
/opt/SUNWam/lib/xmlParserAPIs.jar:/opt/SUNWam/lib/jaas.jar:/opt/SUNWam/lib
/xmlParserAPIs.jar:/opt/SUNWam/lib/servlet.jar:/opt
/SUNWam/locale:/opt/SUNWam/lib/am_services.jar:/opt/SUNWam/lib
/am_sdk.jar:/opt/SUNWam/lib/jss311.jar:/opt/SUNWam/lib:

-Djava.util.logging.manager=com.sun.identity.log.LogManager

-Djava.util.logging.config.file=/opt/SUNwam/lib/LogConfig.properties
<logTestClass>
```

If using an earlier version than JDK 1.4 and `SUNWamsdk` install location is `/opt`:

```
java -Xbootclasspath/a:/opt/SUNWam/lib/jdk_logging.jar -cp

/opt/SUNWam/lib/am_logging.jar:/opt/SUNWam/lib/xercesImpl.jar:
/opt/SUNWam/lib/xmlParserAPIs.jar:/opt/SUNWam/lib/jaas.jar:/opt
/SUNWam/lib/xmlParserAPIs.jar:/opt/SUNWam/lib/servlet.jar:/opt
/SUNWam/locale:/opt/SUNWam/lib/am_services.jar:/opt/SUNWam/lib
/am_sdk.jar:/opt/SUNWam/lib/jss311.jar:/opt/SUNWam/lib:

Djava.util.logging.manager=com.sun.identity.log.LogManager

Djava.util.logging.config.file=/opt/SUNwam/lib/LogConfig.properties
<logTestClass>
```

Known Issues

This section contains a list of the more important known issues at the time of the Identity Server 6.0 Service Pack 1 release for the following functional areas:

- General
- Identity Server Console

- Authentication
- Policy
- Logging
- Migration
- Federation
- Performance

General

Permission/Ownership Change Required for AMConfig.properties and LogConfig.properties

After Identity Server Service Pack 1 is installed, the patched files' permissions and ownership are changed to become root. `AMConfig.properties` and `LogConfig.properties` contain credential data and must be changed back to the original permission and ownership status. See "Installation Notes" on page 4 for more information.

Security Vulnerability In TLS Block Ciphers (#4860088)

If you have Sun ONE Webserver 6.0sp5 installed with Identity Server 6.0, there is a security vulnerability in TLS block ciphers.

To learn more on this vulnerability, see the following URL:

http://www.mozilla.org/projects/security/pki/nss/news/vaudenay-cbc.html

Workaround

To correct this problem, disable TLS or disable the following ciphers:

- Fortezza with 80 bit encryption and SHA message authentication
- DES with 56 bit encryption and SHA message authentication
- RC2 with 40 bit encryption and MD5 message authentication
- (FIPS) Triple DES with 168 bit encryption and SHA message authentication
- (FIPS) DES with 56 bit encryption and SHA message authentication
- Triple DES with 168 bit encryption and SHA message authentication

To Disable TLS or disable the ciphers listed above:

1. Login to the Admin server and click on the instance to be managed.
2. Click on Preferences and select Edit | listen sockets.

3. Click on the attributes for the listen sockets.
4. Click on SSL2 and SSL3/TLS to disable TLS or any of the ciphers mentioned above.

Identity Server Console

Self Registration Feature May Not Work With Invalid Value In Required Service (#4866467)

If you enter an invalid value (such as `test service`), or a subconfig instance, in the Required Services attribute (located in the Administration service), Self Registration will not function. Please enter only valid values (such as `iplanetamauthconfiguration`), or use the default (blank) value.

Authentication

Security Risk in Identity Server In Persistent Cookie Mode (#4786616)

There is a security risk with the default encryption key (DES key) when running Identity Server in Persistent Cookie mode. To fix this problem, you must change the default DES key before running the server in Persistent Cookie mode.

Workaround

The following are the steps to configure or change the DES key:

NOTE If RemoteSDK is installed, follow the directions in this workaround, making sure to copy the DES key that is already generated. The keys should be the same in RemoteSDK and in the server.

1. Make sure the permission and ownership status for `AMConfig.properties` and `LogConfig.properties` are correct. See "Installation Notes" on page 4 for more information.
2. Edit the file `AMConfig.properties` file and add the `am.encryption.pwd` property with the new DES key. For example:

   ```
   am.encryption.pwd=UnWR1MYWDYW4xuqdF5nbm+CXIyOVt
   ```
3. Generate the encoded password for `amldapuser` with the new key and replace it in the directory.

a. Run the ampassword utility with the encode option with the old amldapuser password. This will give you password which is encoded with the new DES key. For example:

```
ampassword -e 12345678
```

```
output : stf4ewqfsdfds89323043r5433443
```

b. Replace the ldapbinddnpwd with this new password in the directory, to replace this password open the directory console and go to the following location:

```
dc=iplanet,dc=com->ou=services->iPlanetAMAuthLdapService->1.0->Organiza
tionConfig->default
```

Look for iplanet-am-auth-ldap-bind-passwd in sunkeyvalue and change it with the newly created password.

4. Generate the encoded password for dsameuser and puser and replace it in serverconfig.xml.

   a. Generate the password for dsameuser. For example:

   ```
   ampassword -e admin123
   ```

   ```
   output: sadfjdksflsdkfjdsfjsdjfkldsjfsdfdsfds
   ```

   b. Replace this password in the following file:

   ```
   /install-dir/SUNWam/config/ums/serverconfig.xml
   ```

   c. Generate the password for puser by repeating the procedure described above.

5. Modify the dsameuser and puser passwords in the directory server.

   a. Modify dsamuser in the directory using the ampassword utility. For example:

   ```
   ampassword -a -o admin123 -n netscape
   ```

   b. Repeat the procedure to modify puser password.

6. Restart the server and login to the console.

Policy

Policy Agent May Deny Access To A Resource (#4863448)

The policy agent may deny access to a resource even if it is allowed by the policy. This problem exists in Identity Server 6.0, however it may happen more frequently when Service Pack 1 is applied. The problem occurs because of performance enhancement fixes.

Workaround

Define the Subject Time To Live attribute in the Policy Configuration service to be higher than the value in the user's Maximum Session Timeout attribute. (Both of these attributes specify time in minutes.) The user's Maximum Session Timeout can be set by modifying the attribute in the Session service assigned to the organization, role or the user.

If the session service is not assigned explicitly, the Subject Time To Live can be set higher than the default session maximum timeout, which is 120 minutes.

Note that the Subject Time To Live needs to be slightly higher than the session time out (for example, 5 minutes) to overcome this problem. This change needs to be applied in all of the organizations where Policy Configuration service is defined.

Loading Multiple Policies With amadmin

(#4869446)

If you would like to simultaneously add multiple policies using the `amadmin` command utility, place all of the policies in one XML file, instead of have having each policy in it's own XML file. If you load policies using amadmin with multiple XML files in quick succession, the policy index used internally by policy the framework may become corrupt and some policies may not participate in policy evaluation.

Logging

Link To Logging Javadocs (#4847614)

The logging Javadocs only document inherited classes. To locate the Javadocs that describe the classes for JDK 1.4, see the following URLs:

```
http://java.sun.com/j2se/1.4.1/docs/guide/util/logging/index.html
http://java.sun.com/j2se/1.4.1/docs/api/java/util/logging/package-frame.html
http://java.sun.com/j2se/1.4.1/docs/api/index.html
```

Migration

5.1 to 6.0 Migration Scripts Not Case Sensitive (#4849890)

Service Pack 1 requires you to have first installed Identity Server 6.0. Please note that if you migrate Identity Server 5.1 data to Identity Server 6.0, the migration scripts are not case sensitive to the attribute / objectclass values. This could result in data loss.

Federation

Incorrect Authentication Redirect For Identity Provider Login (#4845490)

If you configure the Authentication Level for an Identity Provider (for example, authlevel=2 for the Unix Authentication module), the accessing page will redirect you to the LDAP login page, instead of the Unix login page.

Workaround

In `amprovider.xml`, update the `level` parameter to `authlevel` in the `module-indicator-key`. Use `amadmin` to change this attribute schema. This will be consistent with the key used for the authentication.

Login Fails From An Identity Provider When AuthenticationType = Remote (#4839921)

In Identity Server 6.0 SP1, if you set up an identity provider as Remote and then attempt to login to that identity provider, you will receive an error message that reads, "IDP not configured," and you will be unable to successfully login.

Performance

Web Server Requires libmtmalloc, Which Requires Solaris Patch 111308 (#4803350)

Due to memory allocation problems, the policy agents were experiencing slow performance. To fix this problem, we recommend using `libmtmalloc` with Sun ONE Web Server to improve overall performance.

However, the `libmtmalloc` on Solaris 8 originally contained a bug. To fix this problem, it must be patched with patch number 111308, as it provides a fix to `libmtmalloc`. You can locate the patch at the following URL (you can search for the patch number):

```
        http://sunsolve.sun.com
```

After the patch is applied, the Web Server can be started with `libmtmalloc` by doing `LD_PRELOAD`.

To verify that the Web Server is indeed using `libmtmalloc` use the following command to verify the list of shared objects being used by the process:

```
pldd <pid>
```

Make sure this list contains `/usr/lib/libmtmalloc.so`

How to Report Problems and Provide Feedback

If you have problems with Sun ONE Identity Server, contact Sun customer support using one of the following mechanisms:

- Sun Software Support services online at
  http://www.sun.com/service/sunone/software

  This site has links to the Knowledge Base, Online Support Center, and ProductTracker, as well as to maintenance programs and support contact numbers.

- The telephone dispatch number associated with your maintenance contract

So that we can best assist you in resolving problems, please have the following information available when you contact support:

- Description of the problem, including the situation where the problem occurs and its impact on your operation
- Machine type, operating system version, and product version, including any patches and other software that might be affecting the problem
- Detailed steps on the methods you have used to reproduce the problem
- Any error logs or core dumps

Sun Welcomes Your Comments

Sun is interested in improving its documentation and welcomes your comments and suggestions. Email your comments to Sun at this address:

docfeedback@sun.com

Please include the part number (816-6844-10) of the document in the subject line and the book title (*Identity Server 6.0 Service Pack 1 Release Notes*) in the body of your email.

Additional Sun Resources

Useful Sun ONE information can be found at the following Internet locations:

- Documentation for Identity Server 6.0
  http://docs.sun.com/coll/S1_IdServ_60
- Sun ONE Documentation
  http://docs.sun.com/prod/sunone
- Sun ONE Professional Services
  http://www.sun.com/service/sunps/sunone
- Sun ONE Software Products and Service
  http://www.sun.com/software
- Sun ONE Software Support Services
  http://www.sun.com/service/sunone/software
- Sun ONE Support and Knowledge Base
  http://www.sun.com/service/support/software
- Sun Support and Training Services
  http://www.sun.com/supportraining
- Sun ONE Consulting and Professional Services
  http://www.sun.com/service/sunps/sunone
- Sun ONE Developer Information
  http://sunonedev.sun.com
- Sun Developer Support Services
  http://www.sun.com/developers/support
- Sun ONE Software Training
  http://www.sun.com/software/training
- Sun Software Data Sheets
  http://wwws.sun.com/software