Installation and Configuration Guide

Sun™ ONE Identity Server

Version 6.0

816-6685-10
October 2003
Third Edition

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

Contents

About This Guide

The *Installation and Configuration Guide* offers an introduction to Sun™ Open Network Environment (Sun ONE) Identity Server and describes how to plan and install Identity Server.

This preface contains the following sections:

- What You Are Expected to Know
- The Identity Server Documentation Set
- Documentation Conventions Used in This Manual

What You Are Expected to Know

This book is considered the “first” manual in the documentation series provided with Identity Server. It’s essential that you understand directory technologies and have some experience with Java and XML programming languages. You will get the most out of this guide if you are familiar with directory servers and Lightweight Directory Access Protocol (LDAP). Particularly, you should be familiar with Sun ONE Directory Server and the documentation provided with that product.

This guide is intended for use by IT professionals who manage access to their network through Sun ONE servers and services. The functionality contained in Identity Server allows you to manage user data and enforce access policies throughout your enterprise.

Once you understand the concepts described in this guide, you will be ready to install Identity Server 6.0 and its components.

The Identity Server Documentation Set

The Sun ONE Identity Server documentation set contains the following guides:

- *Installation and Configuration Guide* details how to plan and install Identity Server.
- *Administration Guide* documents how to manage user and service data in an Identity Server system once it has been installed.
- *Programmer's Guide* documents how to customize Identity Server interfaces.
- *Policy Agent Guide* documents how to install and deploy Sun ONE Identity Server Policy Agent on Web, Proxy, and Application Servers.
- The *Release Notes* gathers an assortment of information, including a description of what is new in this release, last minute installation changes, known problems and limitations, and how to report problems.

NOTE Be sure to check the Identity Server documentation web site for updates to the release notes and for revisions to the guides.

`http://docs.sun.com/db/prod/s1idsrv`

Documentation Conventions Used in This Manual

In the Identity Server documentation (such as this guide) there are certain typographic and terminology conventions used to simplify discussion and to help you better understand the material. These conventions are described below.

Typographic Conventions

This book uses the following typographic conventions:

- *Italic type* is used within text for book titles, new terminology, emphasis, and words used in the literal sense.
- `Monospace font` is used for sample code and code listings, API and language elements (such as function names and class names), filenames, pathnames, directory names, HTML tags, and any text that must be typed on the screen.

- *Italic serif font* is used within code and code fragments to indicate variable placeholders. For example, the following command uses *filename* as a variable placeholder for an argument to the `gunzip` command:

  ```
  gunzip -d filename.tar.gz
  ```

Terminology

Below is a list of the general terms that are used in the Identity Server documentation set:

- Identity Server refers to Identity Server and any installed instances of the Identity Server software.
- *Policy and Management services* refers to the collective set of Identity Server components and software that are installed and running on a dedicated Web Server. The dedicated Web Server is installed for you automatically when you install the Policy and Management services.
- *Web Server that runs* Identity Server refers to the dedicated Web Server where the Policy and Management Services are installed.
- *Directory Server* refers to an installed instance of Sun ONE Directory Server or Netscape™ Directory Server.
- *Identity_Server_root* is a variable place holder for the home directory where you have installed Identity Server.
- *Directory_Server_root* is a variable place holder for the home directory where you have installed Sun ONE Directory Server.
- *Web_Server_root* is a variable place holder for the home directory where you have installed Sun ONE Web Server.

Chapter 1

Introducing Identity Server

Identity Server is an enterprise infrastructure solution. It's the key to your business relationships, your services, your data, and who has access to what. Identity Server enables you to get your customers, employees, partners and suppliers into one online directory. It also provides a means for establishing policies and permissions regarding who has access to which information in your enterprise. Identity Server is designed to meet the challenges of rapidly expanding extranets or hosting services. This chapter provides an introduction to Identity Server solution.

Topics in this chapter include:

- Identity Server Solution
- Key Features and Benefits
- What's New in Identity Server 6.0

Identity Server Solution

Identity Server is composed of Sun ONE servers, services, and agents. It extends the basic functionality of Sun ONE Directory Server to consolidate user data, services data, and access policies so that all of these can be managed efficiently under one console. You can use Identity Server to define and enforce roles and policies that control access to web resources in your enterprise. These roles and policies also provide the means for delegating user account management—to administrators as well as non-administrators. The Identity Server plug-in architecture makes it relatively easy to add new services and to customize their configuration for users and policies.

When you purchase Identity Server, you receive a full complement of Sun ONE servers and services, which together form the Identity Server solution:

- Sun ONE Directory Server 5.1 SP1
- Identity Server Policy and Management Service
- Identity Server Console
- Identity Server Schema
- Cross-Domain Single Sign-On component (CDSSO)
- Common Domain Services for Federation Management

Web agents that work with Identity Server are available as separate components. For more information about Identity Server web agents, see "Policies and Policy Agents" on page 31.

Sun ONE Directory Server

Sun ONE Directory Server is a powerful and scalable distributed directory server based on the industry-standard Lightweight Directory Access Protocol (LDAP). In an Identity Server deployment, Directory Server is the central repository for user data, services data, and access policies. This allows a variety of servers and applications to share a consistent set of data.

Identity Server Policy Service

The Policy service is made up of four smaller, specialized services: Authentication, Single Sign-On, Logging, and Session. Together, these services provide the means for enforcing access rules. Access rules combine to form the policies, which allow or deny a user to log in to an application.

Authentication

The Authentication service verifies the identities of users trying to access applications. Authentication is implemented through a number of plug-in modules that validate a user's credentials at login.

Single Sign-On

The Single Sign-On (SSO) service uses tokens for storing and transporting user information between applications. This makes it possible for users to log in to the enterprise once, and access multiple web-based applications without having to re-authenticate for each application. The service provides Java APIs for validating SSO tokens and agents for enforcing access rules and policies that are set on specific pages stored on the server.

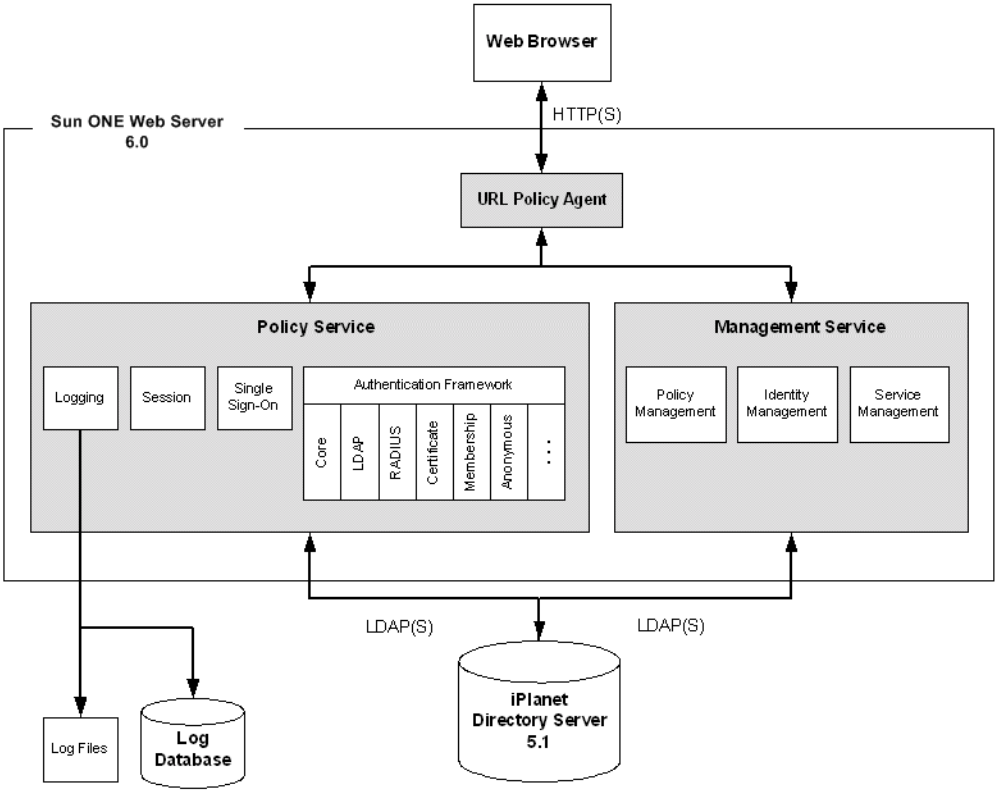
Logging

The Logging service writes log information to log files or to a log database. The log data is used by Authentication modules and by the Identity Server console.

Session

The Session service maintains user session information and validity periods. The session information is used to validate Single Sign-On tokens.

Figure 1-1 Identity Server Architecture.



Identity Server Management Service

The Management service is made up of three smaller services: Policy Management, Identity Management, and Service Management. These three services are consolidated in the Identity Server console, providing a single point for enterprise management. When you use Management service to make changes, the changes are automatically made in Directory Server.

Policy Management

The Policy Management service provides a means for creating, modifying, and deleting access rules and policies for organizations and sub-organizations.

Identity Management

The Identity Management service is also referred to as User Management service. It provides the means for creating and managing users, roles, groups, people containers, organizations, organization units, and sub-organizations.

Service Management

The Service Management service provides the means for registering and de-registering services, and for managing service attributes assigned to objects in the directory.

Identity Server Console

Identity Server Console is a graphical interface that consolidates Identity, Service, and Policy management. It allows users—administrators as well as non-administrators—to create and manage users accounts, service attributes, and access rules in Directory Server using one interface and without having to know LDAP.

Cross-Domain Single Sign-On

The Cross Domain Single Sign-On feature makes it possible for users to authenticate once in a DNS domain in your enterprise, and then access Identity Server services running on other domains. This service is implemented through the use of a controller plus any number of Cross-Domain Single Sign-On (CDSSO) components that you install on the participating domains.

Cross-Domain Controller

The Cross-Domain Controller (CDC) component is automatically installed when you install Identity Services. The controller is responsible for appropriately directing authentication requests. If a request contains no Single Sign-On (SSO) information, the controller directs the request to the Authentication service. If a request contains SSO information the request is directed to the appropriate CDSSO component with the SSO information appended to the query string.

Cross-Domain Single Sign-On Component

The Cross-Domain Single Sign-On (CDSSO) component is primarily responsible for handling cookie-setting for the domain in which cross-domain single sign-on is deployed. The CDSSO component is installed separately on all participating DNS domains.

Web Server

Sun ONE Web Server, although not included in the product CD as a stand-alone product, is an integral part of the Identity Server solution. It is automatically installed and configured when you install the Policy and Management services. Working behind the scenes, this dedicated instance of Web Server provides the engine for policy enforcement, identity management, and service management. It also serves the graphical user interface.

Common Domain Services

Common Domain Services enable machines hosting a common domain to read and write cookies based on parameters passed within redirect URLs. When a user authenticates with an Identity Service Provider (IDP), the IDP would redirect the user's browser to the common domain with a parameter indicating that the user is using that IDP. The server in the common domain writes a cookie that identifies this IDP as the preferred IDP and redirects the user's browser back to the IDP.

Key Features and Benefits

As a business grows, its networking needs change. Efficiency, extensibility, rapid deployment of services, and maintained security become key factors in keeping its enterprise running smoothly and with minimum down-time. Identity Server offers the following features to meet the challenges of growing enterprises.

Administration Console

A graphical interface that consolidates Identity, Service, and Policy management. The Administration console allows users—administrators as well as non-administrators—to create and manage users accounts, service attributes, and access rules in Directory Server using one interface and without having to know LDAP.

Policy Management

A means for creating and enforcing access rules. Grants or denies users' access to resources based on their credentials and based on the rules and policies you create.

Service Management

A means for registering services and service attributes. Allows you to assign service attributes to organizations, groups, or individual users from the same console that you use to perform user management.

Identity Management

A framework that supports several pre-defined administrator roles. Provides a means for creating, modifying, or deleting organizations, groups, and users. Automatically creates appropriate administrator entries, roles, and access control instructions (ACIs) each time you create a new organization or managed group.

Authentication

A framework and a number of modules for verifying user identities. Provides security by requiring users to present credentials in order to log in to applications in the enterprise. The plug-in architecture makes it possible for Sun ONE customers to write and use their own modules with Identity Server. The following Authentication modules come with Identity Server:

- LDAP
- RADIUS
- Membership
- Anonymous
- Certificate-based
- Unix
- SafeWord

NOTE Unix authentication module is found only in Solaris version.

Web-based Single Sign-On

A mechanism that uses tokens to store and transport user information between applications. Enables a user to access multiple web-based applications during a single session without having to re-authenticate for each application.

Policy Agent

A mechanism that enforces access rules and policies that protect web resources. Provides security by requiring additional identification from users who attempt to access protected files or pages in a web server.

Secure Socket Layer (SSL)

A transport protocol that encrypts and secures communications over a network. SSL ensures that communications over the network cannot be viewed by unauthorized individuals.

Directory Replication Support

Identity Server works with multi-master replication of Directory Server to provide a highly available directory service for both read and write operations.

Roles and Class of Service Support

Identity Server works with Directory Server to provide a flexible mechanism for grouping and sharing attributes among entries. Allows you to dynamically change a large number of user, group, or organization entries by making a single change to a role or attribute.

Load-Balancer Support

Identity Server works with load-balancers such as Sun ONE Directory Access Router, to provide high availability and firewall-like security.

What’s New in Identity Server 6.0

Identity Server 6.0 incorporates the following new features:

- Support to Liberty Specifications
- SAML Support

Support to Liberty Specifications

The shreds of our identity are scattered across banks, credit card companies, brokerage firms, the department of motor vehicles, insurance companies, the Social Security Administration, department stores, gas stations, telephone companies; the list seems endless. The Internet, now the prime vehicle for business, community and personal interactions is fragmenting our identity even further. Information about us is doled out across the many computer systems and networks used by our employers, ISPs, bulletin boards, instant messaging systems, and on-line businesses, all with little coordination, interaction or control on our part.

Creating a federated identity infrastructure is the key to correcting this situation. The existence of such an infrastructure opens up new business opportunities, including providing economies of scale that lower business costs and expedite the growth of the Internet and e-commerce. For the consumer, it promises new levels of personalization, security, and control over their identity information. Making this happen is what the Liberty Alliance Project is all about.

SAML Support

Security Assertion Markup Language (SAML) defines an XML framework for exchanging security assertions among security authorities, with the key objective of achieving interoperability across different vendor platforms that provide authentication and authorization services.

Here are some use scenarios where SAML comes to play:

- Enables Single-Sign-On among trusted partners. User authenticates against a source web site, then is allowed to access web resources hosted by different vendors without having to re-authenticate.
- Enables application to grant access based on user's authentication reference.
- Enables two parties in different security domain to validate each other, thus the business transactions between the two sides could proceed.
- Enables user session sharing between two applications.

For detailed information on SAML and how it is used within Identity Server, you can see Chapter 8, Using SAML, in the Programmer's Guide.

Chapter 2

Deployment Considerations

This chapter provides information you should keep in mind as you plan your Identity Server deployment.

Topics in this chapter include:

- Directory Issues
- Policy Management Issues
- Installing Other Products for Use With Identity Services
- Hardware Requirements
- Software Requirements

Directory Issues

The way you install and configure Identity Server will depend upon your company's current directory environment and your long-term directory needs. Before installing Identity Server, you should plan your new directory—or optimize your existing directory—for the highest performance and extensibility. The following sections discuss how you can best leverage the Directory Information Tree (DIT) that comes with Identity Server.

For detailed information regarding general Directory Server planning and implementation, see the Directory Server Deployment Guide available at the following URL:

```
http://docs.sun.com/db/doc/816-5609-10
```

Installing Against an Existing Directory

You can install Identity Server against an existing Sun ONE Directory Server that is already provisioned with user data. But immediately after you run the Identity Server installation program, you must make modifications in both your existing directory and in the Identity Server configuration so the two will work together. Modifications will vary depending upon your DIT structure, but may include:

- Adding Identity Server object classes to your existing directory entries. (This is required.)
- Adding your custom object classes to Identity Server XML files
- Modifying your attribute naming schema

These topics are discussed in detail in Chapter 5, "Installing Identity Server Against an Existing Directory Server".

NOTE If you're installing Identity Server against an existing Directory Server, the required directory modifications are complex. They call for a high level of expertise in LDAP planning and implementation, as well as proficiency in XML. The procedures are complicated and can be time-consuming. Be sure to plan accordingly for this phase of deployment.

Identity Server Schema

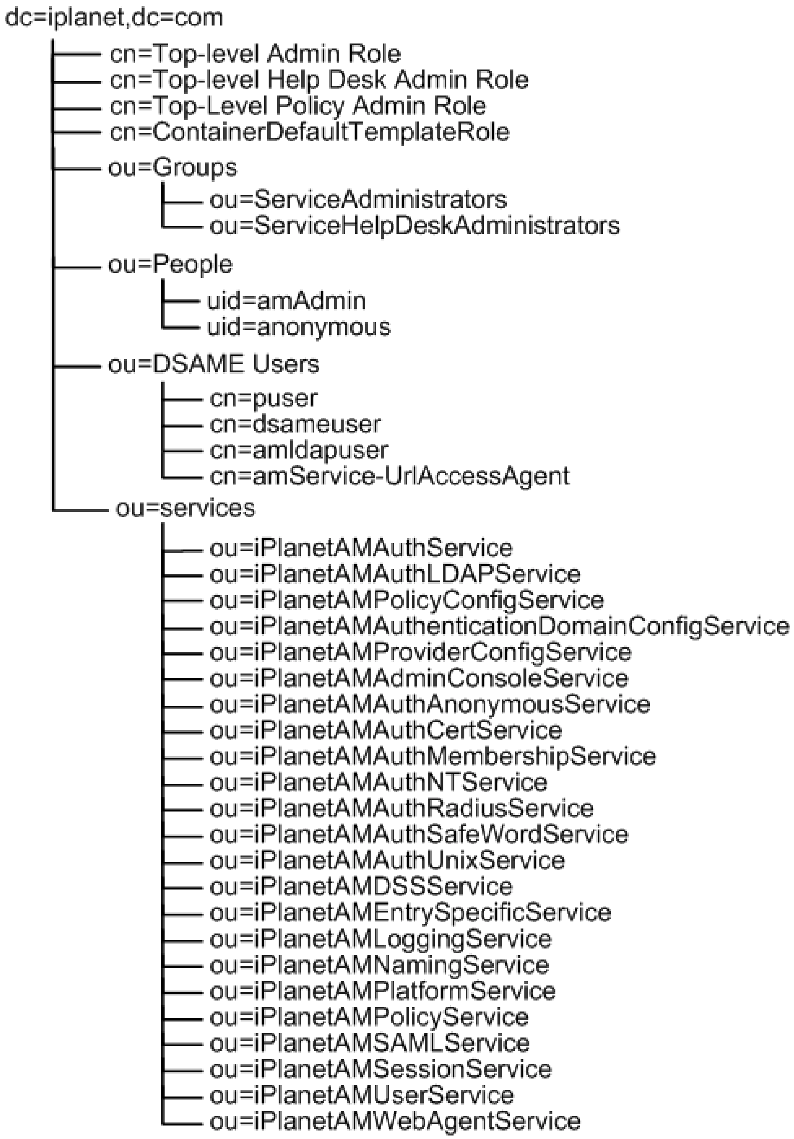
You can install Identity Server schema by choosing the option Configure An Existing Directory Server during the installation program. The Identity Server schema is installed on the server where the Directory Server is installed. The schema file `ds_remote_schema.ldif` is loaded to your Directory Server schema directory.

Whether or not your directory is already provisioned with users, the following Identity Server objects are created and stored in the directory:

- Special object classes
- A single organization
- Administrator roles
- Identity Server service attributes and related policies
- A Top-level Administrator

The Identity Server base suffix that is created during installation is designed for storing and managing user data. Special object classes identify the user and group entries in the directory that will be managed by Identity Server. These object classes make it possible for Identity Server to manage only selected data—user data—and not interfere with other aspects of your tree such as servers or hardware.

Figure 2-1 The default Identity Server directory information tree (DIT).


dc=iplanet,dc=com
cn=Top-level Admin Role
cn=Top-level Help Desk Admin Role
cn=Top-Level Policy Admin Role
cn=ContainerDefaultTemplateRole
ou=Groups
ou=ServiceAdministrators
ou=ServiceHelpDeskAdministrators
ou=People
uid=amAdmin
uid=anonymous
ou=DSAME Users
cn=puser
cn=dsameuser
cn=amldapuser
cn=amService-UrlAccessAgent
ou=services
ou=iPlanetAMAuthService
ou=iPlanetAMAuthLDAPService
ou=iPlanetAMPolicyConfigService
ou=iPlanetAMAuthenticationDomainConfigService
ou=iPlanetAMProviderConfigService
ou=iPlanetAMAdminConsoleService
ou=iPlanetAMAuthAnonymousService
ou=iPlanetAMAuthCertService
ou=iPlanetAMAuthMembershipService
ou=iPlanetAMAuthNTService
ou=iPlanetAMAuthRadiusService
ou=iPlanetAMAuthSafeWordService
ou=iPlanetAMAuthUnixService
ou=iPlanetAMDSSService
ou=iPlanetAMEntrySpecificService
ou=iPlanetAMLoggingService
ou=iPlanetAMNamingService
ou=iPlanetAMPlatformService
ou=iPlanetAMPolicyService
ou=iPlanetAMSAMLService
ou=iPlanetAMSessionService
ou=iPlanetAMUserService
ou=iPlanetAMWebAgentService

Unsupported DITs

It is important to understand that DSAME abstractly represents the entries it manages. This means that, for example, an organization in DSAME is not necessarily the same as an organization in iDS. Whether a specific DIT can be managed or not depends on how the you choose to represent or manage your directory entries, and whether your DIT fits into the limitations of each DSAME type.

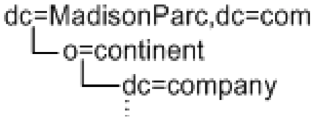
Limitations to Consider

The limitations of DSAME entry types fall into three categories:

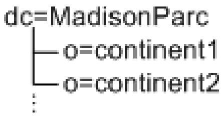
- Only One Type of Entry Can be Marked as an Organization
- People Containers Must be Parent Entries for Users
- Only One Organization Description is Allowed in the DSAME XML

Only One Type of Entry Can be Marked as an Organization

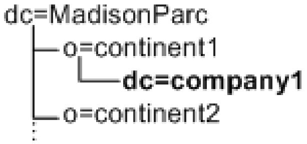
By adding the DSAME `iplanet-am-managed-org` auxiliary class to any entry, DSAME will manage this entry as if it is an organization. But there is a limitation: only one type of entry may be marked as an organization in DSAME. For example, if you have an entry `o=sun`, and another entry `dc=ibm` in your DIT, you cannot mark them both as organizations. In the following example, if you want both `dc` and `o` entries to be organizations, the DIT structure will not be manageable via DSAME.



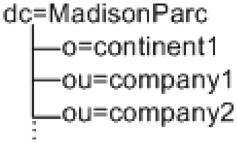
There is one exception to this rule. The entry at the DSAME root suffix does not count as one entry. So in the following example, the DIT structure can indeed be managed by DSAME:



If you were to add `dc=company1` below `o=continent1`, then this DIT would be manageable only if `dc` is marked as a *container*. Container is another abstract type in DSAME that typically maps to an `OrganizationalUnit`. In most DITs, you would add the `iplanet-am-managed-container` entry to all `OrganizationlUnits`.



However, you could add this marker object class to any entry type. The DIT structure in the following example is allowed:



In this example, since you cannot mark both `o=` and `ou=` entries as organizations you could mark the `o=` entries as `organization` and the `ou=` entries as `containers`. When exposed in the UI, both organizations and containers have the same options. You can create subordination or subcontinents, people containers, groups, roles, and users under both of them..

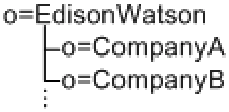
People Containers Must be Parent Entries for Users

Another abstract entry type is the people container. The DSAME type assumes that this entry is a parent entry for users. When you mark an entry as a people container with `iplanet-am-managed-people-container`, the UI will assume it can only contain sub-people containers or users. The attribute `OrganizationUnit` is typically used as a people container, but any entry may be this type in DSAME as long as it has the `iplanet-am-managed-people-container` object class and it has a DSAME manageable parent of type `organization` or `container`.

Only One Organization Description is Allowed in the DSAME XML

The DSAME organization is defined in `amEntrySpecific.xml`. Only one organization description is allowed in this file. As a result, when you customize directory entry properties, or create administration pages or search pages in the UI, your custom attributes apply globally to the entire DSAME configuration. This DSAME requirement may not meet the needs of some companies, especially hosting companies, that require different display attributes for each organization in the deployment.

In the following example, Edison-Watson is a hosting company that provides internet services to a number of companies. CompanyA wants to display fields for capturing a user's name First Name, Surname, and Badge Number. CompanyB wants to display fields for capturing a user's First Name, Last Name, and Employee Number.

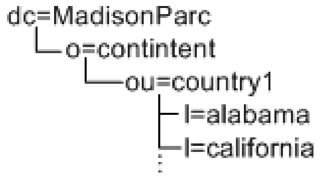


The organization description is defined at the root level (`o=Edison-Watson`), and not at the organization level. By default, the UI for both CompanyA and CompanyB must be identical. Also, all services globally define attributes to be of the subschema type `user`. So if CompanyA has attributes for its users in the auxiliary class `CompanyA-user`, and CompanyB has attributes in `CompanyB-user` then CompanyB's attributes will be overridden, and will not be displayed.

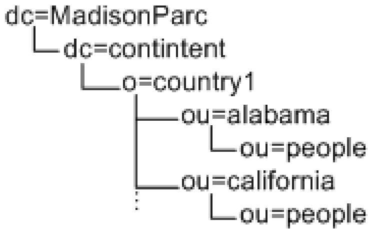
As a workaround, you can modify the ACIs to work for user display. However, this workaround will not address the attributes in Search and Create windows.

Examples of Unsupported DITs

In the following example, you would need three types of organization makers: o, ou, and l. Assuming that l=california and l=alabama are not a people containers, this DIT would not work with DSAME:



In the following example, you would need three types of DSAME markers (dc,o,ou) plus the people container type (ou=people). Under these assumptions, the DIT would not work with DSAME:



Directory Replication

If you plan to use replicated directories with Identity Server, you should define your database replication agreements before running the Identity Server installation program. See "Support for Directory Replication and High Availability" on page 146 of this manual for more information.

Policy Management Issues

Delegated administration and web access management in Identity Server are implemented through the use of specialized roles and policies. These are created for you at installation, and can be viewed and managed in the Identity Server graphical user interface. As you plan your directory structure, consider how you can leverage these pre-defined Identity Server objects to meet your enterprise needs.

Roles

Identity Server roles are an extension of the roles functionality that comes with Directory Server. In Directory Server, a role is an entry grouping mechanism. This grouping mechanism is designed to be more flexible than a static group, and easy to maintain like a dynamic group.

In Identity Server, the concept of roles is the same as in Directory Server, but with an added level of abstraction. When you install Identity Server, several administrator roles are automatically created for you. Each administrator role specifies a different scope of access control, providing a means for delegating user account administration. You can configure a role to contain any combination of access control instructions (ACIs), policy rules or service attributes. You can configure roles in the Roles page of the Administration Console. You can also create roles with specific permissions to provide a customer delegation model.

The following table summarizes the Identity Server administrator roles and the scope of write permissions that correspond to each role.

Table 2-1 Administrator Roles and Permissions

Administrator Role	**Has permissions to modify directory entries at this level of the tree:**					
	Base Suffix	**Role Definitions**	**Organization**	**Group**	**User**	**Own Entry**
Top-Level Administrator	X	X	X	X	X	X
Top-Level Help Desk*			X*			
Organization			X	X	X	X
Organization Help Desk*			X*			
Container				X	X	X

Table 2-1 Administrator Roles and Permissions

Administrator Role	**Has permissions to modify directory entries at this level of the tree:**					
Container Help Desk*			X*			
Group				X	X	X
People Container					X	X
User (self-administrator)						X

* Help Desk Administrators can only modify passwords of users within their own branch of the tree.

When you create a directory entry, the appropriate administrator roles and ACIs are created and assigned to the directory entry. You can then assign a role to an individual user.

For example, when you use Identity Server to create a new organization, two new roles are automatically created and stored in the directory:

- Organization administrator role
- Organization help desk administrator

If you assign the organization administrator role to a user, `mikeb`, within the organization, then `mikeb` inherits all the permissions accorded an organization administrator. If you assign the help desk administrator role to a user, `ginac`, then `ginac` inherits the more restricted permissions of a help desk administrator. Ultimately, you'll find that using roles instead of group-based ACIs is more efficient and requires less maintenance.

Policies and Policy Agents

You can control access to web resources in your enterprise by applying policy to roles and organizations. A policy is made up of rules, subjects, and conditions. A rule grants or denies a user access to a specified resource such as a service or a page of content stored in a server. Subjects specify who the rule will apply to. Conditions specify any constraints on the policy. Policy agents, which you install on the Web Servers in your enterprise, evaluate and enforce the policies you define.

When a user tries to access a protected resource such as a web page stored on a server in your enterprise, the Identity Server Policy Service evaluates the rules attached to the user's organization, role, or userid. Based upon the net result of the rules and conditions assigned to the user, the individual is either granted or denied access to the web page. You can configure rules and policies in the Identity Server Administration Console. For more information about setting up policies, see the *Sun ONE Identity Server Administration Guide*. For comprehensive information about Identity Server Policy Agents and how to install and configure them, see the Sun ONE Policy Agents Guide at `http://docs.sun.com/db/prod/s1.ipdirsame`.

Service Attributes

You can use service attributes to define how services will work with Identity Server. Some service attributes are set at the global level and impact the entire Identity Server installation, some impact only individual users, and some can be set at multiple levels. To specify a value for an attribute, it's important to understand the scope of its effect. To make this easier, service attributes are organized into the following categories: global, dynamic, policy, and user.

Global. Global attributes apply to the entire DIT. You can set these values in Service Management view.

Dynamic. Dynamic attributes can be set in Service Management at the global level or in User Management view for an organization or role. These values can also be inherited from a parent object.

Policy. Policy attributes can be set in Policy Management view. Once policy is defined, it can be applied to one or more roles and organizations. These values can also be inherited from a parent object.

User. User attributes apply to individual user entries. You can set these values in Organization Management view.

You can use the Administration Console to configure and set policy for services. For more information, see the *Sun ONE Identity Server Administration Guide* at `http://docs.sun.com/db/prod/s1.ipdirsame`.

Installing Other Products for Use With Identity Services

You can deploy Identity Server with remote Web Servers, with LDAP load-balancer such as Sun ONE Directory Access Router, and in multi-master replications. Before you run the Identity Server installation program, consider how these products might fit into your deployment. In many cases, you must install and configure these products before you install Identity Server.

Remote Web Servers

In this manual, Web Servers are "remote" relative to the Web Server that runs Identity Server Policy and Management services. You may already have remote Web Servers deployed to serve content pages for your enterprise. You may want to install additional ones. A remote server becomes integrated with Identity Server only when you install a Policy agent on it. For detailed Web Server installation and administration information, see the documentation that comes with the server, or access the documentation on the Internet at `http://docs.sun.com/db/prod/s1websrv`.

Policy Agent

The Identity Server Policy agent can be installed on various web servers installed in your enterprise. The agent enforces access rules and policies that are set on specific pages stored on the server. The agent intercepts each request received by a configured Web Server and communicates with the Policy service. The Policy service authenticates the user's credentials, and then examines the user's roles and policies. If the user has the proper credentials and policy assignment, the agents allow the user to access the URL over HTTP.

The Identity Server Policy Agent is a separate product and is available for download at the following URL:

```
http://wwws.sun.com/software/download/developer/5256.html
```

To install a Policy agent, see the instructions that come with the product.

Multiple Directory Servers for Failover and High Availability

You can use the Identity Server installation program to install Directory server for the purposes of upgrading, setting up failover directories, or for setting up multi-master replication.You should install, configure and deploy Directory Server properly for Identity Server to be successful. For more information, see "Support for Directory Replication and High Availability" on page 146.

For detailed Directory Server deployment and installation information, see the documentation that comes with the server, or access the documentation on the Internet at `http://docs.sun.com/prod/s1dirsrv`.

LDAP Load-Balancers

You can configure Identity Server to work with load-balancers such as Sun ONE Directory Access Router. This might be useful if you want to precisely manage directory high availability. For more information, see "Support for Directory Replication and High Availability" on page 146.

For detailed Sun ONE Directory Access Router installation and administration information, access the documentation on the Internet at `http://docs.sun.com/db/prod/s1.ipdirar`

For information on any other load-balancer, see the documentation that comes with the product.

Hardware Requirements

You must make sure that the systems on which you plan to install Identity Server meet the minimum hardware requirements. While all the Identity Server components can theoretically be installed on a single server machine, you will most likely not want to do this. Please review the installation and deployment information in each component's documentation before designing your Identity Server deployment. The recommended procedure is to consult Sun ONE Professional Services or another Sun ONE-certified system integrator before designing and deploying an Identity Server installation.

Optimal Hardware Requirements

Hardware requirements for optimal performance and scalability are as follows:

- One computer system with 512MB to 2 GB RAM for Directory Server.
- One computer system with 512MB to 1GB RAM for Sun ONE Identity Server.
- If you have existing web servers that need to be protected, the Policy Enforcement Point/Policy agent needs to be installed on each web server and requires 10 MB of disk space.

Typically, directory resource requirements are high. The actual requirements differs from the above. They are based on customer specific, data, and usage characteristics.

Recommended Hardware Configurations

Hardware configurations for typical installations are as follows:

- One computer system for Directory Server with 512MB to 1GB memory and approximately 300MB disk space for minimal data in Directory Server.
- One computer system for Identity Server (and Sun ONE Web Server) and potentially Sun ONE Application Server and Policy agents, with 512MB to 1GB memory and 25MB-100MB disk space. Log and debug files may require additional GB disk space over time.
- For large installations, you should plan at least 2GB disk space to support the product binaries, databases, and log files (log files require 1 GB by default); 4GB and greater may be required for very large directories.
- If you have existing web servers that need to be protected, the Policy agent needs to be installed on each web server. The agent requires 10 MB of disk space.
- Table 2-2 contains some guidelines for disk space and memory requirements depending on the number of entries managed by your Directory Server.

Table 2-2 Directory Server Disk Space Guidelines

Number of Entries	Disk Space and Memory Required
10,000 - 250,000 entries	Free disk space: 2 GB, Free memory: 256MB
250,000 - 1,000,000 entries	Free disk space: 4 GB, Free memory: 512 MB

Table 2-2 Directory Server Disk Space Guidelines

Number of Entries	Disk Space and Memory Required
Over 1,000,000 entries	Free disk space: 8 GB, Free memory: 1 GB

Software Requirements

Ensure that your systems meet the following software, and operating system requirements.

Operating System Requirements

Identity Server is supported on the following platforms:

- Solaris 8 32/64
- Solaris 9 32/64
- Microsoft Windows 2000 Server SP 2
- Microsoft Windows 2000 Advanced Server

Patch Clusters for Solaris

When running Sun ONE Directory Server on a Solaris 8 operating system, you must ensure that the recommended patch cluster is installed. Solaris patches are identified by two numbers, for example 108827-15. The first number (108827) identifies the patch itself. The second number identifies the version of the patch (15). We recommend installing the latest version of the patch in order to benefit from the latest fixes.

Use the command showrev `-p` to list the patches currently installed on your machine. All patches can be downloaded from `http://sunsolve.sun.com`. At that site, go to Patches>Recommended & Security Patches to see the list of Recommended & Security Patch Clusters for Solaris.

For any patches not found in the above cluster, please go to Patches>Patchfinder on `http://sunsolve.sun.com`

Sun ONE Directory Server Patches

The `idsktune` utility, installed with Sun ONE Directory Server, may recommend further patches you should install. For instructions on running `idsktune`, refer to the following section of the Sun ONE Directory Server Installation Guide:

```
http://docs.sun.com/source/816-5610-10/trouble.htm#13651
```

Reboot your machine after installing the patches.

Sun ONE Certificate Server 4.7 Patch Installation

In order to configure the Identity Server Security Service, you must install a patch for the Sun ONE Certificate Server version 4.7. Before you install the patch, Certificate Server must be installed on your system.

For Certificate Server installation instructions, see the Sun ONE Certificate Server Installation and Setup Guide at the following location:

```
http://docs.sun.com/prod/s1certsrv
```

Installing the Certificate Server 4.7 Patch

1. Copy the `CMS47sp1.tar` file to the following location:

UNIX	*CMS_Root*`/bin/cert`
Windows	*CMS_Root*`\bin\cert`

2. Run the following command to unpack the contents of the file:

UNIX	`tar -xvof CMS47sp1.tar`
Windows	`unzip CMS47sp1.zip`

3. Create the `SSOBasedAuthentication` instance, or reconfigure it if it already exists.

4. Restart the Certificate Server.

Once the patch is installed, configure the Identity Server Security Service in the Identity Server Console.

Java Requirement

The Identity Server installation program requires Java version 1.3.1_06.

Remote Web Server Requirements

Identity Server Web Agents use approximately 10MB of disk space. For detailed information on Web Server requirements for Identity Server Web Agents, see the *Sun ONE Policy Agents Installation Guide* at the following URL:

```
http://docs.sun.com/prod/s1.ipdirsame
```

Web Browser Requirements

Administrators and end users use web browsers to perform user management tasks. Identity Server supports the following web browsers:

- Netscape Communicator 4.79 on the following platforms: Solaris 8; Windows versions 2000, NT 4.0 SP6a and 98SE.
- Microsoft Internet Explorer 5.5 SP 2 on the following Windows versions: 2000 Professional, NT 4.0 SP 6a, and 98 SE.
- Microsoft Internet Explorer 6.0 on the following Windows versions: 2000 Professional, XP Professional, XP Home, NT 4.0 Sp6a.

Chapter 3

The Identity Server Installation Program

This chapter provides an overview of the options presented by the installation program, as well as some pointers on determining the installation tasks you'll need to perform. The instructions provided here and in the subsequent chapters are meant for installing Sun ONE Identity Server on the Solaris and the Windows platforms.

Topics in this chapter include:

- Before You Begin
- Installation Methods
- Installation Program Options
- Setting the Domain Name

Before You Begin

You must resolve the following issues before you start the Installation program:

- You must log in as root on Solaris or as Administrator on Windows 2000 to run the Installation program.
- The domain name of the host machine is set. If it is not set, follow the instructions in the section "Setting the Domain Name" on page 42.
- On UNIX, be sure that your DISPLAY variable is set appropriately and that you have authorization to connect to the computer system where you are installing Identity Server or its components.

Installation Methods

Depending upon your use of Identity Server and your installation needs, choose the installation method that best suits your needs. Instructions for installing using these methods are provided in the next chapters.

The three installation methods are:

- Run the `setup` program to launch the Identity Server Installation wizard. This is the recommended and the easiest installation method.
- Run the `setup` program in the `nodisplay` mode. This launches a character-based Installation program that you use at the command line. When you run this command-line interface, you are presented with the same questions as those presented in the Installation Wizard.
- Use silent installation. For detailed information, see Chapter 9, "Silent Installation" on page 155 of this manual.

Installation Program Options

When you run the installation program, it displays a number of options. Determine the installation option you want to choose by first identifying your scenario in Table 3-1, and then follow the detailed instructions that correspond to that scenario.

Table 3-1 Where To Find Identity Server Installation Instructions For Specific Scenarios

Common Installation Scenarios	Where to Find Detailed Installation Instructions
1. Install and deploy Identity Server and Directory Server for the first time or for evaluation purposes; you have no existing user data to work with.	Chapter 4, "Installing Identity Server with a New Directory Server" on page 45.
2. Install Identity Server to work with an existing Directory Server 5.1 that is provisioned with user data.	Chapter 5, "Installing Identity Server Against an Existing Directory Server" on page 57.
3. Install multiple instances of Identity Server against a single Directory Server for agent failover. Identity Server and the master Directory Server are already installed; the directory may or may not be already provisioned with users.	"Installing Multiple Identity Server Instances Against the Same Directory Server" on page 144.

Table 3-1 Where To Find Identity Server Installation Instructions For Specific Scenarios *(Continued)*

Common Installation Scenarios	Where to Find Detailed Installation Instructions
4. Configure an existing Directory Server 5.1 to be used with Identity Server.	"Installing Identity Server Against an Existing Directory Server" on page 57.
5. Install and configure the cross-domain single sign-on (CDSSO) component.	"The Cross-Domain Single Sign-On Component" on page 137.
6. Install Common Domain Services	"Installing Common Domain Services" on page 131.
7. Uninstall Identity Server.	"Uninstalling Identity Server" on page 167.

The following is a brief summary of what happens when you choose each of the main installation options.

Option 1) Sun ONE Identity Server Management and Policy Services

When you choose this option, the following are installed for you:

- Identity Server Management and Policy Services
- Sun ONE Web Server
- Sun ONE Directory Server (optional)
- Sun ONE Identity Server Console (optional)
- Common Domain Services for Federation Management
- JDK 1.3.1_06 (optional)

The optional components listed above are installed depending on your affirmation to the installation queries. When the installation program is done, the complete product is installed, and you can immediately log into Identity Server. No user data will be present in the directory.

Option 2) Sun ONE Identity Server Admin Console

A graphical user interface (GUI) that consolidates Identity, Service and Policy Management, the Identity Server Console allows users—administrators as well as non-administrators—to create and manage user accounts, service attributes, and access rules in Directory Server using one interface and without having to know LDAP.

Option 3) Configure an Existing Directory Server

When you choose this option, you are prompted for the host and port number of your existing Directory Server. Only the Identity Server schema is installed on the server where the Directory Server is installed. The schema file `ds_remote_schema.ldif` is loaded to your Directory Server schema directory. No new Directory Server is installed; no existing data is overwritten. Choose this option only if you plan to use Identity Server with an existing Directory Server 5.1 instance that's already provisioned with user data.

Option 4) Sun ONE Identity Server Cross-Domain Single Sign-On

The Cross-domain Single Sign-on feature makes it possible for users to authenticate in one domain, and then to use applications in many other domains without having to re-authenticate. When you choose this option, only the Cross-Domain Single Sign-On (CDSSO) component is installed. You can install this as part of the existing Identity Server, install on Web Server, or install this by installing Web server. For more information, see "The Cross-Domain Single Sign-On Component" on page 137.

Option 5) Common Domain Services for Federation

Common Domain Services enable machines hosting a common domain to read and write cookies based on parameters passed within redirect URLs. When a user authenticates with an IDP, the IDP would redirect the user's browser to the common domain with a parameter indicating that the user is using that IDP. The server in the common domain writes a cookie that identifies this IDP as the preferred IDP and redirects the user's browser back to the IDP.

Setting the Domain Name

Before you install Identity Server, make sure that the domain name of the machine on which the Identity Server is going to be installed is set. If it is not set, follow these instructions to set the domain name.

On UNIX

1. View your host name setting by running the following command:

   ```
   # uname -n
   ```

   The short format of the host name is returned.

2. To set the domain name, do one of the following:

   - If the file `/etc/resolv.conf` exists, then enter the domain name in the domain configuration entry. Example: `domain madisonparc.com`

   - If the file `/etc/resolv.conf` does not exist, then enter the following command:

     ```
     # domainname domainname
     ```

     Example:

     ```
     # domainname madisonparc.com
     ```

     where `madisonparc.com` is the domain to which this computer system belongs.

3. To verify that the host name and domain name are set properly, you can enter the following command:

   ```
   # ping hostname.domainname
   ```

   If the host name is not returned, contact your network Administrator.

On Windows 2000

1. Go to the desktop.
2. Right-click My Computer and then click Properties. Alternatively, you can go to Control Panel and click System. Either of these actions opens the System Properties window.
3. In the System Properties window, click the Network Identification tab.
4. Click the Properties button to open the Identification Changes window.
5. In the Computer Name field, type a name for your machine if it’s not already present.
6. Click More. In the Primary DNS Suffix of this computer field, type the domain name to which this computer belongs. The Primary DNS Suffix combined with the computer name forms the FQDN for this computer.

7. Run `setup.exe`. You’ll find the program in the root directory of the CD-ROM. If you’ve downloaded the product binaries, you’ll find the program in the directory where you unzipped the binary files.

   Double-click `setup.exe`.

   The installation program begins with a Welcome panel.

Chapter 4

Installing Identity Server with a New Directory Server

This chapter provides instructions for a *greenfield* installation, where there is no existing user data to migrate. These instructions are useful if you are installing Identity Server for evaluation purposes, if or you're building your user and policy management topology for the first time. These instructions assume that you do not already have Sun ONE Directory Server installed on the target computer system. If you already have Sun ONE Directory Serve installed and provisioned with user data, you must follow the instructions in Chapter 5, "Installing Identity Server Against an Existing Directory Server" on page 57.

Topics in this chapter include:

- Before You Begin
- To Install Identity Server Services with a New Directory Server

Before You Begin

You must resolve the following issues before you start the Installation program.

Setting the Domain Name

Be sure the domain name of the computer system where you will install Identity Server is set.

To Set the Domain Name On UNIX

1. View your host name setting by running the following command:

```
# uname -n
```

The short format of the host name is returned.

2. To set the domain name, do one of the following:

   - If the file `/etc/resolv.conf` exists, then enter the domain name in the domain configuration entry. Example: `domain madisonparc.com`

   - If the file `/etc/resolv.conf` does not exist, then enter the following command:

     ```
     # domainname domainname
     ```

     Example:

     ```
     # domainname madisonparc.com
     ```

     where `madisonparc.com` is the domain to which this computer system belongs.

3. To verify that the host name and domain name are set properly, you can enter the following command:

   ```
   # ping hostname.domainname
   ```

   If the host name is not returned, contact your network Administrator.

To Set the Domain Name on Windows 2000

1. On the Windows desktop, right-click My Computer and then click Properties.
2. In the System Properties window, click Network Identification.
3. Click Properties.
4. In the Computer Name field, if there is no name, enter a name for the host.
5. Click More.
6. In the Primary DNS Suffix of this computer field, enter the name of the domain to which this computer belongs.

   The Primary DNS Suffix combined with the computer name forms the fully-qualified domain name for this computer. Example:

   ```
   hostname.MadisonParc.com
   ```

Removing Old Instances of Identity Server

Be sure that Identity Server packages or schema are not already installed in another directory on the computer system. To check for an existing packages, you can use the following command:

```
pkginfo
```

If packages beginning with `SUNWam` exist, Identity Server may have been previously installed on the computer system. If possible, uninstall Identity Server using its Uninstallation program. See "Uninstalling Identity Server" on page 167 and "Uninstalling Identity Server On Windows" on page 170 of this manual.

If Identity Server was not properly uninstalled, then you should manually remove the Identity Server packages and files now. Follow these steps:

1. Remove all Identity Server packages.

   First find all Identity Server packages installed on the computer system, run the following command:

   ```
   pkginfo | grep SUNWam
   ```

   Then use the `pkgrm` command to remove each package identified with either of the following:

   - Sun ONE Identity Server 6.0
   - iPlanet Directory Server Access Management Edition 5.1.

   Important: There may be other Solaris packages beginning with SUNWam that should not be removed.

2. Remove the following files located in the directory `/var/sadm/install` if they exist:

   - `productregistry`
   - `.lockfile`
   - `.pkg.lock`

   Important: Exercise caution when removing the `productregistry` file. If you have other Sun ONE products installed which use the Setup SDK Installation program, then do *not* remove this file.

3. If the directory `/var/sadm/pkg` exists, remove all Identity Server packages from it.

To Install Identity Server Services with a New Directory Server

1. Locate the Identity Server Installation program.

   If you're installing Identity Server schema from the product CD, insert the CD into the drive of the system on which you want to install the software. You'll find the Installation program in the following directory:

UNIX	`/cdrom/is_60/solaris`
Windows	*CDdrive*`\cdrom\is_60\windows`

   If you've downloaded the compressed product binaries, in a temporary directory, unpack the product binaries file. On UNIX, be sure to use the Solaris `tar` utility. To unpack the binaries, enter the following command:

UNIX	`gunzip -dc` *binaryfile*.tar.gz `| tar -xvof -`
Windows	`winzip` *binaryfile*.tar.zip

   where *binaryfile* is the name of the file you have downloaded. You'll find the Installation program in the directory where you unpacked the product binaries.

2. Start the Installation program.

   To run the Installation wizard, in the directory that contains the Installation program, enter the following command:

UNIX	`./setup`
Windows	`setup.exe`

   To run the Installation program from the command line, in the directory that contains the Installation program, enter the following command:

UNIX	`./setup -nosdisplay`
Windows	`setup -nodisplay`

NOTE The remaining steps describe the GUI version of the Installation program. If you're using the command-line version of the Installation program, you'll be prompted to provide the same information as that presented in the Installation wizard. In the command-line version, you can use the following commands:

- Press `Enter` to accept a default value in [brackets], or to continue on after you've entered a new value.
- Press < to go back to the previous screen.
- Enter `Exit` to stop the program and return to the command line.

3. In the Welcome window, click Next.

4. To accept the terms of the License Agreement, click "Yes (Accept License)."

5. In the Installation Directory window, specify the directory where you want to install the product, and then click Next.

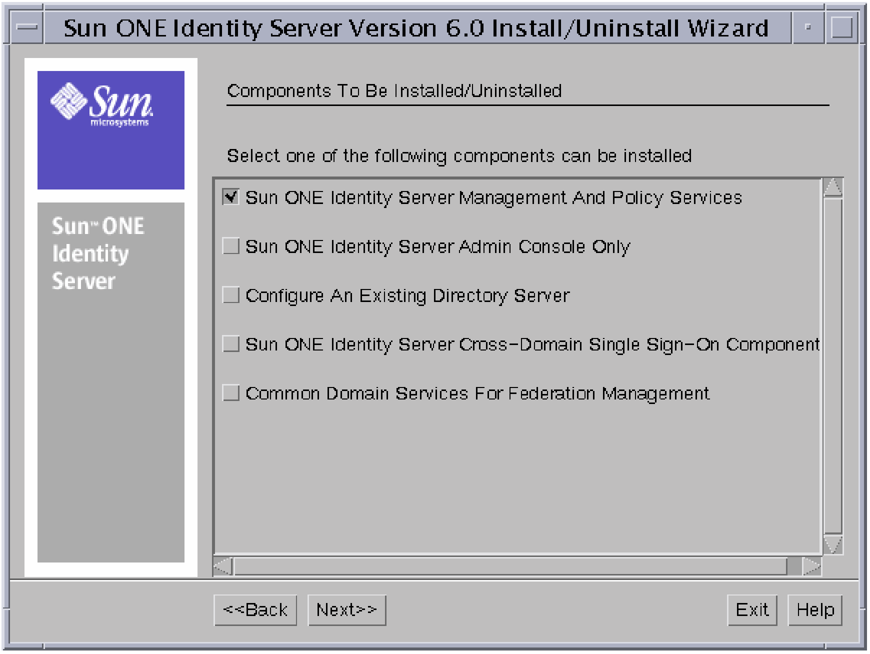
   Note that you should have write and execute permissions in this directory.

   Install Sun ONE Identity Server in this directory: Enter the path to the directory where Identity Server Services will be installed.The default directory is `/opt` on Solaris and `c:\SunONE\SunONEIS` on Windows 2000. You may specify another directory.

6. In the Components to Be Installed / Uninstalled panel, select "Sun ONE Identity Server Management and Policy Services," and then click Next.

   Along with these services, the installation program also installs Sun ONE Web Server, Sun ONE Directory Server, Sun ONE Identity Server Console, Common Domain Services, Identity Server Management and Policy Services and Java SDK 1.3.1_06.

Figure 4-1 Components to Be Installed / Uninstalled Panel



Sun ONE Identity Server Version 6.0 Install/Uninstall Wizard

Components To Be Installed/Uninstalled

Select one of the following components can be installed

☑ Sun ONE Identity Server Management And Policy Services

□ Sun ONE Identity Server Admin Console Only

□ Configure An Existing Directory Server

□ Sun ONE Identity Server Cross-Domain Single Sign-On Component

□ Common Domain Services For Federation Management

7. In the Java Configuration window, provide the following information, and then click Next:

   Do you want to use custom Java SDK? Java support in the Web Server requires Java SDK, version 1.3.1_06, which is provided with Identity Server 6.0. If you want to install the Java SDK available with Identity Server, select No. However, if you want to use a JDK (version 1.3.1_06), that you already have, select Yes and then type the full path to its location.

8. In the Sun ONE Web Server Information window, provide the following information about the Web Server that will run Identity Server services, and then click Next:

   Administrator: Type the user name for the administrator who will access and manage the Web Server.

   Port: Type the port number. Typically, the default is 58888.

   Password: Type the Administrator's password. The password must be a minimum of eight characters in length.

   Confirm Password: To confirm the Administrator password, type it again.

   Enter user to run server as: Type the UNIX user account the Web Server will run as. The default is `nobody`.

   Enter group to run this server as: Type the UNIX group the above user belongs to. The default is `nobody`.

9. In the Web Server that Runs Sun ONE Identity Server Services panel, provide the following information, and then click Next:

   Host: This field displays the fully qualified domain name of the computer where the Identity Server components and a dedicated web server will be installed together.

   Port: Type the port number of the Web Server that runs the Identity Server services. The default port is `58080`.

   Services Deployment URI: The Universal Resource Identifier (URI) prefix tells the Web Server where to look for HTML pages associated with a service and also for web application-specific information such as classes and jars.

   The default URI prefix is `amserver`. You can type a different name.

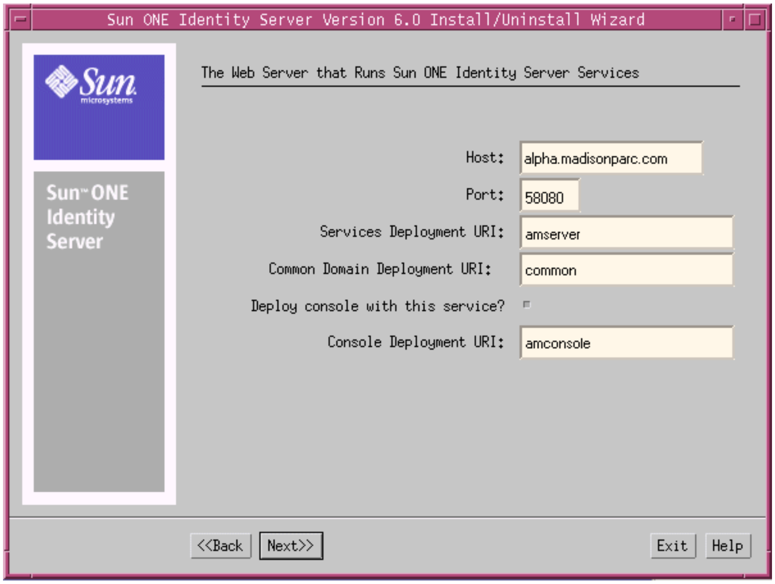
   Common Domain Deployment URI: The URI for accessing the common domain services on the Web Server. The default URI is `common`, which you may change, if required.

   Deploy console with this service? By default, this check box is clicked to indicate that the Identity Server Console will be installed with the Identity Server services. However, if you have an existing console and hence do not want to deploy the console now, click the check box to clear the selection. In this case, the installation program will display another panel to seek more information about the existing console. See the next step for details.

   Console Deployment URI: This URI prefix tells the Web Server where to look for HTML pages associated with the Identity Server console and also for other web application-specific information like classes and jars. The default URI prefix is `amconsole`. You can type a different name. This field is not available, if you cleared the check box Deploy Console with this Service?.

10. If, in the previous panel, you did not choose to deploy the console with this service, provide the following information, and then click Next:

Figure 4-2 Web Server that Runs Sun ONE Identity Server Console Panel



Sun ONE Identity Server Version 6.0 Install/Uninstall Wizard
Sun microsystems
Sun™ ONE Identity Server
<<Back
Next>>
Exit
Help

The Web Server that Runs Sun ONE Identity Server Services

Host: alpha.madisonparc.com

Port: 58080

Services Deployment URI: amserver

Common Domain Deployment URI: common

Deploy console with this service? ☑

Console Deployment URI: amconsole

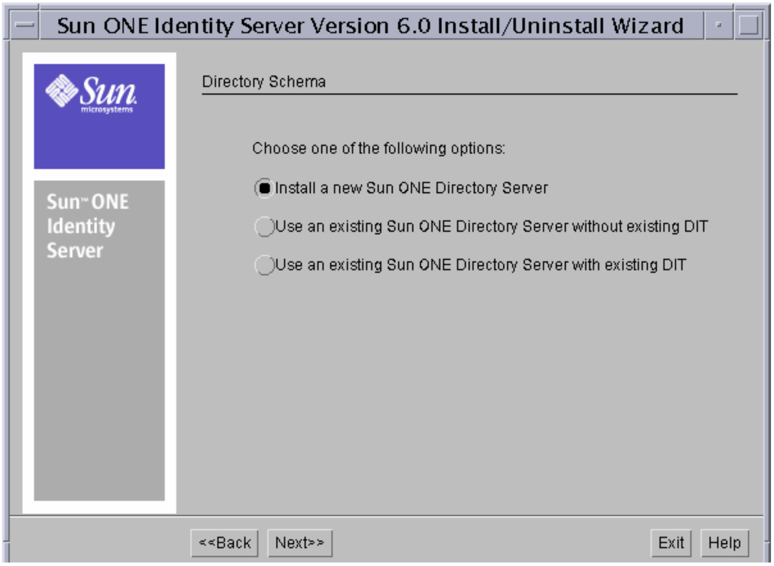
Host: Type the fully qualified domain name of the computer where the Identity Server components and a dedicated web server will be installed together. Make sure that the domain name of the computer is set and you have typed it correctly in the field. See "Setting the Domain Name" on page 42 for instructions on how to set the domain name.

Port: Type the port number of the Web Server that runs the Identity Server services. The default port is `58080`.

Console Deployment URI: This URI prefix tells the Web Server where to look for HTML pages associated with the Identity Server console and also for other web application-specific information like classes and jars. The default URI prefix is `amconsole`. You can type a different name.

11. In the Directory Schema panel, select "Install a new Sun ONE Directory Server," and then click Next.

Figure 4-3 Directory Schema Panel


Sun ONE Identity Server Version 6.0 Install/Uninstall Wizard
Sun microsystems
Sun™ ONE Identity Server
<<Back
Next>>
Exit
Help

Directory Schema

Choose one of the following options:

● Install a new Sun ONE Directory Server

○ Use an existing Sun ONE Directory Server without existing DIT

○ Use an existing Sun ONE Directory Server with existing DIT

12. In the Directory Root Suffix panel, provide the following information:

Sun ONE Identity Server root in your Directory tree: Type a distinguished name (DN) that you want to set as the root suffix. It should have at least one type=value pair. Examples:

```
o=edisonwatson
```

```
dc=madisonparc,dc=com
```

13. Sun ONE Directory Server Information window, provide the following information, and then click Next:

    Host: Type the fully qualified domain name of the computer where Directory Server is installed.

    Port: Type the Directory Server port number.The default port is `389`. If the port is already in use, the installation program will prompt you to type another port number. You can type in another number (between 1 and 65535) that is not in use.

    Installation Directory: Type the full path to the directory where you want to install the Directory Server. It is recommended that you make sure that the default directory `/usr/iplanet/servers` is empty or specify a fresh installation directory. This is because if you ever need to uninstall, the uninstallation program will remove this directory with its contents and you may lose any data that previously resided in it.

    Directory Manager: Type the DN of the user who will have restricted access to Directory Server. Example: `cn=Directory Manager`

    Password: Type the password for Directory Manager. The password must be a minimum of eight characters in length.

    Confirm Password: To confirm the Directory Manager password, type it again.

14. In the Administration Server that Manages Directory Server panel, provide the following information, and then click Next:

    Administrator: Type the username of the administrator who will have access to the Administration Server that manages Sun ONE Directory Server. The default username is `admin`, which you can change.

    Port: Type a port number for the Administration Server that manages Directory Server. By default, this port is set at `58900`.

    Password: Type the password for the user `amAdmin`. the password must be a minimum of 8 characters in length.

    Confirm Password: To confirm the password, type it again.

15. In the Sun ONE Identity Server Internal LDAP Authentication User Information window, provide the following information and then click Next:

    Username: This is the Bind DN user for LDAP / Membership / Policy service. The user name *amldapuser* is hard coded and you cannot change it. This user will have read and search access to Directory Server entries.

    Password: Type the password for the *amldap* user. This password must be unique and different from the Top Level Administrator password that you would provide in the next panel. This password is the shared secret between Identity Server and Agents.

    Confirm Password: Retype the password to confirm.

16. In the Sun ONE Identity Server Top Level Administrator Information panel, provide the following information and then click Next:

    Username: The username for the Top Level administrator is `amAdmin`. This name cannot be reconfigured.

    Password: Type the password for the user `amAdmin`. the password must be a minimum of 8 characters in length. This password must be different from the the amldapuser password you provided in the previous panel.

    Confirm Password: To confirm the `amAdmin` password, type it again.

    Start the Server after installation: Click this option if you want to automatically start the Identity Server after installation. If you do not select this, you may start the server manually after installation. For steps to do this, see "Starting Identity Server Services" on page 165.

17. In the Currently Selected Settings panel, review the configuration information that you've entered. If you need to make changes, click Back, go to the required panels and make the changes. Otherwise, click Next to proceed.

18. In the Ready to Install panel, review the installation information. If you need to make changes, click Back to go to any of the previous panels. Otherwise, click Install Now to begin the installation.

19. In the Installation Summary panel, you can click Details for a detailed summary of the configuration information that was processed during Installation.

20. Click Exit to end the program.

Now that you have installed Identity Server, you can login to the Identity Server Console. For steps to do this, see "Logging In to the Administration Console" on page 167.

Chapter 5

Installing Identity Server Against an Existing Directory Server

This chapter provides instructions for installing Identity Server against an existing directory that contains user data. It also explains how to configure Identity Server to work with your directory information tree (DIT), and how to make the necessary changes to your existing Directory Server and directory entries. The number and scope of changes you must make will depend upon how your existing DIT is structured, and how you plan to use Identity Server.

Topics in this chapter include:

- Overview of Installation Tasks
- Before You Begin
- Installing Identity Server Schema
- Manually Configuring the Directory Server
- Installing User and Policy Management Services
- Starting Identity Server and Logging In
- Automatically Enabling Policy Management Services
- Manually Enabling Policy and User Management Services
- Adding Identity Server Object Classes to Existing Directory Entries
- Adding Custom Object Classes to Identity Server Schema
- Results of Identity Server and Directory Modifications

Overview of Installation Tasks

To install Identity Server against an existing DIT, you must first run the Installation program and then manually configure both Directory Server and Identity Server.

Running the Identity Server Installation Program

Detailed instructions for each of the following steps are provided in this chapter. It is important to follow the steps in the this exact sequence in order to avoid making unwanted changes to your directory.

1. Install Identity Server schema.

   In this step you run the Identity Server Installation program and select the "Configure Existing Directory Server" option. For detailed instructions, see "Installing Identity Server Schema" on page 67 in this chapter.

2. Manually Configure Directory Server to work with Identity Server.

   In this step you enable the Directory Server referential integrity plug-in, and create new database indexes. See "Manually Configuring the Directory Server" on page 69 in this chapter.

3. Install Identity Server user and policy management services.

   In this step you run the Identity Server Installation program a second time. For detailed installation instructions, see "Installing User and Policy Management Services" on page 71 in this chapter.

   Note that during Installation, you'll be asked whether you want to automatically or manually enable User and Policy Management services. For more information, see "Choosing a Procedure for Enabling Services" on page 65.

4. Enable one of three Identity Server modes:

   - Policy Management only
   - User Management only (after Policy Management is enabled)

- ❍ Both User Management and Policy Management at the same time

  If during Installation you chose to automatically enable Policy Management services, you can skip Step 4 and go on to Step 5. For more information, see "Automatically Enabling Policy Management Services" on page 79.

  If during Installation you chosen to manually enable User or Policy Management services, in this step you must manually enable the services. This requires some post-installation configuration. For a quick overview, see the next section "Post-Installation Configuration." For detailed instructions, see "Manually Enabling Policy and User Management Services" on page 81 in this chapter.

5. Start Identity Server.

   For detailed instructions, see "Starting Identity Server and Logging In" on page 88 in this chapter.

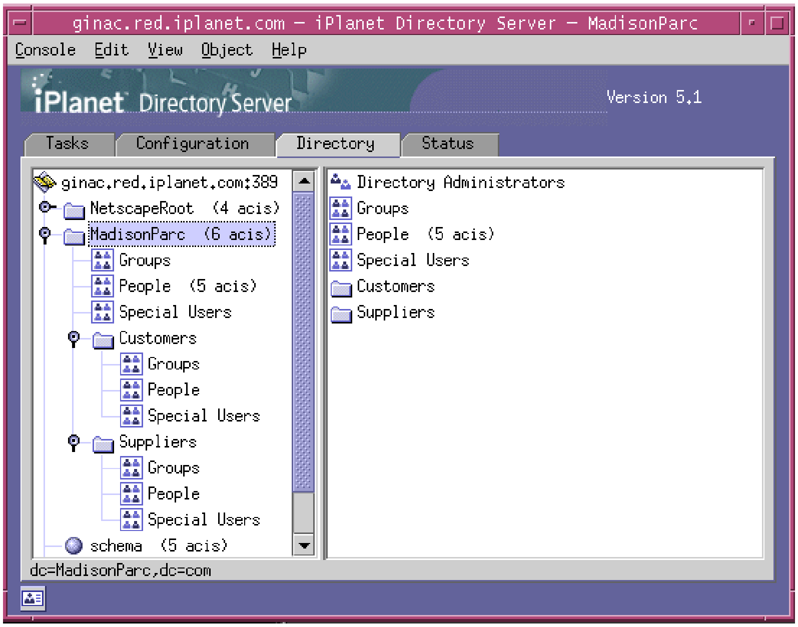
Post-Installation Configuration

If your existing DIT contains custom object classes, Identity Server won't recognize them until you manually configure both Identity Server and Directory Server.The types of changes you need to make are illustrated in this chapter using the DIT for MadisonParc, a fictitious company. The directory entries in the MadisonParc example include two custom object classes. These are object classes that are not already defined in the default Directory Server schema nor in the default Identity Server schema. If your existing DIT contains custom object classes or attributes, you'll need to make similar changes in your directory and in your Identity Server XML files.

Existing DIT Examples in This Chapter

Figure 5-1 illustrates the Directory Server console view of the DIT for MadisonParc. The tree includes three organizational units (ou) at the top level of the tree: Groups, People, and Special Users. These organizational units contain entries for MadisonParc employees. Two organizations (dc), Customers and Suppliers, were created under the root level to contain entries for non-employees.

Figure 5-1 The existing DIT for MadisonParc.



Adding Marker Object Classes to Existing Directory Entries

Before Identity Server can recognize the data in an existing directory, an you must add special object classes to entries for all organizations, groups and users that will be managed by Identity Server. Detailed steps and examples based on the MadisonParc DIT are provided in this chapter. See "Adding Identity Server Object Classes to Existing Directory Entries" on page 90. Sample scripts are bundled in the product to help you automatically add these object classes to your directory.

Adding Custom Object Classes to Identity Server Schema

In the MadisonParc example, there are two custom object classes and three custom attributes. These object classes and attributes are not included in the Identity Server schema nor in the Directory Server 5.1 SP1 schema.Table 5-1 summarizes the custom objects and their uses in the MadisonParc DIT.

Table 5-1 User-defined objects used in the MadisonParc DIT.

Object	Description
`madisonparc-org`	Object class added to all organization entries.

Table 5-1 User-defined objects used in the MadisonParc DIT.

Object	Description
`madisonparc-org-description`	Attribute added to each organization entry; required by `madisonparc-org`.
`company`	Object class added to all user entries.
`acctNumber`	Attribute added to each user entry; required by the `company` object class.
`companyName`	Attribute added to each user entry; required by the `company` object class.

Before a MadisonParc administrator can use Identity Server to manage these extensions, the following modifications would have to be made in the Identity Server schema:

- Add the two custom object classes and three custom attributes to `umsExisting.xml`
- Add `madisonparc-org` to `amEntrySpecific.xml`
- Add `madisonparc-org-description` to `amEntrySpecific.properties`
- Add `companyName` and `acctNumber` to `amUser.xml`.
- Add `companyname` and `acctNumber` to `amUser.properties`.

Detailed steps and examples are provided in this chapter. See "Adding Custom Object Classes to Identity Server Schema" on page 108.

Before You Begin

You must resolve the following issues before you can install Identity Server against an existing Directory Server that is provisioned with users.

Directory Server Issues

Refer to the documentation for Sun ONE Directory Server for detailed information about the following issues.

Migrating Pre-5.1 SP1 Versions of Directory Server

If you are using a pre-5.1 SP1 version of Directory Server, you must upgrade your existing Directory Server to version 5.1 SP1, and then migrate your existing data to the upgraded directory. For detailed instructions, see the Directory Server documentation at the following URL:
`http://docs.sun.com/source/816-5610-10/upgrade.htm#997630`.

Backing Up Directory Server 5.1 SP1

The installation and post-installation tasks described in this chapter require numerous changes to your existing directory. Be sure to back up the Directory Server before you install running the Identity Server installation program. To back up Directory Server, use `db2ldif` or `db2bak`, or use the Directory Server console. For detailed information on backing up your directory, see the *Sun ONE Directory Server Installation Guide* at:

```
http://docs.sun.com/db/doc/816-5602-10
```

Directory Server Access

Before you run the Identity Server Installation program, be sure that Directory Server is running, and that Identity Server can access it.

Migrating Pre-6.0 Versions of Identity Server

If you have iPlanet Directory Server-Access Management Edition (DSAME) 5.0 or 5.1 already installed, you must migrate the data from DSAME 5.1 to Identity Server 6.0. For detailed instructions, see Appendix A, "Migrating Data from DSAME 5.1 to Identity Server 6.0" on page 173.

Using Appropriate Administrator Privileges

- You must log in as root on Solaris or as Administrator on Windows 2000 to run the Installation program.
- You must have appropriate administrator privileges in the Directory Server to modify user entries.

Displaying the Installation Wizard on UNIX

To use the Installation wizard on UNIX, your DISPLAY variable must be set for the computer system where you are installing Identity Server or its components. Also be sure that your have authorization to connect to the computer system where you are installing Identity Server or its components. If you cannot set either of these appropriately, you should use the command-line version of the Installation program.

Using Java 1.3.1_06

Be sure you are using Java 1.3.1_06. If you are using an older version of the JDK, during Identity Server Installation you will be asked to install version that comes with Identity Server, or to provide a path to Java 1.3.1_06.

Setting the Domain Name

Be sure the domain name and host name of the computer system where you will install Identity Server are set, and that the computer system is configured for host name lookup.

To Set the Domain Name On UNIX

1. View your host name setting by running the following command:

   ```
   # uname -n
   ```

   The short format of the host name is returned.

2. To set the domain name, do one of the following:

   - If the file `/etc/resolv.conf` exists, then enter the domain name in the domain configuration entry. Example: `domain madisonparc.com`

   - If the file `/etc/resolv.conf` does not exist, then enter the following command:

     ```
     # domainname domainname
     ```

     Example:

     ```
     # domainname madisonparc.com
     ```

     where `madisonparc.com` is the domain to which this computer system belongs.

3. To verify that the host name and domain name are set properly, you can enter the following command:

   ```
   # ping hostname.domainname
   ```

   If the host name is not returned, contact your network Administrator.

To Set the Domain Name on Windows 2000

1. On the Windows desktop, right-click My Computer and then click Properties.
2. In the System Properties window, click Network Identification.
3. Click Properties.
4. In the Computer Name field, if there is no name, enter a name for the host.
5. Click More.
6. In the Primary DNS Suffix of this computer field, enter the name of the domain to which this computer belongs.

   The Primary DNS Suffix combined with the computer name forms the fully-qualified domain name for this computer. Example:

   ```
   hostname.madisonparc.com
   ```

Removing Old Instances of Identity Server

Be sure that Identity Server packages or schema are not already installed in another directory on the computer system. To check for an existing packages, you can use the following command:

```
pkginfo
```

If packages beginning with `SUNWam` exist, Identity Server may have been previously installed on the computer system. If possible, uninstall Identity Server using its Uninstallation program. See "Uninstalling Identity Server" on page 167 and "Uninstalling Identity Server On Windows" on page 170 of this manual.

If Identity Server was not properly uninstalled, then you should manually remove the Identity Server packages and files now. Follow these steps:

1. Remove all Identity Server packages.

   First find all Identity Server packages installed on the computer system, run the following command:

```
pkginfo | grep SUNWam
```

Then use the pkgrm command to remove each package identified with either of the following:

- Sun ONE Identity Server 6.0
- iPlanet Directory Server Access Management Edition 5.1.

Important: There may be other Solaris packages beginning with SUNWam that should not be removed.

2. Remove the following files located in the directory /var/sadm/install if they exist:

   - productregistry
   - .lockfile
   - .pkg.lock

   Important: Exercise caution when removing the productregistry file. If you have other Sun ONE products installed which use the Setup SDK Installation program, then do *not* remove this file.

3. If the directory /var/sadm/pkg exists, remove all Identity Server packages from it.

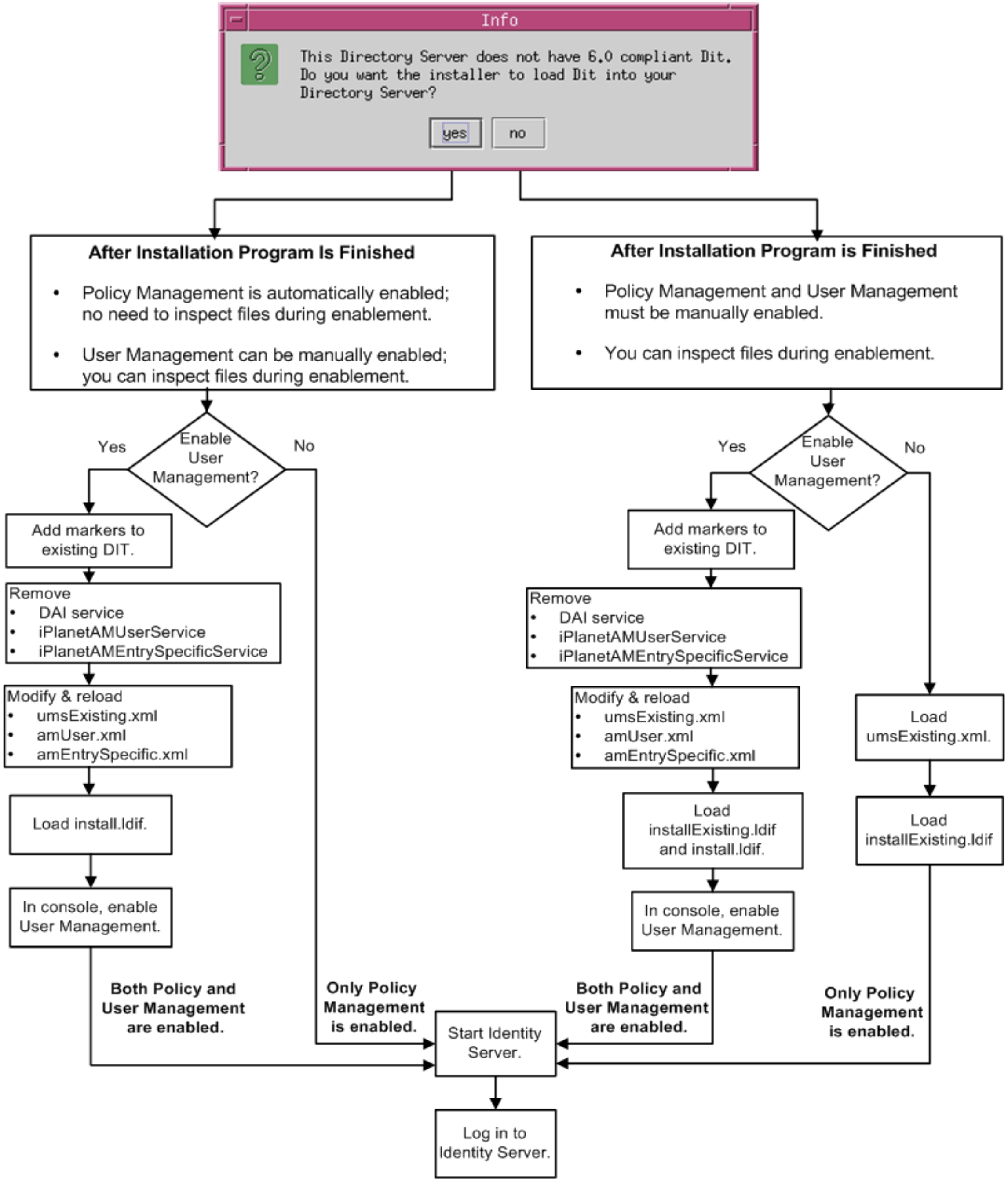
Choosing a Procedure for Enabling Services

During Installation, you'll be asked whether you want to automatically install the Identity Server schema and XML files, or to manually install them. Your choice should be based upon which one of the following you want to achieve:

- Enable Policy Management service only
- Enable User Management service only (after Policy Management is enabled)
- Enable both User Management and Policy Management services at the same time

To help you determine which procedure is best for your needs, Figure 5-2 on the next page provides a flowchart of the post-installation steps associated with each of these goals. For detailed information, see "Automatically Enabling Policy Management Services" on page 79 and "Manually Enabling Policy and User Management Services" on page 81 in this chapter.

Figure 5-2 Automatically vs. manually enabling Policy Management.



Info

This Directory Server does not have 6.0 compliant Dit. Do you want the installer to load Dit into your Directory Server?

yes
no
After Installation Program Is Finished
Policy Management is automatically enabled; no need to inspect files during enablement.
User Management can be manually enabled; you can inspect files during enablement.
After Installation Program is Finished
Policy Management and User Management must be manually enabled.
You can inspect files during enablement.
Yes
Enable User Management?
No
Add markers to existing DIT.
Remove
DAI service
iPlanetAMUserService
iPlanetAMEntrySpecificService
Modify & reload
umsExisting.xml
amUser.xml
amEntrySpecific.xml
Load install.ldif.
In console, enable User Management.
Yes
Enable User Management?
No
Add markers to existing DIT.
Remove
DAI service
iPlanetAMUserService
iPlanetAMEntrySpecificService
Modify & reload
umsExisting.xml
amUser.xml
amEntrySpecific.xml
Load installExisting.ldif and install.ldif.
In console, enable User Management.
Load umsExisting.xml.
Load installExisting.ldif
Both Policy and User Management are enabled.
Only Policy Management is enabled.
Both Policy and User Management are enabled.
Only Policy Management is enabled.
Start Identity Server.
Log in to Identity Server.

Installing Identity Server Schema

To install the Identity Server schema, you must run the Installation program. When you install the Identity Server schema this way, the `SUNWamdsc` package is installed in the Identity Server root directory. No new Directory Server is installed; no existing directory data is overwritten.

To Install Identity Server Schema

1. Log in to the host computer where Directory Server is installed.

2. Locate the Identity Server Installation program.

   If you're installing Identity Server schema from the product CD, insert the CD into the drive of the system on which you want to install the software. You'll find the Installation program in the following directory:

UNIX	`/cdrom/is_60/solaris`
Windows	*CDdrive*`:\cdrom\is_60\windows`

   If you've downloaded the compressed product binaries, in a temporary directory, unpack the product binaries. On UNIX, be sure to use the Solaris `tar` utility. To unpack the binaries, enter the following command:

UNIX	`gunzip -dc` *binaryfile*.tar.gz `| tar -xvof -`
Windows	`winzip` *binaryfile*.tar.zip

   where *binaryfile* is the name of the file you have downloaded. You'll find the Installation program in the directory where you unpacked the product binaries.

3. Start the Installation program.

   To run the Installation wizard, in the directory that contains the Installation program, enter the following command:

UNIX	`./setup`
Windows	`setup.exe`

   To run the Installation program from the command line, in the directory that contains the Installation program, enter the following command:

UNIX	`./setup -nosdisplay`

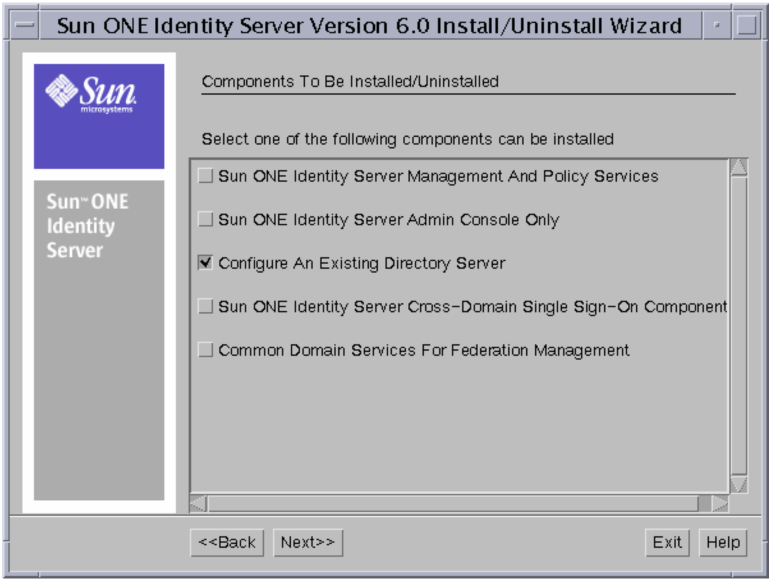
Windows `setup -nodisplay`

NOTE The remaining steps describe the GUI version of the Installation program. If you're using the command-line version of the Installation program, you'll be prompted to provide the same information as that presented in the Installation wizard. In the command-line version, you can use the following commands:

- Press `Enter` to accept a default value in [brackets], or to continue on after you've entered a new value.
- Press < to go back to the previous screen.
- Enter `Exit` to stop the program and return to the command line.

4. In the Welcome window, click Next.
5. To accept the terms of the License Agreement, click "I Accept."
6. In the Installation Directory window, enter the path to the directory where you want to install the Identity Server schema, and then click Next.
7. In the Components to be Installed / Uninstalled window, click "Configure an Existing Directory Server," and then click Next.

Figure 5-3 Components to be Installed / Uninstalled Panel



Sun ONE Identity Server Version 6.0 Install/Uninstall Wizard

Components To Be Installed/Uninstalled

Select one of the following components can be installed

□ Sun ONE Identity Server Management And Policy Services

□ Sun ONE Identity Server Admin Console Only

☑ Configure An Existing Directory Server

□ Sun ONE Identity Server Cross-Domain Single Sign-On Component

□ Common Domain Services For Federation Management

8. In Sun ONE Directory Server Information window, provide the following information, and then click Next:

   Host: Enter the fully qualified domain name of the computer where Directory Server is installed.

   Port: Enter the Directory Server port number.The default port is `389`.

   Directory Manager: Enter the DN of the user who has unrestricted access to Directory Server. This DN was specified when Directory Server was installed. Example: `cn=Directory Manager`

   Password: Enter the password that was entered for the Directory Manager when Directory Server was installed.

9. In the Currently Selected Settings window, review the settings you have selected, and then click Next.
10. In the Ready to Install window, click “Install Now.”
11. When the program is finished, in the Installation Summary window, click Close.

Note that once you’ve successfully installed Identity Server or any of its components on the local host, you can use the command line to automatically to install the Identity Server schema on an additional Directory Server instance. For more information, see “Installing and Uninstalling Identity Server Schema from the Command Line” on page 166.

Manually Configuring the Directory Server

After you’ve installed the Identity Server schema, you must configure the Directory Server to work with Identity Server. Perform the steps in the following procedures:

- Enable the Directory Server referential integrity plug-in
- Add Identity Server indexes

When the referential integrity plug-in is enabled, it performs integrity updates on specified attributes immediately after a delete or rename operation. This ensures that relationships between related entries are maintained throughout the database. Database indexes enhance the search performance in Directory Server.

NOTE Before continuing with these procedures, be sure that Directory Server is running.

To Enable the Referential Integrity Plug-In

1. In Directory Server console, click Configuration.
2. In the navigation tree, double-click Plug-ins to expand the list of Plug-ins.
3. In the Plug-ins list, click “referential integrity postoperation.”
4. In the properties area, check the “Enable plug-in” box.
5. Click Save.

The plug-in is not enabled until you restart Directory Server.

To Add Identity Server Indexes

1. In Directory Server console, click Configuration.
2. Add the `nsroledn` index.
   a. In the navigation tree, expand the root suffix, and then click the database that contains the directory entries you want to use in Identity Server.
   b. Click the Indexes tab.
   c. In the Indexes tab, click "Add attribute..."
   d. In the Select Attributes window, select the attribute `nsroledn`, and then click OK.
   e. In the Indexes tab, for the `nsroledn` attribute, check the following checkboxes: Equality, Presence, and Substring.
   f. Click Save.
   g. In the Indexes window, after the index is successfully created, click Close.
3. Add the `memberof` index.
   a. In the Indexes tab, click "Add attribute..."
   b. In the Select Attributes window, select the attribute `memberof`, and then click OK.
   c. In the Indexes tab, for the `memberof` attribute, check the following checkboxes: Equality and Presence.
   d. Click Save.
   e. In the Indexes window, after the index is successfully created, click Close.

4. Add the `iplanet-am-static-group` index.
   a. In the Indexes tab, click "Add attribute..."
   b. In the Select Attributes window, select the attribute `iplanet-am-static-group`, and then click OK.
   c. In the Indexes tab, for the `iplanet-am-static-group` attribute, check the following checkbox: Equality.
   d. Click Save.
   e. In the Indexes window, after the index is successfully created, click Close.
5. Add the `iplanet-am-modifiable-by` index.
   a. In the Indexes tab, click "Add attribute..."
   b. In the Select Attributes window, select the attribute `iplanet-am-modifiable-by`, and then click OK.
   c. In the Indexes tab, for the `iplanet-am-modifiable-by` attribute, check the following checkbox: Equality.
   d. Click Save.
   e. In the Indexes window, after the index is successfully created, click Close.
6. Add the `iplanet-am-user-federation-info-key` index.
   a. In the Indexes tab, click "Add attribute..."
   b. In the Select Attributes window, select the attribute `iplanet-am-user-federation-info-key`, and then click OK.
   c. In the Indexes tab, for the `iplanet-am-user-federation-info-key` attribute, check the following checkbox: Equality.
   d. Click Save.
   e. In the Indexes window, after the index is successfully created, click Close.
7. Restart Directory Server.

Installing User and Policy Management Services

After you’ve installed the Identity Server schema and manually configured the Directory Server, you must run the Installation program a second time. This time, the following components will be installed:

- Sun ONE Web Server
- Sun ONE Identity Server Console
- Common Domain Services
- Identity Server User Management and Policy Services
- JDK 1.3.1_6

To Install User and Policy Management Services

Important: During installation, you must indicate which procedure you want to use for enabling these services after the Installation program is finished. For detailed information, see "Choosing a Procedure for Enabling Services" on page 65.

1. Start the Installation program.

   To run the Installation wizard, in the directory that contains the Installation program, enter the following command:

UNIX	`./setup`
Windows	`setup.exe`

   To run the Installation program from the command line, in the directory that contains the Installation program, enter the following command:

UNIX	`./setup -nosdisplay`
Windows	`setup -nodisplay`

   NOTE The remaining steps describe the GUI version of the Installation program. If you're using the command-line version of the Installation program, you'll be prompted to provide the same information as that presented in the Installation wizard. In the command-line version, you can use the following commands:

   - Press Enter to accept a default value in [brackets], or to continue on after you've entered a new value.
   - Press < to go back to the previous screen.
   - Enter Exit to stop the program and return to the command line.

2. In the Welcome window, click Next.

3. To accept the terms of the License Agreement, click "I Accept."

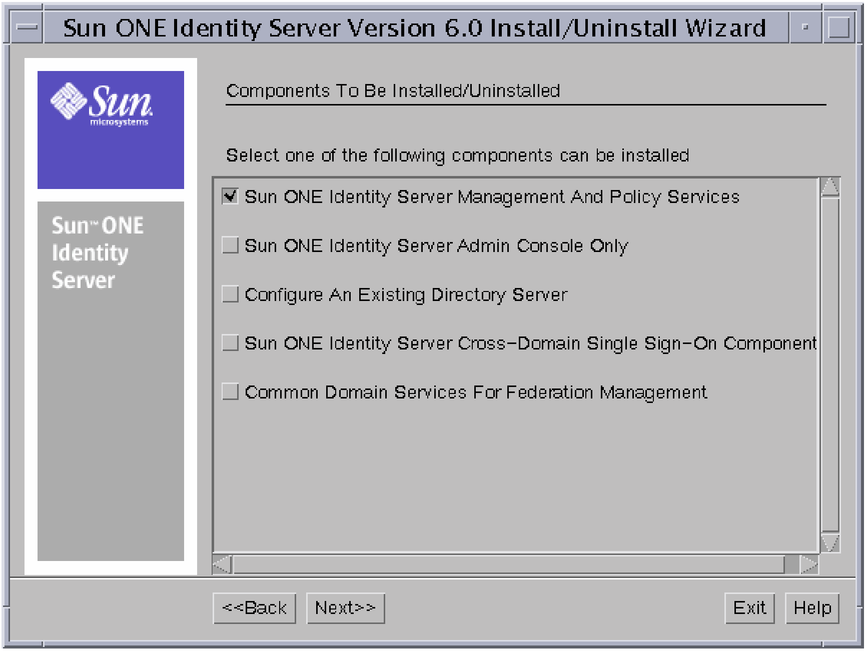
4. In the Installation Directory panel, provide the following information, and then click Next:

   Install Sun ONE Identity Server in this directory: Enter the path to the directory where Identity Server Services will be installed. You must have write and execute permissions in this directory.

NOTE	Plan to install the Identity Server Services and Directory Server in different directories. Ideally, you would install Identity Server Services and Directory Server on different computer systems.

5. In the Components to Be Installed / Uninstalled window, select "Sun ONE Identity Server Management and Policy Services," and then click Next.

Figure 5-4 Components to Be Installed / Uninstalled Panel



Sun ONE Identity Server Version 6.0 Install/Uninstall Wizard

Components To Be Installed/Uninstalled

Select one of the following components can be installed

☑ Sun ONE Identity Server Management And Policy Services

□ Sun ONE Identity Server Admin Console Only

□ Configure An Existing Directory Server

□ Sun ONE Identity Server Cross-Domain Single Sign-On Component

□ Common Domain Services For Federation Management

6. In the Java SDK Configuration window, provide the following information, and then click Next:

   Do you want to use custom JDK? Java support in the Web Server requires Java SDK 1.3.1_06, which is provided with Identity Server 6.0. If you want to install the Java SDK available with Identity Server, select No. If you want to use a JDK (version 1.3.1_06 or higher), that you already have, select Yes and then Enter the full path to its location.

7. In the Sun ONE Web Server Information panel, provide the following information about the Web Server that will run Identity Server services, and then click Next:

   Administrator: Enter the user name for the administrator who will access and manage the Web Server.

   Port: Enter the port number. Typically, the default is 58888.

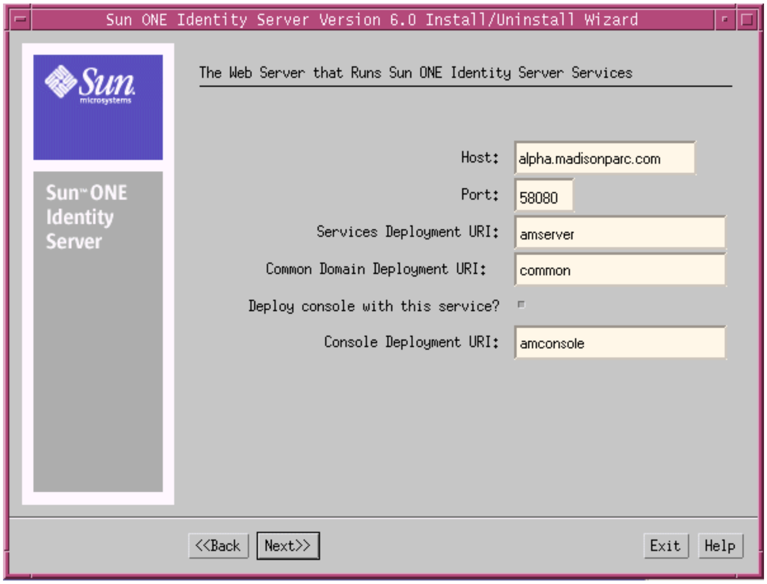
   Password: Enter the Administrator's password. The password must be a minimum of eight characters in length.

   Confirm Password: To confirm the Administrator password, enter it again.

   Enter user to run server as: Enter the user account the Web Server will run as. Example: nobody

   Enter group to run this server as: Enter the group the above user belongs to. Example: nobody

8. In the “Web Server that Runs Sun ONE Identity Server Services” window, provide the following information, and then click Next


Sun ONE Identity Server Version 6.0 Install/Uninstall Wizard
Sun microsystems
Sun™ ONE Identity Server
<<Back
Next>>
Exit
Help

The Web Server that Runs Sun ONE Identity Server Services

Host: alpha.madisonparc.com

Port: 58080

Services Deployment URI: amserver

Common Domain Deployment URI: common

Deploy console with this service? □

Console Deployment URI: amconsole

Host: Enter the fully qualified host name of the computer where the Identity Server components and a dedicated web server will be installed together. Make sure that the domain name of the computer is set and you have entered it correctly in the field. See the section “Setting the Domain Name” on page 63 for instructions on setting the domain name.

Port: Enter the port number of the Web Server that runs the Identity Server services. The default port is `58080`.

Services Deployment URI: The Universal Resource Identifier (URI) prefix tells the Web Server where to look for HTML pages associated with a service and also for web application-specific information such as classes and jars.

The default URI prefix is `amserver`. You can enter a different name.

Common Domain Deployment URI: The URI for accessing the common domain services on the Web Server. The default URI is `common`. You can enter a different name.

Deploy console with this service? By default, this box is checked to indicate that the console will be installed with the Identity Server services. However, if you have an existing console and do not want to deploy the console now, click the check box to clear the selection. In this case, the installation program will display another panel to seek more information about the existing console. See the next step for details.

Console Deployment URI: This URI prefix tells the Web Server where to look for HTML pages associated with the Identity Server console and also for other web application-specific information like classes and jars. The default URI prefix is `amconsole`. You can enter a different name. This field is not available, if you cleared the check box “Deploy Console with this Service?”

9. If, in the previous step, you chose to deploy the console with this server, skip to Step 10.

   If, in the previous step, you chose not to deploy the console with this service, you must provide the following information about the existing console. In the Web Server that Runs Sun ONE Identity Server Console window, provide the following information, and then click Next:

   Host: Enter the fully qualified domain name of the computer where the Identity Server Console is installed.

   Port: Enter the port number of the Web Server that runs the Identity Server services. The default port is `58080`.

   Console Deployment URI: This URI prefix tells the Web Server where to look for HTML pages associated with the Identity Server console and also for other web application-specific information like classes and jars. The default URI prefix is `amconsole`. You can Enter a different name.

10. In the Directory Schema panel, choose **Use an existing Sun ONE Directory Server with an existing DIT**, and then click Next.

    Use an existing Sun ONE Directory Server without existing DIT: Choose this option only if your existing Directory Server is not provisioned with users. This option is useful, for example, when you want to install Directory Server on a separate computer system for enhanced performance.

    Use an existing Sun ONE Directory Server with an existing DIT: Choose this option if you want to install Identity Server against a local Directory Server, and you plan to use its user management functionality.

    Do *not* choose the “Install a new Sun ONE Directory Server” option.

11. In the Directory Root Suffix panel, provide the following information, and then click Next:

    Sun ONE Identity Server Root in the Directory Server: Enter a distinguished name (DN) that you want to set as the root suffix. It should have at least one type=value pair.

    Examples:

    ```
    o=EdisonWatson
    ```

    ```
    dc=MadisonParc,dc=com
    ```

12. In the Sun ONE Directory Server Information panel, provide the following information, and then click Next:

    Host: Enter the fully qualified domain name of the computer where Directory Server is installed.

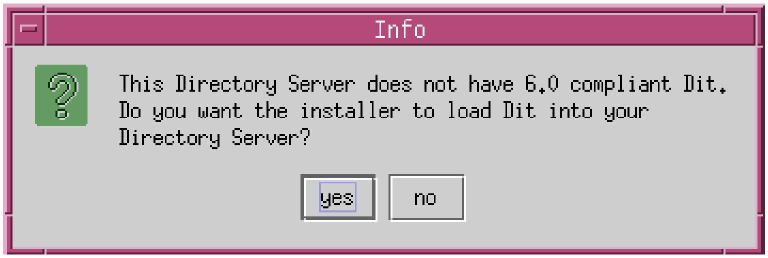
    Port: Enter the Directory Server port number.The default port is `389`.

    Directory Manager: Enter the DN of the user who will have restricted access to Directory Server. Example: `cn=Directory Manager`

    Password: Enter the password for Directory Manager. The password must be a minimum of eight characters in length.

    If the information you provide in any of these fields is inaccurate, the installation program will display an error message. Check the values you have provided and correct them to proceed.

13. The following message displays:



This Directory Server does not have 6.0 compliant Dit.
Do you want the installer to load Dit into your
Directory Server?

- If you click Yes, then the Identity Server schema and LDIF files are automatically loaded into Directory Server for you. Use this option if you want to enable only Policy Management services at this time, and if you are not concerned with reviewing changes to the directory immediately after each file is loaded. When you choose “Yes,” the Policy Management services are automatically enabled for you, but User Management services are not.For more information, see “Automatically Enabling Policy Management Services” on page 79.

If you want to enable User management services at a later time, you must follow the instructions in “Enabling User Management Only” on page 82.

- If you click No, then after installation, you must manually load the schema and LDIF files required to enable either Policy Management or User Management services. At that time, you will have the opportunity to review changes to the directory immediately after each file is loaded. For more information, see “Manually Enabling Policy and User Management Services” on page 81.

14. In the Existing DIT and Schema Information window, provide the following information, and then click Next:

    Marker object class for organizations: Enter the object class defined for the organization in your existing DIT. The default is `organization`. In the `dc=MadisonParc, dc=com` example used in this chapter, the object class defined for the organization is `domain`.

    Naming attribute for organizations: Enter the naming attribute used to define organizations in your existing DIT. If your existing DIT uses `o=organization`, you can accept the default value `o`. In the `dc=MadisonParc, dc=com` example used in this chapter, the naming attribute for organizations is `dc`.

    Marker object class for users: Enter the object class defined for users in your DIT.

    Naming attribute for users: Enter the naming attribute used for users in your existing DIT. If the DIT does not use `uid`, you may overwrite the default value displayed in the field.

15. In the Sun ONE Identity Server Internal LDAP Authentication User Information window, provide the following information, and then click Next.

    Username: This is the `bind DN` user for LDAP, Membership, and Policy services. This user will have read and search access to all Directory Server entries. The user name `amldapuser` is hard-coded and you cannot change it.

    Password: Enter the password for the `amldapuser`. This password must be different from the Top Level Administrator password which you will provide in the next Installation window. The `amldapuser` password is the Shared Secret between Identity Server and Agents.

    Confirm Password: Re-enter the password to confirm.

16. In the Sun ONE Identity Server Top Level Administrator panel, provide the following information, and then click Next:

    Username: The Top Level Administrator has unlimited access to all entries managed by Identity Server. The username for the Top Level Administrator is `amAdmin`; this username is hardcoded. This ensures that the Identity Server administrator role and its privileges are created and mapped properly in the Directory Server so that you can log onto Identity Server immediately after installation. Since this is an administrator role, you can add other users to this role after installation.

    Password: Enter the password for the user `amAdmin`. The password must be a minimum of 8 characters in length.

    Confirm Password: To confirm the `amAdmin` password, enter it again.

    Start the Server after installation: Click this option if you want to automatically start the Identity Server after installation. If you do not select this, you must start the server manually after installation. For steps to do this, see "Starting Identity Server and Logging In" on page 88.

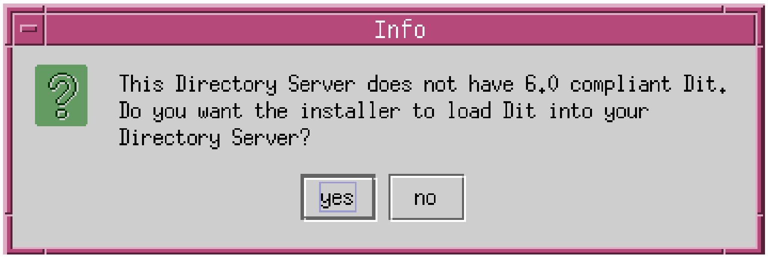
17. In the Currently Selected Settings panel, review the choices you have made in the previous panels. If you want to revisit any of the panels, click Back. When you are ready to proceed with the installation, click Next.

18. When the Installation program is finished, click Next.

Automatically Enabling Policy Management Services

You can automatically enable Policy Management services if you want to use Identity Server to manage policies, but not to create or manage user entries.

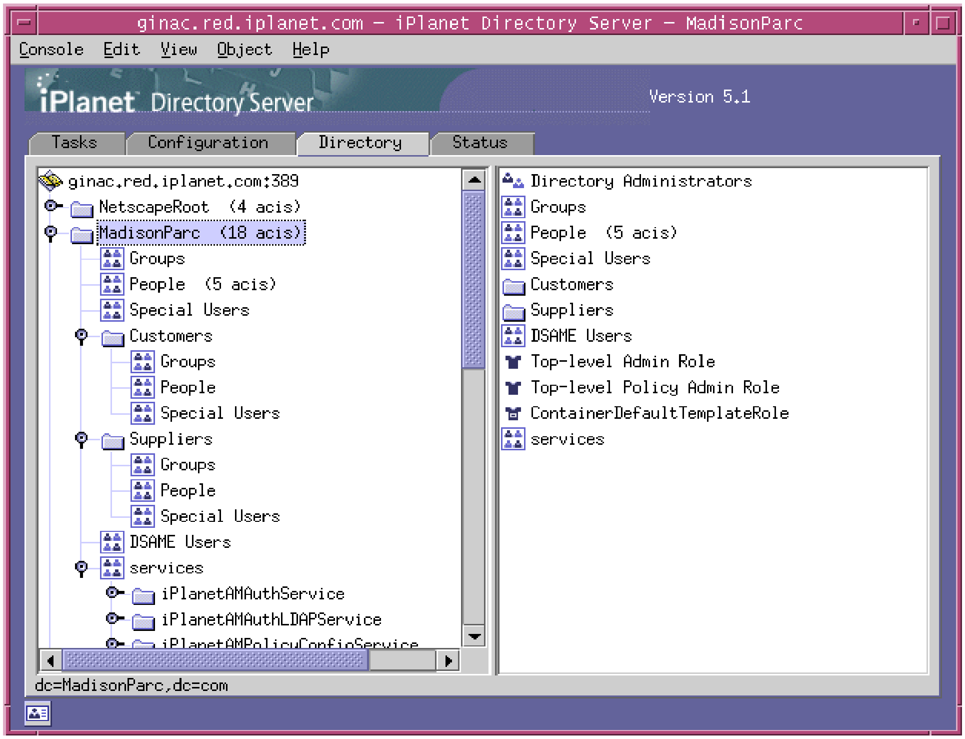
Policy Management is automatically enabled for you only if, during Installation, you answer "Yes" to the following question:



This Directory Server does not have 6.0 compliant Dit. Do you want the installer to load Dit into your Directory Server?

When the Policy Management services are automatically installed against your existing DIT, immediately after Installation you'll see the Identity Server object classes, roles, users, and services in your Directory Server console view. Figure 5-5. illustrates the existing DIT for the MadisonParc examples used in this chapter.

Figure 5-5 Policy Management services installed against the existing MadisonParc DIT.



ginac.red.iplanet.com:389
NetscapeRoot (4 acis)
MadisonParc (18 acis)
Groups
People (5 acis)
Special Users
Customers
Groups
People
Special Users
Suppliers
Groups
People
Special Users
DSAME Users
services
iPlanetAMAuthService
iPlanetAMAuthLDAPService
iPlanetAMPolicyConfigService

Directory Administrators
Groups
People (5 acis)
Special Users
Customers
Suppliers
DSAME Users
Top-level Admin Role
Top-level Policy Admin Role
ContainerDefaultTemplateRole
services

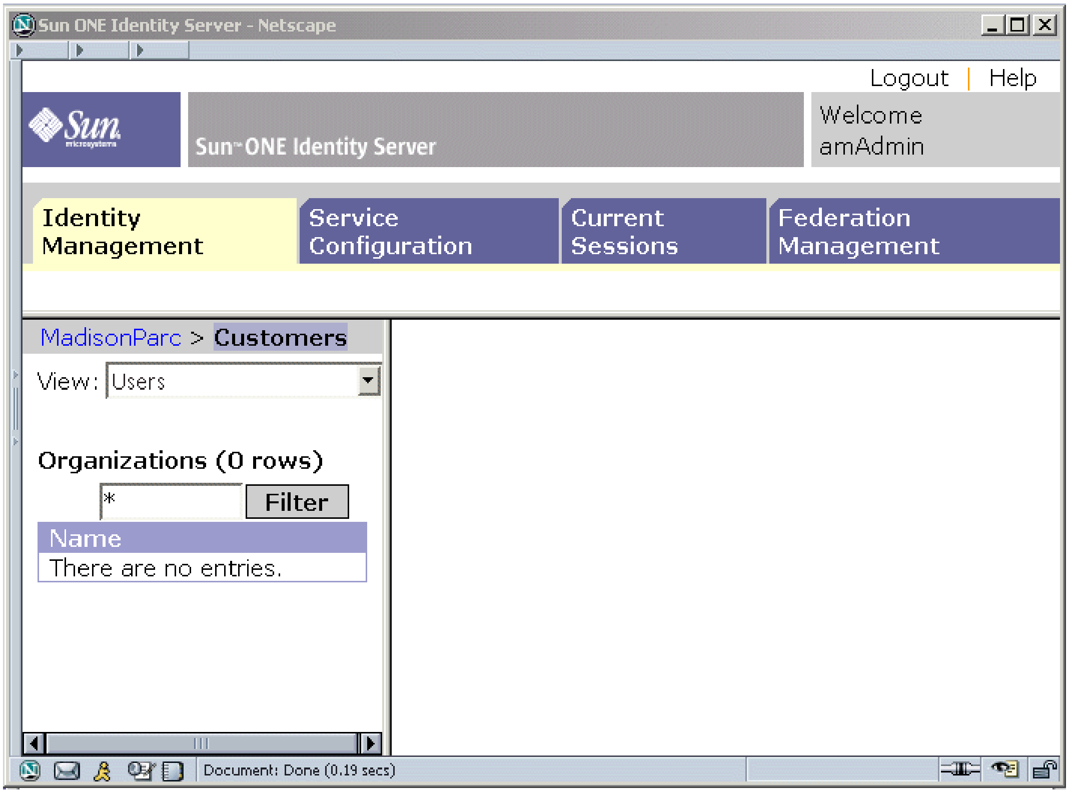
dc=MadisonParc,dc=com

For instructions on starting Identity Server and logging in, see "Starting Identity Server and Logging In" on page 88.

When you log into Identity Server for the first time, you will see the root suffix and organizations you specified during installation. For the MadisonParc example used in the beginning of this chapter, you would see the root suffix `MadisonParc.com`, and the two organizations `Customers` and `Suppliers`. You will not be able to see the rest of your existing directory entries unless you manually enable User Management services. See "Enabling User Management Only" on page 82.

When you see the Identity Server interface (see Figure 5-6), you can immediately begin creating policies. See the *Identity Server Administration Guide* for more information.

Figure 5-6 Identity Server interface at first-time login for MadisonParc.



Sun ONE Identity Server - Netscape

Logout | Help

Sun™ONE Identity Server

Welcome amAdmin

Identity Management | Service Configuration | Current Sessions | Federation Management

MadisonParc > Customers

View: Users

Organizations (0 rows)

* Filter

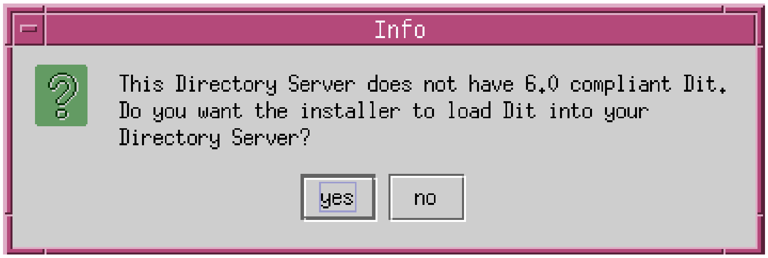
Name
There are no entries.

Document: Done (0.19 secs)

Manually Enabling Policy and User Management Services

You can manually enable Policy and User Management services if you want to use Identity Server to create and manage user entries in your directory, or if you want to visually inspect changes to your directory after each step in the enablement procedures.

You *must* manually enable either User or Policy Management services if, during Installation, you answer “No” to the following question:



Info

This Directory Server does not have 6.0 compliant Dit. Do you want the installer to load Dit into your Directory Server?

If you answer “Yes” to this question, you have the option to manually enable Use Management service. (Policy Management service is automatically enabled.)

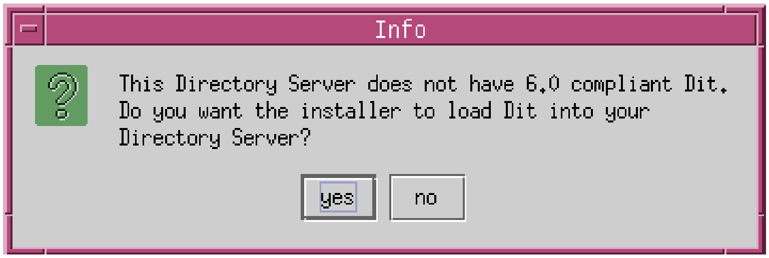
Manually enablement entails reconciling the Identity Server schema with your existing directory entries. Enablement procedures vary depending upon which of the following you want to achieve:

- Enable Policy Management service only
- Enable User Management service only (after Policy Management is enabled)
- Enable both Policy and Management services at the same time

Enabling User Management Only

Follow these steps after automatically enabling Policy Management, and only if both of these are true:

- You want to use Identity Server to create and manage user accounts at this time.
- During Identity Server installation, you answered “Yes” to the following question:



Info

This Directory Server does not have 6.0 compliant Dit. Do you want the installer to load Dit into your Directory Server?

To enable User Management only:

1. Add Identity Server object classes and attributes to your existing DIT.

   For detailed instructions, see “Adding Identity Server Object Classes to Existing Directory Entries” on page 90 in this chapter.

2. Remove the DAI service. In the following directory:

   ```
   Identity_Server_root/bin
   ```

   execute the following command:

   ```
   ./amadmin -u "user_naming_attibute=amadmin,ou=people,root_suffix"
      -w password -r DAI
   ```

   For more information about the DAI service, see “The DAI Service” on page 109 of this chapter.

3. Modify the Identity Server `ums.xml` file.

   See “Adding Identity Server Object Classes to Existing Directory Entries” on page 90 in this chapter for more information. The section provides detailed instructions on performing the following steps:

   a. Modifying the Creation Templates

   b. Adding Attributes to the Organization Schema

   c. Adding Attributes to the User Schema

4. Reload the DAI service by entering the following command:

   ```
   Identity_Server_root/bin/amadmin -u
     "user_naming_attibute=amadmin,ou=people,root_suffix"
        -w password -s ums.xml
   ```

5. Load the `install.ldif` file.

   For detailed information, see “install.ldif” on page 122.

6. Restart Identity Server.

   In the following directory:

   ```
   Identity_Server_root/bin
   ```

   execute the following command:

   ```
   ./amserver start
   ```

7. Log in to Identity Server console as `amAdmin`.

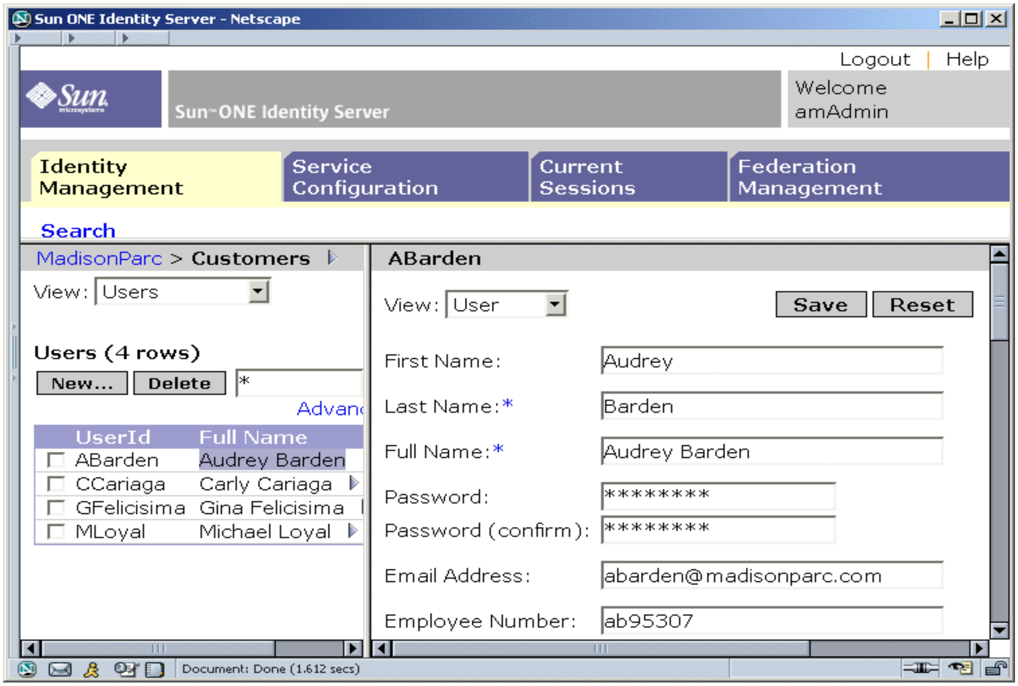
   You will not see your existing groups and users from your existing DIT until you complete the following two steps.

8. In the Identity Server console, click Service Management > Administration.

9. In the Administration window, click the "Enable User Management" box, and then click Save.

Once you've checked the "Enable User Management" box, you should see all entries beneath the organization level in Identity Server. For instructions on using Identity Server to create or manage users and policies, see the *Administration Guide*.

Figure 5-7 Identity Server with data from existing MadisonParc DIT



Users (4 rows)

	UserId	Full Name
□	ABarden	Audrey Barden
□	CCariaga	Carly Cariaga
□	GFelicisima	Gina Felicisima
□	MLoyal	Michael Loyal

ABarden

View: User

First Name: Audrey

Last Name:* Barden

Full Name:* Audrey Barden

Password: ********

Password (confirm): ********

Email Address: abarden@madisonparc.com

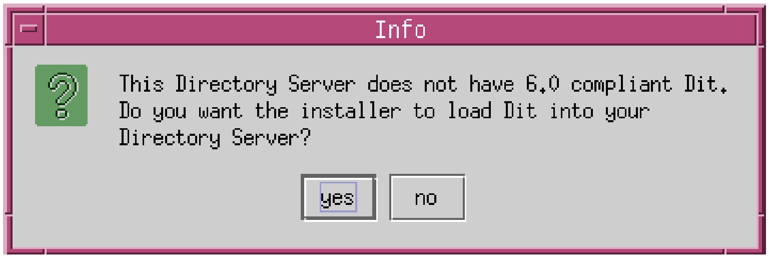
Employee Number: ab95307

Enabling Policy Management Service Only

Follow these steps only if all of these are true:

- You want to use Identity Server to create and manage policies.

- You do *not* want to use Identity Server to create or manage user accounts at this time. (You can enable this feature at a later time.)
- During Identity Server installation, you answered "No" to the following question:



Info

This Directory Server does not have 6.0 compliant Dit. Do you want the installer to load Dit into your Directory Server?

To enable Policy Management only:

1. Load the `installExisting.ldif` file into your existing directory.

For detailed instructions, see "Adding Identity Server Object Classes to Existing Directory Entries" on page 90 of this chapter.

2. In the following file:

Identity_Server_root`/config/ums/amserveradmin`

change the filename `ums.xml` to `umsExisitng.xml`.

3. To load all XML files, enter the following command:

Identity_Server_root`/config/ums/amserveradmin`
`"`*user_naming_attibute*`=amadmin,ou=people,`*root_suffix*`"` *password*

4. Restart Identity Server.

In the following directory:

Identity_Server_root`/bin`

execute the following command:

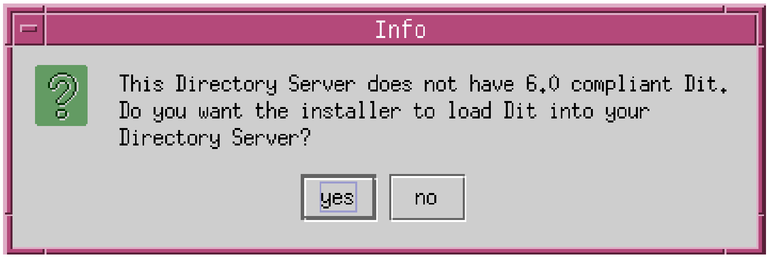
```
./amserver start
```

You can now log in to the Identity Server console to perform policy management tasks. See the *Administration Guide* for more information.If you want to enable user management later, follow steps in the next section.

Enabling Both User and Policy Management Services

Follow these steps only if all of these are true:

- You want to use Identity Server to create and manage policies now.
- You want to use Identity Server to create or manage user entries now.
- During Identity Server installation, you answered “No” to the following question:



Info

This Directory Server does not have 6.0 compliant Dit. Do you want the installer to load Dit into your Directory Server?

To enable both User and Policy Management:

1. Add Identity Server object classes and attributes to your existing DIT.

   For detailed instructions, see “Adding Identity Server Object Classes to Existing Directory Entries” on page 90 in this chapter.

2. Modify the Identity Server schema.

   See “Adding Custom Object Classes to Identity Server Schema” on page 108 in this chapter for more information. The section provides detailed instructions on performing the following steps:

   a. Modifying the Creation Templates

   b. Adding Attributes to the Organization Schema

   c. Adding Attributes to the User Schema

3. To load all XML files, enter the following command:

```
Identity_Server_root/config/ums/amserveradmin
   "user_naming_attibute=amadmin,ou=people,root_suffix" password
```

4. Load `installExisting.ldif` file into your Directory Server.

   For detailed instructions, see “Loading Identity Server LDIF into Your Directory” on page 120 in this chapter.

5. Load `install.ldif` file into your Directory Server.

   For detailed instructions, see “install.ldif” on page 122 in this chapter.

6. Restart Identity Server.

   In the following directory:

   Identity_Server_root/`bin`

   execute the following command:

   ```
   ./amserver start
   ```

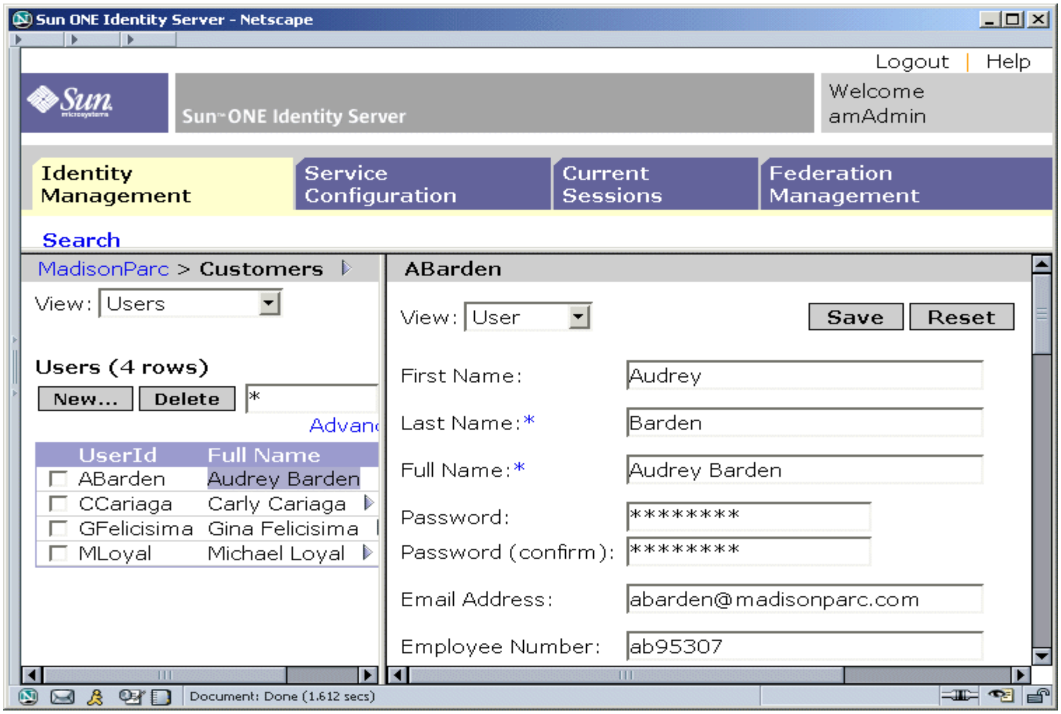
7. Log in to Identity Server as `amAdmin`.

8. In the to Service Configuration view, click Administrator.

9. Check the "Enable User Management" box, and click Save.

Once you’ve checked the “Enable User Management” box, you should see all entries beneath the organization level in Identity Server. For instructions on using Identity Server to create or manage users and policies, see the *Administration Guide*.

Figure 5-8 Identity Server with data from existing MadisonParc DIT



MadisonParc > Customers

View: Users

Users (4 rows)

	UserId	Full Name
□	ABarden	Audrey Barden
□	CCariaga	Carly Cariaga
□	GFelicisima	Gina Felicisima
□	MLoyal	Michael Loyal

ABarden

View: User

First Name: Audrey

Last Name:* Barden

Full Name:* Audrey Barden

Password: ********

Password (confirm): ********

Email Address: abarden@madisonparc.com

Employee Number: ab95307

Document: Done (1.612 secs)

Starting Identity Server and Logging In

After you've installed Identity Server and configured Directory Server appropriately, you can check the installation. Start Identity Server server and log in to the Identity Server Console as the user `amAdmin`. Once you successfully log in, you'll see the Identity Server web interface.

To start Identity Server on UNIX

To start Identity Server manually, at the command line enter the following command:

```
/Identity_Server_root/SUNWam/bin/amserver start
```

To start Identity Server on Windows

You can start Identity Server using the command line, or using the Start Menu.

From the command line

Enter the following commands in a Command Prompt window:

```
cd Identity_Server_root\bin
amserver start
```

From the Start Menu

1. From the Start menu, choose Settings > Control Panel > Administrative Tools > Services.
2. In the Services window, right-click SunONEIS-*hostname* and click Start.

To Log into the Identity Server Console

1. Go to the login URL using the form:

`http://`*host.domain*`:`*port*`/amserver/UI/Login`

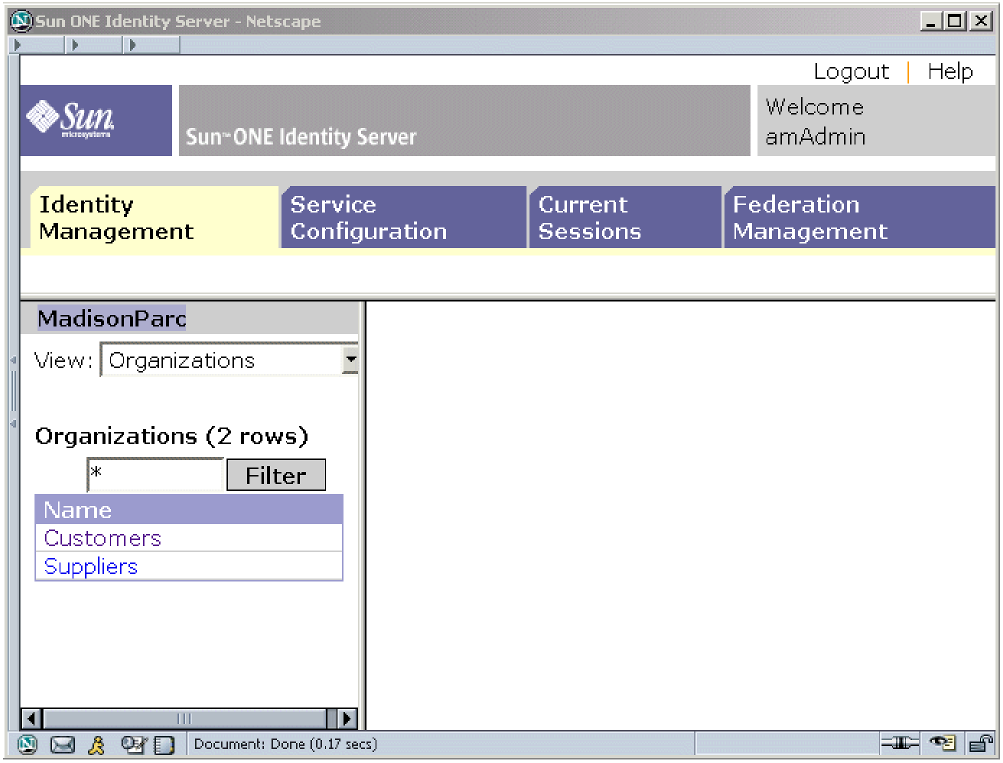
where *host* is the host name of the system, *domain* is the domain name of the server that runs Identity Server services, and *port* is the Identity Server services port number.

Example: `http://ginac.sun.com:58080/amserver/UI/Login`

2. In the Login page, enter the Top-Level Administrator user name `amAdmin`, and then enter the password you specified at installation.

When you log into Identity Server for the first time, you will see the root suffix and organizations you specified during installation. For the MadisonParc example used at the beginning of this chapter, you would see the root suffix `MadisonParc`, and the `two` organizations `Customers` and `Suppliers`.

Figure 5-9 First-time login for MadisonParc.



Sun ONE Identity Server - Netscape

Logout | Help

Sun™ ONE Identity Server

Welcome amAdmin

Identity Management | Service Configuration | Current Sessions | Federation Management

MadisonParc

View: Organizations

Organizations (2 rows)

* Filter

Name
Customers
Suppliers

Document: Done (0.17 secs)

Adding Identity Server Object Classes to Existing Directory Entries

After you've installed configured Identity Server, you must modify your existing directory entries to include the necessary Identity Server object classes and attributes. You can think of the Identity Server object classes as *markers* that indicate the directory entries you want to manage through Identity Server. These markers enable Identity Server to recognize the entries in your directory. The object classes contain special attributes that are necessary to achieve delegated administration.

Before You Begin

There are a number of resources you can use to facilitate the remaining steps for using an existing directory.

Examples Used in This Section

The examples used in this chapter are based on the DIT for a fictitious company named MadisonParc. Figure 5-10 shows two organizations, `Customers` and `Suppliers`, under the root.

Utilities and Scripts You Can Use

You can make these modifications by using Sun ONE Directory Server Console, or by using the `ldapmodify` or `db2ldif` utilities that come with Directory Server. You can also use the sample scripts that come with Identity Server.

Directory Server Utilities

Make sure that you're using the appropriate version of `ldapmodify`. Set your path to use the `ldapmodify` command that is shipped with Sun ONE Directory Server. (Do not use the version shipped with Solaris, which is found in `/bin` or `/usr/bin`.) Follow these procedures:

- On Solaris, add *Identity_Server_root*`/SUNWam/ldaplib/solaris/sparc/ldapsdk` to your `LD_LIBRARY_PATH` to pick up the appropriate Directory Server libraries. At the command line, enter:

  ```
  which ldapmodify
  ```

The following should be displayed:

```
Identity_Server_root/SUNWam/bin/ldapmodify
```

- If you are on Windows, you'll find ldapmodify in this directory of the Identity Server installation:

  ```
  Identity_Server_root\tools
  ```

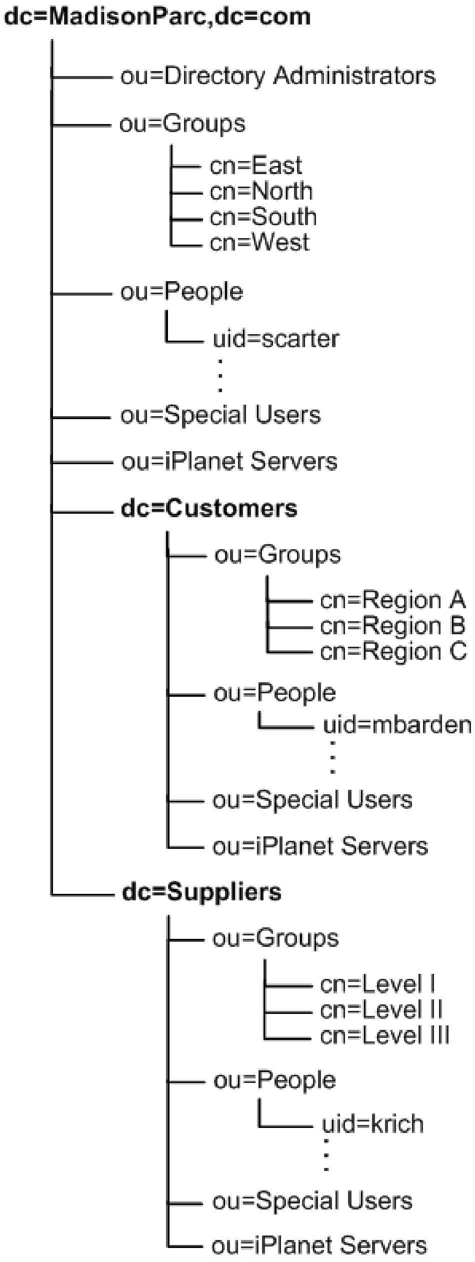
  Open a DOS prompt window and set the path to the ldapmodify tool.

  Example:

  ```
  set PATH=Identity_Server_root\tools;%PATH%
  ```

  For detailed information on how to make changes to the directory using these utilities or by using SunONE Console, see the documentation for Sun ONE Directory Server `http://docs.sun.com/db/prod/s1dirsrv`.

Figure 5-10 The existing MadisonParc DIT



Sample Migration Scripts

The sample scripts included with Identity Server require Perl 5.x or later. Table Table 5-2 provides descriptions of what each script adds to existing directory entries. You'll find the sample scripts in the following location:

UNIX	*Identity_Server_root*`/SUNWam/migration`
Windows	*Identity_Server_root*`\migration`

Table 5-2 Descriptions of scripts for adding Identity Server marker object classes.

Script	What it Does
`update-o.pl`	Adds the following to each organization entry: • `sunManagedOrganization` • `sunNameSpace` • `inetDomain` • `inetDomainStatus`
`update-people.pl`	Adds `iplanet-am-managed-people-container` to each people container.
`update-ou.pl`	Adds `iplanet-am-managed-org-unit` to each organizational unit.
`update-users.pl`	Adds the following to each user entry: • `inetadmin` • `iplanet-am-managed-person` • `iplanet-am-user-service` • `inetuser` • `iPlanetPreferences` • `inetOrgPerson`
`udpate-static-groups.pl`	Adds the following to each static group: • `iplanet-am-managed-static-group` • `iplanet-am-managed-group`
`update-filtered-groups`	Adds the following to each dynamic, or *filtered*, group: • `iplanet-am-managed-group` • `iplanet-am-managed-filtered-group`

Table 5-2 Descriptions of scripts for adding Identity Server marker object classes.

Script	What it Does
`update-assignable-dynamic-groups`	Adds the following to each assignable dynamic group: • `iplanet-am-managed-group` • `iplanet-am-managed-assignable group`
update-groups.pl	Adds `iplanet-am-managed-group-container` to each organizational unit that contains groups.

While these samples should prove useful, keep in mind that they are only tools to assist you in properly formatting the DIT and other data. Each script generates an LDIF file that you can inspect before making actual changes in your directory. You run each script a second time with the last line uncommented to make the actual changes. Steps for using each sample script are included in this chapter under the following headings:

- Marking Organizations
- Marking People Containers
- Marking Organizational Units
- Marking Users
- Marking Static Groups
- Marking Dynamic (Filtered) Groups
- Marking Assignable Dynamic Groups
- Marking Group Containers

Important: The changes made by using these scripts cannot be automatically undone. Be sure to back up your data before running each script.

Two Approaches to Modifying the Existing DIT

You can use one of two approaches for modifying the DIT. One option is to make all the necessary modifications to your DIT before loading the Identity Server LDIF and XML configuration files. This procedure is more error-prone, but may be faster if you have experience using LDAP.

The other option is to make a few modifications in your LDIF and XML files, and then start Identity Server to make sure those modifications were done correctly. This second approach is the recommended approach. For example, you may want to add the Identity Server object classes for each of your organizations, restart Identity Server, and verify that your organizations appear in the Identity Server Administration Console. Then add marker object classes for groups, check them and so forth.

Marking Organizations

If you used an existing organization as your default organization during installation, you do not have to make these changes. The installation program automatically added these object classes and attributes. Skip to "Marking People Containers" on page 97.

If you have sub-organizations or custom organizations you must make the following changes:

1. Add the following object classes to each organization entry:
    - `sunManagedOrganization`
    - `sunNameSpace`
    - `inetDomain`
2. Add the following attribute to each organization entry:
    - `inetDomainStatus`

In the MadisonParc example, these object classes and their attributes are added to the organizations `dc=Customers` and `dc=Suppliers`.

To Mark Organizations Using the Sample Script

1. Copy `update-o.pl` to the following directory:

    Directory_Server_root`/shared/bin`

2. Set the `$base` variable to the base suffix of the DIT to be managed by Identity Server. Example: `dc=MadisonParc,dc=com`
3. In the directory where the script is located, enter the following command:

    ```
    perl update-o.pl
    ```

4. When prompted, provide the following information:

   Enter Host Name: Enter the name of the computer system in which your Directory Server is installed.

   Enter Bind User Name: Enter a username that has sufficient privileges for accessing the entire directory. Example: `cn=Directory Manager`

   Enter Bind password: Enter the password for the user you specified above.

   Enter port number: Enter the Directory Server port number. Example: `389`

5. Check the results in the file `orgs-updated.ldif` that is generated by the script, and verify that the appropriate changes are listed. The changes contained in this file will automatically be made in the directory in the next step.

   Important Note: If there are organizations that you do not want to be managed by Identity Server, you should delete those entries from this `orgs-updated.ldif` now. Then, instead of going on to the next step, manually load the file using the following command:

   ```
   ldapmodify -h hostname -p port -D bind_user -w password -a -c -f
     orgs-updated.ldif
   ```

6. In the script `update-o.pl`, uncomment the last line and replace variables appropriately. For example, to add marker object classes to MadisonParc directory entries, the last line of the script is changed from this:

   ```
   #system("$LDAP_MODIFY -h'$host' -p'$port' -D'$bind_user'
       -w'$bind_pwd' -a -c -f orgs-updated.ldif");
   ```

   to this:

   ```
    system("$LDAP_MODIFY -h'ginac.MadisonParc.com' -p'389'
        -D'cn=Directory Manager' -w'password' -a -c -f
           orgs-updated.ldif");
   ```

In Code Example 5-1, the modifications to the MadisonParc directory entries are indicated in bold:

Code Example 5-1 Organization entries with marker object classes.

```
...
dn: dc=Customers,dc=MadisonParc,dc=com
dc: Customers
objectClass: top
objectClass: domain
objectClass: external
objectClass: sunManagedOrganization
objectClass: sunNameSpace
objectClass: inetDomain
```

Code Example 5-1 Organization entries with marker object classes. *(Continued)*

```
inetDomainStatus: Active


dn: dc=Suppliers,dc=MadisonParc,dc=com
dc: Suppliers
objectClass: top
objectClass: domain
objectClass: external
objectClass: sunManagedOrganization
objectClass: sunNameSpace
objectClass: inetDomain
inetDomainStatus: Active
...
```

Marking People Containers

People containers are typically assigned the ou attribute and are used to store all user entries for a branch of the directory. To each people container, add the `iplanet-am-managed-people-container` object class.

To Mark People Containers Using the Sample Script

1. Copy `update-people.pl` to the following directory:

   Directory_Server_root`/shared/bin`

2. Be sure the `$base` variable is set to the base suffix of the DIT to be managed by Identity Server. Example: `dc=MadisonParc,dc=com`

   In the MadisonParc example, the script was also modified to include people containers located under the organizations. In Code Example 5-2, bold indicates the change in the search scope.

Code Example 5-2 The scope in `update-people-container.pl` is modified.

```
# run search to find all people containers, putting their DNs in to a file
system("$LDAP_SEARCH -h \"$host\" -p \"$port\" -D \"$bind_user\"
   -w \"$bind_pwd\" -b \"$base\" -s sub -T \"(&(ou=$people)
      (!(objectclass=iplanet-am-*)))\" dn > people.dn");
```

3. In the directory where the script is located, at the command line enter the following:

   ```
   perl update-people.pl
   ```

4. When prompted, provide the following information:

   Enter Host Name: Enter the name of the computer system in which your Directory Server is installed.

   Enter Bind User Name: Enter a username that has sufficient privileges for accessing the entire directory. Example: `cn=Directory Manager`

   Enter Bind password: Enter the password for the user you specified above.

   Enter port number: Enter the Directory Server port number. Example: `389`

   Enter People Container: Enter the name of the people container that contains the uids you want to modify. Example: `People`

5. Check the results in the file `people-updated.ldif` which is created in the same directory as the script, and verify that the appropriate changes were made. The changes contained in this file will automatically be made in the directory in the next step.

   Important Note: If there are people containers that you do not want to be managed by Identity Server, you should delete those entries from `people-updated.ldif` now. Then, instead of going on the to next step, manually load the file using the following command:

   ```
   ldapmodify -h hostname -p port -D bind_user -w password -a -c -f
     people-updated.ldif
   ```

6. In the script `update-people.pl`, uncomment the last line and replace variables appropriately. In the MadisonParc example, the last line of the script is changed from this:

   ```
   #system("$LDAP_MODIFY -h'$host' -p'$port' -D'$bind_user'
     -w'$bind_pwd' -a -c -f people-updated.ldif");
   ```

   to this:

   ```
   system("$LDAP_MODIFY -h'ginac.MadisonParc.com' -p'389'
     -D'cn=Directory Manager' -w'password' -a -c -f
       people-updated.ldif");
   ```

   In Code Example 5-3, marker object class for the people container under dc=Customers is indicated in bold.

Code Example 5-3 People container entry with marker object class.

```
...
dn: ou=People,dc=Customers,dc=MadisonParc,dc=com
ou: People
objectClass: top
objectClass: organizationalunit
objectClass: iplanet-am-managed-people-container
```

Marking Organizational Units

Organizational units are typically assigned the ou attribute. To each container that is an organizational unit, add the following object class:

```
iplanet-am-managed-org-unit
```

To Mark Organizational Units Using the Sample Script

1. Copy `update-ou.pl` to the following directory:

   Directory_Server_root`/shared/bin`

2. Set the `$base` variable to the base suffix of the DIT to be managed by Identity Server. Example: `dc=MadisonParc,dc=com`.

3. In the directory where the script is located, at the command line enter the following:

   ```
   perl update-ou.pl
   ```

4. When prompted, provide the following information:

   Enter Host Name: Enter the name of the computer system in which your Directory Server is installed.

   Enter Bind User Name: Enter a username that has sufficient privileges for accessing the entire directory. Example: `cn=Directory Manager`

   Enter Bind password: Enter the password for the user you specified above.

   Enter port number: Enter the Directory Server port number. Example: `389`

5. Check the results in the file `orgunit-updated.ldif` which is created in the same directory as the script, and verify that the appropriate changes are listed. The changes contained in this file will automatically be made in the directory in the next step.

   Important Note: If there are organizational units that you do not want to be managed by Identity Server, you should delete those entries from this `ou-updated.ldif` now. Then, instead of going on the to next step, manually load the file using the following command:

   ```
   ldapmodify -h hostname -p port -D bind_user -w password -a -c -f
     orgunit-updated.ldif
   ```

6. In the script `update-ou.pl`, uncomment the last line and replace variables appropriately. In the MadisonParc example, the last line of the script is changed from this:

```
#system("$LDAP_MODIFY -h'$host' -p'$port' -D'$bind_user'
  -w'$bind_pwd' -a -c -f orgunit-updated.ldif");
```

to this:

```
system("$LDAP_MODIFY -h'ginac.MadisonParc.com' -p'389'
  -D'cn=Directory Manager' -w'password' -a -c -f
    orgunit-updated.ldif");
```

In Code Example 5-4, marker object class for the organizational units under dc=MadisonParc,dc=com is indicated in bold.

Code Example 5-4 Organizational unit entry with marker object class.

```
...
dn: ou=People,dc=Customers,dc=MadisonParc,dc=com
ou: People
objectClass: top
objectClass: organizationalunit
objectClass: iplanet-am-managed-people-container
...
```

Marking Users

To each user entry, add the following object classes:

- iplanet-am-managed-person
- iplanet-am-user-service
- inetuser
- iPlanetPreferences
- inetOrgPerson
- inetadmin

To Mark Users Using the Sample Script

1. Copy update-users.pl to the following directory:

   Directory_Server_root/shared/bin

2. Be sure the $base variable is set to the base suffix of the DIT to be managed by Identity Server. Example: dc=MadisonParc,dc=com

3. Be sure the $base-component variable is set to the base suffix of the DIT.Example: dc=MadisonParc,dc=com

4. In the directory where the script is located, at the command line enter the following:

```
perl udpate-users.pl
```

5. Check the results in the file `users-updated.ldif` which is created in the same directory as the script, and verify that the appropriate changes were made. The changes contained in this file will automatically be made in the directory in the next step.

   Important Note: If there are users that you do not want to be managed by Identity Server, you should delete those entries from `users-updated.ldif` now. Then, instead of going on the to next step, manually load the file using the following command:

```
ldapmodify -h hostname -p port -D bind_user -w password -a -c -f
  users-updated.ldif
```

6. In the script `update-users.pl`, uncomment the last line and replace variables appropriately. In the MadisonParc example, the last line of the script is changed from this:

```
#system("$LDAP_MODIFY -h’$host’ -p’$port’ -D’$bind_user’
  -w’$bind_pwd’ -a -c -f users-updated.ldif");
```

   to this:

```
system("$LDAP_MODIFY -h’ginac.MadisonParc.com’ -p’389’
  -D’cn=Directory Manager’ -w’password’ -a -c -f
    users-updated.ldif");
```

In Code Example 5-5, the user marker object class is indicated in bold.

Code Example 5-5 User entry with user marker object class.

```
dn: uid=scarter, ou=People, dc=MadisonParc,dc=com
nsUniqueId: d8855082-1dd111b2-8024a6c9-802bec30
givenName: Sam
telephoneNumber: +1 408 555 4798
sn: Carter
ou: Accounting
ou: People
l: Sunnyvale
roomNumber: 4612
mail: scarter@MadisonParc.com
facsimileTelephoneNumber: +1 408 555 9751
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: inetuser
objectClass: inetadmin
objectClass: iplanet-am-managed-person
```

Code Example 5-5 User entry with user marker object class. *(Continued)*

```
objectClass: iplanetPreferences
objectClass: iplanet-am-user-service
uid: scarter
cn: Sam Carter
userPassword: {SSHA}3XwjhBgbt6ae5syCndDeANoossEGRJ1NdnLyZw==
employeeType: Manager
departmentNumber: 1000
businessCategory: East
inetUserStatus: Active
```

Marking Static Groups

Static groups formed by adding uids to the group entry.

To each group entry containing values for the `uniquemember` attribute, add the following object classes:

- `iplanet-am-managed-static-group`
- `iplanet-am-managed-group`

To Mark Static Groups Using the Sample Script

1. Copy `update-static-groups.pl` to the following directory:

   Directory_Server_root/`shared/bin`

2. Set the `$base` variable to the base suffix of the DIT to be managed by Identity Server. Example: `dc=MadisonParc,dc=com`.

3. In the directory where the script is located, at the command line enter the following:

   ```
   perl update-static-groups.pl
   ```

   When prompted, provide the following information:

   Enter Host Name: Enter the name of the computer system in which your Directory Server is installed.

   Enter Bind User Name: Enter a username that has sufficient privileges for accessing the entire directory. Example: `cn=Directory Manager`

   Enter Bind password: Enter the password for the user you specified above.

   Enter port number: Enter the Directory Server port number. Example: `389`

4. Check the results in the file `static-groups-updated.ldif` which is created in the same directory as the script, and verify that the appropriate changes are listed. The changes contained in this file will automatically be made in the directory in the next step.

   Important Note: If there are static groups that you do not want to be managed by Identity Server, you should delete those entries from `static-groups-updated.ldif` now. Then, instead of going on the to next step, manually load the file using the following command:

   ```
   ldapmodify -h hostname -p port -D bind_user -w password -a -c -f
     static-groups-updated.ldif
   ```

5. In the script `update-static-groups.pl`, uncomment the last line, and replace variables appropriately. For example, in the MadisonParc example, the last line of the script is changed from this:

   ```
   #system("$LDAP_MODIFY -h'$host' -p'$port' -D'$bind_user'
     -w'$bind_pwd' -a -c -f static-groups-updated.ldif");
   ```

   to this:

   ```
   system("$LDAP_MODIFY -h'ginac.MadisonParc.com' -p'389'
     -D'cn=Directory Manager' -w'password' -a -c -f
       static-groups-updated.ldif");
   ```

In Code Example 5-6, marker object class for static groups is indicated in bold

Code Example 5-6 Static group entry with marker object classes.

```
dn: cn=Directory Administrators, dc=MadisonParc,dc=com
nsUniqueId: 60a72e02-1dd211b2-8003a6c9-802bec30
objectClass: top
objectClass: groupofuniquenames
objectClass: iplanet-am-managed-group
objectClass: iplanet-am-managed-static-group
cn: Directory Administrators
uniqueMember: uid=kvaughan, ou=People, dc=MadisonParc,dc=com
uniqueMember: uid=alutz, ou=People, dc=MadisonParc,dc=com
uniqueMember: uid=gjensen, ou=People, dc=MadisonParc,dc=com
uniqueMember: uid=tcouzens, ou=People, dc=MadisonParc,dc=com
```

Marking Dynamic (Filtered) Groups

Dynamic or filtered groups are formed by building a search construct to find all user entries containing a specific attribute. These groups contain the `memberURL` attribute.

To each group containing the attribute `memberURL`, add the following object classes:

- `iplanet-am-managed-group`
- `iplanet-am-managed-filtered-group`

To Mark Filtered Groups Using the Sample Script

1. Copy `update-filtered-groups.pl` to the following directory:

   ```
   Directory_Server_root/shared/bin
   ```

2. Set the `$base` variable to the base suffix of the DIT to be managed by Identity Server.

   Example: `dc=MadisonParc,dc=com`

3. In the directory where the script is located, at the command line enter the following:

   ```
   perl update-filtered-groups.pl
   ```

4. When prompted, provide the following information:

   Enter Host Name: Enter the name of the computer system in which your Directory Server is installed.

   Enter Bind User Name: Enter a username that has sufficient privileges for accessing the entire directory. Example: `cn=Directory Manager`

   Enter Bind password: Enter the password for the user you specified above.

   Enter port number: Enter the Directory Server port number. Example: `389`

5. Check the results in the file `filtered-groups-updated.ldif` which is created in the same directory as the script, and verify that the appropriate changes were made. The changes contained in this file will automatically be made in the directory in the next step.

   Important Note: If there are filtered or dynamic groups that you do not want to be managed by Identity Server, you should delete those entries from `filtered-groups-updated.ldif` now. Then, instead of going on the to next step, manually load the file using the following command:

   ```
   ldapmodify -h hostname -p port -D bind_user -w password -a -c -f
     filtered-groups-updated.ldif
   ```

6. In the script `update-filtered-groups.pl`, uncomment the last line in the `update-o.pl` file, and replace variables appropriately. In the MadisonParc example, the last line of the script is changed from this:

```
    #system("$LDAP_MODIFY -h'$host' -p'$port' -D'$bind_user'
      -w'$bind_pwd' -a -c -f filtered-groups-updated.ldif");
```

to this:

```
system("$LDAP_MODIFY -h'ginac.MadisonParc.com' -p'389'
  -D'cn=Directory Manager' -w'password' -a -c -f
    filtered-groups-updated.ldif");
```

In Code Example 5-7, marker object class for a filtered group is indicated in bold.

Code Example 5-7 Dynamic or filtered group with marker object classes.

```
dn: cn=North,ou=groups,dc=MadisonParc,dc=com
nsUniqueId: 60a72e35-1dd211b2-8003a6c9-802bec30
objectClass: top
objectClass: groupOfUniqueNames
objectClass: groupofurls
objectClass: iplanet-am-managed-group
objectClass: iplanet-am-managed-filtered-group
ou: groups
cn: North
memberURL:
ldap:///dc=MadisonParc,dc=com??sub?(&(|(objectclass=person)(obje
ctc
 lass=groupofuniquenames))(businessCategory=*North*))
```

Marking Assignable Dynamic Groups

The *assignable* dynamic group is an Identity Server concept. In Identity Server, users in this type of group are typically allowed limited self-registration and account management privileges. In the MadisonParc example, users at the top level have administrators to create and manage their entries to comply with corporate specifications. Users under the Customers or Suppliers organizations are placed in assignable dynamic groups. The users can acquire membership by themselves when they log into the MadisonParc portal. Their membership entitles them to limited access to the MadisonParc portal; the information they provide at registration is minimal.

Add the following object classes to each dynamic group that you want to use as an assignable dynamic group in Identity Server:

- `iplanet-am-managed-group`
- `iplanet-am-managed-assignable-group`

To Mark Assignable Dynamic Groups Using the Sample Script

1. Copy `update-assignable-dynamic-groups.pl` to the following directory:

Directory_Server_root/shared/bin

2. Set the $base variable to the base suffix of the DIT to be managed by Identity Server. Example: dc=MadisonParc,dc=com

3. In the directory where the script is located, at the command line enter the following:

   ```
   perl update-assignable-dynamic-groups.pl
   ```

4. When prompted, provide the following information:

   Enter Host Name: Enter the name of the computer system on which your Directory Server is installed.

   Enter Bind User Name: Enter a username that has sufficient privileges for accessing the entire directory. Example: cn=Directory Manager

   Enter Bind password: Enter the password for the user you specified above.

   Enter port number: Enter the Directory Server port number. Example: 389

5. Check the results in the file assignable-dynamic-groups-updated.ldif which is created in the same directory as the script, and verify that the appropriate changes were made. The changes contained in this file will automatically be made in the directory in the next step.

   Important Note: If there are assignable dynamic groups that you do not want to be managed by Identity Server, you should delete those entries from this assignable-dynamic-groups-updated.ldif now. Then, instead of going on the to next step, manually load the file using the following command:

   ```
   ldapmodify -h hostname -p port -D bind_user -w password -a -c -f
     assignable-dynamic-groups-updated.ldif
   ```

6. In the script update-assignable-dynamic-groups.pl, uncomment the last line in the update-assignable-dynamic-groups.pl file, and replace variables appropriately. In the MadisonParc example, the last line of the script is changed from this:

   ```
   #system("$LDAP_MODIFY -h'$host' -p'$port' -D'$bind_user'
     -w'$bind_pwd' -a -c -f
       assignable-dynamic-groups-updated.ldif");
   ```

   to this:

   ```
   system("$LDAP_MODIFY -h'ginac.MadisonParc.com' -p'389'
     -D'cn=Directory Manager' -w'password' -a -c -f
       assignable-dynamic-groups-updated.ldif");
   ```

Marking Group Containers

Group containers are organizational units (ou) that contain groups. To each group container that includes the `ou:Groups` attribute, add the following object class:

```
iplanet-am-managed-group-container
```

To Mark Group Containers Using the Sample Script

1. Copy `update-groups.pl` to the following directory:

   Directory_Server_root`/shared/bin`

2. Be sure the `$base` variable is set to the base suffix of the DIT to be managed by Identity Server.

   Example: `dc=MadisonParc,dc=com`.

   In the MadisonParc example, the script was also modified to include all group containers located under organizations. In Code Example 5-8, the script changes are indicated in bold.

Code Example 5-8 The scope in `update-groups.pl` is modified.

```
# run search to find all group containers, putting their DNs in to a file
system("$LDAP_SEARCH -h \"$host\" -p \"$port\" -D \"$bind_user\"
   -w \"$bind_pwd\" -b \"$base\" -T \"(&(ou=groups)
    (!(objectclass=iplanet-am-*))(objectclass=organizationalunit))\
      " dn > group-container-updated.dn");
```

3. In the directory where the script is located, at the command line enter the following command:

   ```
   perl update-groups.pl
   ```

4. When prompted, provide the following information:

   Enter Host Name: Enter the name of the computer system in which your Directory Server is installed.

   Enter Bind User Name: Enter a username that has sufficient privileges for accessing the entire directory. Example: `cn=Directory Manager`

   Enter Bind password: Enter the password for the user you specified above.

   Enter port number: Enter the Directory Server port number. Example: `389`

5. Check the results in the file `groups-updated.ldif` which is created in the same directory as the script, and verify that the appropriate changes were made. The changes contained in this file will automatically be made in the directory in the next step.

   Important Note: If there are group containers that you do not want to be managed by Identity Server, you should delete those entries from this `groups-updated.ldif` now. Then, instead of going on the to next step, manually load the file using the following command:

   ```
   ldapmodify -h hostname -p port -D bind_user -w password -a -c -f
     groups-updated.ldif
   ```

6. In the script `update-groups.pl`, uncomment the last line, and replace variables appropriately. In the MadisonParc example, the last line of the script is changed `from this:`

   ```
   #system("$LDAP_MODIFY -h'$host' -p'$port' -D'$bind_user'
     -w'$bind_pwd' -a -c -f groups-updated.ldif");
   ```

   to this:

   ```
   system("$LDAP_MODIFY -h'ginac.MadisonParc.com' -p'389'
     -D'cn=Directory Manager' -w'password' -a -c -f
       groups-updated.ldif");
   ```

In Code Example 5-9, marker object class for a group under `dc=Customers` is indicated in bold.

Code Example 5-9 Group container with marker object class.

```
...
dn: ou=Groups,dc=Customers,dc=MadisonParc,dc=com
nsUniqueId: 7880b101-1dd211b2-8007a6c9-802bec30
ou: Groups
objectClass: top
objectClass: organizationalunit
objectClass: iplanet-am-managed-group-container
...
```

Adding Custom Object Classes to Identity Server Schema

If your existing DIT contains object classes you've created that do not come with Directory Server, then you'll have to add those object classes and attributes to the Identity Server schema. In the examples in this section, the MadisonParc DIT uses two object classes and two user attributes that do not come with the Directory Server schema or with Identity Server schema. These object classes and attributes help to distinguish MadisonParc employees at the top level of the DIT from non-employees in the Customers and Suppliers organizations. Before Identity Server can manage these extensions, changes must be made in the following three Identity Server files:

- `umExisting.xml`
- `amEntrySpecific.xml` (for organization data)
- `amUser.xml` (for user data)

This chapter contains detailed instructions for making these modifications. The instructions are provided here to help you see your existing data in Identity Server after you run the Installation program.

For background information on the Identity Server schema and detailed information about customizing Identity Server, see”Understanding Identity Server XMLs and DTDs” in the *Programmer’s Guide*.

Modifying the Creation Templates

The creation templates configure Identity Server to add or allow specific object classes and attributes when these entries are created. To expose custom object classes in the UI, you must modify the creation templates for both users and organizations in the `umsExisting.xml` file.

In the MadisonParc example, the existing DIT has new object classes for both users and organizations.

The DAI Service

When you install Identity Server services, the `ums.xml file` is stored in Directory Server as the Directory Access Instructions (DAI) service. Identity Server will not allow you to load the `umsExisting.xml` file if the DAI service is already installed in Directory Server. Always remove the DAI service before modifying the `umsExisting.xml` file. Once you’re finished modifying the files, you must reload the DAI service into Directory Server.

To Remove the DAI Service

In the following directory:

Identity_Server_root`/bin`

execute the following command:

```
./amadmin -u "user_naming_attibute=amadmin,ou=people,root_suffix" -w
  password -r   DAI
```

To Load the DAI Service

In the following directory:

Identity_Server_root/`bin`

execute the following command:

```
./amadmin -u "user_naming_attibute=amadmin,ou=people,root_suffix" -w
  password -s umsExisting.xml
```

To Modify the Creation Templates

1. Remove the DAI service. In the following directory:

   Identity_Server_root/`bin`

   execute the following command:

   ```
   ./amadmin -u "user_naming_attibute=amadmin,ou=people,root_suffix" -w
     password -r DAI
   ```

2. Locate the following file:

UNIX	*Identity_Server_root*/`SUNWam/config/ums/umsExisting.xml`
Windows	*Identity_Server_root*`\config\ums\umsExisting.xml`

3. Modify any custom naming attributes. For example, the MadisonParc DIT uses the `domain` attribute instead of the `organization` attribute.

   Under the following SubConfiguration:

   ```
   "BasicOrganization" id="CreationUmsObjects
   ```

   change

   ```
   <Value>objectClass=organization</Value>
   ```

   to

   ```
   <Value>objectClass=domain</Value>
   ```

In Code Example 5-10, bold indicates the changed value. Note that three lines down, the naming attribute `dc` was changed by Identity Server during installation.

Code Example 5-10 Changing the organization naming attribute in the creation template.

```
<SubConfiguration name="BasicOrganization" id="CreationUmsObjects">
                        <AttributeValuePair> <Attribute name="name" />
                            <Value>BasicOrganization</Value>
```

Code Example 5-10 Changing the organization naming attribute in the creation template. *(Continued)*

```
                        </AttributeValuePair>
                        <AttributeValuePair> <Attribute name="javaclass" />
                            <Value>com.iplanet.ums.Organization</Value>
                        </AttributeValuePair>
                        <AttributeValuePair> <Attribute name="required" />
                            <Value>objectClass=top</Value>
                            <Value>objectClass=domain</Value>
                            <Value>objectClass=sunManagedOrganization</Value>
                            <Value>objectClass=sunNameSpace</Value>
                            <Value>dc</Value>
                            <Value>inetdomainstatus=Active</Value>
                        </AttributeValuePair>
                      <AttributeValuePair> <Attribute name="namingattribute"/>
                            <Value>dc</Value>
                        </AttributeValuePair>
                        <AttributeValuePair> <Attribute name="optional" />
                            <Value>*</Value>
                        </AttributeValuePair>
                    </SubConfiguration>
```

4. Add custom organization object classes.

   In the MadisonParc example, madisonparc-org is added to the organization creation template.

   Under the following SubConfiguration:

   ```
   "BasicOrganiation" id="CreationUmsObjects">
   ```

   under the following element:

   ```
   <AttributeValuePair><Attribute name="required" />
   ```

   add the following:

   ```
   <Value>objectClass=madisonparc-org</Value>
   ```

   ```
   <Value>madisonparc-org-description</Value>
   ```

Code Example 5-11

```
<SubConfiguration name="BasicOrganization" id="CreationUmsObjects">
                        <AttributeValuePair> <Attribute name="name" />
                            <Value>BasicOrganization</Value>
                        </AttributeValuePair>
                        <AttributeValuePair> <Attribute name="javaclass" />
                            <Value>com.iplanet.ums.Organization</Value>
                        </AttributeValuePair>
                        <AttributeValuePair> <Attribute name="required" />
                            <Value>objectClass=top</Value>
                            <Value>objectClass=domain</Value>
                            <Value>objectClass=sunManagedOrganization</Value>
```

Code Example 5-11

```
                            <Value>objectClass=sunNameSpace</Value>
                            <Value>objectClass=madisonparc-org</Value>
                            <Value>dc</Value>
                            <Value>inetdomainstatus=Active</Value>
                        </AttributeValuePair>
                      <AttributeValuePair> <Attribute name="namingattribute"/>
                            <Value>dc</Value>
                        </AttributeValuePair>
                        <AttributeValuePair> <Attribute name="optional" />
                            <Value>*</Value>
                            <Value>madisonparc-org-description</Value>
                        </AttributeValuePair>
                    </SubConfiguration>
```

5. Add custom user object classes.

   In the MadisonParc example, company is added to the user creation template.

   Under the following SubConfiguration:

   ```
   "BasicUser" id="CreationUmsObjects">
   ```

   under the following element:

   ```
   <AttributeValuePair><Attribute name="required" />
   ```

   add the following:

   ```
   <Value>objectClass=company</Value>
   ```

   Example:

```
<SubConfiguration name="CreationTemplates" >
                   <SubConfiguration name="BasicUser" id="CreationUmsObjects">
                        <AttributeValuePair> <Attribute name="name" />
                            <Value>BasicUser</Value>
                        </AttributeValuePair>
                        <AttributeValuePair> <Attribute name="javaclass" />
                            <Value>com.iplanet.ums.User</Value>
                        </AttributeValuePair>
                        <AttributeValuePair> <Attribute name="required" />
                            <Value>objectClass=top</Value>
                            <Value>objectClass=person</Value>
                            <Value>objectClass=organizationalPerson</Value>
                            <Value>objectClass=inetOrgPerson</Value>
                            <Value>objectClass=iPlanetPreferences</Value>
                            <Value>objectClass=iplanet-am-user-service</Value>
                            <Value>objectClass=inetuser</Value>
                            <Value>objectClass=inetAdmin</Value>
```

```
      <Value>objectClass=iplanet-am-managed-person</Value>
        <Value>objectClass=company</Value>
        <Value>cn=default</Value>
        <Value>sn=default</Value>
        <Value>uid</Value>
        <Value>inetuserstatus=Active</Value>
    </AttributeValuePair>
    <AttributeValuePair> <Attribute name="optional" />
        <Value>*</Value>
        <Value>companyname</Value>
        <Value>acctname</Value>
    </AttributeValuePair>
  <AttributeValuePair> <Attribute name="namingattribute"/>
        <Value>uid</Value>
    </AttributeValuePair>
</SubConfiguration>
```

6. Reload the DAI service (the `ums.xml` file or `umsExisting.xml` file).

In the following directory:

Identity_Server_root`/bin`

execute the following command:

```
  ./amadmin -u "user_naming_attibute=amadmin,ou=people,root_suffix" -w
password -s
    Identity_Server_root/SUNWam/config/ums/umsExisting.xml
```

Adding Attributes to the Organization Schema

To add attributes to the Organization schema, you must modify two services files:

- `amEntrySpecific.xml`
- `amEntrySpecific.properties.`

The Identity Server console uses the information in `amEntrySpecific.xml` for display purposes. Each Identity Server abstract entry may have a subschema in this XML file. In the following example, you would add the object class `external` to the organization subschema. If the DIT contained customized organizational units, groups, or people containers, you would add or modify their subschemas in the same XML file.

The subschema name for an organizational unit will be OrganizationalUnit. The subschema name for a people container will be PeopleContainer.

NOTE The User subschema is not configured here in the amEntrySpecific.xml file, but in the amUser.xml file (see "Adding Attributes to the User Schema" on page 117.) Although any service XML file may describe an attribute that is only for a user, the amEntrySpecific.xml file can serve as a default place holder for user attributes that are not tied to a particular service.

The "any" attribute

The any attribute in the XML descriptions may have five possible values: filter, display, adminDisplay, userReadOnly, required, or optional. The values tell the Console whether the attribute should appear in the GUI. Typically, required and optional are not both displayed at the same time; they are mutually exclusive.

filter. The attribute is displayed in a search page.

display. The attribute is read / write for administrators and regular users.

adminDisplay. The attribute is read / write for administrators and is not displayed for regular users.

userReadOnly. The attribute is read / write for administrators but is read only for regular users. It is displayed as a label for regular users so that it is not editable. For example, the display, adminDisplay, and userReadOnly settings are used when displaying the user profile page and can be used to customize the page.

required.The attribute is displayed in the create page and requires a value during creation of the entry. If any=required, the attribute must have a value or the Console will not allow the Create operation. In the user interface, required fields are indicated with an asterisk (*). Use an empty string (" ") to tell the Administration Console to display nothing.

optional.The attribute is displayed in the create page but does not require a value during creation of the entry. If any=optional, the attribute will appear on the Create page without an asterisk. This would indicate that you don't have to give it a value to create the entry. In the Create User page, the UserId is a required attribute but the First Name is optional.

In the following MadisonParc example, the attribute `madisonparc-org-description` will be displayed on the Organization page, and will be required for creation. This is indicated by the use of the `required` value. It will also be used on the Search page in Identity Server Console, as indicated by the use of the `filter` value.

```
<AttributeSchema name="madisonparc-org-description"
    type="single"
    syntax="string"
    any=required|filter
    i18nKey="o3"
/>
```

The "type" attribute

The *type* attribute can use a string, string list, single choice, multiple choice, or boolean value. For example, the `madisonparc-org-description` attribute can have only one of two descriptions: internal or external). You would make this attribute a single choice; each description would be one of the choices. The Identity Server Console would display a list containing only these cities. If multiple cities were allowed, the attribute could be a multiple choice.

To Add Attributes from a Custom Organization to the Organization Subschema

1. In the following file add the custom object class to the subschema Organization:

UNIX	*Identity_Server_root*`/SUNWam/config/xml/amEntrySpecific.xml`
Windows	*Identity_Server_root*`\config\xml\amEntrySpecific.xml`

   In this example, the custom object class `madisonparc-org-description` was added to `amEntrySpecific.xml`.

```
<AttributeSchema name="madisonparc-org-description"
    type="single"
    syntax="string"
    any=required|filter
/>
```

2. In the same `amEntrySpecific.xml` file, create internationalization (i18n) keys (also called index keys or localization keys) for each attribute. All i18n Keys in an organization must be made up of unique strings. The Identity Server Administration Console will use this key to look up the display name for the attribute.

```
<AttributeSchema name="madisonparc-org-description"
   type="single"
   syntax="string"
   any="required|filter"
   i18nKey="o3"
/>
```

3. In the following file:

UNIX	*Identity_Server_root*/`SUNWam/locale/`amEntrySpecific.properties
Windows	*Identity_Server_root*`\locale\amEntrySpecific.properties`

add the value for i18n Key you created in Step 2. This is the name that will be displayed in the graphical user interface.

Example:

```
iplanet-am-entry-specific-service-description=Identity Server Entry
Specific
g1=Member List
g2=Users Can Subscribe to this Group
dg1=Membership Filter
r1=Membership Filter
o1=Full DNS name
o2=Organization Status
o3=Organization Description
```

All the attributes listed in the subschema are displayed in the Administration Console when an organization is displayed. If an attribute is not listed, the Administration Console will not display the attribute.

TIP If an attribute has no i18n Key, it will not be displayed on the administration console. If you add an attribute, and you don’t see it in the administration console, be sure to check the i18n Key and properties.

4. Load all XML files.

In the following directory:

Identity_Server_root/bin

execute the following command:

```
./amserveradmin -u
  "user_naming_attibute=amadmin,ou=people,root_suffix"
      -w password
```

If you see any parsing errors, you should go back and double-check the changes you made in the previous steps. Also examine the syntax in the `amEntrySpecific.xml` file, and make sure you've used the correct syntax. If you need to look at syntax examples, look at the other service XML files located in the following directory:

UNIX	*Identity_Server_root*/SUNWam/config/xml
Windows	*Identity_Server_root*\config\xml

Adding Attributes to the User Schema

In this step, you will modify two files for services:

- `amUser.xml`
- `amUser.properties`

The `amUser.xml` file is where user attributes are described, just as organization and group schema are described in the `amEntrySpecific.xml` (see Step 2). The file `amUser.xml` describes the User service for Identity Server. Note that any service may describe an attribute that is for a user only. This file is just the default placeholder for `user` attributes that are not tied to a particular service.

When displaying a user's attributes, the Identity Server Administration Console gets all attributes from all services that are subschema type `User`, and displays them using the same values as used in the `amEntrySpecific.xml file` (see "The "any" attribute" on page 114 and "The "type" attribute" on page 115). In the following examples, a few attributes from the `madisonparc-user` object class are added to the file, thus it is not necessary to create a new service. It's only necessary to modify, or extend, the `iplanetamuserservice`.

Additional Notes About the amUser.xml File

The file `amUser.xml` contains a special attribute. The `any=display` attribute tells Identity Server whether to display the attribute in the user profile page. This is a misleading name since it implies access control. It is strictly used for display. If this attribute is set to `no` then the console will not display the attribute.

Also note that the attributes are defined under subschema `User` and not `Dynamic`. Any attribute defined under `User` is physically an attribute in the user entry. If you want the attribute to be a role-based or organization-based attribute, then you would define it under the `Dynamic` subschema. For detailed information, see”Understanding Identity Server XMLs and DTDs” in the *Programmer's Guide.*

To Add Attributes from a Custom Organization to the User Subschema

1. In the following file, add the attributes from the custom object class to the User subschema:

UNIX	*Identity_Server_root*`/SUNWam/config/xml/amUser.xml`
Windows	*Identity_Server_root*`\config\xml\amUser.xml`

For example, the following two attributes from the custom object class `company` were added to the file:

```
<AttributeSchema name="companyname"
    type=single
    syntax=string
    any=required|display
    />
<AttributeSchema name="acctnumber"
    type=single
    syntax=string
    any=required|filter|display
```

2. In the same `amUser.xml` file, create i18n Keys (also called *index keys* or *localization keys*) for each attribute. All i18n Keys in an organization must be made up of unique strings. The Identity Server Console will use this key to look up the display name for the attribute.:

```
<AttributeSchema name="companyname"
    type=single
    syntax=string
    any=required|display
    i18nKey=u120
/>
<AttributeSchema name="acctnumber"
    type=single
    syntax=string
    any=required|filter|display
    i18nKey=u121
```

3. Add values for the i18n Keys you created in Step 2 to the following file:

UNIX	*Identity_Server_root*`/SUNWam/locale/amUser.properties`
Windows	*Identity_Server_root*`\locale\amUser.properties`

Example:

```
iplanet-am-user-service-description=User
iwtUser-desc=Default User Profile
u101=UserId
u102=First Name
u103=Last Name
u104=Full Name
u105=Password
u106=Email Address
u107=Employee Number
u108=Telephone Number
u109=Manager
u110=Home Address
u111=User Status
u112=Account Expiration date (mm/dd/yyyy  hh:mm)
u113=User Authentication Configuration
u114=User Alias List
u115=Preferred Locale
u116=Success URL
u117=Failure URL
u118=Federation Information Key
u119=Federation Information
u120=Company Name
u121=Account Number
```

4. Load all XML files.

In the following directory:

Identity_Server_root/bin

execute the following command:

```
./amserveradmin -u "user_naming_attibute=amadmin,ou=people,root_suffix"
    -w password
```

If you see any parsing errors, you should go back and double-check the changes you made in the previous steps. Also examine the syntax in the `amUser.xml` file, and make sure you've used the correct syntax. If you need to look at syntax examples, look at the other service XML files located in the following directory:

UNIX	*Identity_Server_root*/SUNWam/config/xml
Windows	*Identity_Server_root*\config\xml

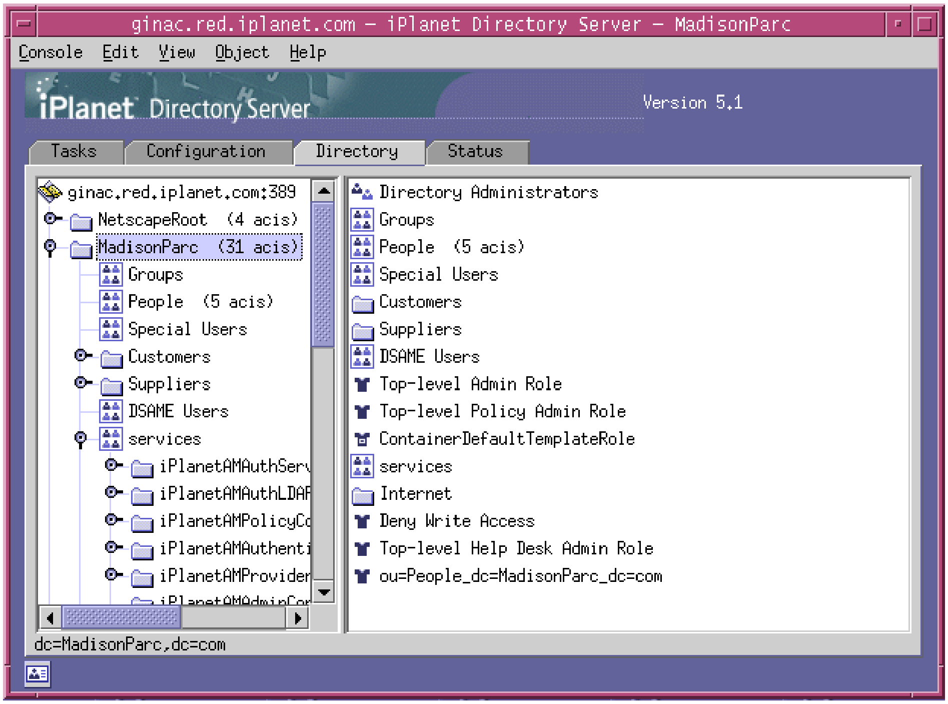
Loading Identity Server LDIF into Your Directory

Identity Server provides two different LDIF files to help you make the necessary modifications in your directory when you are enabling User Management services. To determine which file and instructions you should use, follow these guidelines:

- If you are enabling only Policy Management services (and not User Management services), then the follow the instructions for loading only `installExisting`.
- If you are enabling User Management services you'll need to follow instructions for both loading `installExisting.ldif` and `install.ldif`.

Figure illustrates the MadisonParc DIT after enabling both User Management and Policy Management services. Both `installExisting.ldif` and `install.ldif` files were loaded into an existing directory.

Figure 5-11 The MadisonParc DIT with both `installExisting.ldif` and `install.ldif` added.



installExisting.ldif

The `installExisting.ldif` file contains Identity Server-specific entries that are loaded into Directory Server during installation. Typically, you will not need to modify this file before it gets loaded during the installation process.

You can use the `ldapmodify` utility that comes with Directory Server to load `installExisting.ldif`. In the MadisonParc example, when you load the LDIF, the following occurs:

- Users and marker object classes required for Identity Server are added to `dc=MadisonParc,dc=com` and to `dc=Customers` and `dc=Suppliers`.
- Default roles for organization and help desk administrators are created at the top level.
- Default Access Control Instructions (ACIs) for those administrator entries are set up.

To Load the installExisting.ldif File

1. Go to the following directory:

   UNIX *Identity_Server_root*/SUNWam/config/ldif

   Windows *Identity_Server_root*\config\ldif

2. At the command line, enter the following:

```
ldapmodify -v -c -D "cn=Directory manager" -w password -a
  -f installExisting.ldif
```

NOTE You must specify the `-c` option. Be sure you install only `installExisting.ldif`, and no other files in the same directory.

The Identity Server administration user `amAdmin` will be created under the `ou=People,dc=MadisonParc,dc=com` people container. This is the top level administrator for Identity Server. This administrator has read and write access to the entire `dc=MadisonParc,dc=com` root suffix. You can add one of your users to this top level administrator role after the Identity Server console is started.

install.ldif

To Load the install.ldif File

1. Go to the following directory:

   UNIX *Identity_Server_root*/SUNWam/config/ldif

   Windows *Identity_Server_root*\config\ldif

2. Enter the following command:

```
  ldapmodify -v -c -D "cn=Directory manager" -w password -a -f
    install.ldif
```

NOTE You must specify the `-c` option. Be sure you install only `install.ldif`, and none of the other files in the same directory.

Results of Identity Server and Directory Modifications

After making the modifications in the previous steps, all entries in your existing directory will be manageable by Identity Server. The existing ACIs for the organization administrators do not have to be modified. Even though Identity Server uses roles and ACIs by default, your existing groups and ACIs will still work.

You can convert a groups-based DIT to one that leverages roles and ACIs. If you choose to do this, you can use the Identity Server organization administrator roles and assign them to your existing `organizationList` administrators. For more information, see the *Administrator's Guide*.

Chapter 6

Installing Identity Server Console

When you install Identity Server Management and Policy Services, Identity Server Console is also installed by default. You need not install it again on the same host. However, you may install it independently on another host. This makes it possible for you view Identity Server and manage users and policies from a remote location.

In this chapter, you will find step-by-step instructions to install Sun ONE Identity Server Console. The chapter is organized under the following topics:

- Before You Begin
- To Install the Identity Server Console

Before You Begin

The following issues must be resolved before you start the Installation program:

- You must have root permissions on the host computer where you want to install Sun ONE Identity Server Console.
- The domain name of the host computer be set. If it is not set, follow the instructions in the section "Setting the Domain Name" on page 42.
- All the web browsers are closed during installation.

To Install the Identity Server Console

1. Start the Installation program.

   To run the Installation wizard, in the directory that contains the Installation program, enter the following command:

UNIX	./setup
Windows	setup.exe

   To run the Installation program from the command line, in the directory that contains the Installation program, enter the following command:

UNIX	./setup -nosdisplay
Windows	setup -nodisplay

   NOTE The remaining steps describe the GUI version of the Installation program. If you're using the command-line version of the Installation program, you'll be prompted to provide the same information as that presented in the Installation wizard. In the command-line version, you can use the following commands:

   - Press Enter to accept the default value in brackets, or to continue on after entering a new value.
   - Press < to go back to the previous screen.
   - Enter Exit to stop the program and return to the command line.

2. In the Welcome window, click Next.
3. To accept the terms of the License Agreement, click "Yes (Accept License)."
4. In the Installation Directory window, specify the directory where you want to install the Directory Server, and then click Next.

   Note that you should have write and execute permissions in this directory.

   Install Sun ONE Identity Server in this directory: Type the path to the directory where Identity Server Services will be installed.

   NOTE Plan to install the Identity Server Services and Directory Server in different directories. Ideally, you would install Identity Server Services and Directory Server on different computer systems.

5. In the Components to Be Installed / Uninstalled panel, select Sun ONE Identity Server Console Only, and then click Next.

6. In the Java Configuration window, provide the following information, and then click Next.

   Do you want to use custom JDK? Java support in the Web Server requires Java Development Kit (JDK) of version 1.3.1_06, which is provided with Identity Server 6.0. If you want to install the JDK available with Identity Server, select No. However, if you want to use a JDK (version 1.3.1_06), that you already have, select Yes and then type the full path to its location.

7. In the Sun ONE Web Server Information window, provide the following information, and then click Next:

   Administrator: Type the user name for the administrator who will access and manage the Web Server.

   Port: Type the port number. Typically, the default is 58888.

   Password: Type the Administrator's password. The password must be a minimum of eight characters in length.

   Confirm Password: To confirm the Administrator password, type it again.

   Enter user to run server as: Type the user account the Web Server will run as. Example: nobody

   Enter group to run this server as: Type the group the above user belongs to. Example: nobody

8. In the Web Server that Runs Sun ONE Identity Server Console window, provide the following information, and then click Next:

   Host: Type the fully qualified domain name of the computer where you want to install the Identity Server Console.

   Port: Type the port number of the web server that runs the Identity Server Console. The default port is 58080.

   Console Deployment URI: This URI prefix tells the web server where to look for HTML pages associated with the Identity Server administration console and also for other web application-specific information like classes and jars. The default URI prefix is amconsole. You can type a different name.

9. Provide the following information about the Web Server that runs Sun ONE Identity Server Services, and then click Next:

   Host [nila.madisonparc.com]: Type the name of the computer on which the Web Server will run.

   Port [58080]: Type the port number being used by the Web Server.

   Services Deployment URI [/amserver]: The Universal Resource Identifier (URI) prefix tells the Web Server where to look for HTML pages associated with a service and also for web application-specific information such as classes and jars. The default URI prefix is amserver.

10. In the Directory Root Suffix window, provide the following information, and then click Next:

    Sun ONE Identity Server Root in the Directory Server: Type a distinguished name (DN) that you want to set as the root suffix. It should have at least one type=value pair. Examples:

    ```
    o=edisonwatson
    ```

    ```
    dc=madisonparc,dc=com
    ```

11. In the Sun ONE Directory Server Information panel, provide the following information, and then click Next:

    Host: Type the fully qualified domain name of the computer where Directory Server is installed.

    Port: Type the Directory Server port number.The default port is 389.

    Directory Manager: Type the DN of the user who will have restricted access to Directory Server. Example: cn=Directory Manager

    Password: Type the password for Directory Manager. The password must be a minimum of eight characters in length.

    Note that if the information you provide in any of these fields is inaccurate, the installation program will display an error message. Check the information you have provided and correct them to proceed.

12. In the Sun ONE Identity Server Top Level Administrator window, provide the following information, and then click Next:

    Username: The username for the Super administrator is amAdmin. The Top Level Administrator has unlimited access to all entries managed by Identity Server. The username amAdmin is hardcoded. This ensures that the Identity Server administrator role and its privileges are created and mapped properly in the Directory Server so that you can log onto Identity Server immediately after installation. Since this is an administrator role, you can add other users to this role after installation.

    Password: Type the password for the user amAdmin. The password must be a minimum of 8 characters in length.

    Confirm Password: To confirm the amAdmin password, type it again.

    Start the Server after installation: Click this option if you want to automatically start the Identity Server after installation. If you do not select this, you may start the server manually after installation. For steps to do this, see "Starting Identity Server Services" on page 165.

13. In the Currently Selected Settings panel, review the choices you have made in the previous panels. If you want to revisit any of the panels, click Back and go the required panel.Otherwise, click Next.

14. In the Ready to Install window, view the components that will be installed with Sun ONE Identity Server Console.

    Click Install now to start the installation.

15. At the end of the installation, the Installation Summary panel displays whether the product is successfully installed. In the panel, click the Dismiss button to see where the product is installed.

16. After viewing the details, in the Installation Summary window, click Close to end the Installation program.

Chapter 7

Installing Common Domain Services

In this chapter, you will find step-by-step instructions for installing Common Domain Services, a component of Sun ONE Identity Server. When you install Identity Server Management and Policy Services, Common Domain Services are also installed by default. You need not install this component again. However, you may install it independently on another host. This is useful when you want to use manage the Common Domain Services from a remote location.

The chapter is organized under the following topics:

- Before You Begin
- To Install Common Domain Services

Before You Begin

You must resolve the following issues before you start the Installation program:

- You must have root permissions on the host computer system where you want to install Common Domain Services.
- The domain name of the host computer system must be set. If it is not set, follow the instructions in the section "Setting the Domain Name" on page 42.
- All the web browsers are closed during installation.

NOTE Make sure that Common Domain Services is not already installed in another directory on this computer. To check for an existing instance, you can use the following command: pkginfo | grep SUNWamfcd

To Install Common Domain Services

1. Start the Installation program.

   To run the Installation wizard, in the directory that contains the Installation program, enter the following command:

UNIX	`./setup`
Windows	`setup.exe`

   To run the Installation program from the command line, in the directory that contains the Installation program, enter the following command:

UNIX	`./setup -nosdisplay`
Windows	`setup -nodisplay`

   NOTE The remaining steps describe the GUI version of the Installation program. If you're using the command-line version of the Installation program, you'll be prompted to provide the same information as that presented in the Installation wizard. In the command-line version, you can use the following commands:

   - Press `Enter` to accept a default value in [brackets], or to continue on after you've entered a new value.
   - Press < to go back to the previous screen.
   - Enter `Exit` to stop the program and return to the command line.

2. In the Welcome window, click Next.

3. To accept the terms of the License Agreement, click "I Accept."

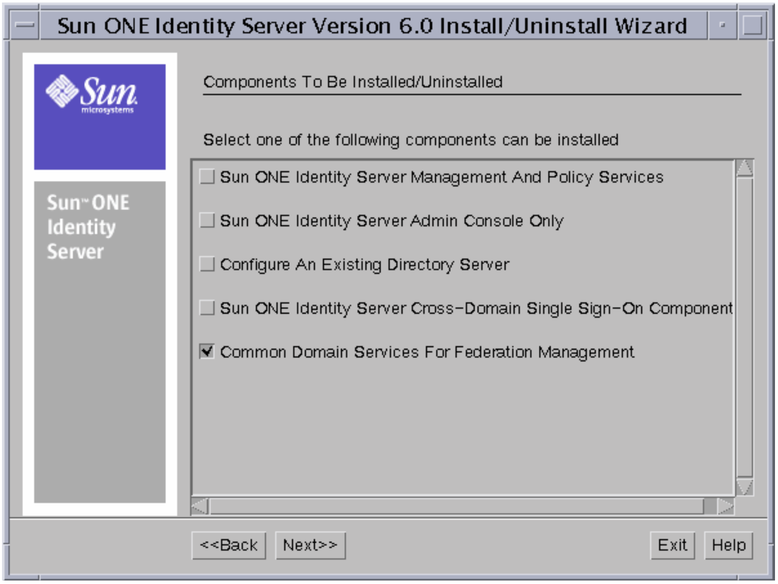
4. Specify the directory where you want to install the Common Domain Service, and then click Next.

   You can either specify the absolute path the field provided, or use the Browse button to select the directory.

   Note that you should have write and execute permissions in this directory.

5. In the Components to be Installed/Uninstalled window, select Common Domain Services, and then click Next.

Figure 7-1 Components to be Installed / Uninstalled Panel



Sun ONE Identity Server Version 6.0 Install/Uninstall Wizard

Components To Be Installed/Uninstalled

Select one of the following components can be installed

□ Sun ONE Identity Server Management And Policy Services

□ Sun ONE Identity Server Admin Console Only

□ Configure An Existing Directory Server

□ Sun ONE Identity Server Cross-Domain Single Sign-On Component

☑ Common Domain Services For Federation Management

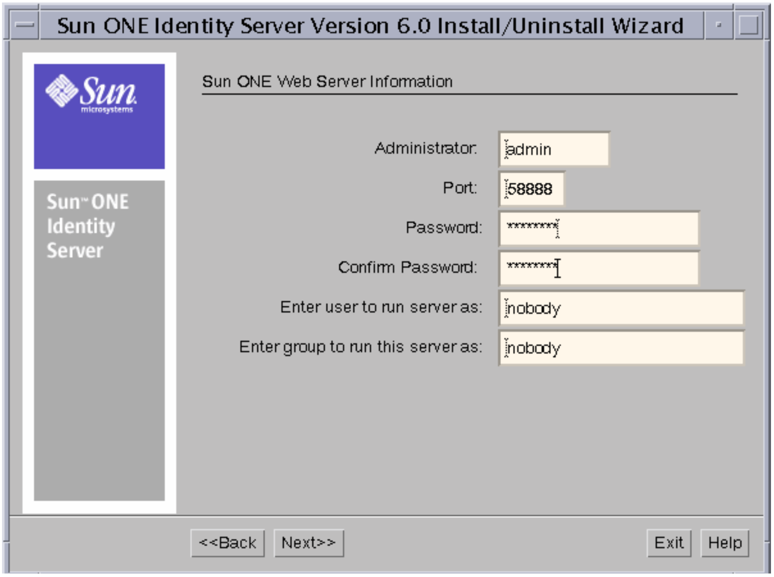
6. In the Existing Web Server panel, provide the following information, and then click Next:

   Do you want to use an existing Web Server? Click Yes, if you want to use your existing Sun ONE Web Server.

   Click No, if you want to install the Sun ONE Web Server available with Identity Server.

7. If you have selected no above, you should provide the following information to install and configure the Sun ONE Web Server available with Identity Server. If you have selected yes, you can skip this step and proceed to Step 8.

Figure 7-2 Sun ONE Web Server Information Panel



Sun ONE Identity Server Version 6.0 Install/Uninstall Wizard

Sun ONE Web Server Information

Administrator: admin

Port: 58888

Password: ********

Confirm Password: ********

Enter user to run server as: nobody

Enter group to run this server as: nobody

Administrator: Type the user name of the administrator who will configure the web server. You may overwrite the default name shown in the field.

Port: Type the port number that the web server will use. You may overwrite the default port number displayed in the field.

Password: Type the Administrator user's password.

Confirm Password: Retype the password to confirm it.

Enter user to run server as: Type the user account the Web Server will run as. Example: nobody.

Enter group to run this server as: Type the group the above user belongs to. Example: nobody.

8. In the Common Domain Services Web Server Information window, provide the following information, and then click Next:

   Host Name: Type the fully qualified domain name of the web server where the Common Domain Services will run.

   Sun ONE Web Server Instance Directory: Type the full path to the directory where Web Server is installed, and the Web Server instance name. For example, https-nila.madisonparc.com. It is the Web Server that hosts the participating DNS domain. This field is available only if you are using an existing web server.

   Web Server Port: Type the port number to be used by the services.

   Services Deployment URI: The URI using which the common domain services can be accessed. The default is `common`, which you may modify.

9. In the Ready to Install panel, review the installation information. If you need to make changes, click Back. Otherwise, click Install Now to begin the installation.

10. In the Installation Summary panel, click Details for a detailed summary of the configuration information that was processed during installation. Then click Close to end the program.

Chapter 8

Basic Configurations

This chapter describes configurations typically implemented when you initially deploy Identity Server.

Topics in this chapter include:

- The Cross-Domain Single Sign-On Component
- Installing Multiple Identity Server Instances Against the Same Directory Server
- Support for Directory Replication and High Availability

The Cross-Domain Single Sign-On Component

Cross-Domain Single Sign-On (CDSSO), a crucial feature of Identity Server, makes it possible for users to authenticate in one domain, and then to use applications in many other domains without having to re-authenticate. Two major components are added to Identity Server to implement cross-domain single sign-on:

- **Cross-Domain Controller**. The controller is responsible for redirecting a request to the authentication service if no Single Sign-On (SSO) information exists, or for redirecting the request to the CDSSO Component with SSO information appended to the query string. The controller is automatically installed when you install Identity Server services. The default URL for the controller is

  `http://`*Identity_Server_root_host:Identity_Server_root:port*`/URI/cdcservlet`

- **CDSSO) Component**. The CDSSO component is primarily responsible for handling cookie setting for the domain in which cross-domain single sign-on is deployed. The CDSSO component is installed separately on all participating DNS domains.

Overview of CDSSO Installation

To enable cross-domain single sign-on, you must follow this sequence:

1. Install Identity Server Management and Policy Services.

   Follow the instructions in Chapter 4, "Installing Identity Server with a New Directory Server" on page 45" or in Chapter 5, "Installing Identity Server Against an Existing Directory Server" on page 57" as appropriate to your needs.

2. Install the CDSSO component on all participating DNS domains. For steps, see "The Cross-Domain Single Sign-On Component" on page 137" in this chapter.

3. Configure the CDSSO component installed on each participating DNS domain. For instructions, see "To Configure the CDSSO Component" on page 143.

4. Optionally, configure Identity Server web agents to work with the CDSSO component. For steps, see "To Configure Identity Server Web Agents to Work With the CDSSO Component" on page 143.

Before You Begin

You must resolve the following issues before running the Installation program:

- Make sure that CDSSO is not already installed in another directory on this computer. To check for an existing instance, you can use the following command:

  ```
  pkginfo | grep SUNWam*
  ```

- You must have root permissions for the host computer system where CDSSO will be installed in order to run the Installation program.

To Install CDSSO

1. Start the Identity Server Installation program.

   To run the Installation wizard, in the directory that contains the Installation program, enter the following command:

   UNIX `./setup`

   Windows `setup.exe`

   To run the Installation program from the command line, in the directory that contains the Installation program, enter the following command:

   UNIX `./setup -nosdisplay`

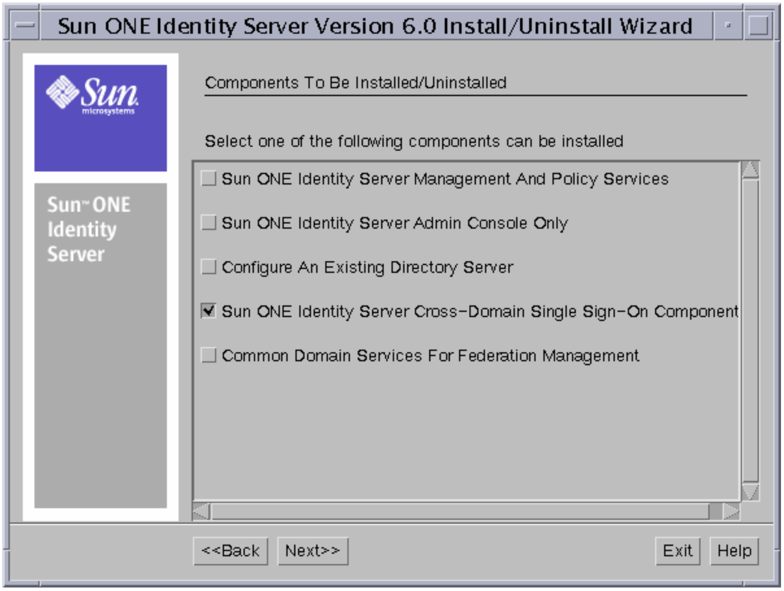
   Windows `setup -nodisplay`

   NOTE The remaining steps describe the GUI version of the Installation program. If you're using the command-line version of the Installation program, you'll be prompted to provide the same information as that presented in the Installation wizard. In the command-line version, you can use the following commands:

   - Press Enter to accept the default value in brackets, or to continue on after entering a new value.
   - Press < to go back to the previous screen.
   - Enter `Exit` to stop the program and return to the command line.

2. In the Welcome window, click Next.
3. To accept the terms of the License Agreement, click "Yes (Accept License)."
4. In the Components to Be Installed / Uninstalled panel, select only Identity Server Cross Domain Single Sign-On Component, and then click Next.

Figure 8-1 Components to Be Installed / Uninstalled Panel


Sun ONE Identity Server Version 6.0 Install/Uninstall Wizard
Sun microsystems
Sun™ ONE Identity Server
<<Back
Next>>
Exit
Help

Components To Be Installed/Uninstalled

Select one of the following components can be installed

□ Sun ONE Identity Server Management And Policy Services
□ Sun ONE Identity Server Admin Console Only
□ Configure An Existing Directory Server
☑ Sun ONE Identity Server Cross-Domain Single Sign-On Component
□ Common Domain Services For Federation Management

5. In the Existing Web Server panel and provide the following information, and then click Next:

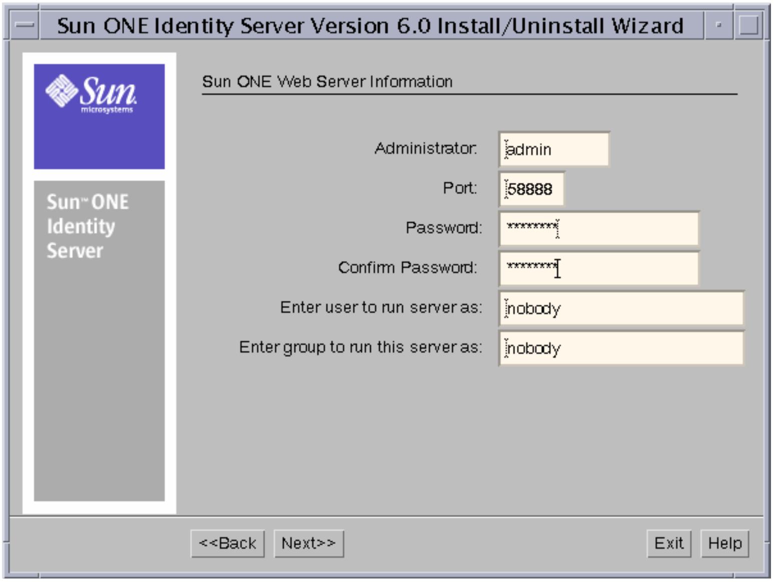
   Do you want to use an existing Web Server? Click Yes, if you want to use your existing Sun ONE Web Server.

   Click No, if you want to install the Sun ONE Web Server available with Identity Server.

6. If you have selected yes, you can skip this step and proceed to Step 7.

   If you have selected no above, you should provide the following information to install and configure the Sun ONE Web Server available with Identity Server, and then click Next.

Figure 8-2 Sun ONE Web Server Information Panel


Sun ONE Identity Server Version 6.0 Install/Uninstall Wizard
Sun microsystems
Sun™ ONE Identity Server
<<Back
Next>>
Exit
Help

Sun ONE Web Server Information

Administrator: admin

Port: 58888

Password: ********

Confirm Password: ********

Enter user to run server as: nobody

Enter group to run this server as: nobody

Administrator: Type the user name of the administrator who will configure the web server. You may overwrite the default name shown in the field.

Port: Type the port number that the web server will use. You may overwrite the default port number displayed in the field.

Password: Type the Administrator user's password.

Confirm Password: Retype the password to confirm it.

Enter user to run server as: Type the user account the Web Server will run as. Example: nobody.

Enter group to run this server as: Type the group the above user belongs to. Example: nobody.

7. In the CDSSO Web Server Information panel, provide the following information, and then click Next.

   Host Name: Type the fully qualified domain name of the computer that hosts the participating DNS domain.

   Instance Directory: Type the full path to the directory where Web Server is installed, and the Web Server instance name. This field is available only if you have selected to use an existing web server in a previous step.

   Web Server Port: Type the port number of the Web Server specified above.

   CDSSO Deployment URI: The Universal Resource Identifier (URI) indicates where HTML pages used by the CDSSO component are stored. Type a URI prefix. The default is `/amcdsso`

8. In the Identity Server Services Information panel, provide the following information, and then click Next:

   Identity Server Services Host: Type the fully qualified domain name of the computer system where Identity Server Management and Policy Services are installed.

   Identity Server Services Port: Type the port number for the Web Server that runs Identity Server services.

   Services Deployment URI: The Universal Resource Identifier (URI) prefix tells the Web Server where to look for HTML pages associated with a Identity Server service and also for other web application-specific information such as classes and jars. Type the URI prefix specified during Identity Server installation. The default is `/amserver.`

9. In the Currently Selected Settings panel, review the configuration information that you've entered. If you need to make changes, click Back. Otherwise, click Next to proceed.

10. In the Ready to Install panel, review the installation information. If you need to make changes, click Back. Otherwise, click Install Now to begin the installation.

To Configure the CDSSO Component

1. Edit `AMConfig.properties` file of the installed CDSSO component, which is found in the *Identity_Server_root*`/SUNWam/web-apps/cdsso/WEB-INF/lib` directory.

   Set the `com.iplanet.services.cdsso.CDCURL` property to the URL of the cross-domain controller service running on the Identity Server services. For example:

   ```
   com.iplanet.services.cdsso.CDCURL =
     http(s)://Identity_Server_root:host:Identity_Server_root:port/services/
       cdcservlet
   ```

2. Edit `CDSSO.properties` file of the installed CDSSO component, which is found in the Identity_Server_root/SUNWam/web-apps/cdsso/WEB-INF/classes directory.

   Set `com.iplanet.services.cdsso.cookieDomain` property to the domain name which hosts the CDSSO component. For example:

   ```
   com.iplanet.services.cdsso.cookieDomain = .sales.com
   ```

   where the CDSSO component is hosted in `sales.com` domain.

   The `com.iplanet.services.cdsso.cookieDomain` property specifies the list of domain names on which CDSSO component is running for which the cookie is set. If the property field is left blank, the cookie domain is assumed to be the hosting domain of CDSSO component. Make sure that all the cookie domains are separated with coma (,).

To Configure Identity Server Web Agents to Work With the CDSSO Component

You can configure Identity Server agents that are installed on remote web servers to work with CDSSO components that are installed on participating DNS domains.

1. Edit the agent's `AMAgent.properties` file. Change the `com.sun.am.policy.agents.url.loginURL` property to point to the agent's domain's cross-domain single sign-on service URL. For example:

   ```
   com.sun.am.policy.agents.url.loginURL =
   http://CDSSO_host:CDSSO_port/CDSSO_URI/cdsso
   ```

   where `loginURL` is the CDSSO component's URL.

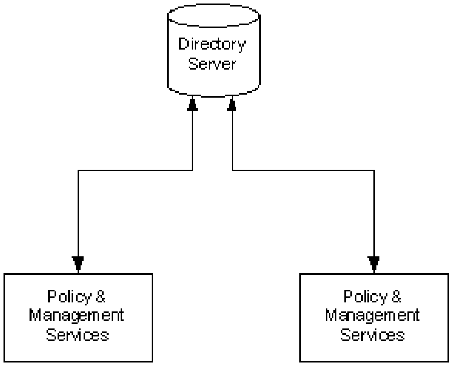
2. Add the CDSSO URL to the agent's not-enforced list.

Installing Multiple Identity Server Instances Against the Same Directory Server

You can install more than one instance of Identity Server against this Directory Server for enhanced performance, to support directory replication, or for agent failover purposes. When you run the Identity Server installation program for the first time, you'll typically install Identity Server Policy and Management Services. When you use this option, Directory Server is automatically installed for you. This is the master Directory Server. If you plan to install multiple installations of Identity Server against this same master directory, you must run `ammultiserverinstall` script.

Figure 8-3 illustrates two Identity Server instances installed against a single Directory Server.

Figure 8-3 Two Identity Server Instances Installed Against a Single Directory Server.



To Install Multiple Identity Server Instances Against the Same Directory Server

You must have root permissions to create and install multiple Identity Server instances.

1. Go to the following directory:

   cd *Identity_Server_root*/SUNWam/bin

2. At the command line, type the following command:

   ```
   ./ammultiserverinstall instance_name port_number
   ```

   where *instance_name* is the new Identity Server instance you want to create and *port_number* is the port number of the new Identity Server instance.

   When a new instance is installed the following files and directory are created:

   - A new `amserver` script file at:

     /Identity_Server_root/`SUNWam/bin/`*amserver.instance_name*

   - A new `AMConfig.properties` file at:

     /Identity_Server_root/`SUNWam/lib/AMConfig-instance_name.properties`

   - A new web server instance directory at:

     /Identity_Server_root/`SUNWam/servers/https-instance_name`

Starting Identity Server Instance

- To start a single Identity Server instance type the following command:

  `./amserver.`*instance_name* `start`

- To start all the Identity Server instances, type the following command:

  ```
  ./amserver startall
  ```

Stopping Identity Server Instance

- To stop a single Identity Server instance, type the following command:

  ./amserver.instance_name `stop`

- To stop all the Identity Server instances, type the following command:

  ```
  ./amserver stopall
  ```

Deleting Identity Server Instance

- To delete an Identity Server instance, type the following command:

  `./amserver delete` *instance_name*

Support for Directory Replication and High Availability

Load balancing across replicated servers and locating replicated servers closer to users are two ways to improve server performance and response time in your enterprise. You can implement directory replication agreements in your Identity Server deployment to increase the availability and performance of the Identity Server servers and services. You can set up Identity Server directory servers in single-supplier or multi-supplier configurations. You can also configure load-balancing applications such as Sun ONE Directory Access Router to work with Identity Server.

Replication Considerations

Configure your directory servers for replication before you install Identity Server. This ensures that the supplier and consumer databases are synchronized from the beginning, and gives you a chance to verify that referrals and updates are working properly. The information must be identical in each Identity Server database.

When you install Identity Server for replication purposes, in each instance of Directory Server and in each instance of Identity Server, specify the same values for the following:

- Directory Manager
- Directory Manager Password
- Directory Server Administrator ID
- Server Administrator Password
- Base suffix
- Default organization

There may be situations in which you cannot implement directory replication in a Identity Server deployment. For example, authentication server host names or IP addresses must be the same. This precludes using geographically separated replicated Identity Server servers. The remote servers would not be able to perform authentication against servers that are only local to their respective LANs.

For comprehensive information on planning and implementing Directory Server replication, see the *Deployment Guide* and the *Installation Guide* for Sun ONE Directory Server. You can access these guides on the Internet at the following URL:

```
http://docs.sun.com/db/prod/s1dirsrv
```

Configuring Identity Server to Support Directory Replication

You can configure Identity Server to work with single-supplier or multi-supplier replication. For each of the configurations pictured in this section, follow the same instructions. See "To Configure Identity Server to Work With Directory Replication" on page 149 of this manual.

Figure 8-4 illustrates a single-supplier configuration where the Consumer is a read-only database. Requests for write operations are referred to the supplier database. This configuration provides some measure of enhanced server performance by distributing the workload to more than one directory.

Figure 8-4 Single-Supplier Replication.

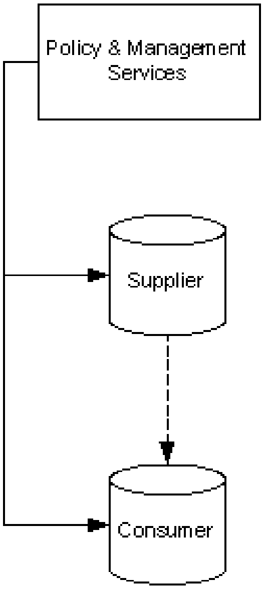


Figure 8-5 illustrates a multi-supplier configuration using multiple instances of Identity Server. This configuration provides failover protection as well as high availability, resulting in further enhanced server performance.

Figure 8-5 Multi-Supplier Configuration. Also known as Multi-Master Replication (MMR)

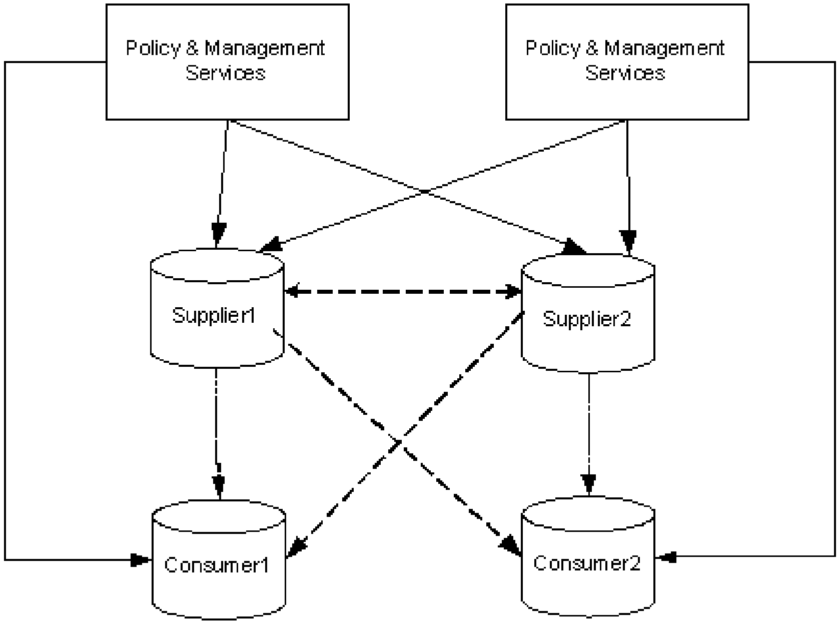
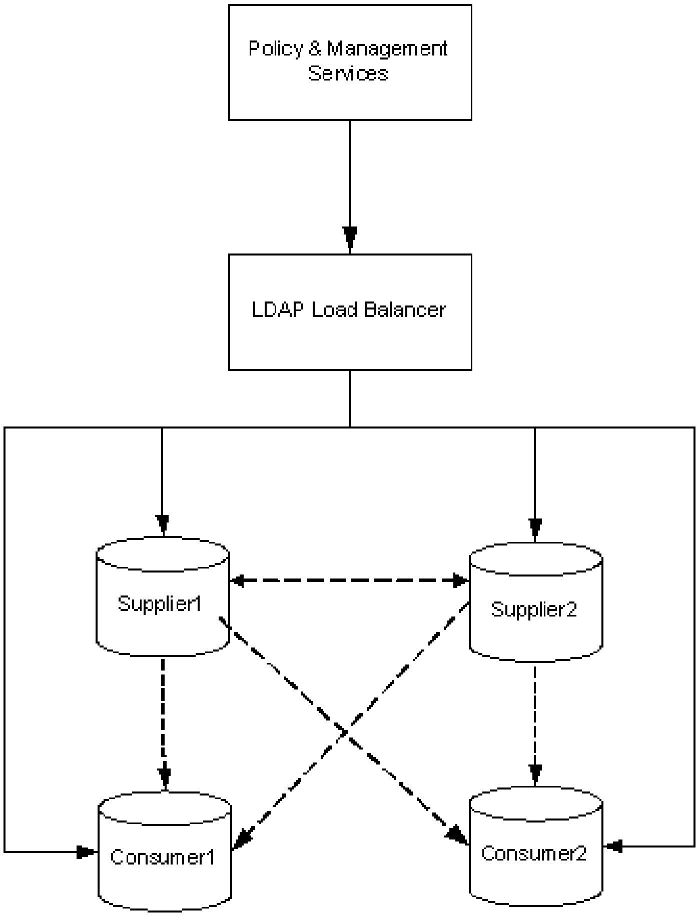


Figure 8-6 illustrates a multi-supplier configuration that includes Sun ONE Access Router. This configuration takes full advantage of Identity Server support for failover, high availability, and managed load-balancing.

Figure 8-6 Multi-Supplier Replication With Load-Balancer.



To Configure Identity Server to Work With Directory Replication

Use the following steps to configure replication at the root or top level of the Identity Server directory tree when Identity Server has not yet been installed. You can also use these steps to configure replication at the default organization level.

1. Install your supplier and consumer Directory Servers (version 5.1). See the Directory Server *Installation Guide* for detailed instructions.

2. Set up replication agreements between your supplier and consumer Directory Servers, and then verify that the directory referrals and updates are working properly. See the Directory Server *Administrator's Guide* for detailed instructions.

3. If you plan to use Identity Server with user data from an existing, pre-5.1 Directory Server, you must migrate the user data and make Directory Information Tree (DIT) changes before proceeding. Follow the detailed instructions in Chapter 5, "Installing Identity Server Against an Existing Directory Server" on page 57 of this manual. Then skip to Step 5.

4. If you are deploying Identity Server and Directory Server for the first time, or if you simply do not plan to use existing user data with Identity Server, then run the Identity Server installation program to install the Identity Server Management and Policy services.

   During installation, you'll be asked if you're using an existing Directory Server. You'll answer yes, and then you'll specify the host name and port number for a supplier Directory Server you installed in Step 1.

   For detailed instructions, see "Installing User and Policy Management Services" on page 71 in Chapter 5.

5. In the server where Identity Server Management and Policy services are installed, modify the following file:

   Identity_Server_root/SUNWam/lib/AMConfig.properties

   a. Modify the following properties to reflect the host and port number of a consumer Directory Server you installed in step 1.

      - `com.iplanet.am.directory.host`
      - `com.iplanet.am.directory.port`

   b. Modify the following properties:

      - `com.iplanet.am.replica.retries`

        Specify the number of times Identity Server should continue to make the same request when the requested entry is not found.

      - `com.iplanet.am.replica.delay.between.retries`

        Specify the number of milliseconds Identity Server should allow to elapse between retries.

6. In each Identity Server Authentication module you've enabled, you must specify the consumer directory that you installed in step 1. In the following substeps, the LDAP Authentication module is used as an example:

a. In the Identity Server console, in the View field, choose Service Management.

b. In the Service Name column, under Authentication, locate the module you need to reconfigure. In the Properties column, click the arrow that corresponds to module you need to reconfigure.

c. In the right pane, there are two fields named **LDAP Server and Port**.

   - In the first field named **LDAP Server and Port**, type the host name and port number for your primary (consumer) Directory Server.
     Example: `consumer1.madisonparc.com:389`

   - In the second field named **LDAP Server and Port**, type the host name and port number for your secondary or (supplier) directory.
     Example: `supplier1.madisonparc.com:399`

d. Click Submit.

7. In the following file:
   Identity_Server_root/`SUNWam/config/ums/serverconfig.xml,` specify the host name and port number of the consumer directory you installed in step 1.
   Example:

```
<iPlanetDataAccessLayer>
<ServerGroup name="default" minConnPool="1"
maxConnPool="10">
<Server name="Server1"
host="consumer1.madisonparc.com" port="389"
type="SIMPLE" />
```

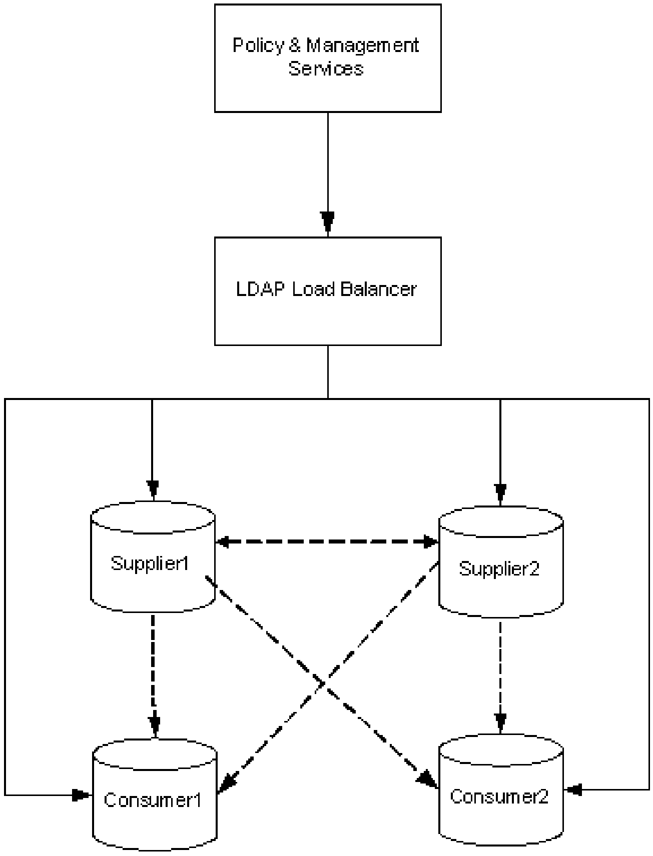
8. Restart Identity Server with the following command:

   /*Identity_Server_root*/`SUNWam/bin/amserver start`

Configuring LDAP Load-Balancers to Work With Identity Server

You can configure LDAP load-balancers such as Sun ONE Directory Access Router to work with Identity Server. Sun ONE Directory Access Router dynamically performs proportional load balancing of LDAP operations across a set of configured directory servers. If one or more directory servers should become unavailable, the load is proportionally redistributed among the remaining servers. When a directory server comes back on line, the load is proportionally—and dynamically—reallocated.

Figure 8-7 Multi-Master Replication With Managed Load-Balancer.



Using LDAP load-balancers, it adds a layer of high availability and directory failover protection beyond the basic level that comes with Identity Server. For example, when you configure Sun ONE Directory Access Router, you can specify what percentage of the load gets redistributed to each of your servers when one server becomes unavailable. Sun ONE Directory Access Router continues to manage request traffic, and begins rejecting client queries when all back-end LDAP servers become unavailable.

By comparison, the Identity Server high availability feature cannot be configured or managed as precisely. But when you add a LDAP load-balancers such as Sun ONE Directory Access Router, Identity Server seamlessly directs all requests to the application for total management.

If you choose to install a load-balancer, you must configure Identity Server to recognize the application.

To Configure Identity Server to Work With a Load-Balancer

1. Before you can perform the following steps, you must:

   - Set up your Directory Servers for replication. For comprehensive information about directory replication and for detailed setup instructions, see “Managing Replication” in the *Sun ONE Directory Server Administrator’s Guide*.

   - Install and configure your LDAP load-balancer. Follow the instructions in the documentation that comes with the product.

2. In the file *Identity_Server_root*/SUNWam/lib/AMconfig.properties, modify the following properties to reflect the host and port number of a consumer Directory Server you installed in step 1.

   - `com.iplanet.am.directory.host`
   - `com.iplanet.am.directory.port`

3. For each Identity Server Authentication module you’ve enabled, specify the consumer directory that you installed in step 1. In the following substeps, the LDAP Authentication module is used as an example:

   a. In the Identity Server console, in the View field, choose Service Management.

   b. In the Service Name column, under Authentication, locate the module you need to reconfigure. In the Properties column, click the arrow that corresponds to module you need to reconfigure.

   c. In the right pane, there are two fields named **LDAP Server and Port**.

- In the first field named **LDAP Server and Port**, type the host name and port number for your primary (consumer) Directory Server using the form:

  proxyhostname:port

- In the second field named **LDAP Server and Port**, enter nothing.

d. Click Submit.

4. In the *Identity_Server_root*/`SUNWam/config/ums/serverconfig.xml`, specify the host name and port number of the consumer directory you installed in step 1.

Example:

```
<iPlanetDataAccessLayer>
<ServerGroup name="default" minConnPool="1"
maxConnPool="10">
<Server name="Server1"
host="idar.madisonparc.com" port="389"
type="SIMPLE" />
```

5. Restart Identity Server with the following command:

/*Identity_Server_root*/`SUNWam/bin/amserver start`

Chapter 9

Silent Installation

In addition to the GUI installation and the CLI, you can do a silent installation of Identity Server. This chapter provides steps for doing that. Topics in the chapter include:

- About Silent Installation
- Generating a StateFile on Solaris
- Installing Using the Statefile
- Generating a StateFile on Windows
- Installing Using the Statefile
- Variables in the Statefile

About Silent Installation

Silent installation provides a means for scripting the installation of Identity Server. When you perform a silent installation, you use a *StateFile*, to provide all the answers that you would normally supply to the setup program interactively. This saves time and is useful when you want to install multiple instances of Identity Server using the same parameters in each instance.

Silent installation is a simple two-step process. First, you generate a *Statefile* that records the installation process and all the inputs you provide. Then you run the installation program with the *StateFile* as the input source.

NOTE Be sure you have write permissions for the directory in which you want to generate the StateFile. Otherwise, the file will not be written.

Generating a StateFile on Solaris

To generate a *StateFile* on Solaris:

1. Change to the directory where the installation program is located.
2. Enter the following command:

   ```
   # ./setup -saveState StateFile
   ```

   You can give a name of your choice to the *Statefile*.
3. Proceed through the installation program. Your answers to the prompts are recorded in the *StateFile*.

   When installation is complete, *StateFile* is created in the same directory as `setup`.

Installing Using the Statefile

To run the silent installation:

Enter the following command to run the silent installation:

```
# ./setup -nodisplay -noconsole -state StateFile
```

The installation takes place hidden from your view. On completion, the program exits automatically and displays the prompt. Change to the installation directory specified in the *Statefile* to check if all the files are copied.

Generating a StateFile on Windows

To generate a *StateFile* on Windows 2000:

1. Run the installation program from the directory where the `setup` program is located. Open a DOS command window and enter the following command:

   ```
   setup -saveState StateFile
   ```
2. Proceed through the installation program. Your answers to the prompts are recorded in the *StateFile*.

When installation is complete, the *StateFile* is created in the same directory as setup.exe.

Installing Using the Statefile

1. Type the following command:

```
setup -nodisplay -noconsole -state StateFile
```

The installation takes place hidden from your view. On completion, the program exits automatically and displays the prompt. Change to the installation directory specified in the *Statefile* to check if all the files are copied.

Variables in the Statefile

The following table presents the variables in the statefile with a brief description and the values they can have.

Table 9-1 Description of Statefile Variables

Variable	Description	Value
defaultInstallDirectory	Displays the default directory prompted by the installation program for installing Identity Server.	The absolute path to the directory. For example /opt on Solaris and `c:\SunONE\SunONEIS` on Windows
currentInstallDirectory	Displays the directory you have selected to install Identity Server.	The absolute path to the directory. For example /identity60
com.iplanet.install.panels.common.ComponentPanel.selectedcomponents	Displays the name of the Identity Server component you have selected for installation.	Name of the component. For example, Sun ONE IdentityServerManagementandPolicyServices SunONEIdentityServerCrossDomainSingleSignon
CUSTOM_JDK	Indicates whether you have specified an existing JDK or have selected to install the JDK available with Identity Server 6.0.	True/False true, if you specified a Custom JDK false, if you selected to install the JDK bundled with Identity Server.
JDK_PATH	Displays the relative path to the JDK on Solaris platform.	java

Table 9-1 Description of Statefile Variables

Variable	Description	Value
JDK_BASE_DIR	Displays the directory where Java SDK is installed.	The absolute path to the JDK directory. For example /identity60/SUNWam/java
IWS_INSTALL	Indicates whether you have installed the CDSSO component and the Common Domain Services with a new web server distributed with Identity Server 6.0.	True/False True if you have installed these components with a new web server.
IWS_ADMIN_ID	Displays the user name for the administrator who will manage the Sun ONE Web Server.	The default value is admin. You can change it.
IWS_ADMIN_PORT	Displays the port number used by Sun ONE Web Server.	The default is 58888. You can change it.
IWS_ADMIN_PASSWD	Displays the Web Server Administrator's password.	The password must be at least eight characters long.
SYS_USR	Displays the UNIX user account the Web Server will run as.	The default user is nobody. You can change it. This variable will not be available in a statefile created on Windows.
SYS_GRP	Displays the UNIX group to which the above user belongs.	The default group is nobody. You can change it. This variable will not be available in a statefile created on Windows.
CDSSO_BASE_WSDIR	Displays the path to the directory where the Sun ONE Web Server is installed.	
CDSSO_HOST	Displays the FQDN of the computer on which you have installed the CDSSO component.	Typically, the value will be in the form *host.madisonparc*.com.
CDSSO_WSDIR	Displays the path to the directory storing Web Server Instance.	The absolute path including the instance name. For example /*Identity_Server_root*/SUNWam/servers/https-*host.madisonparc*.com
CDSSO_PORT	Displays the port number of the Web Server used by the CDSSO component.	The default value is 80.

Table 9-1 Description of Statefile Variables

Variable	Description	Value
CDSSO_PROTOCOL	Displays the protocol used by the CDSSO component.	http or https. The default value is http.
CDSSO_DEPLOY_URI	Displays the URI for accessing CDSSO.	The default is amcdsso. You can change it.
WS_INSTANCE	Displays the name of the web server instance.	The default value is https-*host.madisonparc*.com
DSAME_SERVER	Displays the FQDN of the host machine that runs Sun ONE Identity Server.	Typically, the value is in the format *host.madisonparc*.com
DSAME_PORT	Displays the port used by the web server that runs Identity Server services.	Typically, the default is 58080.
DSAME_PROTOCOL	Displays the protocol used by Identity Server.	http or https. The default is http.
SERVER_DEPLOY_URI	Displays the URI for accessing Identity Server services.	The default is amserver. You can change it.
CDS_HOST	Displays the FQDN of the machine on which you have installed Common Domain Services.	*host.madisonparc*.com
CDS_WSDIR	Displays the path to the web server instance used by Common Domain Services.	The absolute path including the web server instance name. For example, /Is-root/SUNWam/servers/https-*madisonparc60.madisonparc.com*
CDS_PORT	Displays the port number used by the Common Domain Services.	Typically, the default is 58080.
CDS_PROTOCOL	Displays the protocol used by the Common Domain Services.	http or https. The default is http.
CDS_DEPLOY_URI	Displays the URI for accessing the Common Domain Services on the Web Server.	The default is common. You can change it.
CDS_BASE_WSDIR	Displays the path to the web server directory used by Common Domain Services.	*Identity_Server_root*/SUNWam/servers
DSAME_HOST	Displays the host name where you have installed Directory Server. Host name is typically the first label in the FQDN.	*host*

Table 9-1 Description of Statefile Variables

Variable	Description	Value
DSAME_DEF_DOMAIN	Displays the domain on which you have installed Directory Server.	Domain name, for example, *madisonparc*.com
DSAME_FULL_DOMAIN	Displays the domain name (sans the host name) where you have installed Identity Server.	*madisonparc*.com
DSAME_SUB_DOMAIN	Displays the sub-domain label in the FQDN. In an FQDN, the sub-domain as the second label. For example, in *nila.country.madisonparc*.com, *country* is the sub-domain.	Needed only if you have sub-domain.
DEFAULT_ORG1	Displays the same value as DSAME_DEF_DOMAIN.	Domain name, for example, *madisonparc*.com
EXIST_DIT_SCHEMA	Indicates whether you have selected to use an existing DIT and schema.	True/False
ADMIN_COMPONENT_SELECTED	Indicates whether you have selected to deploy the Identity Server Console.	True/False
CONSOLE_DEPLOY_URI	Displays the URI for accessing Identity Server Console.	The default is *amconsole*. You can change it.
DSAME_CONSOLE	Displays the URI for accessing Identity Server Console.	*nila.madisonparc.com*
DSAME_CONSOLE_HOST	Displays the name of the machine that hosts Identity Server Console.	Name of the host machine.
CONSOLE_PROTO	Indicates the protocol used by the Identity Server Console	http
DSAME_CONSOLE_PORT	Indicates the port number used by the Identity Server Console	58080
DSAME_CONSOLE_DEF_DOMAIN	Displays the domain on which you have installed Identity Server.	*madisonparc*.com
DSAME_CONSOLE_FULL_DOMAIN	Displays the domain on which you have installed the Identity Server Console. This is typically identified by the last two labels of the FQDN.	*madisonparc*.com
DSAME_CONSOLE_SUB_DOMAIN	Displays the second label in the FQDN.	Needed only if you have a sub-domain to specify.

Table 9-1 Description of Statefile Variables

Variable	Description	Value
USE_DSAME_SERVICES_WEB_CONTAINER	Indicates if you have installed Identity Server Console with new or existing Identity Server services.	Value is 1 if Identity Server Console is installed with Identity Server Services. Value is 0 (zero) if you have installed only the Identity Server Console.
DIT_COMPLIANCE	Indicates if you have an existing Identity Server-compliant DIT.	false
DS_ALREADY_EXISTS	Indicates whether you have specified to use an existing Directory Server.	true/false
LOAD_DIT	Indicates if you have selected to load an Identity Server-compliant DIT.	Y/N
AUTO_LOAD	Indicates whether you had selected to load the Identity Server 6.0-compliant DIT/Schema during installation.	True, if you had selected to load the DIT/Schema and False, otherwise.
CUSTOM_DIRECTORY	Indicates if you have specified a custom directory that stores the existing Directory Server.	True/False
DS_ROOT_SUFFIX	Displays the root suffix defined in your Directory tree.	dc=*madisonparc* dc=com, o=*madisonparc*.com
DC_TREE	Displays the root suffix defined for your DIT.	dc=*madisonparc*, dc=com, o=*madisonparc*.com
ORG_BASE	Displays the same value as DS_ROOT_SUFFIX.	
DS_SERVER	Displays the FQDN of the computer where you have installed Directory Server.	*host*.*madisonparc*.com
DS_HOST	Displays the name of the computer on which you have installed Directory Server.	Name of the computer.
DS_PORT	Displays the port used by the Directory Server	The default is 389. You can change it to any number between 1 and 65535.
DS_INSTALL_DIR	Displays the path to the directory in which you have installed Directory Server.	The default is /usr/iplanet/servers

Table 9-1 Description of Statefile Variables

Variable	Description	Value
DS_ROOT_DN	Displays the DN defined in your DIT.	cn=Directory manager
DS_ROOT_PASSWD	Displays the password you have set for the Administrator user of the Directory Server.	A password of at least characters long.
LOCAL_IDS	Indicates whether the existing Directory Server is installed locally or on a remote host.	true if the Directory Server is installed on the local host, and false, if it is installed on a remote host.
ORG_OBJECT_CLASS	Displays the marker object class defined for organization in your existing DIT. This variable need to be set only if you are installing Identity Server against an existing Directory Server.	The default is organization.
ORG_NAMING_ATTR	Displays the naming attribute used to define organization in your existing DIT. This variable need to be set only if you are installing Identity Server against an existing Directory Server.	o, dc
USER_OBJECT_CLASS	Displays the object class defined for users in your existing DIT. This variable need to be set only if you are installing Identity Server against an existing Directory Server.	The default is inetorgperson.
USER_NAMING_ATTR	Displays the naming attribute used for users in your existing DIT. This variable need to be set only if you are installing Identity Server against an existing Directory Server.	uid
DS_ADMIN_ID	Displays the user name defined for the Administrator of the Administration Server that manages Directory Server.	the default is admin
DS_ADMIN_PORT	Displays the port number used by the Administration Server.	the default is 58900
DS_ADMIN_PASSWD	Displays the password defined for the Administrator of the Administration Server.	the default is admin123

Table 9-1 Description of Statefile Variables

Variable	Description	Value
LDAPUSER	Displays the user id of *amldapuser*.	This is pre-defined as *amldapuser* and cannot be modified.
LDAPUSERPASSWD	Displays the password you have set for *amldapuser*.	This password should be different from that of the amadmin user.
SUPERADMIN	Displays the user name assigned to the top-level Administrator. This is assigned by Identity Server and cannot be modified.	the default is amAdmin. You must not change this value.
SUPERADMINPASSWD	Displays the password you have assigned for the top-level administrator.	This password should be different from the one set for the amldap user.
START_SERVER	Indicates whether you have selected to start the Identity Server automatically after the installation process.	true/false
COOKIE_DOMAIN_LIST		.madisonparc.com
DOMAINURLS		
FRESH_DS_WITH_SERVICES	Indicates if you have installed the Directory Server available with Identity Server.	Yes/No
STATE_BEGIN	Start tag of the statefile. This tag followed by the product name and wizard id is unique to a build of the product.	
STATE_DONE	End tag of the statefile. This tag followed by the product name and wizard id is unique to a build of the product.	

Chapter 10

Post-installation Tasks

This chapter explains the tasks that you would have to perform after installing Identity Server. This chapter also tells you how you can uninstall Identity Server, if at all you need to.

Topics in the chapter include:

- Starting Identity Server Services
- Logging In to the Administration Console
- Uninstalling Identity Server
- Uninstalling Identity Server On Windows

Starting Identity Server Services

On Solaris

To manually start Identity Server, at the command line enter the following command:

```
/Identity_Server_root/SUNWam/bin/amserver start
```

On Windows

Choose one of the following methods:

- To start Identity Server from the command line, open a DOS prompt window and enter the following commands:

```
cd Identity_Server_root\bin

amserver start
```

- To start Identity Server from the Start menu, first select Programs > Administrative Tools > Services. In the Services window, right-click the icon for Identity Server-*hostname*. From the menu, choose Start.

Installing and Uninstalling Identity Server Schema from the Command Line

After you've successfully installed the SUNWam package, you can install Identity Server from the command line with a single command. This is useful if you need to install the Identity Server schema on an additional instance of Directory Server. You can also uninstall the Identity Server schema with a single command.

To Install Identity Server Schema

1. In the following directory:

   ```
   Identity_Server_root/SUNWam/bin
   ```

   execute the following command:

   ```
   configds Directory_Server_host Directory Server_port bind_dn  bind_password
   ```

   The following message displays:

   ```
   modifying entry cn=schema
   ```

2. Restart Identity Server.

To Uninstall Identity Server Schema

1. In the following directory:

   ```
   Identity_Server_root/SUNWam/bin
   ```

   execute the following command:

   ```
   unconfigds Directory_Server_host Directory Server_port bind_dn  bind_password
   ```

   The following message displays:

   ```
   modifying entry cn=schema
   ```

2. Restart Identity Server.

Logging In to the Administration Console

Log in to Identity Server through your browser.

1. Go to the appropriate URL:

   If Identity Server services are running on Sun ONE Web Server, go to the login URL using the form:

   `http://`*host*`.`*domain*`:`*port*`/amserver/UI/Login`

   where *host* is the host name of the system, *domain* is the domain name of the server that runs Identity Server services, and *port* is the Identity Server services port number. For example:

   `http://ginac.madisonparc.com:58080/amserver/UI/Login`

   where `ginac` is the computer system that hosts Identity Server.

2. In the Login page, enter the Top-Level Administrator user id and password you specified at installation, and then click Login.

Uninstalling Identity Server

Uninstallation of Sun ONE Identity Server can be done using the GUI or using the command line.

Using this program, you can remove the entire product, or you can remove the following individual components of the product:

- JDK 1.3.1_06
- Sun ONE Directory Server
- Sun ONE Web Server
- Misc. Packages including utilities, samples and javadocs.
- Sun ONE Identity Server Management and Policy Services
- Sun ONE Identity Server Console
- Sun ONE Directory Server Configuration for Identity Server
- Sun ONE Identity Server Cross Domain Single Sign-On

- Common Domain Services

NOTE The Uninstallation program deletes all the files, including custom files and directories that you may have created, from the console deployment and service deployment directories. It is recommended that you back up your custom files and directories before you uninstall.

When uninstalling an existing Directory Server with an existing DIT, only the Identity Server schema is removed. The organizations, groups, roles, containers, users, policies, services, ACIs created or modified by Identity Server still remain in the Directory Server. To restore the original DIT, you can use `ldif2db` or `bak2db` to restore data saved before DIT migration.

Uninstalling Identity Server on UNIX

You must have root permissions to run the Identity Server installation program. Be sure all web browsers are closed before starting the uninstall program.

1. Change to the directory where you have installed Identity Server.
2. Start the Uninstallation program.

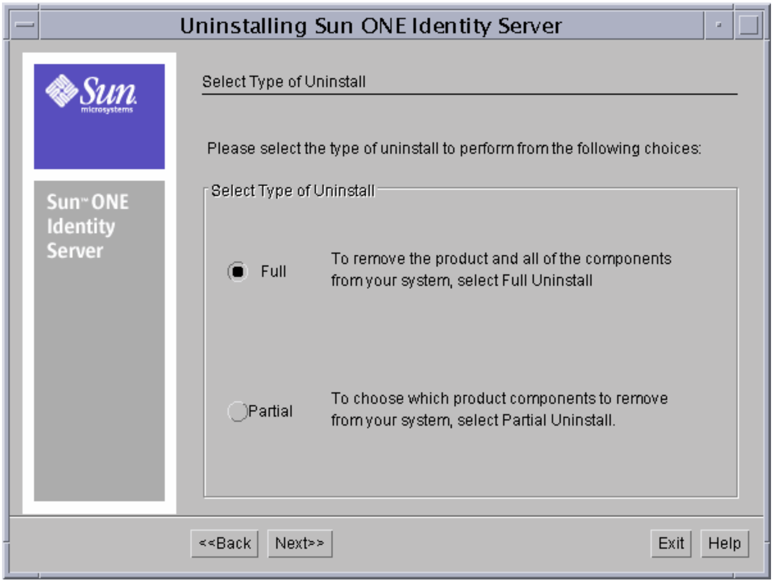
   To run the Uninstallation wizard, in the Identity Server root directory, enter the following command:

   ```
     #./uninstall
   ```

   To start the Uninstallation program from the command line, enter the following command

   ```
   # ./uninstall -no display
   ```
3. In the Welcome window, click Next.
4. In the Select Type of Uninstall window, select the type of uninstallation you want to perform, and then click Next.

Figure 10-1 Select Type of Install Panel



Uninstalling Sun ONE Identity Server

Select Type of Uninstall

Please select the type of uninstall to perform from the following choices:

Select Type of Uninstall

● Full — To remove the product and all of the components from your system, select Full Uninstall

○ Partial — To choose which product components to remove from your system, select Partial Uninstall.

Full: Select this type to remove the product and all the components from your system.

Partial: Select this type if you want to remove only certain components of the Identity Server. When you click Next, you'll see a list of all components that were installed with the services. In the Ready to Uninstall window, review the uninstallation information. If you need to make changes, click Back. Otherwise, click Uninstall Now. The program uninstalls the product or components based on your selection.

5. After you Identity Server is uninstalled, be sure the `SUNWam` package has been deleted. Use the following command to do this:

   pkginfo | grep SUNWam

6. If they exist, remove them manually using the following command:

   pkgrm SUNWam

7. In the following directory `/var/sadm/install, remove these files`:

   - `productregistry`
   - `.lockfile`
   - `.pkg.lock`

Uninstalling Identity Server On Windows

You must have Administrator privileges to run the Sun ONE Identity Server Uninstallation program. Be sure all web browsers are closed before starting the program.

1. Start the Installation program.

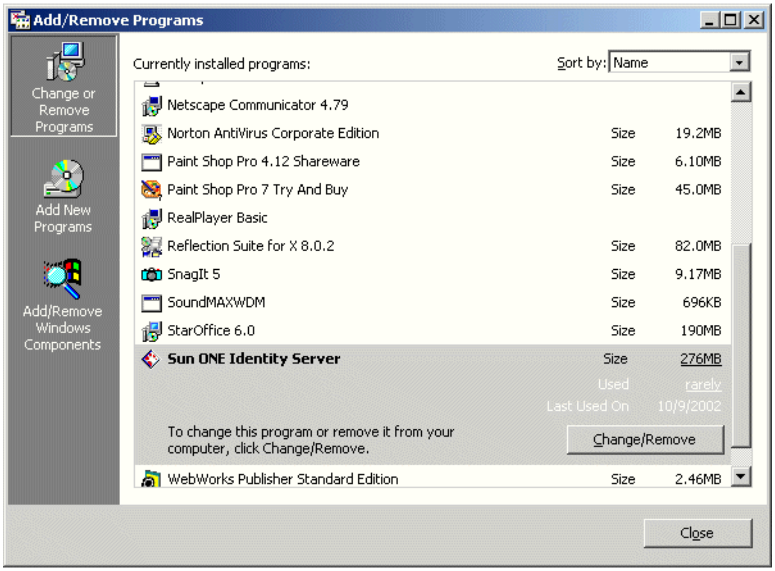
   To use the Start Men:

   a. From the Start Menu, choose Settings > Control Panel.

   b. In the Control Panel, double-click Add/Remove Programs.

   c. In the Add/Remove Programs window, select Sun ONE Identity Server, and then click Change/Remove.

Figure 10-2 Add Remove Programs window.



Currently installed programs: Sort by: Name

Netscape Communicator 4.79		
Norton AntiVirus Corporate Edition	Size	19.2MB
Paint Shop Pro 4.12 Shareware	Size	6.10MB
Paint Shop Pro 7 Try And Buy	Size	45.0MB
RealPlayer Basic		
Reflection Suite for X 8.0.2	Size	82.0MB
SnagIt 5	Size	9.17MB
SoundMAXWDM	Size	696KB
StarOffice 6.0	Size	190MB
Sun ONE Identity Server	Size	276MB
	Used	rarely
	Last Used On	10/9/2002
WebWorks Publisher Standard Edition	Size	2.46MB

To change this program or remove it from your computer, click Change/Remove.

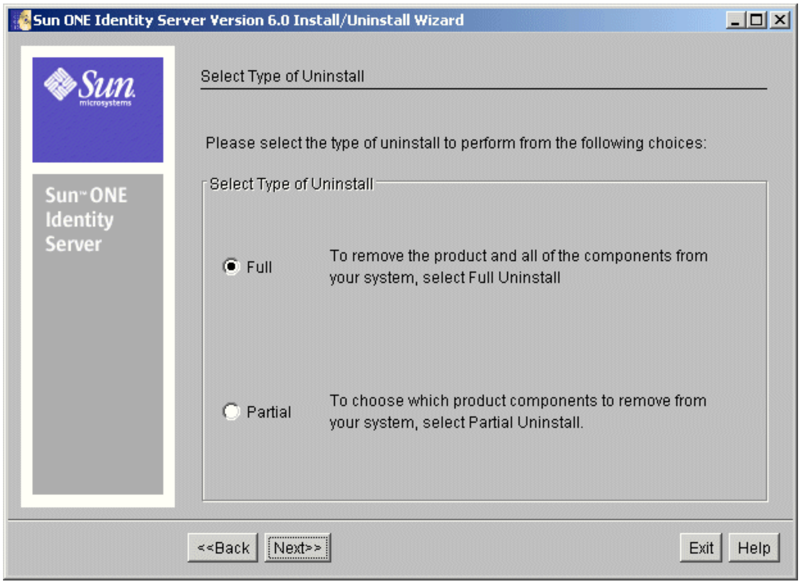
To launch the Uninstallation wizard from the command line, in the Identity Server root directory, run the following command:

```
java uninstall_Sun_ONE_Identity_Server
```

The Sun ONE Identity Server Uninstallation program starts.

2. In the Select Type of Uninstall window, select one of the following options.

Figure 10-3 Select Type of Uninstall Panel



Sun ONE Identity Server Version 6.0 Install/Uninstall Wizard

Select Type of Uninstall

Please select the type of uninstall to perform from the following choices:

Select Type of Uninstall

● Full — To remove the product and all of the components from your system, select Full Uninstall

○ Partial — To choose which product components to remove from your system, select Partial Uninstall.

Full. Select this option if you want to remove Identity Server services and Directory Server installed on the local computer system.

Partial. Select this option if you want to remove only some of the components of Sun ONE Identity Server. When you click Next in this window, the program will display all the components that are installed. Click those you want to uninstall.

3. In the Ready to Uninstall window, click Uninstall Now.

In the Summary Window, you can click Details to see more information about the uninstallation results.

4. Click Exit to exit the program.

Appendix A

Migrating Data from DSAME 5.1 to Identity Server 6.0

Introduction

This appendix describes the process for migrating data from DSAME 5.1 to Identity Server 6.0. The steps in the process must be performed in the order they are listed here.

The migration process involves the following steps:

1. Backing up the entire DSAME 5.1 data.
2. Uninstalling DSAME 5.1 excluding Directory Server 5.1.
3. Configuring the Directory Server for Identity Server 6.0 schema.
4. Installing Identity Server 6.0 with the existing Directory Server and DIT.
5. Migrating DSAME 5.1 services, policies and authentication entries to Identity Server 6.0.

It is expected that the person performing the migration procedure is familiar with Directory Server commands, schema semantics, DIT, Identity Server schema and Identity Server DIT structures. In addition, familiarity with XML and Identity Server installation procedure are required.

Identity Server 6.0 provides a set of Perl scripts to migrate DSAME 5.1 data to Identity Server 6.0. The migration procedure is complex, but these scripts handle many of those complexities. Typically, scripts generate an input file and an output file. Both these files are retained after the scripts are run. This helps in checking the entries in output files. The input files will contain the entries in 5.1 format, while the output files will have the entries in 6.0 format. When using these migration scripts, keep the following in mind:

- The output file needs to be loaded using `ldapmodify` command. It is not done automatically so that entries in the file can be checked before loading them.
- If you are running a script more than once, make sure to remove the old input and output files generated by the script. Some scripts append the output to an existing file because of which you may get errors while running `ldapmodify` commands.
- Each script contains additional information in them, which you must read before running the script. Additionally, in each script, you may have to set some variables or check the values of the variables before running the script.
- The migration scripts are case sensitive. The scripts will look for Identity Server attributes, object classes, and values *that are in lower case*. If you've customized your Identity Server 5.1 deployment with attribute names or object class names that contain upper case letters, then before running the scripts you must change those names to lower case letters.

NOTE The steps mentioned above represents the generic migration procedure. The scripts can be used in different ways to do the migration. For example, the existing Directory Server available with DSAME 5.1 can exported and loaded into a new Directory Server. The migration scripts can be run on this new Directory Server.

Backing up the Existing Installation

Before you start migration, ensure that DSAME 5.1 installation is completely backed up.

- Back up Directory Server data in DSAME 5.1 using Directory Server backup tools. The backup should include all 5.1 data including configuration and schema.
- If you have customized files that are located in the following directory:

  `DSAME_root/SUNWam/locale`

  then be sure to make a back up of the `.../locale` directory to preserve those customized files. After you've installed Identity Server 6.0 using the instructions in this chapter, you must manually copy your customized files back into the `DSAME_root/SUNWam/locale` directory.
- Back up Web Server data by copying any data modified after the DSAME 5.1 installation.

The Web Server data must be backed up manually. You can use the copy and tar commands for this. Any changes done to the Web Server files after the 5.1 installation must be backed up. The following directories must also be backed up.

Table 10-1 Directories to be backed up

Directory to be backed up	Contents
`<IS install dir>/SUNWam/web-apps/applications`	IS Console files
`<IS install dir>/SUNWam/web-apps/services`	IS services files
`<IS install dir>/SUNWam/servers/alias`	certificates
`<IS install dir>/SUNWam/config`	various XML files
`<IS install dir>/SUNWam/lib/`	property files
`<IS install dir>/SUNWam/locale`	locale files

You can refer to these backups, to make corresponding changes once Identity Server 6.0 is installed. These changes need to be done manually after the Identity Server 6.0 is installed.

You should also backup logs, debug and install files. The following table lists the directories that contain these files.

Table 10-2 Files to be backed up

Files	Location
log files	`/var/<IS 5.1 install dir>/SUNWam/logs`
debug files	`/var/<IS 5.1 install dir>/SUNWam/debug`
install files	`/var/<IS 5.1 install dir>/SUNWam/install`

Back up any other data that needs to be updated after the 6.0 migration.

Uninstalling DSAME 5.1

Use the DSAME 5.1 uninstallation program to remove components of DSAME. But, you must NOT remove Directory Server 5.1.

On Solaris

To remove DSAME components on Solaris:

1. Run `aminstall` script from DSAME 5.1.
2. Choose the following option:

   1) Remove existing components, then continue installation

3. At the next prompt, choose the following option to remove DSAME Management and Policy services.

   1) DSAME Management and Policy Services

4. Run `aminstall` script again and choose option 1.
5. At the next prompt, choose the following option to remove Directory Server Configuration.

   3) iPlanet Directory Server Configuration for DSAME

   This will remove the schema configuration for the Directory Server.

6. If Directory Server and Identity Server exist on different computer systems, then after installation is complete, you must manually remove the DSAME 5.1 schema file `95ns-amschema.ldif` from the Directory Server schema directory.
7. Check for the `SUNWamjdk` package after the uninstallation is complete using the following command:

   ```
   pkginfo |grep SUNWamjdk
   ```

8. If the `SUNWamjdk` package is present, remove it using the following command:

   ```
   pkgrm SUNWamjdk
   ```

9. Restart Directory Server after you have uninstalled the DSAME components.

On Windows

To uninstall DSAME 5.1 components, follow these steps:

1. Run the DSAME 5.1 uninstallation program. Refer to DSAME 5.1 Installation and Configuration Guide for detailed steps. You can find this guide online at: `http://docs.sun.com/source/816-5626-10/`.
2. Select partial uninstallation.
3. Choose DSAME Management and Policy services.

The above steps do not remove Directory Server configuration for DSAME on Windows. In order to configure the Directory Server of DSAME 5.1 to Identity Server 6.0 schema in the next step, you must uninstall DSAME 5.1 schema configuration. Remove DSAME 5.1 schema file, `95ns-amschema.ldif` from the Directory Server schema directory. In addition, the `productregistry` file must be updated to remove the directory server configuration component. You may remove the `productregistry` file itself. Please be sure to keep a backup of the `productregistry` file. If you remove the `productregistry` file, you can choose Add/Remove programs to remove Directory Server installation later.

4. Restart Directory Server after you have uninstalled the DSAME components.

Configuring Directory Server for IS 6.0 Schema

Using the Identity Server 6.0 installation program, configure Directory Server to work with Identity Server 6.0. For detailed instructions, see "Installing Identity Server Schema" on page 67 of this guide.

Installing Identity Server 6.0 on Directory Server 5.1

You may need to make some changes to the Directory Server that exists with DSAME. This Directory Server supports a DIT like this:

```
o=isp
|
o=madisonparc.com
```

Here isp is not really an organization. In such cases, the entry *isp* must be updated before you install Identity Server 6.0. If DSAME 5.1 Directory Server has an organization (flat DIT) as top level entry, then this change is not necessary before installing Identity Server 6.0. If the top level entry has iplanet-am-service-status attribute set, Identity Server 6.0 installation does not modify the Directory Server DIT. To retain the 5.1 DIT structure, add this attribute to the top level entry.

1. Run the following command to update the top level entry, if it is not an organization:

```
<5.1 Directory Server install dir>/shared/bin/ldapmodify -D
"cn=directory manager" -w <password>
dn: o=isp
changetype: modify
delete: objectClass
objectClass: iplanet-am-managed-org
-
add: objectClass
objectClass: sunManagedOrganization
-
add: iplanet-am-service-staus
iplanet-am-service-status:iPlanetAMAuthService
```

2. Use the right `dn` in the above command for your installation. If the top level entry in your DSAME 5.1 DIT is already an organization, then you shouldn't run the above command. You may run `ldapsearch` on the top level entry to check if this attribute is set.

3. Now, install Identity Server 6.0 on this Directory Server. During installation, choose the option of installing with an existing DIT.

4. While installing Identity Server 6.0, be sure the following entries have the same values as in DSAME 5.1 installation:

   - directory root suffix
   - directory manager password
   - admin user
   - admin password
   - directory server host
   - directory server port
   - console deployment description
   - services deployment descriptor

   Refer to the `AMConfig.properties` file from the DSAME 5.1 installation backup for any values you are not sure. Also, retain the DSAME 5.1 values for organization object class, organization naming attribute, user object class and user naming attribute.

This step does not modify Directory Server data and schema. It only installs Identity Server 6.0 packages, libraries, configuration files, jar files, etc.

Migrating Directory Server Data

Once Identity Server 6.0 is installed and the Directory Server schema is updated, the Directory Server data must be modified to Identity Server 6.0 format. All the migration scripts needed for this are located under the directory `<install dir>/SUNWam/migration/51to60`. The scripts contain additional information, which you must read before running the scripts. It will help you set some variables in each script or check the values of the variables.

In Identity Server 6.0, policy, authentication and console components have changed significantly from DSAME 5.1 and hence need to be migrated. However, Identity Server entries such as roles, groups, users, organizations, organizationalUnits and ACIs remain as they were in DSAME 5.1. They need not be migrated.

The following entries of DSAME 5.1 need to be updated to Identity Server 6.0.

- Services branch
- Organization
- OrganizationalUnit
- Policies
- Roles
- Users

Migration Tasks

The migration process involves the following tasks:

- Migrating Schema Changes
- Migrating DSAME 5.1 Policies
- Migrating Authentication Entries
- Migrating Services
- Updating Authentication Entries to Identity Server 6.0

- Updating Policies to Identity Server 6.0
- Migrating Agents

Migrating Schema Changes

Identity Server 6.0 has seen some schema changes from DSAME 5.1. For example, objectClass iplanet-am-managed-org for the organization has been changed to sunManagedOrganization. The attribute iplanet-am-domain-name is changed to sunPreferredDomain. Similarly, there are other schema changes. A script, `update-schema.pl` is provided to migrate schema changes. Run this script to migrate schema changes. Refer to the script for additional information. It generates an input file, `51entries.ldif` and an output file, `60entries.ldif`. Run `ldapmodify` on this output `ldif` file. The last line of the script specifies the syntax for running the `ldapmodify` command on this output file. DSAME 5.1 entries are updated to Identity Server 6.0 schema when you run this script.

Migrating DSAME 5.1 Policies

DSAME 5.1 uses Class of Service (COS) templates for policy implementation. The policy definition does not contain subjects to which the policy is assigned. Instead, policy must be explicitly assigned to a role or an organization. When a policy is assigned to an organization or a role, a COS template is created. There is one COS template for each organization or role that has a URL policy assigned.

In Identity Server 6.0, policy implementation is not done using COS templates. The policy definition itself contains the subjects like organization or roles. Using the policy COS templates, the DSAME 5.1 policies must be converted to Identity Server 6.0 policies to contain the subjects in the policy definition itself.

To convert the DSAME 5.1 policies to Identity Server 6.0 policies, `the` script `update-polices.pl` is provided. This script can be run for each organization or top level organization. If only one organization is specified to the script, it generates one output file containing 5.1 policies converted to 6.0 format for that organization. If the top level organization is specified, one XML file for each organization that has policies under the top level organization is generated. The output file name is of the format `<rdn>-<rdn>.xml`. For example, if o=iplanet.com,o=isp has some policies, the output file is `o=iplanet.com-o=isp.xml`. Run `update-policies.pl` script to generate XML files for the organization that have policies in DSAME 5.1. Refer to the script for additional details.

DSAME 5.1 has domain URL service. This service lets you do policy delegation control. This is somewhat similar to referral policies in Identity Server 6.0. If there are any domain URL policies defined, they must be backed up manually in this migration step.

For each domain URL policy, a referral policy may need to be created in Identity Server 6.0. Based on the domain URL policies, corresponding referral policies must be created in Identity Server 6.0. This needs to be done manually. No script is provided for this purpose. Refer to the section "Updating Policies to Identity Server 6.0" on page 187 for more details.

This step must be run before migrating services. The output generated in this step will be used after the step "Updating Policies to Identity Server 6.0" on page 187.

The URL policy DTD for DSAME 5.1 is located under `DSAME_root/SUNWam/dtd`.

The URL policy DTD for Identity Server 6.0 is installed under `Identity_Server_root/SunWam/dtd`.

Migrating Authentication Entries

Authentication services have changed significantly in Identity Server 6.0. These include changes in attribute names, attribute values, and default values and removal of attributes. The authentication information is present for each organization. The migration must update authentication entries for all organizations.

Run the authentication migration script, `update-auth.pl`. The script generates an output file, `51to60auth-entries.ldif`. It also generates an input file `51auth-entries.dn`.

The output files generated in this step will be used in the step "Updating Authentication Entries to Identity Server 6.0" on page 183.

Refer to the section "Changes in Authentication Services" on page 190 for the details on changes in authentication services from DSAME 5.1 to Identity Server 6.0.

Migrating Services

Each of the DSAME services needs to be removed and the corresponding Identity Server 6.0 service loaded. In addition, all the new Identity Server 6.0 services must also be loaded. The services branch has global schema information for each of the services and may contain entries specific to an organization. If the top level

DSAME entry is an organization itself, like o=sun.com, then the services branch under sun.com will contain global schema and organization specific entries as well. The organization-specific entries depend on what services have been registered for this organization. Follow this procedure to update the services branch.

1. If the top level entry is not an organization (such as o=isp, not an Identity Server organization), go to step 3. If the top level is an organization, go to step 2.

2. Run update-toporg-services.pl script. This script backs up organization entries for various authentication services and Identity Server Console service registered for the top level organization. The organization entries for the services reside under the global services entry for the top level organization. In order to update global services to 6.0, those services must be removed and loaded from 6.0. This step keeps a backup of the organization entries that reside under global services entry. Refer to this script for details. Check that it covers all the services which have organization specific entries (refer to step 3 as well).

   This script generates 51to60toporg-template.ldif output file. It also generates, 51toporg-template.dn input file.

3. Use Directory Server console to remove the DSAME services. If you added other services, don't remove them. The following services must be removed.

   iPlanetAMAdminConsoleService

   iPlanetAMAuthService

   iPlanetAMAuthAnonymousService

   iPlanetAMAuthCertService

   iPlanetAMAuthLDAPService

   iPlanetAMAuthMembershipService

   iPlanetAMAuthNTService

   iPlanetAMAuthRadiusService

   iPlanetAMAuthSafewordService

   iPlanetAMAuthUnixService

   iPlanetAMClientDetectionService

   iPlanetAMDomainURLAccessService

   iPlanetAMEntrySpecificService

   iPlanetAMLoggingService

   iPlanetAMNamingService

`iPlanetAMPlatformService`

`iPlanetAMPolicyService`

`iPlanetAMSessionService`

`iPlanetAMUserService`

`iPlanetAMWebAgentService`

`DAI`

If you have not added any additional services, you can remove the entire services branch under the top level entry.

4. Run `load-services.pl` to load Identity Server 6.0 services. This script loads all Identity Server 6.0 services. It uses the services XML `<install dir>/SUNWam/config/ums/ums.xml` and the XML files under `<install dir>/SUNWam/config/xml`.

5. Load the output file generated (`51to60toporg-template.ldif`) in step 2 above. This is required only if top level organization is an Identity Server organization. Use the `ldapmodify` command to load the output file. Refer to the last line in the output file for the syntax ("system" is not required, as that is used to run the script from the Perl script itself).

For details on Identity Server services changes in 6.0, refer to “Services in Identity Server 6.0” on page 195.

Updating Authentication Entries to Identity Server 6.0

Load the output file generated in the step "Migrating Authentication Entries." Use the `ldapmodify` command to load this. You can refer to the last line in the script for the syntax. This step migrates the DSAME 5.1 authentication entries to Identity Server 6.0. In addition, the following procedures may be necessary.

Customized 5.1 HTML templates, if any, need to be changed to 6.0 JSP-based templates.

Any customized authentication module need to be rewritten using `AMLoginModule.java`. Screen properties need to be changed to use the XML- based Authentication module properties. Refer to Identity Server 6.0 documentation for more details on writing custom authentication modules.

User's authentication module configuration will not be migrated automatically. If any authentication module is selected for any user in DSAME 5.1, it will not be available for that user after migration. The required authentication modules need to be configured manually for that user in Identity Server 6.0.

The user's default login URL attribute (iplanet-am-user-default-url) is no longer available in 6.0. This attribute is not migrated to 6.0 automatically. The value of this attribute can be set to iplanet-am-auth-login-success-url in the core authentication service or the planet-am-auth-login-success-url in the authentication configuration service or to a custom attribute depending on the deployment needs. This attribute must be migrated and removed from the user entries. Otherwise user entries that have this attribute can't be modified (you will get object class violation error).

Updating Identity Server Console Service Entries to 6.0

There are changes in the Identity Server 6.0 Console service that affect the Console display. The Domain URL Service is no longer available in 6.0. Because of the policy changes in 6.0, Web Agent service and Domain URL service need not be registered to organization, role and user entries. A script is provided to update entries to reflect these changes.

1. Run `update-services.pl` script to update the Console service if it is registered to any organization. The script generates input files, `51console.ldif` and `51services.ldif` and an output file, `60services.ldif`.
2. Run the `ldapmodify` command on the output file `60services.ldif`. This command migrates console service entries registered for the organization. It also migrates organization, roles and user entries for Domain URL and Web Agent services.

Enabling Federation Management

Identity Server 6.0 implements Liberty Alliance Phase 1 specifications. When you migrate services (see "Migrating Services" on page 181), two services are loaded for Federation Management. They are `iPlanetAMAuthenticationDomainConfigService` and `iPlanetAMProviderConfigService`. These services must be registered before you can use the Federation management features. An ldif file named `liberty-services.ldif` is provided to register these services.

Substitute the value of ROOT_SUFFIX in this file with the top-level organization. Run `ldamodify` on this ldif file. If the entries specified in this file are present in Identity Server 6.0, remove those entries from this ldif file and load the remaining entries. After this step, Federation management is enabled in Identity Server 6.0.

Once the services and authentication entries are migrated, users should be able to successfully log in to Identity Server 6.0. If the Directory Server is on the same machine as Identity Server 6.0, edit <installdir>/bin/amserver script and modify the NDS_SERVER variable to point to the correct Directory Server instance.

Restart the Identity Server and login to the Identity Server 6.0 Console. If the default login URL of 5.1 in the core authentication service is not modified (<protocol>://<host>:<port>/amserver/login), you can use default login URL of Identity Server 6.0 (<protocol>://<host>:<port>/amserver/UI/Login) to login to Identity Server 6.0 Console. There is a known issue in 5.1, where the default login url is set to /amserver/login sometimes instead of <protocol>://<host>/amserver/login in core authentication service. In such cases, you can't use 6.0 default login URL to login. You need to modify the associated domain attribute of the default org to the 6.0 default login URL(<protocol>://<host>/amserver/UI/Login) to access the console using 6.0 default login URL. Use the fully qualified domain name for host and use the correct deployment descriptor in the URL. Note that the associated domain attribute value does not have port number in it but while accessing the console, need to specify the port. You can also use the URL of the form `<protocol>://<host>:<port>/amserver/UI/Login?org=<org RDN>`. It is a good idea to check for login, before migrating other entries. The migration is a step-by-step process; the steps should be validated as and when possible.

User management is not enabled by default. After the login to Identity Server Console, go to Service Configuration tab. Edit Administration service. Click on "Enable User Management" check box and save the service. Now you can go to Identity Management tab for user management functions.

IS 6.0 has introduced a new user, amldapuser. This user is used to bind and search the directory for LDAP, Membership authentication modules. This user is also used in the policy config service. Once the LDAP, Membership or Policy Config Service is registered to an organization, password for this user must be explicitly entered in those services. The password is the amldapuser password entered during Identity Server 6.0 installation. In addition, this user must also be created. Run the following two commands to create this user and to set access rights to this user.

```
<path to ldapmodify>/ldapmodify -D "cn=directory manager" -w
<password>
dn: cn=amldapuser,ou=DSAME Users,ROOT_SUFFIX
changetype: add
objectclass: inetuser
objectclass: organizationalperson
objectclass: person
objectclass: top
cn: amldapuser
sn: amldapuser
userPassword: <password>
<path to ldapmodify>/ldapmodify -D "cn=directory manager" -w
<password>
dn: ROOT_SUFFIX
changetype: modify
add: aci
aci: (target="ldap:///ROOT_SUFFIX")(targetattr="*")(version 3.0;
acl "special ldap auth user rights"; allow (read,search) userdn =
"ldap:///cn=amldapuser,ou=DSAME Users,ROOT_SUFFIX";)
```

In the above commands, specify the Directory Manager password for the `-w` option. Replace ROOT_SUFFIX with the your install root entry. Specify the amldapuser password for the userPassword attribute in the first command.

Note that if the LDAP and Membership services are already registered to an organization in IS 5.1, the bind DN used for the user search is "dsameuser". Change that user to the "amldapuser" created above and the password to the amldapuser password. This should be done in all the organizations where these two services are registered. If they are kept as "dsameuser", it will continue to work, but for Identity Server 6.0, it is recommended that you use "amldapuser".

The Identity Server user's profile has an account expiration date attribute. The account expiration date format in DSAME 5.1 is mm/dd/yy hh:mm, while the account expiration date format in 6.0 is mm/dd/yyyy hh:mm. The attribute format is present in the file `amUser.properties` present in the directory named locale. If the account expiration attribute is set for the users in DSAME 5.1, the format of the date should be changed to 6.0 format, when modifying the users profile from Identity Server Console, to save the users profile changes. Alternatively, the date format can be changed to use the DSAME 5.1 format in `amUser.properties`. The ldapmodify command can also be used to modify the account expiration attribute value.

If there are any specific changes made to `AMConfig.properties` in DSAME 5.1, those changes must also be made in `AMConfig.properties` after Identity Server 6.0 is installed.

Updating Policies to Identity Server 6.0

Before loading the updated policies in the Directory Server, the DSAME 5.1 policies must be deleted. Run the `delete-policies` script to delete all policies. It generates an input file `delete-policies.dn` and an output file, `delete-policies.ldif`. Run `ldapdelete` command on `delete-policies.ldif` to delete all 5.1 policies. Make sure all the entries specified in `delete-policies.ldif` are deleted. If you get errors for the entries that don't exist in the Directory Server, remove those entries from the ldif file and continue deleting other entries of the file. The `delete-policies.ldif` file may have some duplicate entries. It may give errors while deleting already deleted entries (for duplicate entries). You can ignore such errors. You can run `ldapdelete` in continuous mode to ignore such errors.

Identity Server 6.0 has a new Policy Configuration service. This service specifies various configuration attributes used by policy components like subjects, referrals and conditions. In order to create policies in an organization, policy configuration service must be registered. For each organization, before loading the policies to that organization, this service must be registered. You can login to Identity Server 6.0 Console and register these services to each organization. You can also use the `amadmin` command to register this service to each organization.

Starting with the top level organization, run the following command to load Identity Server 6.0 policies:

Identity_Server_root`/bin/amadmin -u` *amadmin id* `-w` *password* `-t` *output migrated policy file for the organization*

In Identity Server 6.0, the policies can have a description along with the policy name. Also individual elements of policy such as rules, subjects, conditions and referrals have names. When importing DSAME 5.1 policies, the names for these elements and description are automatically generated. The names can be modified after the policies are imported.

Identity Server 6.0 has the concept of referral policies. Refer to the Identity Server 6.0 documentation for more details on this. In order to create policies in sub organizations, there must be referral policies from the top level organization. Referral policies do policy delegation based on the resource referrals. Consider the following DIT:

```
o=isp
```

```
          /\
o=madisonparc.com    o=iplanet.com
```

In order to create policies at madisonparc.com or iplanet.com, there must be a referral policy at o=isp.com to madisonparc.com and iplanet.com.

The referral policies at o=isp.com must contain the resource or resource prefix being managed at o=madisonparc.com or o=iplanet.com. If madisonparc.com manages http://www.madisonparc.com/, the referral policy at o=isp.com must contain the resource http://www.madisonparc.com/ in its rule and it must refer to madisonparc.com organization. For other resources being managed at o=madisonparc.com, other referral policies must be created at o=isp. Only after creating the top level referral policies, the policies at the sub-organization must be updated by running the command specified above. If there are no referral policies at the parent level for the resource specified at the sub org level policies, policy creation fails. So it is important to create referral policies at the parent level to the sub organization level before running the above command. Refer to the policy output file for each sub organization and check the resources contained in the XML files. For each of those resources, a referral policy must exist at the top level before loading the policy output XML file for that sub organization.

DSAME 5.1 has domain URL service. This service lets you do policy delegation control. This is somewhat similar to referral policies in 6.0. The key difference is that the domain URL service is enforced during policy evaluation, referral policies are enforced during policy creation as well as policy evaluation. Only the top level administrator can create domain URL policies in DSAME 5.1 by default.

In DSAME 5.1, using the above DIT, one could create policies in madisonparc.com giving access to resources in iplanet.com and vice versa. However the top level admin at o=isp, can create domain URL policies at o=madisonparc.com,o=isp. This policy specifies what is allowed in this organization. If the domain URL policy says, allow http://www.madisonparc.com/*, only those resources allowed in URL policies that match http://www.madisonparc.com/* would be returned during policy evaluation. This is enforced using referral policies in 6.0. For each domain URL policy created in DSAME 5.1, a corresponding referral policy must be created in 6.0. This step must be done manually.

Identity Server 6.0 has policy administrator role for policy management. The policy administrator has privileges to create, delete or modify policies and to assign services to organizations. For each organization in 6.0, policy administrator role must be created. Run update-policy-roles.pl script. It generates an output file, add-policy-roles.ldif. It also generates an input file, 51org-entries.dn. Load the output file generated by this script using ldapmodify. Refer to the syntax at the end of the script.

This step creates various policy admin roles in Directory Server.

Migrating Console Changes

If any console customization has been done in DSAME 5.1, those changes must be migrated to console files in Identity Server 6.0. For example, if you followed the instructions in "Backing up the Existing Installation" on page 174 and you backed up customized files the `DSAME_root/SUNWam/locale` directory, then you must now copy those customized files back into the `DSAME_root/SUNWam/locale` directory.

This step must be done manually. No scripts are provided for this purpose.

The above steps migrate Directory Server Data, Schema and any customized data to 6.0. Once the steps are complete, you should restart Identity Server 6.0.

Migrating Agents

Agents 1.0 or 1.1 do not work with Identity Server 6.0. You must have Agents 2.0 to work with Identity Server 6.0. In order to migrate agents, you must uninstall Agents 1.0 or 1.1 and then install Agents 2.0.

1. Backup any configuration changes made in 1.0 or 1.1 agents. For example changes done to AMAgent.properties.
2. Install 2.0 agents.
3. Make changes to 2.0 configuration files.
4. Restart the agents.

NOTE

1. Any changes done to DSAME 5.1 XML files are not migrated in this procedure. Once Identity Server 6.0 is installed, those changes need to be manually updated in the 6.0 XML files. One way to do this is to update the 6.0 XML files before loading them.
2. The script update-rootsuffix.pl is not used in the migration procedure. This script can be used in step 3.4, if this script is available from another Identity Server 6.0 install. This script updates the top level entry to have iplanet-am-service-staus attribute.

Changes in Authentication Services

This section describes in detail the changes in authentication services.

Authentication Service (Core) [amAuth.xml]

Attribute Changes

Global

1. Removed "iplanet-am-auth-login-worker-classes"
2. Added "iplanet-am-auth-sleep-interval"

Organization

1. Removed "iplanet-am-auth-chaining-modules"
2. Removed "iplanet-am-auth-chaining-enabled"
3. Removed "iplanet-am-auth-non-interactive-modules"
4. Removed "iplanet-am-auth-default-url"
5. Removed "iplanet-am-auth-user-based"
6. Removed "iplanet-am-auth-login-worker-class"
7. Added "iplanet-am-auth-org-config"
8. Added "iplanet-am-auth-login-success-url"
9. Added "iplanet-am-auth-login-failure-url"
10. Added "iplanet-am-auth-post-login-process-class
11. Added "iplanet-am-auth-username-generator-enabled"
12. Added "iplanet-am-auth-username-generator-class
13. Changed "iplanet-am-auth-menu" to "iplanet-am-auth-allowed-modules"
14. In "iplanet-am-auth-admin-auth-module",
    - Changed 'type' from "single_choice" to "single"
    - Changed 'syntax' from "string" to "xml"
    - Added attribute 'propertiesViewBeanURL' set to "/amconsole/auth/ACModuleList"

- Added attribute ’uitype’ set to "link"
- Removed sub-element ChoiceValues
- Changed Default Value from plain string to xml string

15. In "iplanet-am-auth-login-failure-count", Changed Default Value from 3 to 5
16. In "iplanet-am-auth-login-failure-duration", Changed Default Value from 15 to 300
17. In "iplanet-am-auth-lockout-warn-user", Changed Default Value from 1 to 4
18. In "iplanet-am-auth-default-auth-level", Changed ’syntax’ from "string" to "number"

Authentication related attribute changes in User Service [amUser.xml]

Attribute Changes

Dynamic

1. Removed "iplanet-am-user-auth-modules"

User

1. Removed "iplanet-am-user-auth-modules"
2. Removed "iplanet-am-user-default-url"
3. Added "iplanet-am-user-auth-config"
4. Added "iplanet-am-user-alias-list"
5. Added "iplanet-am-user-success-url"
6. Added "iplanet-am-user-failure-url"
7. In "iplanet-am-user-account-life", changed ’syntax’ from "date" to "string"

All "Organization" attributes in the following xml files

- amAuthLDAP.xml
    - In "iplanet-am-auth-ldap-search-filter", changed ’syntax’ from "string" to "xml"

    - In "iplanet-am-auth-ldap-auth-level", changed ’syntax’ from "string" to "number"

- amAuthAnonymous.xml
    - In "iplanet-am-auth-anonymous-auth-level", changed ’syntax’ from "string" to "number"
- amAuthMembership.xml
    - In "iplanet-am-auth-membership-search-filter", changed ’syntax’ from "string" to "xml"
    - In "iplanet-am-auth-membership-auth-level", changed ’syntax’ from "string" to "number"
- amAuthRadius.xml
    - In "iplanet-am-auth-radius-auth-level", changed ’syntax’ from "string" to "number"
- amAuthUnix.xml
    - In "iplanet-am-auth-unix-auth-level", changed ’syntax’ from "string" to "number"
- amAuthCert.xml
    - In "iplanet-am-auth-cert-auth-level", changed ’syntax’ from "string" to "number"
- amAuthSafeWord.xml
    - In "iplanet-am-auth-safeword-auth-level", changed ’syntax’ from "string" to "number"

The following table describes the UI changes for authentication interface.

Table 10-3 GUI Changes in the Authentication Interface

	DSAME 5.1.1 Filename	**Description**	**IS 6.0 Filename**
1.	`account_expired.html`	Your account has expired. Contact your system administrator.	`account_expired.jsp`
2.	`configuration.html`	Configuration error.	`configuration.jsp`
3.	`disclaimer.html`	This is a sample disclaimer template.	`disclaimer.jsp`

Table 10-3 GUI Changes in the Authentication Interface

	DSAME 5.1.1 Filename	Description	IS 6.0 Filename
4.	`invalidPCookieUserid.html`	Persistent Cookie Username does not exist in the Persistent Cookie Domain.	`invalidPCookieUserid.jsp`
5.	`invalidPassword.html`	The password entered does not contain enough characters.	`invalidPassword.jsp`
6.	`invalid_domain.html`	No such domain.	`invalid_domain.jsp`
7.	`login_denied.html`	User has no profile in this organization.	`login_denied.jsp`
8.	`login_fail_template.html`	Authentication failed.	`login_failed_template.jsp`
9.	`login_menu.html`	Authentication Menu the tag rows will be replaced with login_menu_modules.html.	removed
10.	`login_menu_modules.html`	Authentication Menu will loop and display (replace the tag inside) this file with all the available modules	removed
11.	`login_prompt.html`	User based login page.	`Login.jsp`
12.	`login_success.html`	You have logged in successfully, but your system has no default login page.	`Login.jsp`
13.	`login_template.html`	Login / Password page	`Login.jsp`
14.	`login_timeout_template.html`	Your login session has timed out.	`session_timeout.jsp`
15.	`logout.html`	You have logged out.	`Logout.jsp`
16.	`max_sessions.html`	Maximum Sessions Limit Reached.	`Message.jsp`
17.	`membership.html`	Self Registration Module	`membership.jsp`
18.	`membershipSkeleton.html`		removed
19.	`missingReqField.html`	One of the required fields was not completed.	`missingReqField.jsp`

Table 10-3 GUI Changes in the Authentication Interface

	DSAME 5.1.1 Filename	Description	IS 6.0 Filename
20.	`module_denied.html`	Your authentication module is denied.	`module_denied.jsp`
21.	`noConfirmation.html`	Missing the confirmation password field.	`noConfirmation.jsp`
22.	`noLoginWorker.html`	Authentication Page Generator not found.	removed
23.	`noPassword.html`	There was no password entered.	`noPassword.jsp`
24.	`noUserName.html`	There was no user name entered.	`noUserName.jsp`
25.	`noUserProfile.html`	No user profile was found matching the user name.	`noUserProfile.jsp`
26.	`org_inactive.html`	This organization is not active.	`org_inactive.jsp`
27.	`passwordMismatch.html`	The password and the confirm password do not match.	`passwordMismatch.jsp`
28.	`privilege_failure.html`	User does not have access to this operation.	`Message.jsp`
29.	`profileException.html`	An error occurred while storing the user profile.	`profileException.jsp`
30.	`radius_patch.html`	RADIUS authentication requires i-Planet patch 1.	`Message.jsp`
31.	`register.html`	Self Registration	`register.jsp`
32.	`session_invalid.html`	Your session is invalid.	removed
33.	`session_timeout.html`	Your session is timed out.	`session_timeout.jsp`
34.	`userExists.html`	A user already exists with this name.	`userExists.jsp`
35.	`userPasswordSame.html`	The User Name and Password fields cannot have the same value.	`userPasswordSame.jsp`
36.	`user_inactive.html`	This user is not active.	`user_inactive.jsp`
37.	`wrongPassword.html`	The password entered is invalid.	`wrongPassword.jsp`

Table 10-3 GUI Changes in the Authentication Interface

	DSAME 5.1.1 Filename	Description	IS 6.0 Filename
38.	add	Displays internal authentication framework errors.	auth_error_template.jsp
39.	add	No configuration found / defined for a user for an organization.	noConfig.jsp
40.	add	User is not in a Role. (for 'role' based authentication.)	userDenied.jsp

Services in Identity Server 6.0

The following are the new services in Identity Server 6.0:

- SAML service (amSAML.xml)
- Security Service (amDSS.xml)
- Policy Config Service (amPolicyConfig.xml)
- Auth Config service (amAuthConfig.xml)

The following services have been removed in 6.0:

- Domain URL service (amDomainURLAccess.xml)

The following services remain quite similar in DSAME 5.1 and Identity Server 6.0:

- Identity Server Console Service (amAdminConsole.xml)
- Auth Anonymous Service (amAuthAnonymous.xml)
- Auth Membership Service (amAuthMembership.xml)
- Auth Cert Service (amAuthCert.xml)
- Auth LDAP Service (amAuthLDAP.xml)
- Auth NT Service (amAuthNT.xml)
- Auth Radius Service (amAuthRadius.xml)
- Auth SafeWord Service (amAuthSafeWord.xml)
- Auth Unix Service (amAuthUnix.xml)

- Client Detection Service (amClientDetection.xml)
- Naming Service (amNaming.xml)
- Platform Service (amPlatform.xml)
- Session Service (amSession.xml)
- URL Agent Service (amWebAgent.xml)
- Entry Specific Service (amEntrySpecific.xml)
- User (amUser.xml)

The following services have changed significantly in 6.0:

- Auth Service (amAuth.xml)
- Logging Service (amLogging.xml)
- Policy Service (amPolicy.xml)
- User Service (amUser.xml)

Name Changes to Attributes and Object Classes

The following attributes have been renamed in Identity Server 6.0.

Table 10-4 Renamed Attributes

Old Attribute Name	New Attribute Name
iplanetserviceschema	sunserviceschema
iplanetserviceid	sunserviceid
iplanetsmspriority	sunservicepriority
iplanetpluginschema	sunpluginschema
iplanetkeyvalue	sunkeyvalue
iplanetpluginid	sunpluginid
iplanetxmlkeyvalue	sunxmlkeyvalue
iplanet-am-domain-name	sunPrefferedDomain

The following object classes have been renamed in Identity Server 6.0.

Table 10-5 Renamed Object Classes

Old Object Class	**New Object Class**
`iplanetservice`	`sunservice`
`iplanetservicecomponent`	`sunservicecomponent`
`iplanetorgservice`	`sunorgservice`
`iplanetserviceplugin`	`sunserviceplugin`
`iplanet-am-managed-org`	`sunManagedOrganization`

In addition, iplanet-am-unique-attribute-list and iplanet-am-attribute-uniqueness-enabled attributes are removed from Identity Server Console Service. A new attribute sunNameSapceUniqueAttrs in the new object class sunNameSpace is added to the organization entries to accommodate unique attribute list removed from Identity Server Console Service.

Index