Getting Started

Sun™ ONE Identity Server

Version 6.0

December 2002
816-6388-10

Getting Started

This Getting Started guide provides instructions for an administrator installing and configuring the Sun™ One Identity Server software for the first time. This document contains the following sections:

- About This Guide
- Installing Identity Server
- Configuring Identity Server Entries
- Testing The Configurations
- Additional Sample Configurations

About This Guide

The Getting Started guide contains instructions to walk an administrator through the installation and deployment of Sun ONE Identity Server. This guide is not meant to provide a comprehensive review of all Identity Server features or even the Identity Server architecture. This use case is for illustrative purposes only, and is one of many possible applications of the technology.

Case Overview

The following Identity Server functionality will be featured in this use case.

- Installation of Identity Server 6.0 on an UltraSparc machine running the Solaris 8 operating environment with the latest patch set against a fresh installation of Sun ONE Directory Server 5.1sp1.
- Use of the Identity Server console.
- Identity management including creating and modifying groups and users.
- Policy management including creating referral and normal policies.
- Delegated administration including applying default roles and ACIs.
- Self-registration and management of user profiles.

NOTE Although fashioned for a Solaris machine, the steps in this document can be easily applied to the Windows® version of Identity Server. Some translation of directory paths and file locations may be required first. For example, the installation directory on a machine running the Solaris™ operating environment is <identity_server_root> / SUNWam; the same directory on a machine running Windows 2000 is <identity_server_root>.

Case Entries

To illustrate the configuration of the Identity Server, the following directory tree will be used. The top-level organization is MadisonParc which contains two sales offices, one in the east and one in the west. These offices will be configured as sub-organizations, o=salesofficeeast and o=salesofficewest. Each office has two sales persons.

Code Example 0-1 The MadisonParc Directory Tree

```
dc=MadisonParc,dc=com
  cn=SalesAdminRole
  ou=People
    uid=eastsalesmanager
    uid=westsalesmanager
  ou=Groups
    cn=salesmanagergroup
  o=SalesOfficeEast
    cn=EastSalesAdminRole (OrganizationAdminRole)
    ou=People
      uid=eastsalesperson1
      uid=eastsalesperson2
    ou=Groups
      cn=salesinfogroup
  o=SalesOfficeWest
    cn=WestSalesAdminRole (OrganizationAdminRole)
```

Code Example 0-1 The MadisonParc Directory Tree *(Continued)*

```
ou=People
  uid=westsalesperson1
  uid=westsalesperson2
```

Installing Identity Server

Before beginning the installation process, ensure that root permissions is enabled on the machine where Identity Server will be installed. This installation assumes the availability of an UltraSparc® server running the Solaris 8 operating environment with the latest patch set. Identity Server 6.0, Directory Server 5.1sp1 and Sun ONE Web Server 6.0sp5 will be installed and deployed on this one machine.

Before Installation

- Ensure that the DNS domain name for the machine is set and all currently running applications are closed for the installation.
- Allow the machine on which Identity Server is being installed to display a remote application (in this case, the installer itself) by opening a terminal window and typing `xhost <cdservername>`.

  If x-hosting is not an option the comand line install should be used.
- Set the `DISPLAY` variable for the shell that is running using one of the following commands:
  - For the `csh` or `tcsh` shell, type `setenv DISPLAY <server.domain.com>:0.0`.
  - For the `sh`, `ksh` or `bash` shell, type `export DISPLAY=<server.domain.com>:0.0`.

Installation Procedures

The following instructions will install Identity Server 6.0, Directory Server 5.1sp1 and Web Server 6.0sp5 on a server named sparcserver.example.com. Ensure that the information in these instructions is replaced with information particular to your deployment. More in-depth installation instructions can be found in the *Sun ONE Identity Server Installation and Configuration Guide.*

1. Insert the Identity Server CD into the disc drive of the system on which the Identity Server and Directory Server will be installed.
2. Open a terminal window and change to the directory where the Setup program is located.

   ```
   cd /cdrom/is60/solaris
   ```

3. Type `./setup` to run the installation program.

   The installation program opens with a Welcome panel.

4. Click Next to proceed to the Software License Agreement.

   To continue with the installation process, the Software License Agreement must be accepted by clicking Yes (Accept License). Declining the Software License Agreement by clicking No will close the installation program.

5. Assuming acceptance of the Software License Agreement, in the next panel, specify the directory into which Identity Server will be installed and click Next.

   The default directory is `/opt`. Identity Server automatically installs in a directory named `SUNWam`. Plan to install the Identity Server and Directory Server products in different directories.

6. Select Sun ONE Identity Server Management and Policy Services and click Next.

   This option includes installation of Identity Server 6.0, Directory Server 5.1sp1, Web Server 6.0sp5, the Identity Server console, Common Domain Services, and JDK 1.3.1_06.

7. Select No to using a custom Java SDK and click Next.
8. Configure the Web Server by accepting the default information and/or providing custom information and click Next.

   Administrator: admin

   Port: 58888

   Password: password

Confirm Password: password

Enter user to run server as: nobody

Enter group to run this server as: nobody

NOTE Passwords must be a minimum of eight characters in length.

9. Provide additional configuration information for the Web Server by accepting the default information and/or providing custom information and click Next.

   Host: This field should contain the correct fully qualified domain name of the computer where the Identity Server components and a dedicated Web Server will be installed.

   Port: 58080

   Services Deployment URI: amserver

   Common Domain Deployment URI: common

   Deploy console with this service? Check this box.

   Console Deployment URI: amconsole

10. Choose to install a new Directory Server and click Next.

11. Type `dc=madisonparc,dc=com` as the root for the new Directory Server tree and click Next.

12. Configure the Directory Server by accepting the default information and/or providing custom information and click Next.

    Host: This field should contain the correct fully qualified domain name of the computer where the Directory Server will be installed.

    Port: 389

    Installation Directory: The default directory `/usr/iplanet/servers`. The directory used should be empty of other products, directories and/or files.

    Directory Manager: cn=Directory Manager

    Password: password

    Confirm Password: password

NOTE Passwords must be a minimum of eight characters in length.

13. Configure the Administration Server by accepting the default information and / or providing custom information and click Next.

    Administrator: admin

    Port: 58900

    Password: password

    Confirm Password: password

14. Provide a password for the LDAP Auththentication User (`amldapuser`).

    This password (a minimum of eight characters in length) must be different from the one chosen for amAdmin in Step 15.

15. Provide a password for the Top Level Administrator (`amAdmin`), choose to start the server after installation and click Next.

    This password (also a minimum of eight characters in length) must be different from the one chosen for amldapuser in Step 14.

16. Review the configuration information and click Next to proceed.

    Changes can be made by clicking Back until the desired panel is reached.

17. Review the information and click Install Now to begin the installation.

    Changes can still be made by clicking Back until the desired panel is reached.

18. Click Details for a detailed summary of the configuration information processed during installation and / or click Exit to end the program.

Logging Into Identity Server Console

The Authentication Service's graphical user interface (GUI) is the entry point for the Identity Server console. In order to log in to the Identity Server console, type the configured URI (`http://sparcserver.example.com:58080/amconsole`) in a web browser location window and authenticate to the Identity Server using `amadmin`, the top-level administrator user name and corresponding password specified during installation.

Configuring Identity Server Entries

Now that the Identity Server is installed and the top-level administrator is logged in, the case entries must be configured. The top-level organization of the directory tree was configured as dc=madisonparc,dc=com during the installation process; each of the other entries will be created on a sub-level of dc=madisonparc,dc=com.

Creating The Sales Sub-Organizations

Using the Identity Management module, this procedure will create two sub-organizations of the top-level MadisonParc, SalesOfficeEast and SalesOfficeWest.

1. Select Organizations from the View drop down menu in the left frame of the console and click New....
2. Enter the following information in the right frame of the console and click Create.

   Name: SalesOfficeEast

   Organization Status: Active
3. Repeat these steps to configure the sub-organization SalesOfficeWest using the following information.

   Name: SalesOfficeWest

   Organization Status: Active

Adding Employees To The Sub-Organizations

Using the Identity Management module, this procedure will create sales people in the SalesOfficeEast and SalesOfficeWest sub-organizations.

1. If not already there, click on the hyperlinked name MadisonParc in the left frame of the console and select Organizations from the View drop down menu.
2. Click on the hyperlinked name of the new sub-organization SalesOfficeEast.
3. Select Users from the View drop down menu and click New....
4. Enter the following information in the right frame of the console and click Create.

   UserId: eastsalesperson1

First Name: Jim

Last Name: Deer

Full Name: Jim Deer

Password: 11111111

Confirm Password: 11111111

User Status: Active

5. Click New... in the left frame to configure a second sales person for SalesOfficeEast using the following information and click Create.

   UserId: eastsalesperson2

   First Name: Jane

   Last Name: Doe

   Full Name: Jane Doe

   Password: 11111111

   Confirm Password: 11111111

   User Status: Active

6. Repeat these steps to create sales people in the SalesOfficeWest sub-organization using the following user profiles:

   User Profile One

   UserId: westsalesperson2

   First Name: John

   Last Name: Hand

   Full Name: John Hand

   Password: 11111111

   Confirm Password: 11111111

   User Status: Active

   User Profile Two

   UserId: westsalesperson2

   First Name: Joanne

Last Name: Head

Full Name: Joanne Head

Password: 11111111

Confirm Password: 11111111

User Status: Active

Creating Managers For The Sub-Organizations

Using the Identity Management module, this procedure creates users that will serve as managers for the configured sales sub-organizations.

1. If not already there, click on the hyperlinked name MadisonParc in the left frame of the console.
2. Select Users from the View drop down menu in the left frame and click New....
3. Enter the following information in the right frame and click Create.

   UserId: eastsalesmanager

   First Name: Jim

   Last Name: Lake

   Full Name: Jim Lake

   Password: 11111111

   Confirm Password: 11111111

   User Status: Active
4. Repeat these steps to create a second sales manager for SalesOfficeWest using the following information.

   UserId: westsalesmanager

   First Name: Joan

   Last Name: River

   Full Name: Joan River

   Password: 11111111

   Confirm Password: 11111111

User Status: Active

Creating Groups

Identities can be grouped in two different group types. Using the Identity Management module, the following procedures will create a group of each type, one dynamic and one static.

Creating A Membership By Filter Group

This procedure creates a group with membership determined by a filter. The configured filter selects the member entries and dynamically assigns them to the group. Group members are determined each time the filter is run. The filter below will determine all identities with a User ID that includes the word *manager*. It can be used to assign access rights to managers only.

1. If not already there, click on the hyperlinked name MadisonParc in the left frame of the console and select Groups from the View drop down menu.
2. Click New..., define the New Group in the right frame by entering the following information and click Next.

   Type Of Group: Membership By Filter

   Group Name: SalesManagerGroup
3. Configure the filter that determines group membership using the following information and click Create.

   Logical Operator: And

   User Status: Active

   UserId: *manager

NOTE Selecting Users from the View drop down menu in the right frame will run the filter and configure a list of all group members.

Creating A Membership By Subscription Group

This procedure creates a group with membership determined by subscription. The configured filter selects the member entries and assigns them to the group at the time the filter is run. Any new member must subscribe to the group after the filter is run. The filter below will determine all identities with a first name *Jim*. This type of group can be used to configure an email alias for sales persons interested in trading general sales information.

1. If not already there, click on the hyperlinked name MadisonParc in the left frame of the console and select Organizations from the View drop down menu.
2. Click on the hyperlinked name SalesOfficeEast and select Groups from the View drop down menu.
3. Click New..., define the New Group in the right frame using the following information and click Next.

   Type Of Group: Membership By Subscription

   Group Name: SalesInfoGroup
4. Click Add under the Member List field, configure the filter using the following information and click Filter to search for users that meet the filter's criteria.

   Logical Operator: And

   User Status: Active

   First Name: Jim
5. Select eastsalesperson1 from the list of Available Users and click Submit.
6. Check Users Can Subscribe To This Group and click Create to create the group.

NOTE Future members of the group will need to subscribe themselves. Information on how to do this can be found in the *Sun ONE Identity Server Administration Guide*.

Assigning The Groups' Administrator Roles

Group administrator roles with read and write access to all members of the groups are automatically created when a group is created. Thus, in "Creating Groups," on page 12, two group administrator roles were created. These roles can now be assigned to the users chosen as each group's administrator.

1. If not already there, click on the hyperlinked name MadisonParc in the left frame of the console and select Roles from the View drop down menu.
2. Click the properties arrow icon next to SalesManagerGroup Admin.
3. Select Users from the View drop down menu in the right frame and click Add.
4. Configure the filter using the following information and click Filter to search for users that meet the filter's criteria.

   Logical Operator: And

   UserId: *manager
5. Select eastsalesmanager from the list of Available Users and click Submit to assign the SalesManagerGroup Admin role to Jim Lake.
6. Select Organizations from the View drop down menu, click on the hyperlinked name SalesOfficeEast and select Roles from the View drop down menu.
7. Click the properties arrow icon next to SalesInfoGroup Admin.
8. Configure the filter using the following information and click Filter to search for users that meet the filter's criteria.

   Logical Operator: And

   First Name: Jim
9. Select eastsalesperson1 from the list of Available Users and click Submit to assign the SalesInfoGroup Admin role to Jim Deer.

Creating An Access Policy

Privileges defined in normal policies can be assigned to users. To create a normal policy for a sub-organization, a referral policy must first be created in the top-level organization. Referral policies, in effect, allow the sub-organization to create a normal policy. Once a referral policy is configured, the normal policy can be created in the sub-organization to which the referral points. The following procedures will create a policy to allow access to http://sparcserver.example.com:<port>/test.html if the user is a registered member of the SalesInfoGroup and if the user successfully authenticates via LDAP between Monday and Friday from the domain, <example.com>.

NOTE In order for this policy to work, sparcserver.example.com:<port> in the resource URL must be modified to reflect a live resource.

Registering The Policy Configuration Service

By default, the Policy Configuration service is registered and a template created for MadisonParc, the top-level organization, when Identity Server is installed. Because this policy will affect a group in the SalesOfficeEast sub-organization, the Policy Configuration service must also be registered to it. This procedure registers the service to SalesOfficeEast using the Identity Management module.

1. If not already there, click on the hyperlinked name MadisonParc in the left frame of the console and select Organizations from the View drop down menu.
2. Click on the hyperlinked name SalesOfficeEast, select Services from the View drop down menu and click Register....
3. In the right frame, select the Policy Configuration service and click Register.
4. In the left frame, click the Show Properties arrow icon icon next to Policy Configuration.
5. Click Create in the right frame to create the service template.
6. Click Save to save the template for SalesOfficeEast.

NOTE After completing these steps, enter and confirm the LDAP Bind Password created in Step 14 on page 8 in the Policy Configuration service template and click Save.

Registering The Authentication Configuration Service

The Authentication Configuration service must also be registered (and a service template created for the sub-organization) in order to define conditions for the normal policy. This procedure registers the service to both MadisonParc and SalesOfficeEast using the Identity Management module.

1. If not already there, click on the hyperlinked name MadisonParc in the left frame of the console, select Services from the View drop down menu and click Register.
2. In the right frame, select the Authentication Configuration service and click Register.
3. Select Organizations from the View drop down menu in the left frame of the console.
4. Click on the hyperlinked name SalesOfficeEast, select Services from the View drop down menu and click Register....

5. In the right frame, select the Authentication Configuration service and click Register.
6. In the left frame, click the Show Properties arrow icon icon next to Authentication Configuration.
7. Click New... in the right frame to create a new service instance.
8. Enter the following information and click Create to create a new service instance.

   Instance Name: PolicyInstance

Registering The Core And LDAP Authentication Services

By default, the Core and LDAP Authentication services are registered and a template created (for the top-level organization only) when Identity Server is installed. Because this policy will affect a group in the SalesOfficeEast sub-organization, both services must also be registered to it. This procedure registers them to SalesOfficeEast using the Identity Management module.

1. If not already there, click on the hyperlinked name MadisonParc in the left frame of the console, select Organizations from the View drop down menu.
2. Click on the hyperlinked name SalesOfficeEast, select Services from the View drop down menu and click Register....
3. In the right frame, select LDAP and Core and click Register.
4. In the left frame, click the Show Properties arrow icon next to LDAP.
5. Click Create in the right frame to create a service template.
6. Click Save to save the template for SalesOfficeEast.

NOTE After completing these steps, enter and confirm the LDAP Bind Password created in Step 14 on page 8 in the LDAP Authentication service template and click Save.

7. Repeat these steps to create a template for the Core Authentication service.

Configuring The Referral Policy

Once all services have been registered, the referral policy can be configured in MadisonParc. This procedure creates the referral policy for SalesOfficeEast using the Identity Management module.

1. Click on the hyperlinked name `MadisonParc` in the left frame of the console, select Policies from the View drop down menu and click `New...`.
2. Enter the following information in the right frame of the console and click Create.

   Type Of Policy: Referral

   Name: SalesReferralPolicy
3. Select Rules from the View drop down menu in the right frame and click Add....
4. Enter the following rule information in the right frame of the console and click Create.

   Rule Name: Allow Rule

   Resource Name: http://sparcserver.example.com:<port>

   The Resource Name field contains only the prefix of the resource to be protected. Do not include the specific objects to be accessed.
5. Select Referrals from the View drop down menu and click Add....
6. Enter the following referral information in the right frame of the console and click Create.

   Name: SalesOfficeEast Referral

   Value: SalesOfficeEast
7. Click Save to configure the referral policy.

Configuring And Assigning The Normal Policy

With the referral policy defined at MadisonParc, a normal policy can be created for SalesOfficeEast. This procedure creates the normal policy using the Identity Management module.

1. If not already there, click on the hyperlinked name MadisonParc in the left frame of the console and select Organizations from the View drop down menu.
2. Click on the hyperlinked name SalesOfficeEast, select Policies from the View drop down menu and click New....
3. Enter the following information in the right frame and click Create.

   Type Of Policy: Normal

   Name: TestPolicy

4. Select Subjects from the View drop down menu in the right frame and click Add....
5. Select the subject Type in the right frame and click Next.

   Type: LDAP Groups
6. Enter the following information and click Search to find subjects that meet the search criteria.

   Name: TestPolicySubjects

   LDAP Groups: SalesInfoGroup
7. Select `com > madisonparc > SalesOfficeEast > Groups > SalesInfoGroup` from the available subjects and click Add.
8. Click Create to save the selected subjects.
9. Select Rules from the View drop down menu and click Add....
10. Enter the following rule information and click Create.

    Rule Name: TestPolicyRules

    Resource Name: http://sparcserver.example.com:80

    The Resource Name can be chosen from the Super Resources.

    Action: Get

    Value: Allow
11. Select Conditions from the View drop down menu and click Add....

    Three conditions will be configured for this policy.

    a. Select Authentication Scheme for the Condition type and click Next.

    b. Enter the following information and click Create.

       Name: TestPolicyAuthScheme

       Authentication Scheme: LDAP

    c. Click Add... again, select IP Address for the Condition type and click Next.

    d. Enter the following information and click Create.

       Name: TestPolicyAuthScheme

       DNS Name: *.example.com

e. Click Add... for a third time, select Time for the Condition type and click Next.

f. Enter the following information and click Create.

Name: TestPolicyTime

Day: From: Monday To: Friday

12. Click Save to complete the policy creation.

Configuring For User Self-Registration

This procedure configures Identity Server to allow a user to register and authenticate to the Identity Server on the fly.

Registering Membership Authentication

User self-registration is configured by registering the Membership authentication module to the top-level organization, MadisonParc. This procedure does just that using the Identity Management module

1. If not already there, click on the hyperlinked name MadisonParc in the left frame of the console, select Services from the View drop down menu and click Register....
2. In the right frame, select the Membership service and click Register.
3. In the left frame, click on the Show Properties arrow icon next to Membership.
4. Click Create in the right frame to create a service template.
5. Click Save to save the template for dc=madisonparc,dc=com.

NOTE After completing these steps, enter and confirm the LDAP Bind Password created in Step 14 on page 8 in the Membership Authentication service template and click Save.

Activating Membership Authentication

1. If not already there, click on the hyperlinked name MadisonParc in the left frame of the console and select Services from the View drop down menu.
2. Click on the Show Properties arrow icon next to the Core service.

3. In the right frame, select Membership in the Organization Authentication Modules field listing and click Save.

   Do not de-select any highlighted authentication types.

Assigning A Service

This procedure registers the Session Service and assigns it to a user for management purposes.

Registering Session Service

This procedure registers the Session Service to the top-level organization using the Identity Management module.

1. If not already there, click on the hyperlinked name MadisonParc in the left frame of the console, select Services from the View drop down menu and click Register....
2. In the right frame, select the Session service and click Register.
3. In the left frame, click on the Show Properties arrow icon next to Session.
4. Click Create in the right frame to create a service template.
5. Click Save to save the template for dc=madisonparc,dc=com.

Assigning The Session Service

This procedure assigns the Session Service to a user for management purposes using the Identity Management module.

1. If not already there, click on the hyperlinked name MadisonParc in the left frame of the console and select Users from the View drop down menu.
2. Click on the Show Properties arrow icon next to eastsalesmanager.
3. Select Services from the View drop down menu in the right frame.
4. Select the Session service and click Save.

Testing The Configurations

The following steps can be used to test the configurations defined in the previous section.

To Test The Group Policy

From a browser, attempt to access http://<server>:<port>/test.html. When prompted for credentials, log in as one of the users from the SalesInfoGroup. The contents of test.html should be visible after a successful authentication.

To Test User Self-Management

This procedure allows a user to change their own information.

1. Access http://<server>:<port>/amserver from a web browser.
2. Log in as westsalesperson2.
3. Enter in a new address in the Home Address field.
4. Click Save.

To Test User Self-Registration

This procedure allows a user to register themselves to the MadisonParc organization.

1. Access http://<server>:<port>/amserver/UI/Login?module=Membership from a web browser and select the New User option.
2. Enter the following required information and click Register.

   User Name: ceo

   Password: 11111111

   Confirm Password: 11111111

   First Name: Jim

   Last Name: Creek

   Full Name: Jim Creek
3. Click Agree at the sample disclaimer window to create the user in the top-level organization MadisonParc.

Additional Sample Configurations

There are a number of samples included with Identity Server that can be used to illustrate certain features as well as one of many possible applications of the Identity Server technology.

Command Line Sample

This sample provides information on how to use the Identity Server command line tool `amadmin`. The sample is located in the directory `<identity_server_root>/SUNWam/samples/admin/cli/`. Detailed instructions on how to implement this sample can be found in the `Readme.html` file.

Application Server Deployment

This sample provides information on how to deploy the Identity Server on the iPlanet Application Server. The sample is located in `<identity_server_root>/SUNWam/samples/appserver/`. Detailed information can be found in the `Readme.html` file.

Authentication Samples

Authentication Service samples have been provided and can be found in the directory `<identity_server_root>/SUNWam/samples/authentication`. They include:

- Remote Client API
- Login Module

Remote Client API

This sample program demonstrates how to integrate the Remote Client API for authenticating users with the Identity Server. It uses LDAP authentication although it can be modified to use other existing or customized authentication modules. The instruction file is the `readme.html` file found in the `<identity_server_root>/SUNWam/samples/authentication/LDAP` directory.

Login Module

This sample demonstrates the steps needed to integrate a custom login module into the Identity Server. All the files needed to compile, deploy and run the sample authentication module that is shipped with Identity Server can be found in the `<identity_server_root>/SUNWam/samples/authetnication/providers` directory. The instruction file is the `Readme.html` file in the same directory.

Console Sample

Sample files have been included to help understand how the Identity Server console can be customized. They help to explain the Java™ 2 Enterprise Edition (J2EE) web application framework used. In addition, Java classes are extended from the console APIs and new JSP files are created. Existing xml and properties files are also used. These files are located in `<identity_server_root>/SUNWam/samples/console`. Open the `README` file in this directory for instructions on how to run the sample.

Federation Management Sample

There are three samples that provide information on how to use the Federation management module. The samples are located in `<identity_server_root>/SUNWam/samples/liberty/`. Detailed instructions on what each sample illustrates and how to implement them can be found in the `README` file.

Policy Samples

Policy samples are provided to illustrate how to create policies and use the Policy Configuration Service. The samples are located in `<identity_server_root>/SUNWam/samples/policy/`. Detailed instructions on what each sample illustrates and how to implement them can be found in the `Readme.html` file.

SAML Samples

There are several samples that illustrate how the SAML service can be used. They include:

- A sample that serves as the basis for using the SAML client API. This sample is located in `<identity_server_root>/SUNWam/samples/saml/client`.

- A sample that illustrates how to form a Query, and write an AttributeMapper as well as how to send and process a SOAP message using the SAML SDK. This sample is located in `<identity_server_root>/SUNWam/samples/saml/query`.
- A sample application for achieving SSO using the Web Artifact profile or the Web POST profile. This sample is located in `<identity_server_root>/SUNWam/samples/SAML/sso`.
- A sample that illustrates how to use the XMLSIG API . It is located in `<identity_server_root>/SUNWam/samples/SAML/xmlsig`.

Sample SSO Java Files

Identity Server provides three groups of sample Java files. With these samples, a developer can create an SSO token in several ways:

1. An SSO token can be created for an application that runs on the Identity Server server.
2. An SSO token can be created for an application that runs on a server other than the Identity Server server.
3. An SSO token can be created by a session ID string can be passed through the command line.

The files are in the `<identity_server_root>/SUNWam/samples/sso` directory.

SSO Servlet Sample

This sample can be used to create a token for an application that resides on the same server as the Identity Server application. The files used for this sample are:

- `Readme.html`
- `SampleTokenListener.java`
- `SSOTokenSampleServlet.java`

The instructions in `Readme.html` can be followed to run this code.

Remote SSO Sample

This sample can be used to create a token for an application that resides on a different server from the one on which the Identity Server application lives. The files used for this sample are:

- `remote.html`
- `SSOTokenFromRemoteServlet.java`
- `SSOTokenSampleServlet.java`

The instructions in `remote.html` can be followed to run this code.

Command Line SSO Sample

This sample illustrates how to validate a user from the command line using a session ID string. The files used for this sample are:

- `ssocli.txt`
- `CommandLineSSO.java`
- `SSOTokenSample.java`

The instructions in `ssocli.txt` can be followed to run this code.

User Management Samples

User management samples are provided to illustrate how to use the Identity Server SDK as well as how to add new attributes to a user profile. The samples are located in `<identity_server_root>/SUNWam/samples/um/`. Detailed instructions on what each sample illustrates and how to implement them can be found in the `Readme.html` file.