Installation and Configuration Guide

iPlanet™ Directory Server
Access Management Edition

Version 5.1

May 2002

THIS DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

CETTE DOCUMENTATION EST FOURNIE "EN L'ÉTAT", ET TOUTES CONDITIONS EXPRESSES OU IMPLICITES, TOUTES REPRÉSENTATIONS ET TOUTES GARANTIES, Y COMPRIS TOUTE GARANTIE IMPLICITE D'APTITUDE À LA VENTE, OU À UN BUT PARTICULIER OU DE NON CONTREFAÇON SONT EXCLUES, EXCEPTÉ DANS LA MESURE OÙ DE TELLES EXCLUSIONS SERAIENT CONTRAIRES À LA LOI.

Contents

About This Guide

This *Installation and Configuration Guide* offers an introduction to iPlanet Directory Server Access Management Edition (DSAME) and describes how to plan and install a DSAME system.

This preface contains the following sections:

- What You Are Expected to Know
- The iPlanet Directory Server Access Management Edition Documentation Set
- Documentation Conventions Used in This Manual
- Related Information

NOTE Sun™ One Identity Server was previously known as iPlanet Directory Server Access Management Edition (DSAME). It was renamed shortly before launch. The late renaming of the product has resulted in a situation where the new product name is not fully integrated into the shipping product. In particular, you will see the product referred to as DSAME within the product GUI and within the product documentation. For this release, please consider Sun™ One Identity Server and iPlanet Directory Server Access Management Edition as interchangeable names for the same product.

What You Are Expected to Know

This book is considered the "first" manual in the documentation series provided with iPlanet™ Directory Server Access Management Edition. 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 iPlanet 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 iPlanet servers and services. The functionality contained in iPlanet DSAME 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 manage and customize an iPlanet Directory Server Access Management Edition system, as described in the *iPlanet DSAME Administration Guide* and the *iPlanet DSAME Programmer's Guide*.

The iPlanet Directory Server Access Management Edition Documentation Set

The DSAME documentation set contains the following guides:

- *Installation and Configuration Guide* (this guide) describes DSAME and provides details on how to plan and install DSAME on Solaris and Windows 2000 Server systems.
- *Administration Guide* documents how to manage user and service data in an iPlanet Directory Server Access Management Edition system once it has been installed.
- *Programmer's Guide* documents how to customize DSAME interfaces.
- 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 Directory Server Access Management Edition documentation web site for updates to the release notes and for revisions to the guides.

`http://docs.iplanet.com/docs/manuals/dsame.html`

Documentation Conventions Used in This Manual

In the iPlanet Directory Server Access Management Edition 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 iPlanet Directory Server Access Management Edition documentation set:

- *DSAME* refers to iPlanet Directory Server Access Management Edition and any installed instances of the iPlanet Directory Server Access Management Edition software.
- *Policy and Management services* refers to the collective set of iPlanet Directory Server Access Management Edition 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 DSAME* refers to the dedicated Web Server where the Policy and Management Services are installed.
- *Directory Server* refers to an installed instance of iPlanet Directory Server or Netscape™ Directory Server.
- *DSAME_root* is a variable place holder for the home directory where you have installed iPlanet Directory Server Access Management Edition.
- *Directory_Server_root* is a variable place holder for the home directory where you have installed iPlanet Directory Server.
- *Web_Server_root* is a variable place holder for the home directory where you have installed iPlanet Web Server.

- *AppServer_root* is a variable place holder for the home directory where you have installed iPlanet Application Server.

Related Information

In addition to the documentation provided with iPlanet Directory Server Access Management Edition, you should be familiar with several other sets of documentation. Of particular interest are the iPlanet Directory Server and iPlanet Web Server documentation sets.

This sections lists additional sources of information that can be used with iPlanet Directory Server Access Management Edition.

iPlanet Directory Server Documentation

You can find the iPlanet Directory Server documentation at the following site:

`http://docs.iplanet.com/docs/manuals/directory.html`

Directory Server Developer Information

In addition to the Directory Server documentation, you can find information on Directory Server Access Management Edition, LDAP, the iPlanet Directory Server, and associated technologies at the following iPlanet developer sites:

`http://developer.iplanet.com/tech/directory/`

`http://www.iplanet.com/downloads/developer/`

iPlanet Web Server Documentation

You can find the iPlanet Web Server documentation at the following site:

`http://docs.iplanet.com/docs/manuals/enterprise.html`

iPlanet Application Server Documentation

You can find the iPlanet Application Server documentation at the following site:

`http://docs.iplanet.com/docs/manuals/ias.html`

Other iPlanet Product Documentation

Documentation for all iPlanet and Netscape servers and technologies can be found at the following web site:

`http://docs.iplanet.com/docs/manuals/`

iPlanet Technical Support

You can contact iPlanet Technical Support through the following location:

`http://www.iplanet.com/support/`

Part 1

Read This First

Chapter 1

Introducing iPlanet Directory Server Access Management Edition

iPlanet Directory Server Access Management Edition (DSAME) is an enterprise infrastructure solution. It's the key to all your business relationships, all your services, all your data, and who has access to what. DSAME enables you to get your customers, your employees, your 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. DSAME is designed to meet the challenges of rapidly expanding extranets or hosting services. This chapter provides an introduction to the DSAME solution.

Topics in this chapter include:

- iPlanet Products Form the DSAME Solution
- Key Features and Benefits

iPlanet Products Form the DSAME Solution

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

When you purchase DSAME, you receive a full complement of iPlanet servers and services which together form the DSAME solution. The product CD includes the following:

- iPlanet Directory Server 5.1
- DSAME Management Service
- DSAME Policy Service
- DSAME schema
- Cross-Domain Single Sign-On component (CDSSO)

Web agents that work with DSAME are available as separate components. For more information about DSAME web agents, see "URL Policy Agent," on page 32.

Directory Server

iPlanet Directory Server is a powerful and scalable distributed directory server based on the industry-standard Lightweight Directory Access Protocol (LDAP). In a DSAME 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

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 pluggable 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.

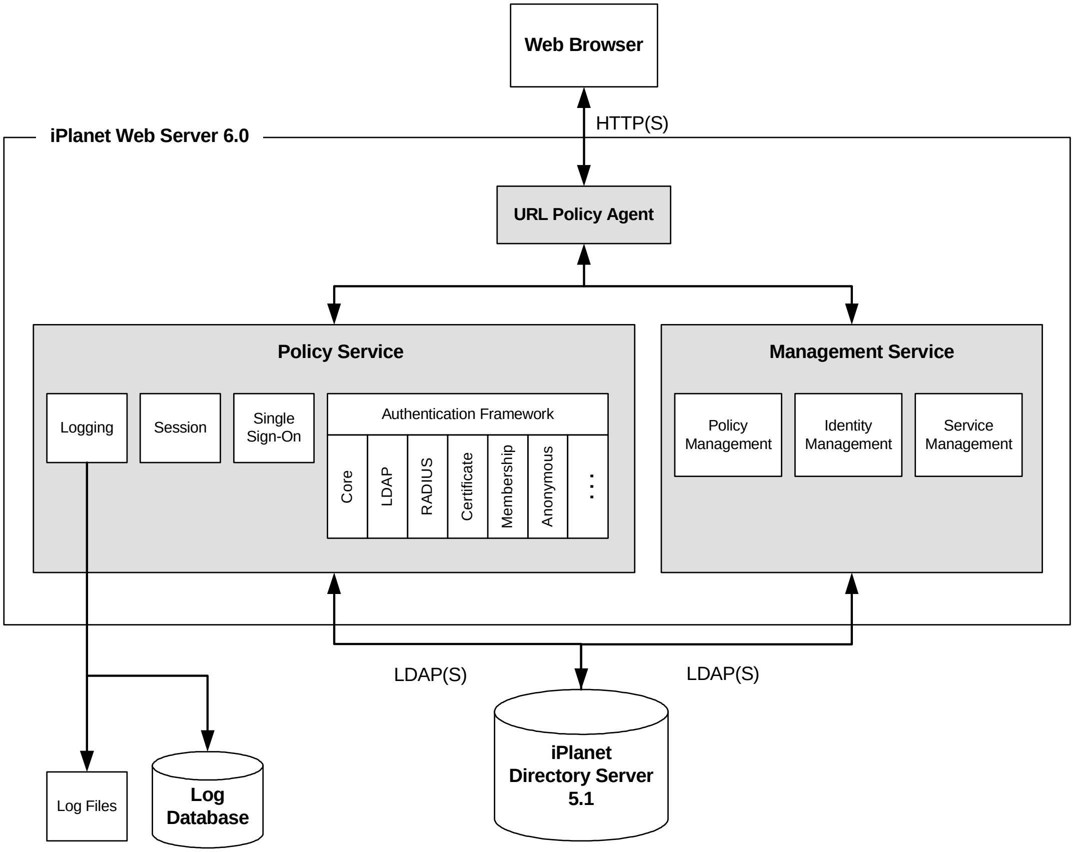
Logging

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 DSAME administration 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 DSAME Architecture.



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 DSAME administration 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.

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 DSAME 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 DSAME 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

iPlanet Web Server, although not included in the product CD as a stand-alone product, is an integral part of the DSAME 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.

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. DSAME offers the following features to meet the challenges of growing enterprises.

Administration Console

A graphical interface that consolidates Identity, Service, and Policy management. 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 iPlanet customers to write and use their own modules with DSAME. The following Authentication modules come with DSAME:

- 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.

URL 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. Ensures that communications over the network can not be viewed by unauthorized individuals.

Directory Replication Support

DSAME 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

DSAME 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

DSAME works with load-balancers such as iPlanet Directory Access Router, to provide high availability and firewall-like security.

Chapter 2

Deployment Considerations

There are a number of issues you must resolve and options you should consider before you run the iPlanet Directory Server Access Management Edition (DSAME) installation program. This chapter provides information you should keep in mind as you plan your DSAME deployment.

Topics in this chapter include:

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

Directory Issues

The way you install and configure DSAME will depend upon your company's current directory environment and your long-term directory needs. Before attempting to install DSAME, 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 DSAME.

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

`http://docs.iplanet.com/docs/manuals/directory.html`

If You Already Have an Existing Directory

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

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

These topics are discussed in detail in "Using an Existing Directory Server," on page 63.

NOTE If you're installing DSAME against an existing directory, the required directory modifications are complex. They require 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.

DSAME Schema

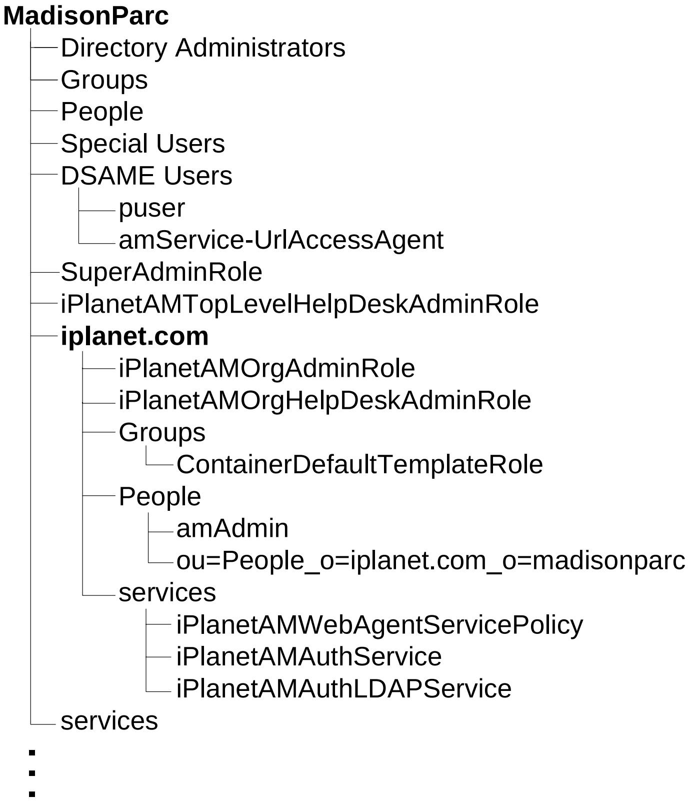
You can install DSAME schema by choosing option 3) iPlanet Directory Server Configuration for DSAME. Only the DSAME schema is installed on the server where the Directory Server is installed. The schema file `95ns-amschema.ldif` file is added to your server schema directory.

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

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

The DSAME 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 DSAME. These object classes make it possible for DSAME to manage only selected data—user data—and not interfere with other aspects of your tree such as servers or hardware.

Figure 2-1 A Default Directory Information Tree (DIT).



Default DITs

A default DIT is simply any DIT that does not comply with the rigid iPlanet-DIT specification. Most DSAME customers choose this option. You should choose the default DIT option if any of these are true:

- You plan to install DSAME against an existing directory that is already provisioned with user data.
- You will use DSAME in an intranet or extranet environment.
- You don't want to use the structure imposed by the iPlanet DIT.

In Figure 2-1, the root suffix is named `MadisonParc`.The root suffix can contain groups and userids for MadisonParc's employees and enterprise administration. In Default DIT you can configure the default root suffix to the organization name. A default organization, `o=iplanet.com`, is created under the root. This might be used to store directory entries for MadisonParc's non-administrator employees, partners, or customers.

Unsupported DITs

While most provisioned DITs can be reconfigured to work with DSAME, in some cases reconfiguration is not recommended. In general, if your existing DIT uses more than one type of directory entry (examples: `dc`, `o`, and `ou`) to define organizations, your user data will be recognized by DSAME only under certain conditions. For detailed information, see "DITs That Cannot Be Managed by DSAME," on page 218 of this manual.

Directory Replication

If you plan to use replicated directories with DSAME, you should define your database replication agreements before running the DSAME installation program. See "Support for Directory Replication and High Availability," on page 119 of this manual for more information.

Policy Management Issues

Delegated administration and web access management in DSAME 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 DSAME graphical user interface. As you plan your directory structure, consider how you can leverage these pre-defined DSAME objects to meet your enterprise needs.

Roles

DSAME 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 DSAME, the concept of roles is the same as in Directory Server, but with an added level of abstraction. When you install DSAME, 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 DSAME administrator roles and the scope of write permissions that correspond to each role.

Table 2-1 The Default DSAME Administrator Roles

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
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 DSAME 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 URL 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. 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. URL 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 DSAME Policy feature evaluates the rules attached to the user's organization, role, or userid. Based upon the net result of the rules and policies assigned to the user, the individual is either granted or denied access to the web page. You can configure rules and policies in the Administration Console. For more information about setting up policies, see the *iPlanet DSAME Administration Guide*. For comprehensive information about DSAME policy agents and how to install and configure them, see the iPlanet Agent Pack documentation at `http://docs.iplanet.com/docs/manuals/dsame.html#agent10`

Service Attributes

You can use service attributes to define how services will work with DSAME. Some service attributes are set at the global level and impact the entire DIT, 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 *iPlanet DSAME Administration Guide* at `http://docs.iplanet.com/docs/manuals/dsame.html`

Installing Other Products for Use With DSAME Services

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

Remote Web Servers

In this manual, Web Servers are “remote” relative to the Web Server that runs DSAME 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 DSAME only when you install a URL policy agent on it. For more information, see “URL Policy Agent,” on page 32.

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.iplanet.com/docs/manuals/enterprise.html`

iPlanet Application Server

You can install and configure DSAME Services to run on iPlanet Application Server for Solaris instead of on the default Web Server. This option is not available on the Windows platform.

URL Policy Agent

The DSAME URL 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 DSAME Policy Agent Pack contains a number of URL policy agents designed to work with DSAME. The Policy Agent Pack is a separate product and is available for download at the following URL:

`http://www.iplanet.com/downloads/developer/5167.html`

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

Multiple Directory Servers for Failover and High Availability

For your convenience, a stand-alone version of Directory Server 5.1 is included in the DSAME product CD. You can use the DSAME installation program to install this version of Directory server for the purposes of upgrading, setting up failover directories, or for setting up multi-master replication.You should install, configure and deploy iDS properly for DSAME to be successful. For more information, see "Support for Directory Replication and High Availability," on page 119 for Solaris, or on page 199 for Windows.

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.iplanet.com/docs/manuals/directory.html`

LDAP Load-Balancers

You can configure DSAME to work with load-balancers such as iPlanet 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 119 for Solaris, or on page 199 for Windows.

For detailed iPlanet Directory Access Router installation and administration information, access the documentation on the Internet at `http://docs.iplanet.com/docs/manuals/dar.html`

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

Hardware and Software Requirements

You must make sure that the systems on which you plan to install DSAME meet the minimum hardware, software, and operating system requirements. While all the DSAME 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 DSAME deployment. The recommended procedure is to consult with iPlanet Professional Services or another iPlanet-certified system integrator before designing and deploying an iPlanet DSAME 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 iPlanet DSAME.
- If you have existing web servers that need to be protected, the URL 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 DSAME (and iPlanet Web Server) and potentially iPlanet Application Server and URL 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 URL 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: 256 MB
250,000 - 1,000,000 entries	Free disk space: 4 GB, Free memory: 512 MB
Over 1,000,000 entries	Free disk space: 8 GB, Free memory: 1 GB

Operating System Requirements

DSAME Version 5.1 is supported on the following platforms:

- Sun Solaris 2.8 (32-bit and 64-bit)
- Microsoft Windows 2000 Server SP 2

Patch Clusters for Solaris

When running iPlanet 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`.

Remote Web Server Requirements

DSAME Web Agents use approximately 10 MB of disk space. For detailed information on Web Server requirements for DSAME Web Agents, see the iPlanet Agent Pack documentation at the following URL:

`http://docs.iplanet.com/docs/manuals/dsame.html#agent10`

Application Server Requirements

If you choose to install DSAME services on iPlanet Application Server, both the Application Server as well as its iPlanet Web Server must already be installed and running. This deployment requires the following:

- iPlanet Web Server 6.0 SP2 on Solaris 2.8 (32-bit or 64-bit)
- iPlanet Application Server 6.5 on Solaris 2.8 (32-bit or 64-bit)

Web Browser Requirements

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

- Netscape Communicator 4.79 on the following platforms: Solaris 8; Windows versions 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.

Part 2

Solaris Installation Instructions

Chapter 3

The DSAME Installation Program for Solaris

The iPlanet Directory Server Access Management Edition (DSAME) installation program is used to install or uninstall the complete product all at once, or components of the product one at a time. You can use the DSAME installation program in a number of ways depending upon your deployment needs. This chapter provides an overview of the options presented in the installation program, as well as some pointers on determining the installation tasks you'll need to perform.

Topics in this chapter include:

- Before You Begin
- Installation Program Options
- Determining Which Installation Options to Use
- Starting DSAME Services
- Logging In to DSAME
- Uninstalling DSAME

Before You Begin

Be sure to resolve the following before you start the installation program:

- You must have root permissions to run the installation program.
- You can only install DSAME, or any of the components, on a machine local to you. You can not install across a network on remote machines.

- Determine whether or not you will be configuring an existing Directory Server. For more information, see "If You Already Have an Existing Directory," on page 26 and "Unsupported DITs," on page 28.
- Determine whether or not you will be installing DSAME Services to run using iPlanet Application Server or using iPlanet Web Server. In either case, you will need the computer system name and port number for the server when you install DSAME Services.
- Determine whether or not you will be installing DSAME policy agents. For more information, see "URL Policy Agent," on page 32.
- Determine whether or not you will be installing cross-domain single sign-on components. For more information, see "Cross-Domain Single Sign-On," on page 21.

Installation Program Options

Each time you run the installation program, a number of installation options are displayed. Determine which installation option to choose by first identifying your scenario in Table 3-1, and then follow the detailed instructions that correspond to that scenario. The following is a brief summary of what happens when you choose each of the main installation options.

Option 1) DSAME Management and Policy Services

When you choose this option, if you don't already have an existing Directory Server, the following are installed for you:

- iPlanet Directory Server (optional)
- iPlanet Web Server
- DSAME Policy Service
- DSAME Management Service

When the installation program is done, the complete product is installed, and you can immediately log into DSAME. No user data will be present in the directory.

Option 2) iPlanet Directory Server 5.1

When you choose this option, only Directory Server 5.1 is installed; no DSAME services are installed. When you choose this option, you're given the opportunity to install DSAME schema. For detailed information on installing Directory Server 5.1 or upgrading to version 5.1, see the documentation that comes with *iPlanet Directory Server 5.1 Installation Guide*. Or you can access the documentation on the Internet at `http://docs.iplanet.com/docs/manuals/directory.html`

Option 3) iPlanet Directory Server Configuration for DSAME

When you choose this option, you are prompted for the host and port number of your existing Directory Server. Only the DSAME schema is installed on the server where the Directory Server is installed. The schema file `95ns-amschema.ldif` file is added to your server schema directory. No new Directory Server is installed; no existing data is overwritten. Choose this option only if you plan to use DSAME with an existing Directory Server 5.1 instance that's already provisioned with user data.

Option 4) DSAME 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 DSAME, install on Web Server, or install this by installing Webserver. For more information, see "Cross-Domain Single Sign-On," on page 21.

Exiting the Installation Program

After you've started the DSAME installation program, you can exit the program at any time by pressing `Ctrl-C`.

Determining Which Installation Options to Use

You will probably run the DSAME installation program multiple times in order to install Directory Servers, DSAME services and DSAME web agents in the proper number and sequence. Table 3-1 summarizes the common installation scenarios, and where to find the step-by-step instructions for each scenario.

Table 3-1 Where To Find DSAME Installation Instructions For Specific Solaris Scenarios

Common Installation Scenarios on Solaris	Where to Find Detailed Installation Instructions
1. Install DSAME and for evaluation purposes.	
OR	
2. Install and deploy Directory Server and DSAME for the first time for production purposes; you have no existing user data to work with.	Chapter 4, “Simple Installations With No Existing Directory Server.
3. Install DSAME to work with a single directory that is already provisioned with user data.	Chapter 5, “Using an Existing Directory Server”.
4. Install multiple instances of DSAME against a single Directory Server for agent failover. DSAME and the master Directory Server are already installed; the directory may or may not be already provisioned with users.	“Installing Multiple DSAME Instances Against the Same Directory Server,” on page 117.
5. Install a stand-alone version of Directory Server; useful in setting up multi-master replication.	“To Install iPlanet Directory Server With Package Format,” on page 58.
6. Upgrade an existing directory by installing a stand-alone version of Directory Server 5.1, without DSAME schema.	“To Install Directory Server Without DSAME Package Format,” on page 62.
7. Configure an existing Directory Server 5.1 to be used with DSAME; the existing directory is already provisioned with user data.	Chapter 5, “Using an Existing Directory Server“ .
8. Install and configure the cross-domain single sign-on (CDSSO) component.	“Installing the Cross-Domain Single Sign-On Component,” on page 113.
9. Uninstall or re-install DSAME.	“Uninstalling DSAME,” on page 43.

Starting DSAME Services

If you choose not to start DSAME automatically, you must start it manually before you can login. At the command line enter the following command:

```
/DSAME_root/SUNWam/bin/amserver start
```

Logging In to DSAME

If, at the end of installation, you chose to start DSAME automatically, you can log in to DSAME through your browser.

1. Go to the appropriate URL:

   - If DSAME services are running on iPlanet Web Server, go to the login URL using the form:

     `http://host.domain:port/amconsole`

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

     For example: `http://tintin.india.sun.com:58080/amconsole`

   - If DSAME services are running on iPlanet Application Server, go to the login URL using the form:

     `http://host.domain:port/NASApp/amconsole`

     where *host* is the host name of the system, *domain* is the domain name of the server that runs DSAME services, *port* is the DSAME services port number, and `NASApp` is the Universal Resource Identifier (URI) prefix automatically assigned to Application Server.

2. In the Login page, enter the Top-Level Administrator user id and password you specified at installation.

Uninstalling DSAME

The installation program in DSAME is also used to uninstall the DSAME application. You can remove the entire product, or you can remove the following individual components of the product:

- DSAME Management and Policy Services
- iPlanet Directory Server 5.1
- iPlanet Directory Server Configuration for DSAME
- DSAME Cross Domain Single Sign-On

To Uninstall DSAME Components

You must have root permissions to run the DSAME installation program. Be sure all web browsers are closed before starting the installation program.

1. Insert the DSAME product CD into the drive of the system on which DSAME components are installed.
2. In the DSAME directory, at the command line, enter `aminstall`.

   The `aminstall` command accepts the `-v [verbose]` option. The verbose option gives brief progress messages as the actions of the install program take place.
3. Read the License Agreement. At the prompt, **Do you agree to the license terms?** enter `y` for Yes.
4. When the following message displays, enter `1`.

```
Checking for DSAME 5.1 components ...done.
The following DSAME Components are installed:

DSAME Management and Policy Services
iPlanet Directory Server 5.1
iPlanet Directory Server Configuration for DSAME

One or more components that are part of DSAME 5.1
have been detected on this system.

If you are going to install components which already exist, you
must uninstall them first.
Otherwise, choose option 2 to continue the installation.

What would you like to do?

1) Remove existing components, then continue installation
2) Continue installation without removing existing components
3) Exit
```

5. The following message displays.

```
Please select one of the bundles to remove from ...

1) DSAME Management and Policy Services
2) iPlanet Directory Server 5.1
3) iPlanet Directory Server Configuration for DSAME
4) DSAME Cross Domain Single Sign-On
5) All
6) Continue with installation
7) Quit
```

- If you want to remove nothing but the Policy and Management Services, then enter 1.
- If you want to remove nothing but the Directory Server 5.1 application, then enter 2.
- If you want to remove nothing but the DSAME schema, then enter 3.
- If you want to remove only the cross-domain single sign-on controller, then enter 4.
- If you want to remove all bundles related to DSAME, then enter 5.
- If you have changed your mind and do not want to uninstall any packages, but you want to install other DSAME components, then enter 6.
- If you have changed your mind and do not want to uninstall any bundles, and you do not want to install additional bundles, then enter 7 to exit the installation program.

Chapter 4

Simple Installations With No Existing Directory Server

This chapter provides instructions for installing iPlanet Directory Server Access Management Edition (DSAME) for evaluation purposes, or for deploying a DSAME directory or services for the first time. These instructions assume that you do not already have iPlanet Directory Server installed on the target computer system.

Topics in this chapter include:

- Installing DSAME Services
- Installing iPlanet Directory Server 5.1

NOTE If you plan to use DSAME with an existing Directory Server that is already provisioned with users, see Chapter 5, "Using an Existing Directory Server".

Installing DSAME Services

Use these instructions when you want to do a quick and simple installation to explore the product. You can also use these instructions when you are installing multiple instances of DSAME Services to support directory replication. For more information on directory replication, see"Installing Multiple DSAME Instances Against the Same Directory Server," on page 117.

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

- Directory Server 5.1
- DSAME Policy service and Management service
- A Web Server that runs the DSAME Policy and Management services

To Install DSAME Services with Directory Server

You must have root permissions when you run the DSAME installation program. Be sure all web browsers are closed before starting the installation program.

1. If you're installing DSAME from the product CD, insert the CD into the drive of the system on which you want to install the software.

   If you've downloaded the product, unpack the product binaries file using the following command:

   ```
   gunzip -dc dsame-5.1-domestic-us.sparc-sun-solaris2.8.tar.gz |
   tar -xvof -
   ```

2. Run the `aminstall` program. On the product CD, you'll find the program in the directory `/cdrom/DSAME_51`. If you've downloaded the product binaries, you'll find the program in the directory where you untarred the binary files.

   At the command line, enter `aminstall`.

   The `aminstall` command accepts the `-v [verbose]` option. The verbose option gives brief progress messages as the actions of the install program take place. Otherwise, installation messages are written to log files in the following directory:

   ```
   /var/opt/SUNWam/install
   ```

3. Read the License Agreement. When prompted, **Do you agree to the license terms?** Enter `y` for Yes.

4. If the following message does not display, then skip to the Step 5.

```
One or more components that are part of DSAME 5.1 have been
detected on this system.

If you are going to install components which already exist, you
must uninstall them first.

What would you like to do?
1) Remove existing components, then continue installation.
2) Continue installation without removing existing components.
3) Exit
```

- If the above message is displayed, and you want to re-install components listed in the message, then enter `1` to remove the existing components. After uninstallation, the installation program will automatically start again from the beginning.
- If the message (above) is displayed, and you want to install components that are not listed, then enter `2` to proceed to the next step.

5. The following options are displayed.

```
Select which component to install:

1) DSAME Management and Policy Services
2) iPlanet Directory Server 5.1
3) iPlanet Directory Server Configuration for DSAME
4) DSAME Cross Domain Single Sign-On
5) Exit
```

When prompted, provide the following information:

Select which component to install: Enter `1` to install DSAME Services.

Do you want to install the DSAME Management and Policy Services on iPlanet Application Server? By default, DSAME will be installed with its own Web Server which will power the DSAME services and user interface.

- If you want to use the default Web Server that comes with DSAME, enter `n` for No, and then skip to Step 6.

- If you want to use Application Server instead of the default Web Server to run DSAME services, *and Application Server is already installed and running*, provide the following information when prompted:

  What directory is the iPlanet Application Server installed in? Enter the full path to the directory where Application Server is installed.

  What is the host name of the machine running the iPlanet Application Server Webserver? This is the Webserver host name that the iPlanet Application Server uses as its web connector.

  What is the sub-domain name ("." for none)? For example, in the name `mycomputer.organizationname.madisonparc.com`, the sub-domain name is `organizationname.` If your host computer does not have a sub-domain, enter a period (`.`).

  What is the domain name? For example, in the name `mycomputer.organizationname.madisonparc.com`, the domain name is `madisonparc.com`

  What is the iPlanet Application Server Webserver port? This is the Webserver port number that the Application Server uses as its port.

  Will you be using an existing DIT and schema? Enter `n` for No**.**

  What is the root suffix of your directory tree? This is the DSAME root suffix, or the point in your directory where you want DSAME to start managing entries. Enter a distinguished name (DN) that includes at least one *type*=*value* pair.

  Examples:

  `o=isp`

  `o=madisonparc`

  `dc=sun,dc=com`

  If you want the default organization to be the root suffix, enter a period (.).

NOTE The default organization uses the `organization (o) object class`. If you want to use a different naming attribute such as `dc`, you must follow the installation instructions in Chapter 5, "Using an Existing Directory Server".

What is your organization name? Enter a name for the first organization to be created in your DSAME Directory Information Tree (DIT). This name will be displayed in the DSAME graphical user interface. Examples: `iPlanet` or `iplanet.com`.

Do you want to use an existing iPlanet Directory Server? Enter `n` for No.

What directory do you want to install the Directory Server in? Enter the path to the directory where Directory Server will be installed. Do not install Directory Server in the same directory as DSAME Services. Ideally, you would install DSAME Services and Directory Server on different computer systems.

What port should the LDAP server use? The following is an excerpt from *iPlanet Directory Server Installation Guide* regarding this topic:

“Port numbers can be any number from 1 to 65535. Keep the following in mind when choosing a port number for your Directory Server:

The standard Directory Server (LDAP) port number is 389.

Port 636 is reserved for LDAP over SSL. Therefore, do not use port number 636 for your standard LDAP installation, even if 636 is not already in use. You can also use LDAP over TLS on the standard LDAP port.

Make sure the ports you choose are not already in use.

If you are using both LDAP and LDAPS communications, make sure the port numbers chosen for these two types of access are not identical.”

Directory Server Administration userid: Administration Server user ID is used only when the Directory Server is down and you are unable to log in as the configuration directory administrator. The existence of this user ID means that you can access Administration Server and perform disaster recovery activities such as starting Directory Server, reading log files, and so forth.

Normally, Administration Server user and password should be identical to the configuration directory administrator ID and password.

Admin password (8 chars minimum): Enter a password for the Directory Server administrator.

Re-enter Admin password: Enter the password again to confirm it.

What is the Directory Server admin port? The default port number is 58900.

Directory Manager DN: The Directory Server administrative user, or Directory Manager, is the administrator who has unlimited access to Directory Server data and configuration. The default DN for the Directory Manager is `cn=Directory Manager.`

Directory Manager password (8 chars minimum): Enter a password for the Directory Manager.

Re-enter Directory Manager password: Enter the password again to confirm it.

The Top Level Administrator user id is: This is the Administrator who has unlimited access to all entries managed by DSAME. The Super Administrator user id is hardcoded `amAdmin`. This ensures that the DSAME administrator role and its privileges are created and mapped properly in the Directory Server so that you can log into DSAME product immediately after installation.

Admin password (8 chars minimum): Enter a password for the Super Administrator.

Re-enter Admin password: Enter the Super Administrator password again to confirm it.

Skip to Step 7.

6. If you're using Application Server instead of the default Web Server that comes with DSAME, then skip to Step 7.

   If you're using the default Web Server that comes with DSAME, provide the following information when prompted:

   Do you wish to continue this installation without the required patches? Enter y for Yes to proceed with the installation. If you wish to install the patches, then enter n for No. For information on installing patches see "Patch Clusters for Solaris," on page 35.

   What directory do you want to install the Services in? Enter the path to the directory where DSAME Services will be installed. Plan to install the DSAME Services and Directory Server in different directories. Ideally, you would install DSAME Services and Directory Server on different computer systems.

   Do you want to use the existing JDK? Java support in DSAME requires Java Development Kit (JDK) of version 1.3.1 or higher. While a default JDK is provided, you can use your own JDK with the Web Server. If you want to use your own JDK version, then enter n for No and then enter the full path to the version of JDK you want to use. Otherwise, enter y for Yes.

   What is the host name of the machine where the DSAME Services will run? This is the computer system where DSAME components and Web Server are installed together. For example, in the name `mycomputer.organizationname.madisonparc.com`, the host name is `mycomputer`.

   What is the sub-domain name ("." for none)? For example, in the name `mycomputer.organizationname.madisonparc.com`, the `organizationname` is the sub-domain name. If your host computer does not have a sub-domain, enter a period `(.)`.

   What is the domain name? For example, in the name `mycomputer.organizationname.madisonparc.com`, the domain name is `madisonparc.com`

   What is the DSAME Management and Policy Services port? Enter a port number for the Web Server that runs the DSAME services. The default port is `58080`.

   Web Server Administration user id: This is the server administrator who has access to the Web Server that runs DSAME services. The default user id is `admin`.

   Admin password (8 chars minimum): Enter a password for the Web

Server Administrator.

Re-enter Admin password: Re-enter the Web Server Administrator password to confirm it.

What is the Web Server admin port? Enter a port number for administering the Web Server. The default port number is `58888`.

System User: This is the user the Directory Server will run as. If you have a Directory Server already running, enter the same System User used by that Directory Server. The default is `nobody`.

System Group: This is the group the user (above) belongs to. The default is `nobody`.

Will you be using an existing DIT and schema? Enter `n` for No**.**

What is the DSAME root of your directory tree? This is the DSAME root suffix, or the point in your directory where you want DSAME to start managing entries. Enter a distinguished name (DN) that includes at least one *type*=*value* pair.

Examples:

`o=isp`

`o=madisonparc`

`dc=sun,dc=com`

If you want the default organization to be the root suffix, enter a period (.).

The default is `o=isp`.

NOTE The default organization uses the `organization (o) object class`. If you want to use a different naming attribute such as `dc`, you must follow the installation instructions in Chapter 5, “Using an Existing Directory Server”.

What is your organization name? Enter a name for the first organization to be created in your DSAME Directory Information Tree (DIT). This name will be displayed in the DSAME graphical user interface. Examples: `iPlanet` or `iplanet.com`. The default is `iplanet.com`.

Do you want to use an existing iPlanet Directory Server? Enter `n` for No.

What directory do you want to install the Directory Server in? Enter the path to the directory where Directory Server will be installed. Do not install Directory Server in the same directory as DSAME Services. Ideally, you would install DSAME Services and Directory Server on different computer systems. The default directory is `/usr/iplanet/servers`.

<Path> does not exist, create? If this prompt displays, DSAME can automatically creates a new for you. Enter `y` for Yes.

What port should the LDAP server use? The following is an excerpt from *iPlanet Directory Server Installation Guide* regarding this topic:

“Port numbers can be any number from 1 to 65535. Keep the following in mind when choosing a port number for your Directory Server:

The standard Directory Server (LDAP) port number is 389.

Port 636 is reserved for LDAP over SSL. Therefore, do not use port number 636 for your standard LDAP installation, even if 636 is not already in use. You can also use LDAP over TLS on the standard LDAP port.

Make sure the ports you choose are not already in use.

If you are using both LDAP and LDAPS communications, make sure the port numbers chosen for these two types of access are not identical.”

Directory Server Administration user id: Administration Server user id is used only when the Directory Server is down and you are unable to log in as the configuration directory administrator. The existence of this user id means that you can access Administration Server and perform disaster recovery activities such as starting Directory Server, reading log files, and so forth. The default user id is `admin`.

Normally, Administration Server user and password should be identical to the configuration directory administrator ID and password.

Admin password (8 chars minimum): Enter a password for the Directory Server administrator.

Re-enter Admin password: Enter the password again to confirm it.

What is the Directory Server admin port? The default port number is `58900`.

Directory Manager DN: The Directory Server administrative user, or Directory Manager, is the administrator who has unlimited access to Directory Server data and configuration. The default DN for the Directory Manager is `cn=Directory Manager`

Directory Manager password (8 chars minimum): Enter a password for the Directory Manager.

Re-enter Directory Manager password: Enter the password again to confirm it.

What is the deployment URI prefix for the DSAME Management and Policy Services? The Universal Resource Identifier (URI) prefix tells the Web Server where to look for HTML pages associated with a service and also for other web application specific information like classes and jars.

For example, an authentication service may store a customized login page for each organization in the enterprise. If you are an employee of the Jones Company, you'll see an HTML login page with the Jones logo. If you are an employee of the Smith Company, you'll see an HTML login page with the Smith logo. The HTML pages for each company should be stored in different locations.

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

What is the deployment URI prefix for the DSAME Administration Console? The Universal Resource Identifier (URI) prefix tells the Web Server where to look for HTML pages that an administration console needs to display and also for other web application specific information like classes and jars.

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

The Top-Level Administrator user id is amAdmin: This is the Administrator who has unlimited access to all entries managed by DSAME. The Top-Level Administrator user id is hard coded `amAdmin`. This ensures that the DSAME administrator role and its privileges are created and mapped properly in the Directory Server so that you can log into DSAME product immediately after installation. Since this is an administrator role, you can add other users to this role after installation.

Admin password (8 chars minimum): Enter a password for the Super Administrator.

Re-enter Admin password: Enter the Super Administrator password again to confirm it.

Do you want to start the iPlanet Directory Server Access Management Edition Server when installation is complete? If you enter `y` for Yes, DSAME will automatically start up immediately after installation. If you enter `n` for No, you must start DSAME manually after installation.

To start DSAME manually, at the command line enter the following command:

/DSAME_root/`SUNWam/bin/amserver start`

7. **Are all settings correct?** If the settings displayed are not correct, enter `n` for No and the installation program will start again from close to the beginning. If the settings are correct, enter `y` for Yes to continue with the installation.

   Select which component to install: When you see the following options displayed, enter `5` to exit the installation program.

```
Select which component to install:

1) DSAME Management and Policy Services
2) iPlanet Directory Server 5.1
3) iPlanet Directory Server Configuration for DSAME
4) DSAME Cross Domain Single Sign-On
5) Exit
```

8. **Check the installation log file for errors:** The installation log file was indicated after agreeing to the license terms in Step 3. If you have forgotten the file name, the installation log files are in `/var/opt/SUNWam/install`, and the most recent one can be identified by entering the command:

```
ls -ltr /var/opt/SUNWam/install
```

Installing iPlanet Directory Server 5.1

You can use the DSAME product CD to install iPlanet Directory Server as a stand-alone product. For example, you might want to install Directory Server by itself when you need to upgrade to version 5.1 or when you want to install multiple servers for directory replication. For your convenience, there is a stand-alone version of iPlanet Directory Server 5.1 that you can install by running the DSAME installation program; the DSAME package format is installed automatically. On the DSAME product CD, there is also a Directory Server 5.1 installation program. When you run the Directory Server installation program, the DSAME package format is not installed.

Installing Directory Server With the DSAME Package Format

When you use the DSAME installation program, if you choose the iPlanet Directory Server 5.1 option, Directory Server is installed with the package format. When you use this installation option, you can only install one Directory Server per computer host. If you need to install more than one Directory Server on a single computer, see "Installing Directory Server Without the DSAME Package Format," on page 62.

To Install iPlanet Directory Server With Package Format

You must have root permissions when you run the DSAME installation program. Be sure all web browsers are closed before starting the installation program.

1. If you're installing DSAME from the product CD, insert the CD into the drive of the system on which you want to install the software.

   If you've downloaded the product, unpack the product binaries file using the following command:

   ```
   gunzip -dc dsame-5.1-domestic-us.sparc-sun-solaris2.8.tar.gz |
   tar -xvof -
   ```

2. Run the `aminstall` program. On the product CD, you'll find the program in the directory `/cdrom/DSAME_51`. If you've downloaded the product binaries, you'll find the program in the directory where you untarred the binary files.

   At the command line, enter `aminstall`.

   The `aminstall` command accepts the following `-v [verbose]` option. The verbose option gives brief progress messages as the actions of the install program take place. Otherwise, installation messages are written to log files in the following directory:

   ```
   /var/opt/SUNWam/install
   ```

3. Read the License Agreement. At the prompt, **Do you agree to the license terms?** enter `y` for Yes.

4. If the following message does not display, then skip to the step 5.

```
One or more components that are part of DSAME 5.1 have been
detected on this system.
...
If you are going to install components which already exist, you
must uninstall them first.

What would you like to do?
1) Remove existing components, then continue installation.
2) Continue installation without removing existing components.
3) Exit
```

- If the message (above) is displayed, and Directory Server 5.1 is listed in the message, then enter `1` to remove it. After uninstallation, the installation program will automatically start again from the beginning and you can re-install all DSAME components.
- If the above message is displayed, and Directory Server 5.1 is not listed in the message, then enter `2` to proceed to the next step.

5. The following options are displayed.

```
Select which component to install:

1) DSAME Management and Policy Services
2) iPlanet Directory Server 5.1
3) iPlanet Directory Server Configuration for DSAME
4) DSAME Cross Domain Single Sign-On
5) Exit
```

When prompted, provide the following information:

Select which component to install: Enter `2`.

What directory do you want to install the Directory Server in? Enter the path to the directory where Directory Server will be installed. Do not install Directory Server in the same directory as DSAME Services. Ideally, you would install DSAME Services and Directory Server on different computer systems.

<Path> does not exist, create? If this prompt displays, DSAME can automatically create a new for you. Enter y for Yes.

What is the host name of the machine where the Directory Server will run? For example, in the fully qualified domain name `mymachine.organizationname.madisonparc.com`, the host computer system name is `mymachine`.

What is the sub-domain name ("." for none)? For example, in the name `mycomputer.organizationname.madisonparc.com`, the sub-domain name is `organizationname.` If your host computer does not have a sub-domain, enter a period `(.)`.

What is the domain name? For example, in the name `mycomputer.organizationname.madisonparc.com`, the domain name is `madisonparc.com`

What port should the LDAP server use? The following is an excerpt from *iPlanet Directory Server Installation Guide* regarding this topic:

“Port numbers can be any number from 1 to 65535. Keep the following in mind when choosing a port number for your Directory Server:

- The standard Directory Server (LDAP) port number is 389.
- Port 636 is reserved for LDAP over SSL. Therefore, do not use port number 636 for your standard LDAP installation, even if 636 is not already in use. You can also use LDAP over TLS on the standard LDAP port.
- Make sure the ports you choose are not already in use.
- If you are using both LDAP and LDAPS communications, make sure the port numbers chosen for these two types of access are not identical.”

Directory Server Administration userid: Administration Server user ID is used only when the Directory Server is down and you are unable to log in as the configuration directory administrator. The existence of this user ID means that you can access Administration Server and perform disaster recovery activities such as starting Directory Server, reading log files, and so forth.

Normally, Administration Server user and password should be identical to the configuration directory administrator ID and password.

Admin password (8 chars minimum): Enter a password for the Directory Server administrator.

Re-enter Admin password: Enter the password again to confirm it.

What is the Directory Server admin port? The default port number is `58900`

System User: This is the user the Directory Server will run as. If you have a Directory Server already running, enter the same System User used by that Directory Server. Example: `nobody`

System Group: This is the group the user (above) belongs to. Example: `nobody`**.**

What is the root suffix of your directory tree? This is the DSAME root suffix, or the point in your directory where you want DSAME to start managing entries. Enter a distinguished name (DN) that includes at least one equals sign (=).

Examples:

```
o=isp
```

```
o=madisonparc
```

```
dc=sun,dc=com
```

If you want the default organization to be the root suffix, enter a period (.).

Do you want to configure this Directory Server for use by DSAME? If you want to install DSAME schema, enter `y` for `Yes`. If you do not want to install DSAME schema, enter `n` for `No`.

Directory Manager DN: The Directory Server administrative user, or Directory Manager, is the administrator who has unlimited access to Directory Server data and configuration. The default DN for the Directory Manager is cn=Directory Manager. Enter the DN you specified when you first installed Directory Server.

Directory Manager password (8 chars minimum): Enter a password for the Directory Manager. Confirm the password when prompted.

Do you want to start the iPlanet Directory Server Access Management Edition iDS when installation is complete? If you enter `y` for Yes, then Directory Server will automatically start up immediately after installation. If you enter `n` for No, then you must restart DSAME manually after installation.

To restart Directory Server, enter the commands with root permissions:

`cd` *Directory_Server_root*`/slapd-`*instance_name*

```
start-slapd
```

Are all settings correct? Confirm that the settings are correct. If they are not, choose `n` for `no` and the installation program will prompt you for the setting information again.

6. Enter `5` to exit the installation program.

Installing Directory Server Without the DSAME Package Format

When you use the Directory Server setup program, Directory Server is installed without the DSAME package format. You can use the setup program to install multiple Directory Servers on a single computer host.

If you plan to use directory replications, you'll need to install stand-alone versions of Directory Server 5.1 on more than one computer system. If you want to set up your replications before you install DSAME schema, you can use the Directory Server setup program that comes on the DSAME product CD.

To Install Directory Server Without DSAME Package Format

You must have root privileges when installing Directory Server.

1. Locate the Directory Server setup program.

   - If you're installing from the DSAME product CD, insert the CD into the drive of the machine where you want to install Directory Server.

   - If you've downloaded the product, unpack the product binaries file using the following command:

     ```
     gunzip -dc dsame-5.1-domestic-us.sparc-sun-solaris2.8.tar.gz
     | tar -xvof -
     ```

2. In the DSAME directory, at the command line, enter the following commands:

   ```
   cd SUNWamds/reloc/*/
   
   cp directory.5.1.us.sparc-solaris.tar /tmp
   
   cd /tmp
   
   tar -xvof directory.5.1.us.sparc-solaris.tar
   
   setup
   ```

For detailed installation instructions, see the *iPlanet Directory Server Installation Guide* that comes with the product. Or access the documentation on the Internet at `http://docs.iplanet.com/docs/manuals/directory.html`

Chapter 5

Using an Existing Directory Server

If you're using an existing Directory Server that is already provisioned with users, you must make several changes in your Directory Information Tree (DIT) before iPlanet Directory Server Access Management Edition (DSAME) will recognize your user data. The number and scope of changes you must make will depend upon how your existing DIT is structured, and upon how you plan to use DSAME.

This chapter provides instructions for installing DSAME services against an existing directory that contains user data. It also explains how to configure DSAME to work with your DIT, and how to make the necessary changes to your existing directory entries.

Topics in this chapter include:

- Before You Begin
- Step 1: Install Directory Server 5.1 and Configure it to Work with DSAME
- Step 2: Install DSAME Services
- Step 3: (Optional) Add Your Custom Object Classes to DSAME Schema
- Step 4: (Optional) Configure Alternative Naming Attributes
- Step 5: Load DSAME LDIF into Your Directory
- Step 6: Load DSAME Service Attributes into Your Directory
- Step 7: (Optional) Add DSAME ACIs to Your Default Organization
- Step 8: Start DSAME
- Step 9: Add DSAME Object Classes and Attributes to Existing Directory Entries
- Step 10: Load the Modified LDIF Files

Before You Begin

The requisite directory modifications are complex. They require a high level of expertise in LDAP planning and implementation, as well as some familiarity with XML. The procedures are complicated and can be time-consuming. Be sure to plan accordingly for this phase of deployment.

NOTE If you do not already have an existing directory that is provisioned with users, you do not need to perform the steps described in this chapter. See "Simple Installations With No Existing Directory Server," on page 47.

Supported DITs and Unsupported DITs

While DSAME can be reconfigured to support most existing DITs, in some situations reconfiguration may not be recommended. To determine whether your DIT may be compatible with DSAME, see "DITs That Cannot Be Managed by DSAME," on page 218.

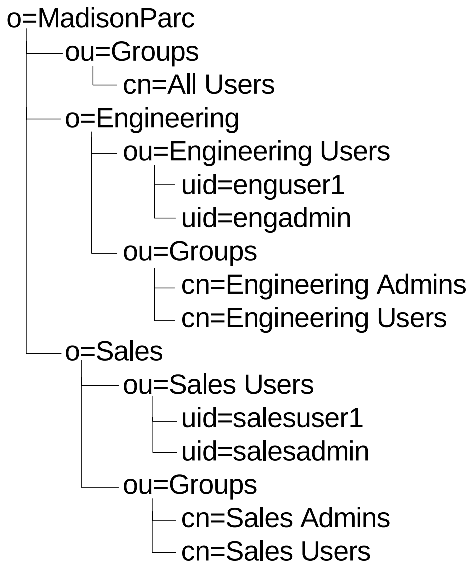
Background for Examples Used in This Chapter

In order to illustrate the types of changes you'll need to make to your directory, we'll use a simple DIT for a fictitious company. The directory entries for this company, represented by `o=madisonparc`, contain two custom object classes. These are object classes that are not already defined in DSAME schema. If your DIT contains custom object classes, you'll also need to make changes to the DSAME XML files.

Basic DIT Structure

The examples used in this chapter are based on a simple DIT for a fictitious company. Figure 5-1 on page 65 shows two organizations, `Engineering` and `Sales`, under the root. All groups in this example are *static* groups. This means that entries for these groups use the `groupOfUniqueNames` object class, which contains values naming the members of the group.

Figure 5-1 Directory Information Tree (DIT) used in examples in this chapter.



The following summarizes the use of groups in this sample DIT:

- There is one group containing the administrators for Engineering, and one group with the administrators for Sales.
- Very simple ACIs are set for the groups Engineering and Sales to allow members of these groups to manage their respective organizations.
- In each organization, there is a group that contains non-administrator users.
- There is another group at the root level, or *top level*. It contains all users in the directory.

Custom Object Classes

The fictitious company used in this example uses two object classes that are not included in the DSAME schema nor in the Directory Server 5.1 schema. An auxiliary object class `madisonparc-org` is in every organization entry, and an auxiliary object class `madisonparc-user` is in every user entry. In order to manage these extensions, changes must be made in the following three files:

- `amEntrySpecific.xml`
  (Changes are not required if you're modifying only user entries.)
- `amUser.xml`
- `ums.xml`

These changes are described in detail in the section "Step 3: (Optional) Add Your Custom Object Classes to DSAME Schema," on page 80. If you use custom object classes in your existing directory, you will need to make similar changes.

Step 1: Install Directory Server 5.1 and Configure it to Work with DSAME

DSAME will work only with iPlanet Directory Server 5.1. If you have a pre-5.1 version installed, you must upgrade to version 5.1 and migrate your data before you can install DSAME services. If your existing directory uses Directory Server 5.1, you'll need to install only DSAME schema. In either case, follow these instructions.

Step 1a: Back Up Your Directory Data

For detailed information on backing up your directory, see the *iPlanet Directory Server Installation Guide* at:

`http://docs.iplanet.com/docs/manuals/directory.html`

Step 1b: Install and Configure Directory Server 5.1 with DSAME Schema

You must have root permissions when you run the DSAME installation program. Be sure all web browsers are closed before starting the installation program.

1. If you're installing DSAME from the product CD, insert the CD into the drive of the system on which you want to install the software.

   If you've downloaded the product, unpack the product binaries file using the following command:

   ```
   gunzip -dc dsame-5.1-domestic-us.sparc-sun-solaris2.8.tar.gz |
   tar -xvof -
   ```

2. Run the `aminstall` program. On the product CD, you'll find the program in the directory `/cdrom/DSAME_51`. If you've downloaded the product binaries, you'll find the program in the directory where you untarred the binary files.

   At the command line, enter `aminstall`.

   The `aminstall` command accepts the `-v [verbose]` option. The verbose option gives brief progress messages as the actions of the install program take place. Otherwise, installation messages are written to log files in the following directory:

   ```
   /var/opt/SUNWam/install
   ```

3. Read the License Agreement. At the prompt, **Do you agree to the license terms?** enter `y` for Yes.

4. **Do you wish to continue this installation without the required patches?** Enter `y` for Yes to proceed with the installation. If you wish to install the patches, then enter `n` for No. For information on installing patches see "Patch Clusters for Solaris," on page 35.

5. In the Installation Directory window, provide the following information, and then click Next:

   Select which component to install: Enter `2`.

   What directory do you want to install the Directory Server in? Enter the path to the directory where Directory Server will be installed. Do not install Directory Server in the same directory as DSAME Services. Ideally, you would install DSAME Services and Directory Server on different computer systems.

   <Path> does not exist, create? If this prompt displays, DSAME can automatically creates a new for you. Enter `y` for Yes.

   What is the host name of the machine where the Directory Server will run? For example, in the fully qualified domain name `mymachine.organizationname.madisonparc.com`, the host computer system name is `mymachine`.

   What is the sub-domain name ("." for none)? For example, in the name `mycomputer.organizationname.madisonparc.com`, the sub-domain name is `organizationname.` If your host computer does not have a sub-domain, enter a period `(.)`.

   What is the domain name? For example, in the name `mycomputer.organizationname.madisonparc.com`, the domain name is `madisonparc.com`

   What port should the LDAP server use? The following is an excerpt from *iPlanet Directory Server Installation Guide* regarding this topic:

   "Port numbers can be any number from 1 to 65535. Keep the following in mind when choosing a port number for your Directory Server:

   - The standard Directory Server (LDAP) port number is 389.
   - Port 636 is reserved for LDAP over SSL. Therefore, do not use port number 636 for your standard LDAP installation, even if 636 is not already in use. You can also use LDAP over TLS on the standard LDAP port.
   - Make sure the ports you choose are not already in use.
   - If you are using both LDAP and LDAPS communications, make sure the port numbers chosen for these two types of access are not identical."

   Directory Server Administration userid: Administration Server user ID is used only when the Directory Server is down and you are unable to log in as the configuration directory administrator. The existence of this user ID means that you can access Administration Server and perform disaster recovery activities such as starting Directory Server, reading log files, and so forth.

Normally, Administration Server user and password should be identical to the configuration directory administrator ID and password.

Admin password (8 chars minimum): Enter a password for the Directory Server administrator.

Re-enter Admin password: Enter the password again to confirm it.

What is the Directory Server admin port? The default port number is `58900`

System User: This is the user the server runs as. Example: `nobody`

System Group: This is the group to which the user (above) belongs. Example: `nobody`.

What is the root suffix of your directory tree? This is the root suffix of your existing directory tree. Enter a distinguished name (DN) that includes at least one *type*=*value* pair.

Examples:

```
o=isp
```

```
o=madisonparc
```

```
dc=sun,dc=com
```

Do you want to configure this Directory Server for use by DSAME? Enter `y` for yes.

Directory Manager DN: The Directory Server administrative user, or Directory Manager, is the administrator who has unlimited access to Directory Server data and configuration. The default DN for the Directory Manager is cn=Directory Manager. Enter the DN you specified when you first installed Directory Server.

Directory Manager password (8 chars minimum): Enter a password for the Directory Manager. Confirm the password when prompted.

Do you want to start the iPlanet Directory Server Access Management Edition Directory Server when installation is complete? If you enter `y` for Yes, then Directory Server will automatically start up immediately after installation. If you enter `n` for No, then you must restart Directory Server manually after installation.

To restart Directory Server, with root permissions, enter the commands:

```
cd Directory_Server_root/slapd-instance_name
```

```
start-slapd
```

Are all settings correct? Confirm that the settings you've entered are correct. If they are not, choose `n` for No and the installation program will prompt you for the setting information again.

6. Enter `5` to exit the installation program.

Step 1c: Migrate Existing Data to Directory Server 5.1

In this step, you will update your pre-5.1 data to work with Directory Server 5.1. This process, called *migration*, is performed by running the `migrateInstance5` script that comes with Directory Server. The migration script performs the following tasks in sequence:

- Checks the schema configuration files, and notifies you of any changes between the standard configuration files and the ones present on your system.
- Creates a database for each suffix stored in the legacy Directory Server. (In Directory Server 5.0 you can have multiple databases, but just one suffix per database).
- Migrates the server parameters and database parameters. (In Directory Server 5.0, these are stored as LDAP entries in the `dse.ldif` file.)
- Migrates user-defined schema objects.
- Migrates indexes.
- Migrates standard server plug-ins.
- Migrates the certificate database, and SSL parameters.

NOTE Your existing user data must be migrated to Directory Server 5.1 before you go on to Step 2. Otherwise, DSAME may not be able to recognize your existing user data.

You must run the script on the system where your existing Directory Server is installed. You must shut down your directory service before running the migration script. For detailed migration instructions, see the *iPlanet Directory Server Installation Guide* at:
`http://docs.iplanet.com/docs/manuals/directory.html`

Once you've migrated your data to Directory Server 5.1, you can skip to "Step 1e: Back Up Your Existing Data," on page 72.

Step 1d: Install DSAME Schema

NOTE The instructions in this section, Step 1d, assume that you have already deployed and provisioned Directory Server 5.1, but your existing directory tree does not contain DSAME 5.1 schema.

You must have root permissions when you run the DSAME installation program. Be sure all web browsers are closed before starting the installation program.

1. If you're installing DSAME from the product CD, insert the CD into the drive of the system on which you want to install the software.

   If you've downloaded the product, unpack the product binaries file using the following command:

   ```
   gunzip -dc dsame-5.1-domestic-us.sparc-sun-solaris2.8.tar.gz |
   tar -xvof -
   ```

2. Run the `aminstall` program. On the product CD, you'll find the program in the directory `/cdrom/DSAME_51`. If you've downloaded the product binaries, you'll find the program in the directory where you untarred the binary files.

   At the command line, enter `aminstall`.

   The `aminstall` command accepts the `-v [verbose]` option. The verbose option gives brief progress messages as the actions of the install program take place. Otherwise, installation messages are written to log files in the following directory:

   ```
   /var/opt/SUNWam/install
   ```

3. Read the License Agreement. At the prompt, **Do you agree to the license terms?** enter `y` for Yes.

4. When the following message displays, enter `3`.

```
Select which component to install:

1) DSAME Management and Policy Services
2) iPlanet Directory Server 5.1
3) iPlanet Directory Server Configuration for DSAME
4) DSAME Cross Domain Single Sign-On
5) Exit
```

5. Provide the following information when prompted:

   What is the host name of the machine where the iPlanet Directory Server is located? Enter the host name of the computer system where your existing Directory Server is installed.

   What is the sub-domain name ("." for none)? For example, in the name `mycomputer.organizationname.madisonparc.com`, the sub-domain name is `organizationname.` If your host computer does not have a sub-domain, enter a period (`.`).

   What is the domain name? For example, in the name `mycomputer.organizationname.madisonparc.com`, the domain name is `madisonparc.com`

   What port should the LDAP server use? Enter the port number used by the your existing Directory Server.

   What directory is the Directory Server installed in? Enter the full path to the directory where the your existing Directory Server is installed.

   What is the Directory Server Instance? Enter the instance identifier for the existing Directory Server.

   Will you be using an existing DIT and schema? Enter `n` for No.

   Do you want to restart the Directory Server when configuration is complete? Enter `y` for Yes.

   Are all settings correct? Enter `y` for Yes.

6. When the following message is displayed, enter `5` to exit the program.

```
Select which option to install:

1) DSAME Management and Policy Services
2) iPlanet Directory Server 5.1
3) iPlanet Directory Server Configuration for DSAME
4) DSAME Cross Domain Single Sign-On
5) Exit
```

Step 1e: Back Up Your Existing Data

Back up your existing DIT before proceeding further with the other steps. Many of the changes described in this chapter must be done manually and can be error-prone.

For detailed information on backing up your directory, see the *iPlanet Directory Server Installation Guide* at:

`http://docs.iplanet.com/docs/manuals/directory.html`

Step 2: Install DSAME Services

You must have root permissions when you run the DSAME installation program. Be sure all web browsers are closed before starting the installation program.

1. Run the `aminstall` program. On the product CD, you'll find the program in the directory `/cdrom/DSAME_51`. If you've downloaded the product binariers, you'll find the program in the directory where you untarred the binary files.

   At the command line, enter `aminstall`.

   The `aminstall` command accepts the following `-v [verbose]` option. The `verbose` option gives brief progress messages as the actions of the install program take place. Otherwise, installation messages are written to log files in the following directory:

   `/var/opt/SUNWam/install`

2. Read the License Agreement. When prompted, **Do you agree to the license terms?** Enter `y` for Yes.

3. If the following message does not display, then skip to step 4.

```
One or more components that are part of DSAME 5.1 have been
detected on this system.
...
If you are going to install components which already exist, you
must uninstall them first.

What would you like to do?
1) Remove existing components, then continue installation.
2) Continue installation without removing existing components.
3) Exit
```

- If the above message above is displayed, and you want to re-install components listed in the message, then enter `1` to remove the existing components. After uninstallation, the installation program will automatically start again from the beginning.

- If the above message above is displayed, and you want to install components that are not listed in the message, then enter 2 to proceed to the next step.

4. The following options are displayed.

```
Select which option to install:

1) DSAME Management and Policy Services
2) iPlanet Directory Server 5.1
3) iPlanet Directory Server Configuration for DSAME
4) DSAME Cross Domain Single Sign-On
5) Exit
```

When prompted, provide the following information:

Select which component to install: Enter `1`.

Do you want to install the DSAME Management and Policy Services on iPlanet Application Server? By default, DSAME will be installed with its own Web Server which will power the DSAME services and user interface.

- If you want to use the default Web Server that comes with DSAME, enter No, and then skip to Step 5.
- If you want to use Application Server instead of the default Web Server to run DSAME services, *and Application Server is already installed and running*, provide the following information when prompted:

  What directory is the iPlanet Application Server installed in? Enter the full path to the directory where Application Server is installed.

  What is the host name of the machine running the iPlanet Application Server Webserver? This is the computer system where DSAME components and a either dedicated web Server or Application Server are installed together. In the name `mycomputer.organizationname.madisonparc.com`, the host name is `mycomputer`.

  What is the sub-domain name ("." for none)? For example, in the name `mycomputer.organizationname.madisonparc.com`, the sub-domain name is `organizationname.` If your host computer does not have a sub-domain, enter a period (`.`).

What is the domain name? For example, in the name `mycomputer.organizationname.madisonparc.com`, the domain name is `madisonparc.com`

What is the iPlanet Application Server Webserver port? Enter a port number for the Application Server that runs the DSAME services.

Will you be using an existing DIT and schema? Enter `y` for Yes**.**

What is the root suffix of your directory tree? This is the DSAME root suffix, or the point in your directory where you want DSAME to start managing entries. Enter a distinguished name (DN) that includes at least one *type*=*value* pair.

Examples:

`o=isp`

`o=madisonparc`

`dc=sun,dc=com`

NOTE The default organization uses the `organization (o) object class`. If you want to use a different naming attribute such as `dc`, you must follow the installation instructions in Chapter 5, "Using an Existing Directory Server".

What is your organization name? Enter a name for the first organization to be created in your DSAME Directory Information Tree (DIT). This name will be displayed in the DSAME graphical user interface. Examples: `iPlanet` or `iplanet.com`.

If you want the default organization to be the root suffix, enter a period (.).

Is the existing iPlanet Directory Server installed on a local host or on a remote host? Enter `l` for Local if the Directory Server is installed on the same computer system as DSAME (it's "local" relative to DSAME). Enter `r` for Remote if the Directory System is installed on a different computer system, or remote from, the computer that runs DSAME services.

What is the Directory Server Instance? Enter the instance identifier for the existing Directory Server.

What port should the LDAP server use? Enter the port number used by the your existing Directory Server.

Directory Manager DN: The Directory Server administrative user, or Directory Manager, is the administrator who has unlimited access to Directory Server data and configuration. The default DN for the Directory Manager is `cn=Directory Manager`. Enter the DN you specified when you first installed Directory Server.

Directory Manager password (8 chars minimum): Enter a password for the Directory Manager.

Re-enter Directory Manager password: Enter the password again to confirm it.

The Top Level Administrator user id is: This is the Administrator who has unlimited access to all entries managed by DSAME. The Top Level Administrator user id is hardcoded `amAdmin`. This ensures that the DSAME administrator role and its privileges are created and mapped properly in the Directory Server so that you can log into DSAME product immediately after installation.

Admin password (8 chars minimum): Enter a password for the Super Administrator.

Re-enter Admin password: Enter the Super Administrator password again to confirm it.

Do you want to start the iPlanet Directory Server Access Management Edition Server when installation is complete? If you enter `y` for Yes, DSAME will automatically start up immediately after installation. If you enter `n` for No, you must start DSAME manually after installation.

To start DSAME manually, perform the following:

- Start the authentication modules.

  /*DSAME_root*/`SUNWam/bin/amserver start`

- Make sure that DSAME web applications are ready for access:

  /*AppServer_root*/`ias/bin/iascontrol start`

- Refresh the web connector.

  /*AppServer_webconnector_dir*/`servers/start`

5. If you're using Application Server instead of the default Web Server that comes with DSAME, then skip to Step 6.

   If you're using the default Web Server that comes with DSAME, provide the following information when prompted:

   What directory do you want to install the Management and Policy Services in? Enter the path to the directory where DSAME Services will be installed. Plan to install the DSAME Services and Directory Server in different directories. Ideally, you would install DSAME Services and Directory Server on different computer systems.

   Do you want to use the existing JDK? Java support in DSAME requires Java Development Kit (JDK) of version 1.3.1 or higher. While a default JDK is provided, you can use your own JDK with the Web Server. If you want to use your own JDK version, then enter `n` for No and then enter the full path to the version of JDK you want to use. Otherwise, enter `y` for Yes.

   What is the host name of the machine where the DSAME Management and Policy Services will run? This is the computer system where DSAME components and Web Server are installed together. In the name `mycomputer.organizationname.madisonparc.com`, the host name is `mycomputer`.

   What is the sub-domain name ("." for none)? For example, in the name `mycomputer.organizationname.madisonparc.com`, the sub-domain name is `organizationname.` If your host computer does not have a sub-domain, enter a period (`.`).

   What is the domain name? For example, in the name `mycomputer.organizationname.madisonparc.com`, the domain name is `madisonparc.com`

   What is the DSAME Management and Policy Services port? Enter a default port number `58080` for the Web Server that runs the DSAME services.

   Web Server Administration user id: This is the server administrator who has access to the Web Server that runs DSAME services.

   Admin password (8 chars minimum): Enter a password for the Web Server Administrator.

   Re-enter Admin password: Re-enter the Web Server password to confirm it.

   What is the Web Server admin port? Enter the default port number `58888`

System User: This is the user the Directory Server will run as. If you have a Directory Server already running, enter the same System User used by that Directory Server. Example: `nobody`

System Group: This is the group the user (above) belongs to. Example: `nobody`

Will you be using an existing DIT and schema? Enter `y` for Yes**.**

What is the root suffix of your directory tree? This is the DSAME root suffix, or the point in your directory where you want DSAME to start managing entries. Enter a distinguished name (DN) that includes at least one *type=value* pair.

Examples:

`o=isp`

`o=madisonparc`

`dc=sun,dc=com`

If you want the default organization to be the root suffix, enter a period (.).

NOTE The default organization uses the `organization (o) object class`. If you want to use a different naming attribute such as `dc`, you must follow the installation instructions in Chapter 5, "Using an Existing Directory Server".

What is your organization name? Enter organization name with naming attribute prefixed. Example: `o=iplanet.com` or `dc=iplanet.com`.

Is the existing iPlanet Directory Server installed on a local host or on a remote host? Enter `l` for Local if the Directory Server is installed on the same computer system as DSAME (it's "local" relative to DSAME). Enter `r` for Remote if the Directory System is installed on a different computer system, or remote from, the computer that runs DSAME services.

What is the Directory Server Instance? Enter the instance identifier for the existing Directory Server.

What port should the LDAP server use? Enter the port number used by the your existing Directory Server.

Directory Manager DN: The Directory Server administrative user, or Directory Manager, is the administrator who has unlimited access to

Directory Server data and configuration. The default DN for the Directory Manager is `cn=Directory Manager`. Enter the DN you specified when you first installed Directory Server.

Directory Manager password (8 chars minimum): Enter a password for the Directory Manager.

Re-enter Directory Manager password: Enter the password again to confirm it.

What is the deployment URI prefix for the DSAME Management and Policy Services? The Universal Resource Identifier (URI) prefix tells the Web Server where to look for HTML pages associated with a DSAME service and also for other web application specific information like classes and jars. Enter the URI prefix specified during DSAME installation. The default is `/amserver`

What is the deployment URI prefix for the DSAME Administration Console? The Universal Resource Identifier (URI) prefix tells the Web Server or Application Server where to look for HTML pages that the administration console needs to display and also for other web application specific information like classes and jars.

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

The Top-Level Administrator user id is: This is the Administrator who has unlimited access to all entries managed by DSAME. The Top-Level Administrator user id is hardcoded `amAdmin`. This ensures that the DSAME administrator role and its privileges are created and mapped properly in the Directory Server so that you can log into DSAME product immediately after installation. Since this is an administrator role, you can add other users to this role after installation.

Admin password (8 chars minimum): Enter a password for the Super Administrator.

Re-enter Admin password: Enter the Super Administrator password again to confirm it.

Do you want to start the iPlanet Directory Server Access Management Edition Server when installation is complete? If you enter `y` for Yes, DSAME will automatically start up immediately after installation. If you enter `n` for No, you must start DSAME manually after installation.

To start DSAME manually, at the command line enter the following command:

```
/DSAME_root/SUNWam/bin/amserver start
```

6. **Are all settings correct?** If the settings displayed are not correct, enter n for No and the installation program will start again from close to the beginning. If the settings are correct, enter y for Yes to continue with the installation.

   Select which component to install: When you see the following options displayed, enter 5 to exit the installation program.

```
Select which component to install:

1) DSAME Management and Policy Services
2) iPlanet Directory Server 5.1
3) iPlanet Directory Server Configuration for DSAME
4) DSAME Cross Domain Single Sign-On
5) Exit
```

NOTE After installation you will not be able to login to the DSAME administration console because the appropriate LDIF and XML files have not yet been loaded. See the following sections for instructions.

Step 3: (Optional) Add Your Custom Object Classes to DSAME Schema

If your existing DIT contains object classes you've created and that do not come with Directory Server, then you'll have to add those object classes and attributes to the DSAME schema. For background information, see"Understanding DSAME XMLs and DTDs" in the *Programmer's Guide*.

If you do not use custom object classes in your DIT, this step is not necessary. Skip to "Step 5: Load DSAME LDIF into Your Directory," on page 92.

In the examples in this section, the company Madison Park uses two object classes that do not come with the DSAME schema. An auxiliary object class madisonparc-org is in every organization entry, and an auxiliary object class madisonparc-user is in every user entry.

Code Example 5-1 MadisonParc's Customized Schema

```
dn: cn=schema
attributeTypes: ( madisonparc-org-description-oid NAME
  'madisonparc-org-description' DESC 'org description'
  SYNTAX 1.3.6.1.1466.115.121.1.15
```

Code Example 5-1 MadisonParc's Customized Schema *(Continued)*

```
  SINGLE-VALUE X-ORIGIN ‘madisonparc’
attributeTypes: ( madisonparc-org-city-oid NAME
  ‘madisonparc-org-city’ DESC ‘org city location’
  SYNTAX 1.3.6.1.4.1.1666.115.121.1.15
  SINGLE-VALUE X-ORIGIN ‘madisonparc’ )
attributeTypes: ( madisonparc-user-id-oid NAME
  ‘madisonparc-user-id’ DESC ‘user madisonparc id’
  SYNTAX 1.3.6.1.4.1.1666.115.121.1.15
  SINGLE-VALUE X-ORIGIN ‘madisonparc’ )
attributeTypes: ( madisonparc-user-building-oid NAME
  ‘madisonparc-user-building’ DESC ‘priority of a service
  with respect to its siblings’
  SYNTAX 1.3.6.1.4.1.1666.115.121.1.15
  SINGLE-VALUE X-ORIGIN ‘madisonparc’ )
objectClasses: ( madisonparc-org-oid NAME
  ‘madisonparc-org’ DESC ‘custom attributes
  for madisonparc org’ SUP top MAY
  (madisonparc-org-description $ madisonparc-org-city )
  X-ORIGIN ‘madisonparc’ )
objectClasses: ( madisonparc-user-oid NAME
  ‘madisonparc-user’ DESC ‘custom attributes
  for madisonparc user’ SUP top MAY
  ( madisonparc-user-id $ madisonparc-user-building )
  X-ORIGIN ‘madisonparc’ )
```

In order to manage these extensions, changes must be made in the following three files:

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

Step 3a: Add Attributes to the Organization Schema

In this step, you will modify two services files:

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

The DSAME console uses the information in amEntrySpecific.xml for display purposes. Each DSAME abstract entry may have a subschema in this XML file. In the following example, you would add the two attributes from the madisonparc-org object class 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 “Step3b: Add Attributes to the User Schema,” on page 85.) Although any service XML file may describe an attribute that is for a user only, the amentryspecific.xml file can serve as a default place holder for user attributes that are not tied to a particular service.

To Add Attributes from a Custom Organization to the Organization Subschema

NOTE In XML, attribute names must be all lowercase. When DSAME retrieves attributes names from Directory Server, it converts all names to lowercase.

1. In the following file:

   DSAME_root/SUNWam/config/xml/amEntrySpecific.xml

   add the attributes from the custom object class to the subschema Organization. For example, the following two attributes from the custom object class madisonparc-org were added to the file.

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

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

/>
```

2. Also in the `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 DSAME 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"
    i18nKey="o3"
/>
<AttributeSchema name="madisonparc-org-city"
    type="single"
    syntax="string"
    any="required|filter"
    i18nKey="o4"
/>
```

3. In the following file, add the values for i18n Keys you created in Step 2:

DSAME_root`/SUNWam/locale/amEntrySpecific.properties`

Example:

```
iplanet-am-entry-specific-service-description=DSAME 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=Org Description
o4=Organization Location
```

All the attributes listed in the subschema are displayed in the Administration Console when the 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.

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 readonly for regular users. It is displayed as a label for regular users so that it is not editable.For e.g. the display, adminDisplay, and userReadOnly settings are usedwhen displaying the user profilepage 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. 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 example, both attributes will be displayed on the Organization page, and both attributes are required for creation. This is indicated by the use of the `required` value. Only the `madisonparc-org-city` attribute will be used on the Search page in DSAME Administration Console, as indicated by the use of the `filter` value.

```
<AttributeSchema name="madisonparc-org-description"
    type="single"
    syntax="string"
    any="required"
    i18nKey="o3"
/>
<AttributeSchema name="madisonparc-org-city"
    type="single"
    syntax="string"
    any=required|filter
    i18nKey="o4"
/>
```

The "type" attribute

The *type* attribute can use a string, string list, single choice, multiple choice, or boolean value. For example, if the `madisonparc-org-city` attribute can have only one of the cities Concord, San Francisco, or Palo Alto, as a valid value, then you would make this attribute a single choice; each city would be one of the choices. The DSAME Administration Console would display a list containing only these cities. If multiple cities were allowed, the attribute could be a multiple choice.

Step3b: Add 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 DSAME. 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 DSAME 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 84 `and` "The "type" attribute," on page 85). 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 DSAME 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 background information, see"Understanding DSAME XMLs and DTDs" in the *Programmer's Guide.*

For example, you could make the `madison-user-building` attribute Dynamic, and have DSAME create a role with this attribute. This way if all employees in a division moved to a different building, you would only have to modify the role attribute instead having to modify of every single user entry.

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:

   DSAME_root/`SUNWam/config/xml/amUser.xml`

2. For example, the following two attributes from the custom object class `madisonparc-user` were added to the file:

```
<AttributeSchema name="madisonparc-user_id"
    type=single
    syntax=string
    any=required|display
    i18nKey=u13
/>
<AttributeSchema name="madisonparc-user-building"
    type=single
    syntax=string
    any=required|filter|display
    i18nKey=u14
```

3. In the `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 DSAME Administration Console will use this key to look up the display name for the attribute. See the example above.

4. Add values for the i18n Keys created in the previous step to the following file: *DSAME_root*/`SUNWam/locale/amUser.properties`

Example:

```
iplanet-am-user-service-description=DSAME User
iwtUser-desc=Default User Profile
u1=User Name
u2=First Name
u3=Last Name
u4=Full Name
u5=Password
u6=Email Address
u7=Employee Number
u8=Telephone Number
u9=Manager
u10=Home Address
u11=User Status
u12=User Auth Modules
u13=User Id
u14=Employee Building
```

The value is the exact field to be displayed on the administration console page; the key will be localized for the locale. In this example, the administration console will display the text fields "User Id" and "Employee Building."

Step 3c: Modify the Creation Templates

In this step, you will modify the `ums.xml` file.

In Figure 5-3 on page 98, the sample DIT has new object classes for both users and organizations. To expose the new object classes in the UI, you would modify the Creation Templates for both users and organizations in the `ums.xml` file. The Creation Templates configure DSAME to add or allow specific object classes and attributes when these entries are created.

To Modify the Creation Templates

Make the following modifications in the file *DSAME_root*/`SUNWam/config/ums/ums.xml`

1. Under `<SubConfiguration name="BasicOrganization" id="CreationUmsObjects">`, in the `<AttributeValuePair> <Attribute name="required" />` element, add the following:

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

   Example:

```
<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=organization</Value>
                        <Value>objectClass=nsManagedDomain</Value>
                        <Value>objectClass=inetDomain</Value>
                        <Value>objectClass=iplanet-am-managed-org</Value>
                        <Value>objectClass=madisonparc-org</Value>
                        <Value>o</Value>
                        <Value>inetdomainstatus=Active</Value>
                     </AttributeValuePair>
```

2. Under `<SubConfiguration name="BasicUser" id="CreationUmsObjects">`, in the `<AttributeValuePair><Attribute name="optional" />` element, add the following:

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

   Example: *(Continued)*

```
<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=iplanet-am-managed-person</Value>
             <Value>objectClass=madisonparc-user</Value>
             <Value>cn=default</Value>
             <Value>sn=default</Value>
             <Value>uid</Value>
             <Value>inetuserstatus=Active</Value>
        </AttributeValuePair>
```

3. Under `<SubConfiguration name="BasicOrganization" id="CreationUmsObjects">`, in the `<AttributeValuePair> <Attribute name="optional" />` element, add the following:.

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

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

Example:

```
<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=organization</Value>
                <Value>objectClass=nsManagedDomain</Value>
                <Value>objectClass=inetDomain</Value>
                <Value>objectClass=iplanet-am-managed-org</Value>
                <Value>objectClass=madisonparc-org</Value>
                <Value>o</Value>
                <Value>inetdomainstatus=Active</Value>
           </AttributeValuePair>
           <AttributeValuePair> <Attribute name="namingattribute" />
                <Value>o</Value>
           </AttributeValuePair>
           <AttributeValuePair> <Attribute name="optional" />
                <Value>*</Value>
                <Value>madisonparc-org-description</Value>
                <Value>madisonparc-org-city</Value>
           </AttributeValuePair>
```

4. Under `<SubConfiguration name="BasicUser" id="CreationUmsObjects">`, in the `<AttributeValuePair> <Attribute name="optional" />` element, add the following:

   `<Value>madisonparc-user-id</Value>`

   `<Value>madisonparc-user-building</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=iplanet-am-managed-person</Value>
                         <Value>objectClass=madisonparc-user</Value>
                         <Value>cn=default</Value>
                         <Value>sn=default</Value>
                         <Value>uid</Value>
                         <Value>inetuserstatus=Active</Value>
                      </AttributeValuePair>
                      <AttributeValuePair> <Attribute name="optional" />
                         <Value>nsroledn</Value>
                         <Value>madisonparc-user-id</Value>
                         <Value>madisonparc-user-building</Value>
                         <Value>*</Value>
```

Step 4: (Optional) Configure Alternative Naming Attributes

If you used a naming attribute other than `o=`*organization* to define organizations in your DIT, you must modify the `ums.xml` file to accommodate the non-standard naming attributes. If you used a naming attribute other than `uid=`*username* to define users in your DIT, your must make similar modifications in the `ums.xml` file. For detailed reference information, see "Using Alternative Naming Attributes," on page 218.

To Configure Alternative Naming Attributes for Organizations

The following steps assume that dc is the naming attribute used for an organization. Perform the modifications in the file:

DSAME_root/SUNWam/config/ums/ums.xml

1. Replace any appearance of o=org with dc=org.
2. In the BasicOrganization section, replace value of o with dc.
3. In the BasicOrganizationSearch SubConfiguration section, replace value of o with dc.
4. In the BasicOrganization section, change the objectClass of organization to domain. If you use ou for an organization, then you need to change it to organizationalUnit.

To Configure Alternative Naming Attributes for Users

The following steps assume that cn is the naming attribute used for users.

Make the following modifications in the following directories:

DSAME_root/SUNWam/config/ums

DSAME_root/SUNWam/config/xml

1. In the file ldif/installExisting.ldif, *with two exceptions*, replace uid with cn. The exceptions are:
   - The occurrence under ACI.
   - The uid: amAdmin attribute in the amAdmin entry.
2. In xml/amAuth.xml, replace uid with cn for user naming attribute.
3. In xml/amMembership.xml, replace uid with cn for the user naming attribute.
4. In xml/amAuthLDAP.xml, replace uid with cn for the user naming attribute.
5. In AMConfig.properties, replace uid=amAdmin with cn=amAdmin.
6. In ums/ums.xml, in BasicUser subconfiguration, replace uid with cn for namingattribute.

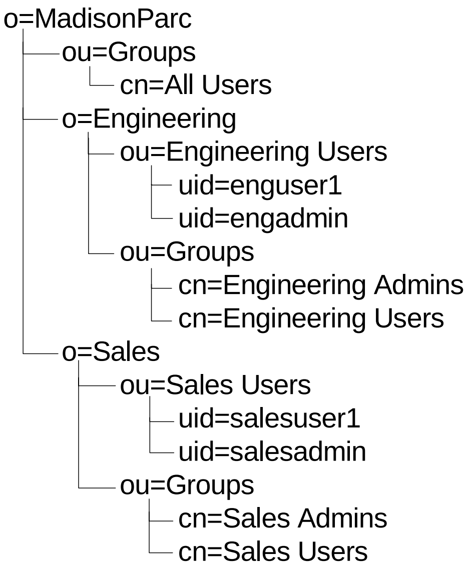
7. In `ums/ums.xml,` in `BasicUser` required values, change `cn=default` to `cn` and `uid` to `uid=default`.

Step 5: Load DSAME LDIF into Your Directory

The `installExisting.ldif` file contains DSAME-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 DSAME are added to `o=madisonparc` and `o=Engineering,o=madisonparc`
- Default roles for organization and help desk administrators are created.
- Default Access Control Instructions (ACIs) for those administrator entries are set up.



Before You Begin

1. Make sure that you're using the appropriate version of `ldapmodify`. Follow these procedures:

   - Make sure that your path is set to use the `ldapmodify` command that is shipped with iPlanet Directory Server 5.1. (Do not use the version shipped with Solaris, which is found in `/bin` or `/usr/bin`.)

   - You will also need to add `/usr/iplanet/servers/lib` to your `LD_LIBRARY_PATH` to pick up Directory Server libraries. At the command line, enter:

     ```
     which ldapmodify
     ```

     Directory_Server_root/`shared/bin/ldapmodify` will be displayed.

2. DSAME provides two different LDIF files to help you make the necessary modifications. Determine which file and instructions you should use.

   - If the DSAME default organization is at any level below the root suffix of your directory tree, then use the instructions in the section "To Load the installExisting.ldif File."

   - If your root suffix is entered as period (.) for the DSAME default organization, then use the instructions in the section "To Load the installrootorg.ldif File."

To Load the installExisting.ldif File

1. Go to the following directory:

   `cd` *DSAME_root*`/SUNWam/web-apps/services/WEB-INF/config/ldif`

   If DSAME is installed on iPlanet Application Server, then go to:

   `cd` *DSAME_root*`/ias/APPS/modules/amserver/WEB-INF/config/ldif`

2. At the command line, enter the following:

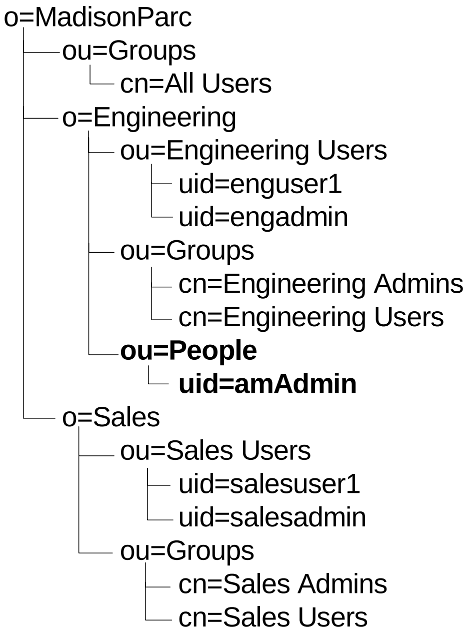
```
ldapmodify -v -c -D "cn=Directory manager" -w password -a -f
installExisting.ldif
```

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

If you encounter error messages regarding "already existing" entries or values for the default organization, see "Step 7: (Optional) Add DSAME ACIs to Your Default Organization," on page 96.

The DSAME administration user `amAdmin` will be created under the `ou=People,o=Engineering,o=madisonparc` people container. This is the top level administrator for DSAME. This administrator has read and write access to the entire subtree for `o=madisonparc`. You can add one of your users to this top level administrator role after the DSAME console is started.

Figure 5-2 Directory Information Tree (DIT) Used in Examples in This Chapter.



To Load the installrootorg.ldif File

1. Go to the following directory:

   cd *DSAME_root*/SUNWam/web-apps/services/WEB-INF/config/ldif

   If DSAME is installed on iPlanet Application Server, then go to:

   cd *DSAME_root*/ias/APPS/modules/amserver/WEB-INF/config/ldif

2. At the command line, enter the following:

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

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

Step 6: Load DSAME Service Attributes into Your Directory

You can load the `ums.xml` file and all services files with the same command.

1. Go to the following directory:

   cd *DSAME_root*/SUNWam/config/ums

2. Run the following command:

   amserveradmin *amAdmin_DN 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` and `amEntrySpecific.xml` files, 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:

DSAME_root/SUNWam/config/xml

Step 7: (Optional) Add DSAME ACIs to Your Default Organization

You only need to perform this step if, during installation, you specified an existing organization as your default organization. (By default, DSAME creates one new organization with the an RDN `o=iplanet`. If you accepted the default RDN, skip to the Step 8: Start DSAME.

In this step, you will manually add the DSAME default ACIs to the organization you specified as the default, or first, organization.

1. Copy the DSAME default organization ACIs a text file.
   - If you loaded the file `installExisting.ldif`, then copy the ACI's from the following file:

     DSAME_root`/web-apps/services/WEB-INF/config/ldif`

   - If you loaded the file `installrootorg.ldif`, then copy the ACI's from the following file:

     DSAME_root`/web-apps/services/WEB-INF/config/ldif`

   - If you loaded the file `installrootorg.ldif` on Application Server, then copy the ACI's from the following file:

     DSAME_root`/ias/APPS/modules/amserver/WEB-INF/config/ldif`

2. In the directory where your `ldapmodify` utility is located, enter the following command:

   `ldapmodify -D` *bind_DN* `-w` *password* `-p` *port_number* `-h` *hostname* `-a -f` *textfile_name*

Step 8: Start DSAME

At this point, you can start the DSAME server and you will be able to log in to the DSAME Administration Console as `amAdmin` user. You should see the root suffix and organization you specified during installation. In the MadisonParc example, you would see `o=madisonparc` and `o=Engineering`. You will not be able to see the rest of your entries since they do not yet contain the DSAME marker object classes.

To start DSAME

To start DSAME manually, at the command line enter the following command:

```
/DSAME_root/SUNWam/bin/amserver start
```

To log into the Administration Console

1. Go to the appropriate URL:

   - If DSAME services are running on iPlanet Web Server, go to the login URL using the form:

     `http://`*host*`.`*domain*`:`*port*`/amconsole`

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

     Example: `http://tintin.india.sun.com:58080/amconsole`

   - If DSAME services are running on iPlanet Application Server, go to the login URL using the form:

     `http://`*iaswebconnector_host*`:`*iaswebconnector_port*`/NASApp/amserver`

     where *host* is the host name of the web connector, *port* is the web connector port number, and `NASApp` is the Universal Resource Identifier (URI) prefix automatically assigned to Application Server.

2. In the Login page, enter the Top-Level Administrator user id and password you specified at installation.

Step 9: Add DSAME Object Classes and Attributes to Existing Directory Entries

In this step, you modify your existing directory entries to include the necessary DSAME object classes and attributes. You can think of the DSAME object classes as *markers* that indicate the directory entries you want to manage through DSAME. These markers enable DSAME to recognize the entries in your directory. The object classes contain special attributes that are necessary to achieve delegated administration.

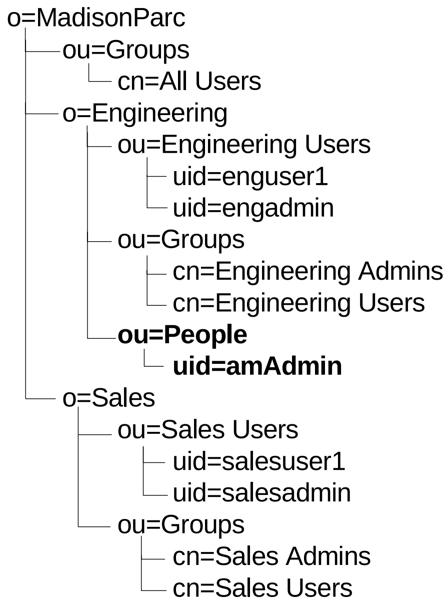
Before You Begin

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 MadisonParc DIT. Figure 5-3 shows two organizations, `Engineering` and `Sales`, under the root. All groups in this example are static groups.

Figure 5-3 The MadisonParc DIT.



Utilities and Scripts You Can Use

You can make these modifications by using iPlanet Directory Server Console, or by using the `ldapmodify or db2ldif` utilities that come with Directory Server. For detailed information on how to make directory changes by using the Console or by using these utilities, see the documentation for iPlanet Directory Server at:

```
http://docs.iplanet.com/docs/manuals/directory.html
```

You can also use the sample scripts that are included in this product. The sample scripts require Perl 5.x or later. You'll find the sample scripts in the following location:

DSAME_root`/SUNWam/migration`

While these samples should prove useful, they are only tools to assist you in properly formatting the DIT and other data. Each script has one or more variables at the top of the file that must be edited before the script is executed. After each script is executed, it generates an LDAP Data Interchange Format (LDIF) file.

If you encounter error messages regarding "already existing" entries or values, you must add the object classes or attributes manually. See the iPlanet Directory Server documentation for detailed instructions.

Steps for using each sample script are included in this chapter in the instructions for marking each object class.

NOTE Before you can follow the steps for using the sample scripts, you must copy the following sample script files from *DSAME_root*/`SUNWam/migration` into the directory *Directory_Server_root*/`shared/bin`:

- `update-users.pl`
- `update-static-groups.pl`
- `update-assignable-dynamic-groups.pl`
- `update-filtered-groups.pl`
- `update-people.pl`
- `update-ou.pl`
- `update-o.pl`
- `update-groups.pl`

Also note that the changes made by using these scripts cannot be automatically undone. Be sure to back up your data before running each script.

Related Information

Detailed reference information is provided in Appendix A, “DSAME ObjectClasses and Attributes." See information on the following topics:

- Using DSAME Object Classes as Markers
- Using Alternative Naming Attributes
- DITs That Cannot Be Managed by DSAME
- Object Class and Attribute Descriptions

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 DSAME 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 DSAME to make sure those modifications were done correctly. This second approach is the recommended approach. For example, you may want to add the DSAME object classes for each of your organizations, restart DSAME, and verify that your organizations appear in the DSAME Administration Console. Then add marker classes for groups, check them and so forth.

Step 9a: Mark 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 Step 10b.

In this step you will:

1. Add the following object classes to each organization entry:
   - `iplanet-am-managed-org`
   - `inetDomain`
2. Add the following attribute to each organization entry:
   - `inetDomainStatus`

In the MadisonParc example, these object classes and attributes were automatically added to the default organization, `o=Engineering`, which was the organization specified and created during DSAME installation. The object classes and attributes were manually added to the `o=Sales` organization.

Example:

```
dn: o=Engineering,o=madisonparc
objectClass: top
objectClass: organization
objectClass: madisonparc-org
madisonparc-org-description: Engineering Organization
madisonparc-org-city: Santa Clara
aci: (targetattr = "*")(version 3.0; acl "madisonparc Org admin";
allow (all)groupdn="ldap:///cn=Engineering
Admins,o=Engineering,o=madisonparc";)
objectclass: iplanet-am-managed-org
objectlcass: inetDomain
inetDomainStatus: Active

dn: o=Sales,o=madisonparc
objectClass: top
objectClass: organization
objectClass: madisonparc-org
madisonparc-org-description: Sales Organization
madisonparc-org-city: Menlo Park
aci: (targetattr = "*")(version 3.0; acl "madisonparc Org admin";
allow (all)groupdn="ldap:///cn=Sales
Admins,o=Sales,o=madisonparc";)
objectclass: iplanet-am-managed-org
objectlcass: inetDomain
inetDomainStatus: Active
```

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 DSAME. Example: `o=madisonparc`

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. To check the results, open the `ldif` file that is created (for example: `o-update.ldif`) and verify that the appropriate changes were made.

Step 9b: Mark People Containers

To each people container, add the `iplanet-am-managed-people-container` object class.

Example:

```
dn: ou=Engineering Users,o=Engineering,o=madisonparc
objectClass: top
objectClass: organizationalunit
objectclass: iplanet-am-managed-people-container

...

dn: ou=Sales Users,o=Sales,o=madisonparc
objectClass: top
objectClass: organizationalunit
objectclass: iplanet-am-managed-people-container

...
```

To Mark People Containers Using the Sample Script

1. Copy `update-people.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 DSAME. Example:
   `o=madisonparc`.

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. To check the results, open the LDIF file that is created (for example: `people-update.ldif`) and verify that the appropriate changes were made.

Step 9c: Mark Organizational Units

To each container that is an organizational unit, add the following object class: `iplanet-am-managed-org-unit`

`Example:`

```
dn: ou=Groups,o=Engineering, o=madisonparc
objectClass: top
objectClass: organizationalunit
objectClass: inetAdmin
objectclass: iplanet-am-managed-org-unit

dn: cn=Engineering Admins,o=Engineering,o=madisonparc
objectClass: top
objectClass: groupofuniquenames
uniquemember: uid=engadmin,ou=Engineering
Users,o=Engineering,o=madisonparc

dn: cn=Engineering Users,o=Engineering,o=madisonparc
objectClass: top
objectClass: groupofuniquenames
uniquemember: uid=enguser1,ou=Engineering
Users,o=eng,o=madisonparc
uniquemember: uid=enguser2,ou=Engineering
Users,o=eng,o=madisonparc
```

```
dn: ou=Groups,o=Engineering, o=madisonparc
uniquemember: uid=enguser3,ou=Engineering
Users,o=eng,o=madisonparc
uniquemember: uid=enguser4,ou=Engineering
Users,o=eng,o=madisonparc

dn: ou=Groups,o=Sales, o=madisonparc
objectClass: top
objectClass: organizationalunit
objectClass: inetAdmin
objectclass: 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 DSAME. Example: `o=madisonparc`.

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. To check the results, open the LDIF file that is created (for example: `ou-update.ldif`) and verify that the appropriate changes were made.

Step 9d: Mark Users

To each user entry, add the following object classes:

- `iplanet-am-web-agent-service`

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

Example:

```
dn: ou=Engineering Users,o=Engineering,o=madisonparc
objectClass: top
objectClass: organizationalunit

dn: uid=engadmin,ou=Engineering Users,o=Engineering,o=madisonparc
objectClass: inetorgperson
objectClass: organizationalperson
objectClass: person
objectClass: top
objectClass: iplanet-am-web-agent-service
objectClass: iplanet-am-managed-person
objectClass: iplanet-am-user-service
objectClass: inetuser
objectClass: iPlanetPreferences
objectClass: inetOrgPerson
inetuserstatus:active
cn: engadmin
sn: engadmin
userPassword: engadmin

dn: uid=enguser1,ou=Engineering Users,o=Engineering,o=madisonparc
objectClass: inetorgperson
objectClass: organizationalperson
objectClass: person
objectClass: top
objectClass: madisonparc-user
objectClass: iplanet-am-web-agent-service
objectClass: iplanet-am-managed-person
objectClass: iplanet-am-user-service
objectClass: inetuser
objectClass: iPlanetPreferences
objectClass: inetOrgPerson
inetuserstatus:active
madisonparc-user-id: 11111
madisonparc-user-building: SCA16
cn: enguser1
sn: enguser1
userPassword: enguser1
```

To Mark Users Using the Sample Script

1. Copy `udpate-users.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 DSAME. Example: `o=madisonparc`

3. Set the `$base-component` variable to the base suffix of the DIT. Example: `madisonparc`

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

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

5. 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`

6. To check the results, open the LDIF file that is created (for example: `users-update.ldif`) and verify that the appropriate changes were made.

Step 9e: Mark Static Groups

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

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

Example:

```
dn: cn=Engineering Users,o=Engineering,o=madisonparc
objectClass: top
objectClass: groupofuniquenames
objecClass: iplanet-am-managed-static-group
objecClass: ipanet-am-managed-group
uniquemember: uid=enguser1,ou=Engineering
Users,o=eng,o=madisonparc
```

```
dn: cn=Engineering Users,o=Engineering,o=madisonparc
uniquemember: uid=enguser2,ou=Engineering
Users,o=eng,o=madisonparc
uniquemember: uid=enguser3,ou=Engineering
Users,o=eng,o=madisonparc
uniquemember: uid=enguser4,ou=Engineering
Users,o=eng,o=madisonparc

dn: ou=Groups,o=Sales, o=madisonparc
objectClass: top
objectClass: organizationalunit

dn: cn=Sales Admins,o=Sales,o=madisonparc
objectClass: top
objectClass: groupofuniquenames
objecClass: iplanet-am-managed-static-group
objecClass: ipanet-am-managed-group
uniquemember: uid=salesadmin,ou=Sales Users,o=Sales,o=madisonparc

dn: cn=Sales Users,o=Sales,o=madisonparc
objectClass: top
objectClass: groupofuniquenames
objecClass: iplanet-am-managed-static-group
objecClass: ipanet-am-managed-group
uniquemember: uid=salesuser1,ou=Sales Users,o=sales,o=madisonparc
uniquemember: uid=salesuser2,ou=Sales Users,o=sales,o=madisonparc
uniquemember: uid=salesuser3,ou=Sales Users,o=sales,o=madisonparc
uniquemember: uid=salesuser4,ou=Sales Users,o=sales,o=madisonparc
```

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 DSAME. Example: `o=madisonparc`.

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. To check the results, open the LDIF file that is created (for example: `static-groups-update.ldif`) and verify that the appropriate changes were made.

Step 9f: Mark Filtered (Dynamic) Groups

In *filtered groups,* users are included in a single group based on their DN.

Add the following object classes (no attribute) to each filtered group:

- `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 DITto be managed by DSAME. Example: `o=madisonparc`

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. To check the results, open the LDIF file that is created (for example: `update-filtered-groups-update.ldif`) and verify that the appropriate changes were made.

Step 9g: Mark Assignable Dynamic Groups

An *assignable dynamic group* is similar to a filtered group, but uses a DN in the user entry to point to the group.

Add the following object classes to each assignable dynamic group:

- `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 DITto be managed by DSAME. Example: `o=madisonparc`

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 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. To check the results, open the LDIF file that is created (for example: `assignable-dynamic-groups-update.ldif`) and verify that the appropriate changes were made.

Step 9h: Mark Group Containers

Group containers are organizational units (ou) that contain groups. To each group container, 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. Set the `$base` variable to the base suffix of the DITto be managed by DSAME. Example: `o=madisonparc`.

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. To check the results, open the LDIF file that is created (for example: `groups-update.ldif`) and verify that the appropriate changes were made.

Step 10: Load the Modified LDIF Files

After you run the scripts in the previous steps, the various LDIF files are created in the same directory where the Perl scripts are run. Until now, no changes have actually been made in the directory. Before loading the modified files into the directory, it is a good practice to inspect the files to make sure that all DSAME object classes and attributes have been properly added to the existing directory entries. Once you're satisfied that the appropriate changes have been made, load each file using the following `ldapmodify` command:

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

Results of DSAME and Directory Modifications

After making the modifications in the previous steps, all entries in the DIT will be manageable by DSAME. The existing ACIs for the organization administrators do not have to be modified. Even though DSAME 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 DSAME organization administrator roles and assign them to your existing `organizationList` administrators.

Chapter 6

Basic Configurations

This chapter describes configurations typically implemented when you initially deploy iPlanet Directory Server Access Management Edition (DSAME).

Topics in this chapter include:

- Installing the Cross-Domain Single Sign-On Component
- Installing Multiple DSAME Instances Against the Same Directory Server
- Support for Directory Replication and High Availability
- Secure Sockets Layer (SSL)

Installing the Cross-Domain Single Sign-On Component

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. Two major components are added to DSAME 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 DSAME services. The default URL for the controller is `http://`*DSAME_host*`:`*DSAME_port*`/`*URI*`/cdcservlet`
- **Cross-Domain Single Sign-On (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.

Installation Overview

To enable cross-domain single sign-on, you must follow this sequence:

1. Install DSAME Services.

   Follow the instructions in Chapter 4, “Simple Installations With No Existing Directory Server” or in Chapter 5, “Using an Existing Directory Server” as appropriate for your needs.

2. Install the CDSSO component on all participating DNS domains.

   DSAME Services and a remote Web Server must already be installed and running. See “To Install the CDSSO Component” in this chapter”.

3. Configure the CDSSO component installed on each participating DNS domain.

   See “To Configure the CDSSO Component,” on page 115.

4. (Optional) Configure DSAME web agents to work with the CDSSO component.

   See “To Configure DSAME Web Agents to Work With the CDSSO Component”.

To Install the CDSSO Component

DSAME Services and a remote Web Server must already be installed and running. You must have root permissions when you run the DSAME installation program. Be sure all web browsers are closed before starting the installation program.

1. Run the `aminstall` program. On the product CD, you’ll find the program in the directory `/cdrom/DSAME_51`. If you’ve downloaded the product binaries, you’ll find the program in the directory where you untarred the binary files.

   At the command line, enter `aminstall`

   The `aminstall` command accepts the `-v [verbose]` option. The verbose option gives brief progress messages as the actions of the install program take place. Otherwise, installation messages are written to log files in the following directory:

   ```
   /var/opt/SUNWam/install
   ```

2. Read the License Agreement. When prompted, **Do you agree to the license terms?** Enter `y` for Yes.

3. When the following message displays, enter 4.

```
Select which component to install:

1) DSAME Management and Policy Services
2) iPlanet Directory Server 5.1
3) iPlanet Directory Server Configuration for DSAME
4) DSAME Cross Domain Single Sign-On
5) Exit
```

4. Provide the following information when prompted:

   DSAME Policy and Management Services have been detected on this host. Do you want to install the Cross-domain SSO as part of these Services? Enter `y` for Yes to install the CDSSO as part of the DSAME Services.

   What is the deployment URI prefix for the DSAME Cross Domain SSO? Enter a URI prefix that indicates where HTML pages associated with the CDSSO component will be located and also where to look for other web application specific information like classes and jars. The default is `/amcdsso`.

   Are all settings correct? Enter `y` for Yes.

5. When the following message displays, enter `5` to exit the installation program:

```
Select which component to install:

1) DSAME Management and Policy Services
2) iPlanet Directory Server 5.1
3) iPlanet Directory Server Configuration for DSAME
4) DSAME Cross Domain Single Sign-On
5) Exit
```

To Configure the CDSSO Component

1. Edit `AMConfig.properties` file of the installed CDSSO component, which is found in the *DSAME_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 DSAME services. For example:

```
com.iplanet.services.cdsso.CDCURL =
http(s)://DSAME_host:DSAME_port/services/cdcservlet
```

2. Edit `CDSSO.properties` file of the installed CDSSO component, which is found in the *DSAME_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 DSAME Web Agents to Work With the CDSSO Component

You can configure DSAME 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 `AMConfig.properties` file. Change the `com.iplanet.am.policy.agents.url.authLoginUrl` property to point to the agent’s domain’s cross-domain single sign-on service URL. For example:

   ```
   com.iplanet.am.policy.agents.url.authLoginUrl =
   http://CDSSO_host:CDSSO_port/CDSSO_URI/cdsso
   ```

   where `authLoginUrl` is the CDSSO component’s URL.

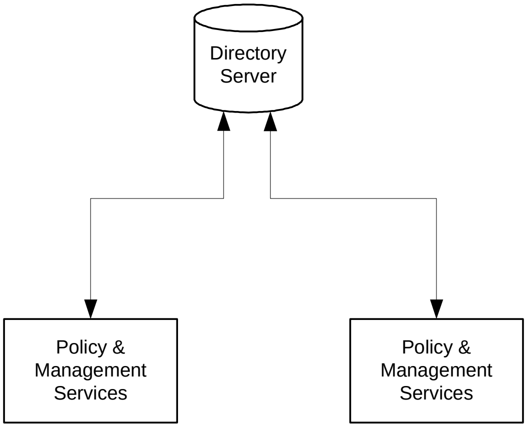
2. Add the cross-domain single sign-on service URL to the agent’s not-enforced list.

Installing Multiple DSAME Instances Against the Same Directory Server

You can install more than one instance of DSAME against this Directory Server for enhanced performance, to support directory replication, or for agent failover purposes. When you run the DSAME installation program for the first time, you'll typically use Option 1) Install DSAME 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 DSAME against this same master directory, you must run `ammultiserverinstall` script.

Figure 6-1 illustrates two DSAME instances installed against a single Directory Server.

Figure 6-1 Two DSAME Instances Installed Against a Single Directory Server.



To Install Multiple DSAME Instances Against the Same Directory Server

You must have root permissions to create and install multiple DSAME instances.

1. Go to the following directory:

`cd` *DSAME_root*`/SUNWam/bin`

2. At the command line, enter the following command:

   ```
   ./ammultiserverinstall instance_name port_number
   ```

   where *instance_name* is the new DSAME instance you want to create and *port_number* is the port number of the new DSAME instance.

   When a new instance is installed the following files and directory are created:

   - A new `amserver` script file at:

     /*DSAME_root*/`SUNWam/bin/amserver.`*instance_name*

   - A new `AMConfig.properties` file at:

     /*DSAME_root*/`SUNWam/lib/AMConfig-`*instance_name*`.properties`

   - A new web server instance directory at:

     /*DSAME_root*/`SUNWam/servers/https-`*instance_name*

Starting DSAME Instance

- To start a single DSAME instance enter the following command:

  ```
  ./amserver.instance_name start
  ```

- To start all the DSAME instances, enter the following command:

  ```
  ./amserver startall
  ```

Stopping DSAME Instance

- To stop a single DSAME instance, enter the following command:

  ```
  ./amserver.instance_name stop
  ```

- To stop all the DSAME instances, enter the following command:

  ```
  ./amserver stopall
  ```

Deleting DSAME Instance

- To delete a DSAME instance, enter 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 DSAME deployment to increase the availability and performance of the DSAME servers and services. You can set up DSAME directory servers in single-supplier or multi-supplier configurations. You can also configure load-balancing applications such as iPlanet Directory Access Router to work with DSAME.

Replication Considerations

Configure your directory servers for replication before you install DSAME. 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 DSAME database.

When you install DSAME for replication purposes, in each instance of Directory Server and in each instance of DSAME, 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 DSAME deployment. For example, authentication server host names or IP addresses must be the same. This precludes using geographically separated replicated DSAME 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 iPlanet Directory Server. You can access these guides on the Internet at:

`http://docs.iplanet.com/docs/manuals/directory.html`

Configuring DSAME to Support Directory Replication

You can configure DSAME 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 DSAME to Work With Directory Replication,” on page 122 of this manual.

Figure 6-2 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 6-2 Single-Supplier Replication.

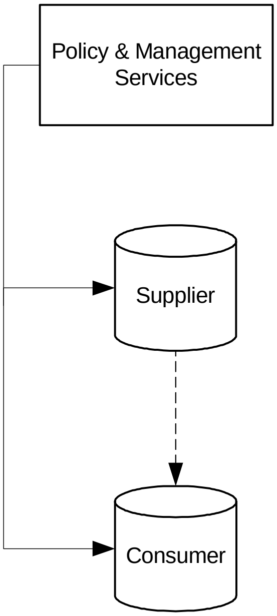


Figure 6-3 illustrates a multi-supplier configuration using multiple instances of DSAME. This configuration provides failover protection as well as high availability, resulting in further enhanced server performance.

Figure 6-3 Multi-Supplier Configuration. Also known as Multi-Master Replication (MMR)

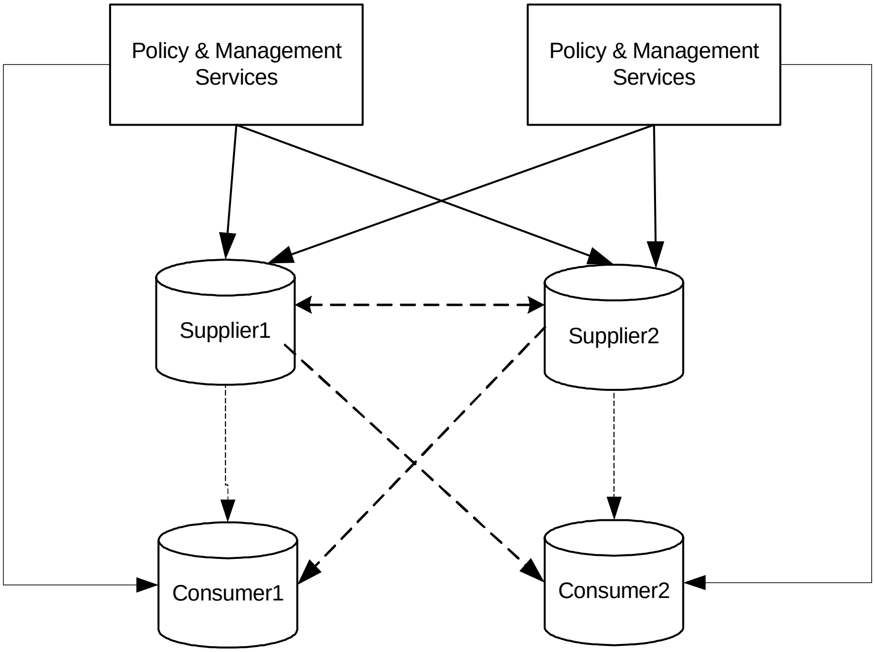
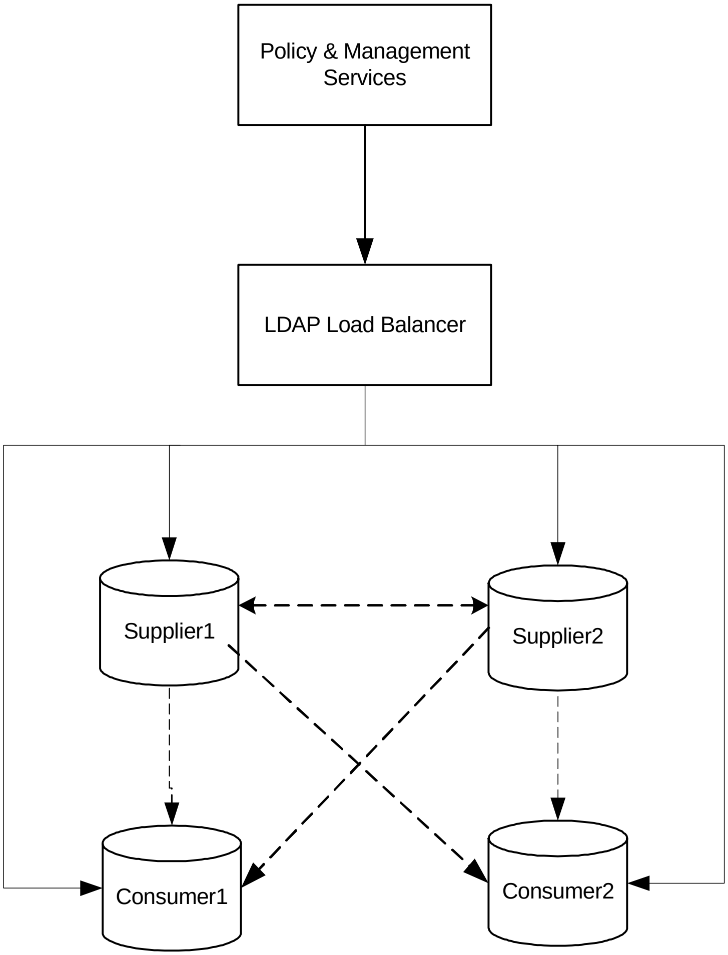


Figure 6-4 illustrates a multi-supplier configuration that includes iPlanet Access Router. This configuration takes full advantage of DSAME support for failover, high availability, and managed load-balancing.

Figure 6-4 Multi-Supplier Replication With Load-Balancer.



To Configure DSAME to Work With Directory Replication

Use the following steps to configure replication at the root or top level of the DSAME directory tree. 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 DSAME 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, "Using an Existing Directory Server" of this manual. Then skip to Step 5.

4. If you are deploying DSAME and Directory Server for the first time, or if you simply do not plan to use existing user data with DSAME, then run the DSAME installation program to install the DSAME 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 "Step 2: Install DSAME Services," on page 73 in Chapter 5.

5. In the server where DSAME Management and Policy services are installed, modify the following file:

   DSAME_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:

      - `replica.enabled=true`
      - `com.iplanet.am.replica.retries`

        Specify the number of times DSAME 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 DSAME should allow to elapse between retries.

6. In each DSAME 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 DSAME 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**, enter 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**, enter 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: *DSAME_root*`/SUNWam/config/ums/serverconfig.xml`, specify the host name and port number of the consumer directory you installed in step1. Example:

```
<iPlanetDataAccessLayer>
     <ServerGroup name="default" minConnPool="1"
            maxConnPool="10">
                 <Server name="Server1"
                     host="consumer1.madisonparc.com" port="389"
                        type="SIMPLE" />
```

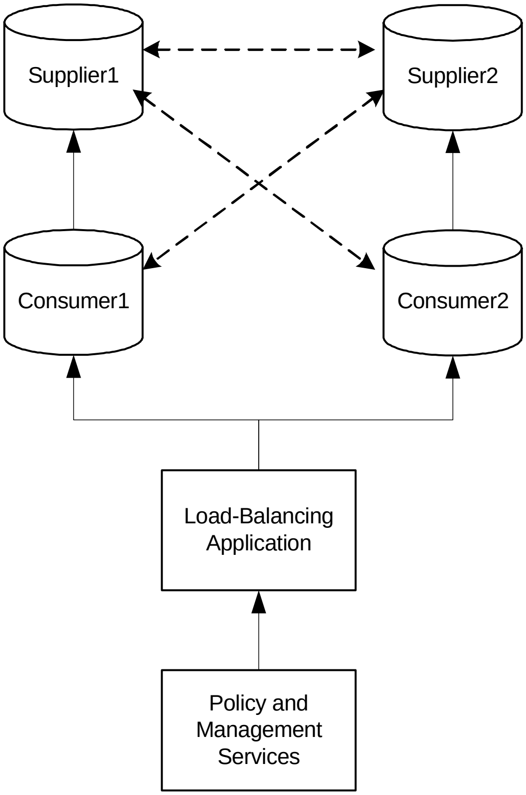
8. Restart DSAME with the following command:

```
/etc/init.d/amserver start
```

Configuring a LDAP Load-Balancers to Work With DSAME

You can configure LDAP load-balancers such as iPlanet Directory Access Router to work with DSAME. iPlanet 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 6-5 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 DSAME. For example, when you configure iPlanet Directory Access Router, you can specify what percentage of the load gets redistributed to each of your servers when one server becomes unavailable. iPlanet Directory Access Router continues to manage request traffic, and begins rejecting client queries when all back-end LDAP servers become unavailable.

By comparison, the DSAME high availability feature cannot be configured or managed as precisely. But when you add a LDAP load-balancers such as iPlanet Directory Access Router, DSAME seamlessly directs all requests to the application for total management.

If you choose to install a load-balancer, you must configure DSAME to recognize the application.

To Configure DSAME 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 *iPlanet 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, *DSAME_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 DSAME 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 DSAME 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**, enter 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 *DSAME_root*/`SUNWam/config/ums/serverconfig.xml,`specify the host name and port number of the consumer directory you installed in step1.

Example:

```
<iPlanetDataAccessLayer>
     <ServerGroup name="default" minConnPool="1"
          maxConnPool="10">
               <Server name="Server1"
                   host="idar.madisonparc.com" port="389"
                      type="SIMPLE" />
```

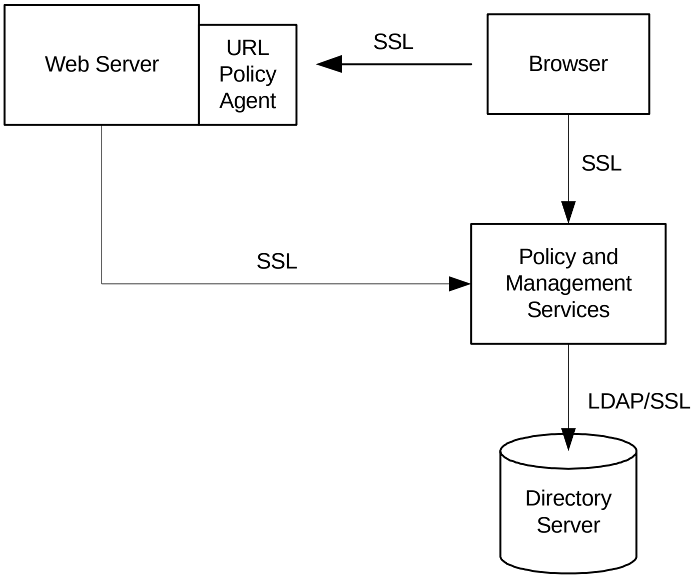
5. Restart DSAME with the following command:

`/etc/init.d/amserver start`

Secure Sockets Layer (SSL)

You can use the Secure Sockets Layer (SSL) protocol to provide secure connections between Directory Server and the DSAME services you use in your enterprise. The SSL protocol consists of rules governing server authentication, client authentication, and encrypted communication between servers and clients. When you enable SSL to work with DSAME, the requests and transactions between Directory Server and the DSAME console are encrypted and protected from intrusion by unauthorized entities.

Figure 6-6 How SSL Works in DSAME.



Enabling SSL for DSAME is a two-step process:

- Step 1: Enable LDAP Over SSL
- Step 2: Enable DSAME to Run in SSL Mode

This section explains how to enable SSL for DSAME services and URL access agents. It references the following resources for SSL information, which are appended to this manual for your convenience:

- *iPlanet Directory Server Administrator's Guide*

  Chapter 11, "Managing SSL"

- *iPlanet Web Server Administrator's Guide*

  Chapter 5, "Securing Your Web Browser Directory"

For comprehensive information on SSL and on determining your SSL needs, see Chapter 7, "Designing a Secure Directory" in *iPlanet Directory Server Deployment Guide*. This guide comes with iPlanet Directory Server, and is also available on the Internet at
`http://docs.iplanet.com/docs/manuals/directory.html`

Step 1: Enable LDAP Over SSL

1. Install a Server Certificate in Directory Server.

   Follow the detailed instructions in “Obtaining and Installing Server Certificates,” on page 277 of this manual to perform the following steps. Or access the iPlanet Directory Server documentation on the Internet at `http://docs.iplanet.com/docs/manuals/directory.html`

   - Step 1: Generate a Certificate Request
   - Step 2: Send the Certificate Request
   - Step 3: Install the Certificate (on Directory Server)
   - Step 4: Trust the Certificate Authority (Install the Root CA Certificate)
   - Step 5: Confirm That Your New Certificates Are Installed

2. Activate SSL in the Directory Server.

   Follow the detailed instructions in “Activating SSL,” on page 282 of this manual.

3. In the Web Server that runs DSAME services, in the Web Server console, create a trust database. Follow the detailed instructions “Creating a Trust Database,” on page 229.

4. In the Web Server that runs DSAME services, install the root CA Certificate for Directory Server’s server certificate. (This is the certificate you obtained in Step 2.) Follow the detailed instructions in “Requesting and Installing Other Server Certificates,” on page 233.

5. Edit the following DSAME configuration file:

   DSAME_root/`SUNWam/config/ums/serverconfig.xml`

   For the server corresponding to the Directory Server configured for SSL, provide the following values:

   port. Enter the SSL port number you specified in Step 2.

   type. Enter `SSL`.

   Example:

```
<?xml version="1.0" encoding="ISO-8859-1" standalone="yes"?>
<iPlanetDataAccessLayer>
    <ServerGroup name="default" minConnPool="1" maxConnPool="10">
        <Server name="Server1"
            host="adam.red.madisonparc.com" port="636"
```

```
           type="SSL" />
               <User name="User1" type="proxy">
                     <DirDN>
                          cn=puser,ou=People,o=isp
                     </DirDN>
                     <DirPassword>
                          AQAA5Q9jwkb4pAJ2LGFYRDlqWxXxId+5v4nU
                     </DirPassword>
               </User>
...
```

6. Restart DSAME with the following command:

   `/etc/init.d/amserver start`

7. If the Directory Server is not yet running, you are prompted for the internal key. Enter the key (password) you specified when creating the trust database in Step 3.

When DSAME starts up, its connection to Directory Server will be secured with SSL.

Step 2: Enable DSAME to Run in SSL Mode

When you enable DSAME to run in SSL mode, requests and transactions between the DSAME console and other SSL-configured Web Servers are encrypted and protected from intrusion by unauthorized entities.

1. Login to DSAME as Top Level Administrator.
2. In the Service Name column, choose DSAME Platform.
3. In the Server List box:
   a. Remove this DSAME server from the list. First select its name in the list, and then click Remove.
   b. Change Protocol to `https` (instead of `http`).
   c. To add the same server with `https`, click Add.
4. Edit the following DSAME configuration file: *DSAME_root*`/SUNWam/lib/AMConfig.properties`

   Modify values for the following to reflect the HTTPS protocol and new port number (if the port number was changed):

- `com.iplanet.am.server.protocol`
- `com.iplanet.am.server.port`
- `com.iplanet.am.profile.port`
- `com.iplanet.am.naming.url`
- `com.iplanet.am.notification.url`

5. In the Web Server that runs DSAME services, using the Web Server console, obtain and install a server certificate if one is not already installed.

NOTE In the following substeps, the following warning message might display:

`Warning: Manual edits not loaded`.

In this case, first click the Apply link in the upper right corner of the console, and then click Load Configuration Files

---

a. To obtain a server certificate, follow the detailed instructions for "Requesting Other Server Certificates," on page 234.

b. To install the server certificate, follow the detailed instructions for "Installing Other Server Certificates," on page 236.

6. In the Web Server console, select the Web Server that runs DSAME services, and click Manage.

a. In the Web Server instance, choose Preferences.

b. Click Edit Sockets.

c. In the Security field for the default DSAME port, enter `On`.

d. Click OK to save the change.

e. Click Apply.

f. To save changes to Web Server configuration files, click Apply Changes.

7. Restart DSAME with the following command:

```
/etc/init.d/amerserver start
```

8. You are prompted for server certificate password. Enter the password.

Configuring DSAME Instance to SSL

You can configure new DSAME instance that is installed using the `ammultiserverinstall` script, to run in SSL mode. Perform the following steps:

1. Enable SSL for DSAME. Follow the steps, Step 1: Enable LDAP Over SSL and Step 2: Enable DSAME to Run in SSL Mode

2. Copy the `server.xml` and `magnus.conf` files from /*DSAME_root*/`SUNWam/https-`*instance_name*/`conf_bk` to /*DSAME_root*/`SUNWam/https-`*instance_name*/`config`

3. Run the following command:

```
./amserver startall
```

Part 3

Windows 2000 Installation Instructions

Chapter 7

The DSAME Installation Program for Windows 2000

The iPlanet Directory Server Access Management Edition (DSAME) installation program is used to install or uninstall the complete product all at once, or components of the product one at a time. You can use the DSAME installation program in a number of ways depending upon your deployment needs. This chapter provides an overview of the options presented in the Windows version of the installation program, as well as some pointers on determining the installation tasks you'll need to perform. Topics include:

- Before You Begin
- Installation Program Options
- Silent Installation
- Determining Which Installation Options to Use
- Starting DSAME Services
- Logging In to DSAME
- Uninstalling DSAME

Before You Begin

Be sure to resolve the following before you start the installation program:

- You must have Administrator privileges to run the installation program.
- You can only install DSAME, or any of the components, on a machine local to you. You can not install across a network on remote machines.

- Determine whether or not you will be configuring an existing Directory Server. For more information, see "If You Already Have an Existing Directory," on page 26 and "Unsupported DITs," on page 28.
- Determine whether or not you will be installing DSAME policy agents. For more information, see "URL Policy Agent," on page 32.
- Determine whether or not you will be installing cross-domain single sign-on components. For more information, see "Cross-Domain Single Sign-On," on page 21.

Installation Program Options

Each time you run the installation program, a number of installation options are displayed. Determine which installation option to choose by first identifying your scenario in Table 7-1, and then following the detailed the instructions that correspond to that scenario. The following is a brief summary of what happens when you choose each of the main installation options.

Option 1) iPlanet Directory Server

When you choose this option, iPlanet Directory Server 5.1 is installed on the local computer system. This option, when selected by itself, is useful if you want to install a stand-alone Directory Server. For example, you can choose this option if you're setting up Directory Server replication. If you want to install DSAME for evaluation purposes, choose this option in addition to Option 2) DSAME Management and Policy Services.

When you select this option in addition to the DSAME Management and Policy Services option, DSAME schema is automatically installed. When you select this option by itself, you can specify whether or not you want to install DSAME schema.

Option 2) DSAME Management and Policy Services

When you choose this option, DSAME Management and Policy Services are installed on the local computer system. Select this option by itself when you want to install DSAME components to work with an existing Directory Server. When you want to install DSAME for evaluation purposes, select this option in addition to Option 1) iPlanet Directory Server.

Option 3) Configure an Existing Directory Server

When you choose this option, only the DSAME schema is installed. No new Directory Server is installed; no existing data is overwritten. Choose this option only if you plan to use DSAME with an existing Directory Server 5.1 that's already provisioned with user data. For more information, see "Using an Existing Directory Server," on page 63.

Option 4) DSAME 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 DSAME, install on Web Server, or install this by installing Web Server. For more information, see "Cross-Domain Single Sign-On," on page 21.

Exiting the Installation Program

After you've started the DSAME installation program, you can exit the program at any time by clicking Exit.

Silent Installation

Silent installation provides a means for scripting the installation of DSAME services, Directory Server, DSAME schema, or the Cross-Domain Single Sign-On component. When you perform a silent installation, you use a text file, or `StateFile`, to predefine 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 DSAME or its components using the same parameters in each instance.

Silent installation is a two-step process. First you generate a `StateFile` that contains all the parameter information the installation program needs. Then you run the silent installation program that automatically reads in the parameters you've defined in the `StateFile`.

To Generate a StateFile

1. Copy the setup program and installer files from the CD to your local directory.
2. Run the installation program using the graphical user interface (GUI). In the directory where the `setup.exe` file is located, open a DOS command prompt window and enter the following command:

   ```
   setup.exe
   ```

3. Proceed through the Welcome and License screens as prompted. When you get to the Select Components to Install window, click Exit. The `am.class` file is created in the same directory as the `setup.exe`.
4. In the same directory, enter the following command:

   ```
   java am -saveState DSAME51_StateFile
   ```

   where *DSAME51* is your name for the StateFile.

5. The installation program GUI displays. Proceed through the installation program GUI, keeping in mind that your answers to the prompts are being recorded in the `StateFile`.

   Follow the instructions for “Simple Installations With No Existing Directory Server,” on page 143 or for “Using an Existing Directory Server,” on page 151.

When installation is complete, the file `DSAME51_StateFile` is created in the same directory as `setup.exe`.

To Run the Silent Installation Program

1. Open a DOS command prompt window. In the directory where the files `am.class` and `DSAME51_StateFile` are located, enter the following command:

   ```
   java am -nodisplay -noconsole -state DSAME51_StateFile
   ```

2. When installation is complete, reboot the computer system.

Determining Which Installation Options to Use

You will probably run the DSAME installation program multiple times in order to install Directory Servers, DSAME services and Single Sign-On components in the proper number and sequence. Table 7-1 summarizes the common installation scenarios, and where to find the step-by-step instructions for each scenario.

Table 7-1 Where To Find DSAME Installation Instructions for Specific Scenarios.

Common Installation Scenarios	Where to Find Detailed Installation Instructions
1. Install DSAME and for evaluation purposes.	
OR	
2. Install and deploy Directory Server and DSAME for the first time for production purposes; you have no existing user data to work with.	"Simple Installations With No Existing Directory Server," on page 143.
3. Install DSAME to work with single directory that is already provisioned with user data.	"Using an Existing Directory Server," on page 151.
4. Install multiple instances of DSAME against a single Directory Server for agent failover. DSAME and the master Directory Server are already installed; the directory may or may not be already provisioned with users.	"Support for Directory Replication and High Availability," on page 199.
5. Install a stand-alone version of Directory Server with DSAME schema; useful in setting up multi-master replication.	"Installing a Stand-Alone iPlanet Directory Server," on page 148.
6. Upgrade an existing directory by installing a stand-alone version of Directory Server 5.1, without the DSAME schema.	"Installing a Stand-Alone iPlanet Directory Server," on page 148.
7. Configure an existing Directory Server 5.1 to be used with DSAME; the existing directory is already provisioned with user data.	"Step 2: Install DSAME Services," on page 160.
8. Install and configure the cross-domain single sign-on (CDSSO) component.	"Installing the Cross-Domain Single Sign-On Component," on page 195.
9. Uninstall or re-install DSAME.	"Uninstalling DSAME," on page 140.

Starting DSAME Services

You must start DSAME Services manually before you can login. You can start DSAME by using one of the following methods:

- Open a DOS prompt window and enter the following commands:

  ```
  cd DSAME_root\bin
  ```

  ```
  amserver start
  ```

- From the Start menu, select Programs > Administrative Tools > Services. In the Services window, right-click the icon for DSAME-*hostname*. From the menu, choose Start.

Logging In to DSAME

You can log in to DSAME through your browser.

1. Go to the appropriate login URL:

   - If DSAME services are running on iPlanet Web Server, go to the login URL using the form:

     `http://`*host*`.`*domain*`:`*port*`/amconsole`

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

     For example: `http://tintin.india.sun.com:58080/amconsole`

2. In the Login page, enter the Top-Level Administrator user id and password you specified at installation.

Uninstalling DSAME

The installation program in DSAME is also used to uninstall the DSAME application. You can the remove the entire product, or you can remove the following individual components of the product:

- DSAME Management and Policy Services
- iPlanet Directory Server 5.1

- iPlanet Directory Server Configuration for DSAME
- DSAME Cross Domain Single Sign-On

To Uninstall DSAME Components

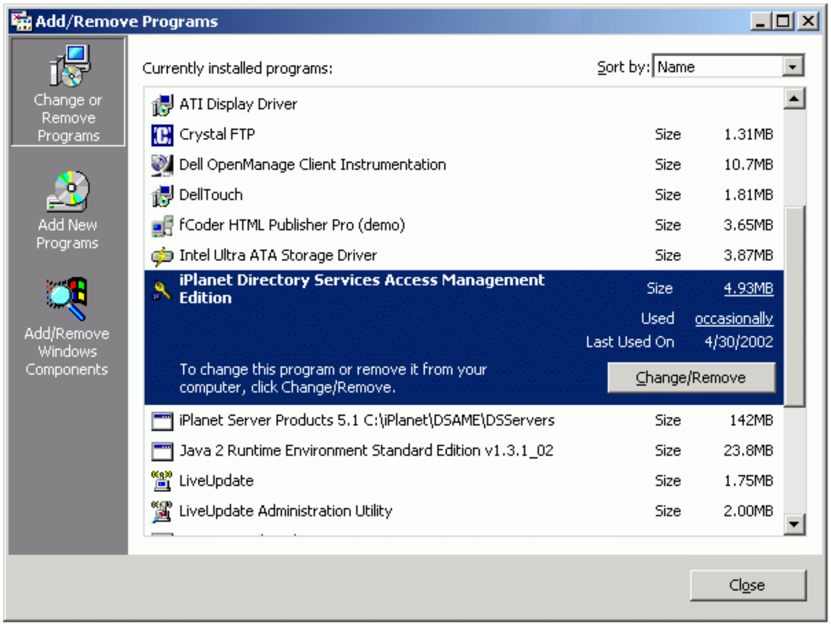
You must have Administrator privileges to run the DSAME Installation/Uninstallation program. Be sure all web browsers are closed before starting the program.

1. From the Start Menu, choose Settings > Control Panel.

NOTE As an alternative, you can start the Uninstallation program from DOS command prompt window. In the *DSAME_root* directory, enter the following command:

```
java uninstall_DSAME
```

2. In the Control Panel, double-click Add/Remove Programs.
3. In the Add/Remove Programs window, select iPlanet Directory Services Access Management Edition, and then click Change/Remove.



Currently installed programs:

ATI Display Driver		
Crystal FTP	Size	1.31MB
Dell OpenManage Client Instrumentation	Size	10.7MB
DellTouch	Size	1.81MB
fCoder HTML Publisher Pro (demo)	Size	3.65MB
Intel Ultra ATA Storage Driver	Size	3.87MB
iPlanet Directory Services Access Management Edition	Size	4.93MB
	Used	occasionally
	Last Used On	4/30/2002
To change this program or remove it from your computer, click Change/Remove.		
iPlanet Server Products 5.1 C:\iPlanet\DSAME\DSServers	Size	142MB
Java 2 Runtime Environment Standard Edition v1.3.1_02	Size	23.8MB
LiveUpdate	Size	1.75MB
LiveUpdate Administration Utility	Size	2.00MB

4. In the Select Type of Uninstall window, select one of the following options, and then click Next:

   Full. Select this option if you want to remove DSAME services and Directory Server installed on the local computer system.

   Partial. Select this option if you want to remove only either the DSAME Service or Directory Server installed on the local computer system.

5. In the Ready to Uninstall window, click Uninstall Now.

6. In the Summary Window, you can click Details to see more information about the uninstallation results. Click Exit to exit the program.

Chapter 8

Simple Installations With No Existing Directory Server

This chapter provides instructions for installing iPlanet Directory Server Access Management Edition (DSAME) for evaluation purposes, or for deploying a DSAME directory and services for the first time. The instructions here assume that you don’t already have a Directory Server installed and deployed.

Topics in this chapter include:

- Installing DSAME Services and Directory Server
- Installing a Stand-Alone iPlanet Directory Server

NOTE If you plan to use DSAME with an existing Directory Server that is already provisioned with users, see Chapter 9, “Using an Existing Directory Server.

Installing DSAME Services and Directory Server

Use these instructions when you want to do a quick and simple installation for the purpose of evaluating or exploring the product, and when you’re not concerned with connecting to an existing Directory Server or existing user data. When you choose this option, the following components are installed:

- Directory Server 5.1
- DSAME Policy service and Management service
- A Web Server that runs the DSAME Policy and Management services

To Install DSAME Services with a New Directory Server

You must have Administrator privileges when you run the DSAME installation program. Be sure all web browsers are closed before starting the installation program.

1. If you're installing DSAME from the product CD, insert the CD into the drive of the system on which you want to install the software. If you've downloaded the product, unzip the product binaries file.

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

   Double-click the `setup.exe` icon.

   Installation messages are written to log files in the following directory:

   ```
   C:\Documents and Settings\Administrator\Local Settings\Temp
   ```

3. Read the License Agreement. When prompted, **Do you agree to the license terms?** Click Yes (Accept License).

4. In the Installation Directory window, provide the following information:

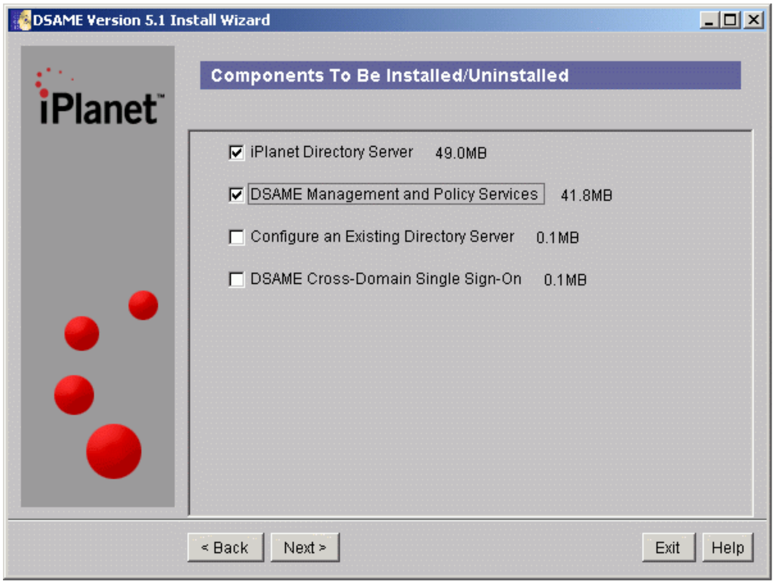
   Install DSAME in this directory: Enter the path to the directory where DSAME Services will be installed. Plan to install the DSAME Services and Directory Server in different directories. Ideally, you would install DSAME Services and Directory Server on different computer systems.

5. In the Components to Be Installed / Uninstalled window, select only the following components:

   - iPlanet Directory Server
   - DSAME Management and Policy Services

   Deselect all other components.

Figure 8-1 Installing DSAME Services with a New Directory Server.



DSAME Version 5.1 Install Wizard

Components To Be Installed/Uninstalled

☑ iPlanet Directory Server 49.0MB

☑ DSAME Management and Policy Services 41.8MB

☐ Configure an Existing Directory Server 0.1MB

☐ DSAME Cross-Domain Single Sign-On 0.1MB

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

   Do you want to use your own JDK? Java support in the Web Server requires Java Development Kit (JDK) of version 1.3.1 or higher. While a default JDK is provided, you can use your own JDK with the Web Server. If you want to use your own JDK version, then select Yes and then enter the full path to the version of JDK you want to use. Otherwise, select No.

7. In the iPlanet Web Server Information window, provide the following information about the Web Server that will run DSAME services, and then click Next:

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

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

   Password: Enter the password for the Administrator specified above. The Password must be a minimum of 8 characters in length.

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

8. In The Web Server that Runs DSAME Services window, provide the following information, and then click Next:

   Host: This is the computer system where DSAME components and a dedicated web server will be installed together.

   Port: Enter a port number for the Web Server that runs the DSAME services.

   Protocol: If the Web Server will not be using the Secure Socket Layer (SSL) protocol, then select HTTP. If it will be enabled for SSL, then select HTTPS.

   Domain: Enter the domain name of the computer system where DSAME Services will be installed.

   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 like classes and jars.

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

   DSAME Console Deployment URI: This URI prefix tells the Web Server where to look for HTML pages associated with the DSAME administration 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.

9. In the Directory Schema window, provide the following information, and then click Next:

   Root Suffix: This is the point in your directory where you want DSAME to start managing entries. Enter a distinguished name (DN) that contains at least one *type=value* pair. Examples:

   `o=isp`

   `o=madisonparc`

   `dc=sun,dc=com`

   If you want the default organization to be the root suffix, then enter a period (.).

   Organization Name: Enter a name for the first organization to be used or created in your DSAME Directory Information Tree (DIT). This name will be displayed in the DSAME graphical user interface. Examples: `iPlanet` or `iplanet.com`.

   Directory Component Node: This is the point in DIT where DSAME will start managing entries. Example: `o=isp`

10. In the iPlanet Directory Server Information window, enter the following, and then click Next.

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

    Port: Enter the Directory Server port number.

    Installation Directory: Enter the full path to the directory where Directory Server is installed.

    Directory Manager: Enter the DN of the user who has 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.

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

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

    Administrator: Enter the user name of the administrator who will have access to the Administration Server that manages iPlanet Directory Server.

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

    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.

12. In the DSAME Super Administrator Information window, provide the following information, and then click Next:

    User name: The user name for the Super administrator is `amAdmin`. This name cannot be reconfigured.

    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.

13. In the Currently Selected Settings window, review the configuration information that you’ve entered. If you need to make changes, click Back. Otherwise, click Next to proceed.

14. In the Ready to Install window, review the installation information. If you need to make changes, click Back. Otherwise, click Install Now to begin the installation.

15. In the Installation Summary window, click Details for a detailed summary of the configuration information that was processed during Installation. Then click Exit to end the program.

Installing a Stand-Alone iPlanet Directory Server

You can use the DSAME product CD to install iPlanet Directory Server as a stand-alone product that does not contain DSAME schema. This is useful when you need to modify the DIT or configuration before adding DSAME schema. For example, you might want to install a stand-alone Directory Server when you are upgrading an existing Directory Server to version 5.1, or when you are setting up directory replication.

If you plan to use directory replication, you'll need to install stand-alone versions of Directory Server 5.1 on more than one computer system. If you want to set up replication before you install DSAME schema, you can use the Directory Server setup program that comes on the DSAME product CD.

To Install a Stand-Alone iPlanet Directory Server

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

   Double-click the `setup.exe` icon.

   Installation messages are written to log files in the following directory:

   ```
   C:\Documents and Settings\Administrator\Local Settings\Temp
   ```

2. Read the License Agreement. When prompted, **Do you agree to the license terms?** Click Yes (Accept License).

3. In the Installation Directory, provide the following information:

   Install DSAME in this directory: Enter the full path to the directory where you want to install DSAME components. Plan to install the DSAME Services and Directory Server in different directories. Ideally, you would install DSAME Services and Directory Server on different computer systems.

4. In the Components to Be Installed / Uninstalled window, select only iPlanet Directory Server. De-select all other components.

5. In the Directory Schema window, provide the following information, and then click Next:

   Root Suffix: This is the point in your directory where you want DSAME to start managing entries. Enter a distinguished name that includes at least one equals sign. Examples:

   `o=isp`

   `o=madisonparc`

   `dc=sun,dc=com`

   If you want the default organization to be the root suffix, then enter a period (.).

   Install DSAME Schema: If you want to install DSAME schema along with the Directory Server, then click the checkbox until a checkmark is displayed.

6. In the iPlanet Directory Server Information window, provide the following information, and then click Next:

   Host: Enter the fully qualified domain name for the computer system where Directory Server will be installed.

   Port: Enter a port number. Directory Server typically uses port `389`.

   Installation Directory: Enter the full path to the directory where Directory Server will be installed.

   Directory Manager: Enter the distinguished name (DN) of the user who has unrestricted access to Directory Server. Example: `cn=Directory Manager`

   Password: Enter a password for the Directory Server administrator.The password must be at least eight characters in length.

   Confirm Password: Enter the password again to confirm it.

7. In The Administration Server that Manages Directory Server window, provide the following information, and then click Next:

   Administrator: This administrator user ID is used only when the Directory Server is down and you are unable to log in as the configuration directory administrator (typically, `cn=Directory Manager`). The existence of this user ID means that you can access Administration Server and perform disaster recovery activities such as starting Directory Server, reading log files, and so forth.

   Normally, Administration Server user and password should be identical to the configuration directory administrator ID and password.

   Port: Enter a port number. The Administration Server that manages Directory Server typically uses port `58900`.

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

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

8. In the Currently Selected Settings window, review the configuration information that you've entered. If you need to make changes, click Back. Otherwise, click Next to proceed.

9. In the Ready to Install window, 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 window, click Details for a detailed summary of the configuration information that was processed during Installation. Then click Exit to end the program.

Chapter 9

Using an Existing Directory Server

If you're using an existing Directory Server that is already provisioned with users, you must make several changes in your Directory Information Tree (DIT) before iPlanet Directory Server Access Management Edition (DSAME) will recognize your user data. The number and scope of changes you must make will depend upon how your existing DIT is structured, and upon how you plan to use DSAME.

This chapter provides instructions for installing DSAME services against an existing directory that contains user data. It also explains how to configure DSAME to work with your DIT, and how to make the necessary changes to your existing directory entries.

Topics in this chapter include:

- Before You Begin
- Step 1: Install Directory Server 5.1 and Configure it to Work With DSAME
- Step 2: Install DSAME Services
- Step 3: (Optional) Add Your Custom Object Classes to DSAME Schema
- Step 4: (Optional) Configure Alternative Naming Attributes
- Step 5: Load DSAME LDIF Into Your Directory
- Step 6: Load DSAME Service Attributes into Your Directory
- Step 7: (Optional) Add DSAME ACIs to Your Default Organization
- Step 8: Start DSAME
- Step 9: Add DSAME Object Classes and Attributes to Existing Directory Entries
- Step 10: Load the Modified LDIF Files

Before You Begin

The requisite directory modifications are complex. They require a high level of expertise in LDAP planning and implementation, as well as some familiarity with XML. The procedures are complicated and can be time-consuming. Be sure to plan accordingly for this phase of deployment.

NOTE If you do not already have an existing directory that is provisioned with users, you do not need to perform the steps described in this chapter. See Simple Installations With No Existing Directory Server, on page 143.

Supported DITs and Unsupported DITs

While DSAME can be reconfigured to support most existing DITs, in some situations reconfiguration may not be recommended. To determine whether your DIT may be compatible with DSAME, see DITs That Cannot Be Managed by DSAME, on page 218.

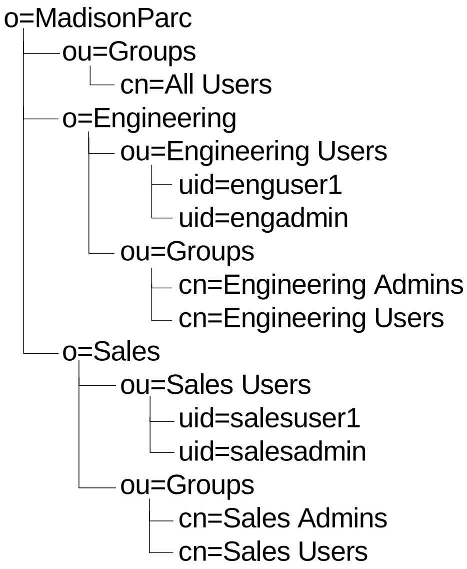
Background for Examples Used in This Chapter

In order to illustrate the types of changes you'll need to make to your directory, we'll use a simple DIT for a fictitious company. The directory entries for this company, represented by `o=madisonparc`, contain two custom object classes. These are object classes that are not already defined in DSAME schema. If your DIT contains custom object classes, you'll also need to make changes to the DSAME XML files.

Basic DIT Structure

The examples used in this chapter are based on a simple DIT for a fictitious company. Figure 9-3 on page 181 shows two organizations, `Engineering` and `Sales`, under the root. All groups in this example are *static* groups. This means that entries for these groups use the `groupOfUniqueNames` object class, which contains values naming the members of the group.

Figure 9-1 Directory Information Tree (DIT) Used in Examples in this Chapter.



The following summarizes the use of groups in this sample DIT:

- There is one group containing the administrators for Engineering, and one group with the administrators for Sales.
- Very simple ACIs are set for the groups Engineering and Sales to allow members of these groups to manage their respective organizations.
- In each organization, there is a group that contains non-administrator users.
- There is another group at the root level, or *top level*. It contains all users in the directory.

Custom Object Classes

The fictitious company used in this example uses two object classes that are not included in the DSAME schema nor in the Directory Server 5.1 schema. An auxiliary object class `madisonparc-org` is in every organization entry, and an auxiliary object class `madisonparc-user` is in every user entry. In order to manage these extensions, changes must be made in the following three files:

- `amEntrySpecific.xml`
  (Changes are not required if you're modifying only user entries.)
- `amUser.xml`
- `ums.xml`

These changes are described in detail in the section Step 3: (Optional) Add Your Custom Object Classes to DSAME Schema, on page 163. If you use custom object classes in your existing directory, you will need to make similar changes.

Step 1: Install Directory Server 5.1 and Configure it to Work With DSAME

DSAME will work only with iPlanet Directory Server 5.1. If you have a pre-5.1 version installed, you must upgrade to version 5.1 and migrate your data before you can install DSAME services.

Step 1a: Back Up Your Directory Data

For detailed information on backing up your directory, see the *iPlanet Directory Server Installation Guide* at:

`http://docs.iplanet.com/docs/manuals/directory.html`

Step 1b: Install and Configure Directory Server 5.1 With DSAME Schema

You must have administrative privileges when you run the DSAME installation program. Be sure all web browsers are closed before starting the installation program.

1. If you're installing DSAME from the product CD, insert the CD into the drive of the system on which you want to install the software. If you've downloaded the product, unzip the product binaries file.

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

   Double-click the `setup.exe` icon.

   Installation messages are written to log files in the following directory:

   ```
   C:\Documents and Settings\Administrator\Local Settings\Temp\
   ```

3. Read the License Agreement. When prompted, **Do you agree to the license terms?** Click Yes (Accept License).

4. In the Installation Directory, provide the following information:

   Install DSAME in this directory: Enter the full path to the directory where you want to install DSAME components. Plan to install the DSAME Services and Directory Server in different directories. Ideally, you would install DSAME Services and Directory Server on different computer systems.

5. In the Components to Be Installed / Uninstalled window, select only iPlanet Directory Server. De-select all other components.

6. In the Directory Schema window, provide the following information, and then click Next:

   Root Suffix: This is the root suffix of your existing directory tree. Enter a distinguished name (DN) that includes at least one *type*=*value* pair. Examples:

   ```
   o=isp
   ```

   ```
   o=madisonparc
   ```

   ```
   dc=sun,dc=com
   ```

   If you want the default organization to be the root suffix, then enter a period (.).

   Install DSAME Schema: Select this option. Click the checkbox until a checkmark displays.

7. In the iPlanet Directory Server Information window, provide the following information, and then click Next:

   Host: Enter the fully qualified domain name for the computer system where Directory Server will be installed.

   Port: Enter a port number. Directory Server typically uses port 389.

   Installation Directory: Enter the full path to the directory where Directory Server will be installed.

   Directory Manager: Enter the distinguished name (DN) of the user who has unrestricted access to Directory Server. Example: `cn=Directory Manager`

   Password: Enter a password for the Directory Server administrator.The password must be at least eight characters in length.

   Confirm Password: Enter the password again to confirm it.

8. In The Administration Server that Manages Directory Server window, provide the following information, and then click Next:

   Administrator: This administrator user ID is used only when the Directory Server is down and you are unable to log in as the configuration directory administrator (typically, `cn=Directory Manager`). The existence of this user ID means that you can access Administration Server and perform disaster recovery activities such as starting Directory Server, reading log files, and so forth.

   Normally, Administration Server user and password should be identical to the configuration directory administrator ID and password.

   Port: Enter a port number. The Administration Server that manages Directory Server typically uses port 58900.

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

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

9. In the Currently Selected Settings window, 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 window, review the installation information. If you need to make changes, click Back. Otherwise, click Install Now to begin the installation.

11. In the Installation Summary window, click Details for a detailed summary of the configuration information that was processed during Installation. Then click Exit to end the program.

Step 1c: Migrate Existing Data to Directory Server 5.1

In this step, you will update your pre-5.1 data to work with Directory Server 5.1. This process, called *migration*, is performed by running the `migrateInstance5` script that comes with Directory Server. The migration script performs the following tasks in sequence:

- Checks the schema configuration files, and notifies you of any changes between the standard configuration files and the ones present on your system.
- Creates a database for each suffix stored in the legacy Directory Server. (In Directory Server 5.0 you can have multiple databases, but just one suffix per database).
- Migrates the server parameters and database parameters. (In Directory Server 5.0, these are stored as LDAP entries in the `dse.ldif` file.)
- Migrates user-defined schema objects.
- Migrates indexes.
- Migrates standard server plug-ins.
- Migrates the certificate database, and SSL parameters.

NOTE Your existing user data must be migrated to Directory Server 5.1 before you go on to Step 2. Otherwise, DSAME may not be able to recognize your existing user data.

You must run the script on the system where your existing Directory Server is installed. You must shut down your directory service before running the migration script. For detailed migration instructions, see the *iPlanet Directory Server Installation Guide* at:

`http://docs.iplanet.com/docs/manuals/directory.html`

Step 1d: Install DSAME Schema

NOTE The instructions in this section, Step 1d, assume that you have already deployed and provisioned Directory Server 5.1, but your existing directory tree does not contain DSAME 5.1 schema.

You must have administrative privileges when you run the DSAME installation program. Be sure all web browsers are closed before starting the installation program.

1. If you're installing DSAME from the product CD, insert the CD into the drive of the system on which you want to install the software. If you've downloaded the product, unzip the product binaries file.

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

   Double-click the `setup.exe` icon.

   Installation messages are written to log files in the following directory:

   ```
   C:\Documents and Settings\Administrator\Local Settings\Temp\
   ```

3. Read the License Agreement. When prompted, **Do you agree to the license terms?** Click Yes (Accept License).

4. In the iPlanet Directory Server Information window, provide the following information, and then click Next:

   Host: Enter the fully qualified domain name for the computer system where Directory Server will be installed.

   Port: Enter a port number. Directory Server typically uses port 389.

   Installation Directory: Enter the full path to the directory where Directory Server will be installed.

   Directory Manager: Enter the distinguished name (DN) of the user who has unrestricted access to Directory Server. Example: `cn=Directory Manager`.

   Password: Enter a password for the Directory Server administrator.The password must be at least eight characters in length.

   Confirm Password: Enter the password again to confirm it.

   Will you be using an existing DIT and schema? Select Yes.

5. In the next Directory Schema window, provide the following information, and then click Next:

   Root Suffix of Your Directory Tree: This DSAME root suffix, or the point in your directory where you want DSAME to start managing entries. Enter a distinguished name (DN) that includes at least one *type*=*value* pair.

   Examples:

   `o=isp`

   `o=madisonparc`

   `dc=sun,dc=com`

   Organization Name: Enter a name for the first organization to be used or created in your DSAME Directory Information Tree (DIT). This name will be displayed in the DSAME graphical user interface. Examples: `iPlanet` or `iplanet.com`.

   Directory Component Node: This is the point in the DIT where DSAME will start managing entries. Example: `o=isp`.

6. In the Remote or Local Host window, when prompted **Is the existing iPlanet Directory Server installed on a local host or on a remote host?** Select Local if Directory Server is installed on the same computer system as DSAME services; otherwise select Yes.

7. In The Web Server that Runs DSAME Services window, provide the following information about the computer system where DSAME will be installed, and then click Next:

   Host: Enter the name of the computer system where DSAME will be installed.

   Port: Enter the port number of the Web Server that will run DSAME services.

   Protocol: If the Web Server that will run DSAME services will not be using Secure Socket Layer (SSL) protocol, then select HTTP. If it will be SSL-enabled, then select HTTPS.

   Domain: Enter the domain name of the computer system where DSAME will be installed.

   Deployment URI: Enter the Deployment Universal Resource Identifier (URI) that was specified when DSAME was installed. The default is `/amserver`.

   Deployment URI prefix for the DSAME Administration Console:

8. In the DSAME Super Administrator Information window, provide the following information, and then click Next:

   User name: The user name for the Super administrator is `amAdmin` This name cannot be reconfigured.

   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.

9. In the Currently Selected Settings window, 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 window, review the installation information. If you need to make changes, click Back. Otherwise, click Install Now to begin the installation.

11. In the Installation Summary window, click Details for a detailed summary of the configuration information that was processed during Installation. Then click Exit to end the program.

Step 1e: Back Up Your Existing Data

Back up your existing DIT before proceeding further with the other steps. Many of the changes described in this chapter must be done manually and can be error-prone.

For detailed information on backing up your directory, see the *iPlanet Directory Server Installation Guide* at:

`http://docs.iplanet.com/docs/manuals/directory.html`

Step 2: Install DSAME Services

You must have root permissions when you run the DSAME installation program. Be sure all web browsers are closed before starting the installation program.

1. If you're installing DSAME from the product CD, insert the CD into the drive of the system on which you want to install the software. If you've downloaded the product, unzip the product binaries file.

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

   Double-click the `setup.exe` icon.

   Installation messages are written to log files in the following directory:

   `C:\Documents and Settings\Administrator\Local Settings\Temp\`

3. Read the License Agreement. When prompted, **Do you agree to the license terms?** Click Yes (Accept License).

NOTE After installation you will not yet be able to login to the DSAME administration console. The appropriate LDIF and XML files have not yet been loaded. See the following sections for instructions.

4. In the Installation Directory window, provide the following information:

   Install DSAME in this directory: Enter the path to the directory where DSAME Services will be installed. Plan to install the DSAME Services and Directory Server in different directories. Ideally, you would install DSAME Services and Directory Server on different computer systems.

5. In the Components to Be Installed window, select only DSAME Management and Policy Services. De-select all other components.

6. In the iPlanet Web Server Information window, provide the following information about the Web Server that will run DSAME services, and then click Next:

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

   Port: Enter a port number. Typically, this administration port is set to `58888`.

   Password: Enter the password for the Administrator specified above. The password must be a minimum of 8 characters in length.

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

7. In The Web Server that Runs DSAME Services window, provide the following information about the computer system where DSAME will be installed, and then click Next:

   Host: Enter the name of the computer system where DSAME will be installed.

   Port: Enter the port number of the Web Server that will run DSAME services.

   Protocol: If the Web Server that will run DSAME services will not be using Secure Socket Layer (SSL) protocol, then select HTTP. If it will be SSL-enabled, then select HTTPS.

   Domain: Enter the domain name of the computer system where DSAME will be installed.

   Deployment URI: Enter the Deployment Universal Resource Identifier (URI) that was specified when DSAME was installed. The default is `/amserver`.

8. In the next Directory Schema window, provide the following information, and then click Next:

   Root Suffix of Your Directory Tree: This DSAME root suffix, or the point in your directory where you want DSAME to start managing entries. Enter a distinguished name (DN) that includes at least one *type*=*value* pair.

   Examples:

   `o=isp`

   `o=madisonparc`

   `dc=sun,dc=com`

   Organization Name: Enter a name for the first organization to be used or created in your DSAME Directory Information Tree (DIT). This name will be displayed in the DSAME graphical user interface. Examples: `iPlanet` or `iplanet.com`.

   Directory Component Node: This is the point in the DIT where DSAME will start managing entries. Example: `o=isp`.

9. In the iPlanet Directory Server Information window, provide the following information, and then click Next:

   Host: Enter the fully qualified domain name for the computer system where Directory Server will be installed.

   Port: Enter a port number. Directory Server typically uses port `389`.

   Directory Manager: Enter the distinguished name (DN) of the user who has unrestricted access to Directory Server. Example: `cn=Directory Manager`

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

10. In the DSAME Super Administrator Information window, provide the following information, and then click Next:

    User name: The user name for the Super administrator is `amAdmin.` This name cannot be reconfigured.

    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.

11. In the Currently Selected Settings window, review the configuration information that you’ve entered. If you need to make changes, click Back. Otherwise, click Next to proceed.

12. In the Ready to Install window, review the installation information. If you need to make changes, click Back. Otherwise, click Install Now to begin the installation.

13. In the Installation Summary window, click Details for a detailed summary of the configuration information that was processed during installation. Then click Exit to end the program.

Step 3: (Optional) Add Your Custom Object Classes to DSAME Schema

If your existing DIT contains object classes you’ve created and that do not come with Directory Server, then you’ll have to add those object classes and attributes to the DSAME schema. For background information, see “Understanding DSAME XMLs and DTDs” in the *Programmer’s Guide*.

If you do not use custom object classes in your DIT, this step is not necessary. Skip to Step 5: Load DSAME LDIF Into Your Directory, on page 175.

In the examples in this section, the company MadisonParc uses two object classes that do not come with the DSAME schema. An auxiliary object class `madisonparc-org` is in every organization entry, and an auxiliary object class `madisonparc-user` is in every user entry.

Code Example 9-1 MadisonParc’s Customized Schema

```
dn: cn=schema
attributeTypes: ( madisonparc-org-description-oid NAME
  ‘madisonparc-org-description’ DESC ’org description’
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  SINGLE-VALUE X-ORIGIN ’madisonparc’ )
attributeTypes: ( madisonparc-org-city-oid NAME
  ’madisonparc-org-city’ DESC ’org city location’
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  SINGLE-VALUE X-ORIGIN ’madisonparc’ )
attributeTypes: ( madisonparc-user-id-oid NAME
  ’madisonparc-user-id’ DESC ’user madisonparc id’
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  SINGLE-VALUE X-ORIGIN ’madisonparc’ )
attributeTypes: ( madisonparc-user-building-oid NAME
   ’madisonparc-user-building’ DESC ’priority of a service
  with respect to its siblings’
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  SINGLE-VALUE X-ORIGIN ’madisonparc’ )
objectClasses: ( madisonparc-org-oid NAME
  ’madisonparc-org’ DESC
  ’custom attributes for madisonparc org’ SUP top MAY
  ( madisonparc-org-description $ madisonparc-org-city )
  X-ORIGIN ’madisonparc’ )
objectClasses: ( madisonparc-user-oid NAME ’madisonparc-user’
  DESC ’custom attributes for madisonparc user’ SUP top MAY
  ( madisonparc-user-id $ madisonparc-user-building )
  X-ORIGIN ’madisonparc’ )
```

In order to manage these extensions, changes must be made in the following three files:

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

Step 3a: Add Attributes to the Organization Schema

In this step, you will modify two services files:

- amEntrySpecific.xml
- amEntrySpecific.properties.

The DSAME console uses the information in amEntrySpecific.xml for display purposes. Each DSAME abstract entry may have a subschema in this XML file. In the following example, you would add the two attributes from the madisonparc-org object class to the organization subschema. If the DIT contained customized organizational units, groups, or people containers, you would add or modify their subschemas in this 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 Step3b: Add Attributes to the User Schema, on page 168.) Although any service XML file may describe an attribute that is for a user only, the amentryspecific.xml file can serve as a default placeholder for user attributes that are not tied to a particular service.

To Add Attributes from a Custom Organization to the Organization Subschema

NOTE In XML, attribute names must be all lowercase. When DSAME retrieves attributes names from Directory Server, it converts all names to lowercase.

1. In the following file:

DSAME_root\config\xml\amEntrySpecific.xml

add the attributes from the custom object class to the subschema Organization. For example, the following two attributes from the custom object class madisonparc-org were added to the file.

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

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

/>
```

2. Also in the `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 DSAME 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"
    i18nKey="o3"
/>
<AttributeSchema name="madisonparc-org-city"
    type="single"
    syntax="string"
    any=required|filter
    i18nKey="o4"
/>
```

3. In the following file, add the values for i18n Keys you created in Step 2:

   DSAME_root`\locale\amEntrySpecific.properties`

   Example:

```
iplanet-am-entry-specific-service-description=DSAME 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=Org Description
o4=Organization Location
```

All the attributes listed in the subschema are displayed in the Administration Console when the 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.

The "any" attribute

The any attribute in the XML descriptions may have six 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 readonly for regular users. It is displayed as a label for regular users so that it is not editable.For e.g. the display, adminDisplay, and userReadOnly settings are usedwhen displaying the user profilepage 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. 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 Full Name is optional.

In the following example, both attributes will be displayed on the Organization page, and both attributes are required for creation. This is indicated by the use the `required` value. Only the `madisonparc-org-city` attribute will be used on the Search page in DSAME Administration Console, as indicated by the use of the `filter` value.

```
<AttributeSchema name="madisonparc-org-description"
    type="single"
    syntax="string"
    any="required"
    i18nKey="o3"
/>
<AttributeSchema name="madisonparc-org-city"
    type="single"
    syntax="string"
    any=required|filter
    i18nKey="o4"
/>
```

The "type" attribute

The *type* attribute can use a string, string list, single choice, multiple choice, or boolean value. For example, if the `madisonparc-org-city` attribute can have only one of the cities Concord, San Francisco, or Palo Alto, as a valid value, then you would make this attribute a single choice; each city would be one of the choices. The DSAME Administration Console would display a list containing only these cities. If multiple cities were allowed, the attribute could be a multiple choice.

Step3b: Add 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 DSAME. 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 DSAME 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 167 and The "type" attribute, on page 168). 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 `amUser` service.

Additional Notes About the amUser.xml File

The file `amUser.xml` contains the special any attribute. The `any=display` attribute tells DSAME 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 background information, see “Understanding DSAME XMLs and DTDs” in the *Programmer’s Guide*.

For example, you could make the `madison-user-building` attribute Dynamic, and have DSAME create a role with this attribute. This way if all employees in a division moved to a different building, you would only have to modify the role attribute instead having to modify of every single user entry.

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:

   DSAME_root`\config\xml\amUser.xml`

2. For example, the following two attributes from the custom object class `madisonparc-user` were added to the file:

```
<AttributeSchema name="madisonparc-user_id"
    type=single
    syntax=string
    any=required|display
    i18nKey=u13
/>
<AttributeSchema name="madisonparc-user-building"
    type=single
    syntax=string
    any=required|filter|display
    i18nKey=u14
/>
```

3. In the `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 DSAME Administration Console will use this key to look up the display name for the attribute. See the example above.

4. Add values for the i18nKeys created in the previous step to the following file: *DSAME_root*`\locale\amUser.properties`

   Example:

```
iplanet-am-user-service-description=DSAME User
iwtUser-desc=Default User Profile
u1=User Name
u2=First Name
u3=Last Name
u4=Full Name
u5=Password
u6=Email Address
u7=Employee Number
u8=Telephone Number
u9=Manager
u10=Home Address
u11=User Status
u12=User Auth Modules
u13=User Id
u14=Employee Building
```

   The value is the exact field to be displayed on the administration console page; the key will be localized for the locale. In this example, the administration console will display the text fields “User Id” and “Employee Building.”

Step 3c: Modify the Creation Templates

In this step, you will modify the `ums.xml` file.

In Figure 9-3 on page 181, the sample DIT has new object classes for both users and organizations. To expose the new object classes in the UI, you would modify the Creation Templates for both users and organizations in the `ums.xml` file. The Creation Templates configure DSAME to add or allow specific object classes and attributes when these entries are created.

To Modify the Creation Templates

Make the following modifications in the file:

DSAME_root`\config\ums\ums.xml`

1. Under `<SubConfiguration name="BasicOrganization" id="CreationUmsObjects">`, in the `<AttributeValuePair> <Attribute name="required" />` element, add the following:

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

```
<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=organization</Value>
                <Value>objectClass=nsManagedDomain</Value>
                <Value>objectClass=inetDomain</Value>
                <Value>objectClass=iplanet-am-managed-org</Value>
                <Value>objectClass=madisonparc-org</Value>
                <Value>o</Value>
                <Value>inetdomainstatus=Active</Value>
         </AttributeValuePair>
```

2. Under `<SubConfiguration name="BasicUser" id="CreationUmsObjects">`, in the `<AttributeValuePair><Attribute name="optional" />` element, add the following:

   `<Value>objectClass=madisonparc-user</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=iplanet-am-managed-person</Value>
          <Value>objectClass=madisonparc-user</Value>
          <Value>cn=default</Value>
          <Value>sn=default</Value>
```

```
            <Value>uid</Value>
            <Value>inetuserstatus=Active</Value>
         </AttributeValuePair>
```

3. Under `<SubConfiguration name="BasicOrganization" id="CreationUmsObjects">`, in the `<AttributeValuePair> <Attribute name="optional" />` element, add the following:.

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

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

   Example:

```
<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=organization</Value>
           <Value>objectClass=nsManagedDomain</Value>
           <Value>objectClass=inetDomain</Value>
           <Value>objectClass=iplanet-am-managed-org</Value>
           <Value>objectClass=madisonparc-org</Value>
           <Value>o</Value>
           <Value>inetdomainstatus=Active</Value>
        </AttributeValuePair>
        <AttributeValuePair> <Attribute name="namingattribute" />
           <Value>o</Value>
        </AttributeValuePair>
        <AttributeValuePair> <Attribute name="optional" />
           <Value>*</Value>
           <Value>madisonparc-org-description</Value>
           <Value>madisonparc-org-city</Value>
        </AttributeValuePair>
```

4. Under `<SubConfiguration name="BasicUser" id="CreationUmsObjects">`, in the `<AttributeValuePair> <Attribute name="optional" />` element, add the following:

   `<Value>madisonparc-user-id</Value>`

   `<Value>madisonparc-user-building</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=iplanet-am-managed-person</Value>
               <Value>objectClass=madisonparc-user</Value>
               <Value>cn=default</Value>
               <Value>sn=default</Value>
               <Value>uid</Value>
               <Value>inetuserstatus=Active</Value>
          </AttributeValuePair>
          <AttributeValuePair> <Attribute name="optional" />
               <Value>nsroledn</Value>
               <Value>madisonparc-user-id</Value>
               <Value>madisonparc-user-building</Value>
               <Value>*</Value>
          </AttributeValuePair>
```

Step 4: (Optional) Configure Alternative Naming Attributes

If you used a naming attribute other than `o=`*organization* to define organizations in your DIT, you must modify the `ums.xml` file to accommodate the non-standard naming attributes. If you used a naming attribute other than `uid=`*username* to define users in your DIT, your must make similar modifications in the `ums.xml` file. For detailed reference information, see Using Alternative Naming Attributes, on page 218.

To Configure Alternative Naming Attributes for Organizations

The following steps assume that `dc` is the naming attribute used for an organization. Perform the modifications in the following file:

DSAME_root`\config\ums\ums.xml`

1. Replace any appearance of `o=org` with `dc=org`.
2. In the `BasicOrganization` section, replace value of `o` with `dc`.
3. In the `BasicOrganizationSearch SubConfiguration` section, replace value of `o` with `dc`.
4. In the `BasicOrganization` section, change the object class of `organization` to `domain`. If you use `ou` for an organization, then you need to change it to `organizationalUnit`.

To Configure Alternative Naming Attributes for Users

The following steps assume that `cn` is the naming attribute used for users.

Make modifications in the following directory:

DSAME_root`\web-apps\services\WEB-INF\config`

1. In the file `ldif\installExisting.ldif`, *with two exceptions*, replace `uid` with `cn`. The exceptions are:
   - The occurrence under ACI.

- The uid: amAdmin attribute in the amAdmin entry.

2. In xml\amAuth.xml, replace uid with cn for user naming attribute.
3. In xml\amMembership.xml, replace uid with cn for the user naming attribute.
4. In xml\amAuthLDAP.xml, replace uid with cn for the user naming attribute.
5. In AMConfig.properties, replace uid=amAdmin with cn=amAdmin.
6. In ums\ums.xml, in BasicUser subconfiguration, replace uid with cn for namingattribute.
7. In ums\ums.xml, in BasicUser required values, change cn=default to cn and uid to uid=default.

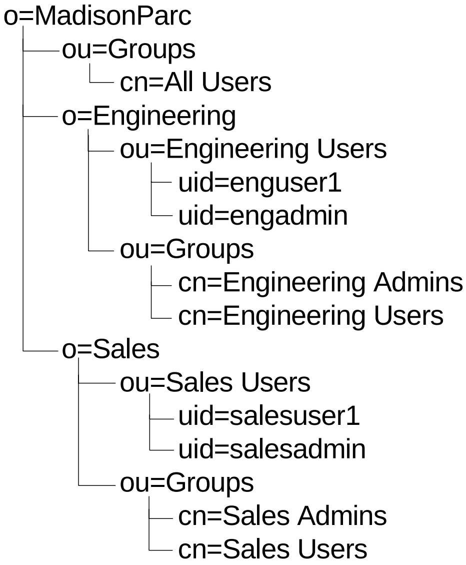
Step 5: Load DSAME LDIF Into Your Directory

The installExisting.ldif file contains DSAME-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 DSAME are added to o=madisonparc and o=Engineering,o=madisonparc
- Default roles for organization and help desk administrators are created.

- Default Access Control Instructions (ACIs) for those administrator entries are set up.



Before You Begin

1. You can use the version of `ldapmodify` that comes with Directory Server 5.x, or you can use the version that comes with DSAME. If your Directory Server is installed on a computer system other than the one where DSAME services are installed, you can use the `ldapmodify` utility that comes with DSAME. You'll find `ldapmodify` in this directory of the DSAME installation:

   ```
   DSAME_root\tools
   ```

   To run commands in the following procedures, open a DOS prompt window and set the path to the ldapmodify tool, for example:

   ```
   set PATH=DSAME_root\tools;%PATH%"
   ```

2. DSAME provides two different LDIF files to help you make the necessary modifications. Determine which file and instructions you should use.

   - If the DSAME default organization is at any level below the root suffix of your directory tree, then use the instructions in the section " To Load the `installExisting.ldif` File."

- If your root suffix is the same as the DSAME default organization, then use the instructions in the section "To Load the `installrootorg.ldif` File."

To Load the installExisting.ldif File

1. Go the following the directory:

   cd *DSAME_root*\web-apps\services\WEB-INF\config\ldif

2. Run the following command:

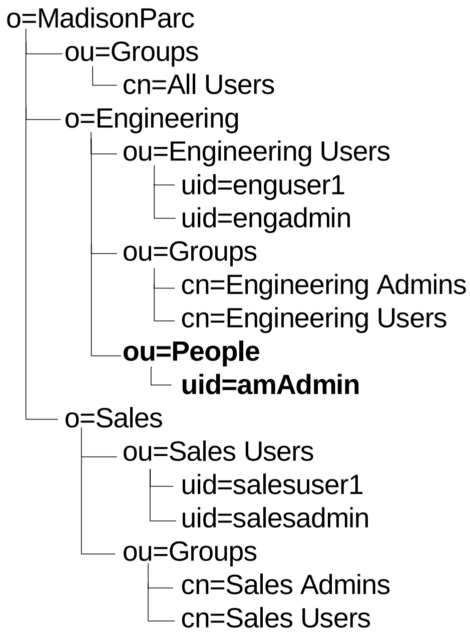
   ```
   ldapmodify -v -c -D "cn=Directory manager" -w password -a -f
   installExisting.ldif
   ```

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

If you encounter error messages regarding “already existing” entries or values for the default organization, see Step 7: (Optional) Add DSAME ACIs to Your Default Organization, on page 179.

The DSAME administration user `amAdmin` will be created under the `ou=People,o=Engineering,o=madisonparc` people container. This is the top level administrator for DSAME. This administrator has read and write access to the entire subtree for `o=madisonparc`. You can add one of your users to this top level administrator role after the DSAME console is started.

Figure 9-2 Directory Information Tree (DIT) Used in Examples in This Chapter.



To Load the installrootorg.ldif File

1. Go the following directory:

   `cd` *DSAME_root*`\web-apps\services\WEB-INF\config\ldif`

2. At the command line, enter the following:

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

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

Step 6: Load DSAME Service Attributes into Your Directory

You can load the `ums.xml` file and all services files with the same command.

1. Go to the following directory:

   DSAME_root`\config\ums`

2. At the command line, enter the following command:

   `amserveradmin` *amAdmin_DN 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` and `amEntrySpecific.xml` files, 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:

DSAME_root`\config\xml`

Step 7: (Optional) Add DSAME ACIs to Your Default Organization

You only need to perform this step if, during installation, you specified an existing organization as your default organization. (By default, DSAME creates one new organization with the an RDN `o=iplanet`. If you accepted the default RDN, skip to the Step 8.)

In this step, you will manually add the DSAME default ACIs to the organization you specified as the default, or first, organization.

1. Copy the DSAME default organization ACIs.

   - If you loaded the file `installExisting.ldif`, then copy the ACI's from the following file:

     DSAME_root`\web-apps\services\WEB-INF\config\installExisting.ldif`

   - If you loaded the file `installrootorg.ldif`, then copy the ACI's from the following file:

     DSAME_root`\web-apps\services\WEB-INF\config\installrootorg.ldif`

2. In the directory where your `ldapmodify` utility is located, enter the following command:

   ```
   ldapmodify -D bind_DN -w password -p port_number -h hostname -a -f
   textfile_name
   ```

Step 8: Start DSAME

At this point, you can start the DSAME server and you will be able to log in to the DSAME Administration Console as `amAdmin` user. You should see the root suffix and organization you specified during installation. In the MadisonParc example, you would see `o=madisonparc` and `o=Engineering`. You will not be able to see the rest of your entries since they do not yet contain the DSAME marker object classes.

To start DSAME

You can start DSAME by using one of the following methods:

- Enter the following commands in a DOS prompt window:

  ```
  cd DSAME_root\bin
  ```

  ```
  amserver start
  ```

- From the Start menu, select Programs > Administrative Tools > Services. In the Services window, right-click the icon for DSAME-*hostname*. From the menu, choose Start.

To Log Into the Administration Console

1. Go to the appropriate URL:

   - Go to the login URL using the form:

     ```
     http://host.domain:port/amserver
     ```

     where *host* is the host name, *domain* is the domain name of the server that runs DSAME services, *port* is the DSAME services port number, and `amserver` is the URI_prefix.

2. In the Login page, enter the Top-Level Administrator user id and password you specified at installation.

Step 9: Add DSAME Object Classes and Attributes to Existing Directory Entries

In this step, you modify your existing directory entries to include the necessary DSAME object classes and attributes. You can think of the DSAME object classes as *markers* that indicate the directory entries you want to manage through DSAME. These markers enable DSAME to recognize the entries in your directory. The object classes contain special attributes that are necessary to achieve delegated administration.

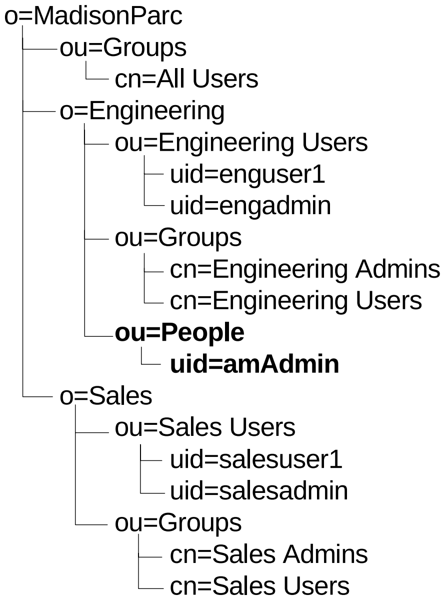
Before You Begin

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 MadisonParc DIT. Figure 9-3 shows two organizations, `Engineering` and `Sales`, under the root. All groups in this example are static groups.

Figure 9-3 The MadisonParc DIT.



Utilities and Scripts You Can Use

You can make these modifications by using iPlanet Directory Server Console, or by using the `ldapmodify or ldif2db` utilities that come with Directory Server. For detailed information on how to make directory changes by using the Console or by using these utilities, see the documentation for iPlanet Directory Server at:

`http://docs.iplanet.com/docs/manuals/directory.html`

You can also use the sample scripts that are included in this product. The sample scripts require Perl 5.x or later. You'll find the sample scripts in the following location:

DSAME_root`\migration`

While these samples should prove useful, they are only tools to assist you in properly formatting the DIT and other data. Each script has one or more variables at the top of the file that must be edited before the script is executed. After each script is executed, it generates an LDAP Data Interchange Format (LDIF) file.

If you encounter error messages regarding "already existing" entries or values, you must add the object classes or attributes manually. See the iPlanet Directory Server documentation for detailed instructions.

Steps for using each sample script are included in this chapter in the instructions for marking each object class.

NOTE Before you can follow the steps for using the sample scripts, you must copy the following sample script files from *DSAME_root*`\migration` into the directory *Directory_Server_root*`\shared\bin`:

- `update-users.pl`
- `update-static-groups.pl`
- `update-assignable-dynamic-groups.pl`
- `update-filtered-groups.pl`
- `update-people.pl`
- `update-ou.pl`
- `update-o.pl`
- `update-groups.pl`

Also note that the changes made by using these scripts cannot be automatically undone. Be sure to back up your data before running each script.

Related Information

Detailed reference information is provided in Appendix A, "DSAME ObjectClasses and Attributes." See for information on the following topics:

- Using DSAME Object Classes as Markers
- Using Alternative Naming Attributes
- DITs That Cannot Be Managed by DSAME
- Object Class and Attribute Descriptions

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 DSAME 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 DSAME to make sure those modifications were done correctly. This second approach is the recommended approach. For example, you may want to add the DSAME object classes for each of your organizations, restart DSAME, and verify that your organizations appear in the DSAME Administration Console. Then add marker classes for groups, check them and so forth.

Step 9a: Mark 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 Step 10b.

In this step you will:

1. Add the following object classes to each organization entry:
   - `iplanet-am-managed-org`
   - `inetDomain`
2. Add the following attribute to each organization entry:
   - `inetDomainStatus`

In the MadisonParc example, these object classes and attributes were automatically added to the default organization, `o=Engineering`, which was the organization specified and created during DSAME installation. The object classes and attributes were manually added to the `o=Sales` organization.

Example:

```
dn: o=Engineering,o=madisonparc
objectClass: top
objectClass: organization
objectClass: madisonparc-org
madisonparc-org-description: Engineering Organization
madisonparc-org-city: Santa Clara
aci: (targetattr = "*")(version 3.0; acl "madisonparc Org admin";
allow (all)groupdn="ldap:///cn=Engineering
Admins,o=Engineering,o=madisonparc";)
objectclass: iplanet-am-managed-org
objectclass: inetDomain
inetDomainStatus: Active

dn: o=Sales,o=madisonparc
objectClass: top
objectClass: organization
objectClass: madisonparc-org
madisonparc-org-description: Sales Organization
madisonparc-org-city: Menlo Park
aci: (targetattr = "*")(version 3.0; acl "madisonparc Org admin";
allow (all)groupdn="ldap:///cn=Sales
Admins,o=Sales,o=madisonparc";)
objectclass: iplanet-am-managed-org
objectclass: inetDomain
inetDomainStatus: Active
...
```

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 DSAME. Example:
   `o=madisonparc`

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

   ```
   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. To check the results, open the `ldif` file that is created (for example: `o-update.ldif`) and verify that the appropriate changes were made.

Step 9b: Mark People Containers

To each people container, add the `iplanet-am-managed-people-container` object class.

Example:

```
dn: ou=Engineering Users,o=Engineering,o=madisonparc
objectClass: top
objectClass: organizationalunit
objectclass: iplanet-am-managed-people-container

...

dn: ou=Sales Users,o=Sales,o=madisonparc
objectClass: top
objectClass: organizationalunit
objectclass: iplanet-am-managed-people-container

...
```

To Mark People Containers Using the Sample Script

1. Copy `update-people.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 DSAME. Example:
   `o=madisonparc`

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. To check the results, open the LDIF file that is created (for example: `people-update.ldif`) and verify that the appropriate changes were made.

Step 9c: Mark Organizational Units

To each *container*, or organizational unit, add the following object class: `iplanet-am-managed-org-unit`

Example:

```
dn: ou=Groups,o=Engineering, o=madisonparc
objectClass: top
objectClass: organizationalunit
objectClass: inetAdmin
objectclass: iplanet-am-managed-org-unit

dn: cn=Engineering Admins,o=Engineering,o=madisonparc
objectClass: top
objectClass: groupofuniquenames
uniquemember: uid=engadmin,ou=Engineering
  Users,o=Engineering,o=madisonparc

dn: cn=Engineering Users,o=Engineering,o=madisonparc
objectClass: top
objectClass: groupofuniquenames
uniquemember: uid=enguser1,ou=Engineering
  Users,o=eng,o=madisonparc
uniquemember: uid=enguser2,ou=Engineering
  Users,o=eng,o=madisonparc
uniquemember: uid=enguser3,ou=Engineering
  Users,o=eng,o=madisonparc
uniquemember: uid=enguser4,ou=Engineering
```

```
    Users,o=eng,o=madisonparc

dn: ou=Groups,o=Sales, o=madisonparc
objectClass: top
objectClass: organizationalunit
objectClass: inetAdmin
objectclass: 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 DSAME. Example:
   `o=madisonparc`

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. To check the results, open the LDIF file that is created (for example: `ou-update.ldif`) and verify that the appropriate changes were made.

Step 9d: Mark Users

To each user entry, add the following object classes:

- `iplanet-am-web-agent-service`
- `iplanet-am-managed-person`
- `iplanet-am-user-service`
- `inetuser`

- `iPlanetPreferences`
- `inetOrgPerson`

Example:

```
dn: ou=Engineering Users,o=Engineering,o=madisonparc
objectClass: top
objectClass: organizationalunit

dn: uid=engadmin,ou=Engineering Users,o=Engineering,o=madisonparc
objectClass: inetorgperson
objectClass: organizationalperson
objectClass: person
objectClass: top
objectClass: iplanet-am-web-agent-service
objectClass: iplanet-am-managed-person
objectClass: iplanet-am-user-service
objectClass: inetuser
objectClass: iPlanetPreferences
objectClass: inetOrgPerson
inetuserstatus:active
cn: engadmin
sn: engadmin
userPassword: engadmin

dn: uid=enguser1,ou=Engineering Users,o=Engineering,o=madisonparc
objectClass: inetorgperson
objectClass: organizationalperson
objectClass: person
objectClass: top
objectClass: madisonparc-user
objectClass: iplanet-am-web-agent-service
objectClass: iplanet-am-managed-person
objectClass: iplanet-am-user-service
objectClass: inetuser
objectClass: iPlanetPreferences
objectClass: inetOrgPerson
inetuserstatus:active
madisonparc-user-id: 11111
madisonparc-user-building: SCA16
cn: enguser1
sn: enguser1
userPassword: enguser1
```

To Mark Users Using the Sample Script

1. Copy `update-users.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 DSAME. Example:
   `o=madisonparc`

3. Set the `$base-component` variable to the base suffix of the DIT. Example:
   `madisonparc`

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

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

5. 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`

6. To check the results, open the LDIF file that is created (for example: `users-update.ldif`) and verify that the appropriate changes were made.

Step 9e: Mark Static Groups

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

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

Example:

```
dn: cn=Engineering Users,o=Engineering,o=madisonparc
objectClass: top
objectClass: groupofuniquenames
objecClass: iplanet-am-managed-static-group
objecClass: ipanet-am-managed-group
uniquemember: uid=enguser1,ou=Engineering
Users,o=eng,o=madisonparc
uniquemember: uid=enguser2,ou=Engineering
Users,o=eng,o=madisonparc
uniquemember: uid=enguser3,ou=Engineering
Users,o=eng,o=madisonparc
```

```
dn: cn=Engineering Users,o=Engineering,o=madisonparc
uniquemember: uid=enguser4,ou=Engineering
Users,o=eng,o=madisonparc

dn: ou=Groups,o=Sales, o=madisonparc
objectClass: top
objectClass: organizationalunit

dn: cn=Sales Admins,o=Sales,o=madisonparc
objectClass: top
objectClass: groupofuniquenames
objecClass: iplanet-am-managed-static-group
objecClass: ipanet-am-managed-group
uniquemember: uid=salesadmin,ou=Sales Users,o=Sales,o=madisonparc

dn: cn=Sales Users,o=Sales,o=madisonparc
objectClass: top
objectClass: groupofuniquenames
objecClass: iplanet-am-managed-static-group
objecClass: ipanet-am-managed-group
uniquemember: uid=salesuser1,ou=Sales Users,o=sales,o=madisonparc
uniquemember: uid=salesuser2,ou=Sales Users,o=sales,o=madisonparc
uniquemember: uid=salesuser3,ou=Sales Users,o=sales,o=madisonparc
uniquemember: uid=salesuser4,ou=Sales Users,o=sales,o=madisonparc
```

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 DSAME. Example: `o=madisonparc`

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. To check the results, open the LDIF file that is created (for example: `static-groups-update.ldif`) and verify that the appropriate changes were made.

Step 9f: Mark Filtered (Dynamic) Groups

In *filtered groups*, users are included in a single group based on their DN.

Add the following object classes (no attribute) to each filtered group:

- `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 DSAME. Example: `o=madisonparc`

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. To check the results, open the LDIF file that is created (for example: `update-filtered-groups-update.ldif`) and verify that the appropriate changes were made.

Step 9g: Mark Assignable Dynamic Groups

An *assignable dynamic group* is similar to a filtered group, but uses a DN in the user entry to point to the group.

Add the following object classes to each assignable dynamic group:

- `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 DSAME. Example: `o=madisonparc`

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 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. To check the results, open the LDIF file that is created (for example: `assignable-dynamic-groups-update.ldif`) and verify that the appropriate changes were made.

Step 9h: Mark Group Containers

Group containers are organizational units (ou) that contain groups. To each group container, 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. Set the $base variable to the base suffix of the DIT to be managed by DSAME. Example: `o=madisonparc`.

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

   ```
   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. To check the results, open the LDIF file that is created (for example: `groups-update.ldif`) and verify that the appropriate changes were made.

Step 10: Load the Modified LDIF Files

After you run the scripts in the previous steps, the various LDIF files are created in the same directory where the Perl scripts are run. Until now, no changes have actually been made in the directory. Before loading the modified files into the directory, it is a good practice to inspect the files to make sure that all DSAME object classes and attributes have been properly added to the existing directory entries. Once you're satisfied that the appropriate changes have been made, load each file using the following `ldapmodify` command:

`ldapmodify -h` *hostname* `-p` *port* `-D` *bind_user*`, -w` *password* `-a -c -f` *filename*`.ldif`

Results of DSAME and Directory Modifications

After making the modifications in the previous steps, all entries in the DIT will be manageable by DSAME. The existing ACIs for the organization administrators do not have to be modified. Even though DSAME 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 DSAME organization administrator roles and assign them to your existing `organizationList` administrators.

Chapter 10

Basic Configurations

This chapter describes configurations typically implemented when you initially deploy iPlanet Directory Server Access Management Edition (DSAME).

Topics in this chapter include:

- Installing the Cross-Domain Single Sign-On Component
- Support for Directory Replication and High Availability
- Support for Directory Replication and High Availability
- Secure Sockets Layer (SSL)

Installing the Cross-Domain Single Sign-On Component

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. Two major components are added to DSAME 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 DSAME services. The default URL for the controller is `http://`*DSAME_host*`:`*DSAME_*`port/`*URI*`/cdcservlet`
- **Cross-Domain Single Sign-On (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.

Installation Overview

To enable cross-domain single sign-on, you must follow this sequence:

1. Install DSAME Services.

   Follow the instructions in Chapter 8, “Simple Installations With No Existing Directory Server” or in Chapter 9, “Using an Existing Directory Server” on appropriate for your needs.

2. Install the CDSSO component on all participating DNS domains.

   DSAME Services and a remote Web Server must already be installed and running. See “To Install the CDSSO Component” in this chapter.

3. Configure the CDSSO component installed on each participating DNS domain.

   See “To Configure the CDSSO Component,” on page 198.

4. (Optional) Configure DSAME web agents to work with the CDSSO component.

   See “To Configure DSAME Web Agents to Work with the CDSSO Component,” on page 198.

To Install the CDSSO Component

DSAME Services and a remote Web Server must already be installed and running. You must have root permissions when you run the DSAME installation program. Be sure all web browsers are closed before starting the installation program.

1. If you’re installing DSAME from the product CD, insert the CD into the drive of the system on which you want to install the software. If you’ve downloaded the product, unzip the product binaries file.

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

   Double-click the `setup.exe` icon.

   Installation messages are written to log files in the following directory:

   ```
   C:\Documents and Settings\Administrator\Local Settings\Temp\
   ```

3. Read the License Agreement. When prompted, **Do you agree to the license terms?** Click Yes (Accept License).

4. In the Components to Be Installed / Uninstalled window, select only DSAME Cross Domain Single Sign-On Component. Deselect all other options, and then click Next.

5. In the Existing Web Server window, a message is displayed saying Existing Web Server has been detected. Click Next to install the Cross-Domain Single Sign-On.

6. In the CDSSO Web Server Information window, provide the following information, and then click Next.

   Host Name: Enter the fully qualified name of the computer system of the Web Server that hosts the participating DNS domain.

   iPlanet Web Server Instance Directory: Enter the full path to the directory where Web Server is installed and the Web Server instance name. It is the Web Server that hosts the participating DNS domain. This Web Server is remote relative to the Web Server that runs DSAME services.

   Web Server Port: Enter the port number of the Web Server specified above.

   Protocol: If the Web Server where the CDSSO component will be installed runs on Secure Socket Layer (SSL) protocol, then select HTTPS. Otherwise, select HTTP.

   CDSSO Deployment URI: The Universal Resource Identifier (URI) indicates where HTML pages used by the CDSSO component are stored. Enter a URI prefix. The default is `/amcdsso`

7. In the DSAME Services Information window, provide the following information, and then click Next:

   DSAME Services Host: Enter the fully qualified name of the computer system where DSAME Management and Policy Services are installed.

   DSAME Services Port: Enter the port number for the Web Server that runs DSAME services.

   Protocol: If the Web Server where the DSAME is installed runs on Secure Socket Layer (SSL) protocol, then select HTTPS. Otherwise, select HTTP.

   Deployment URI: The Universal Resource Identifier (URI) prefix tells the Web Server where to look for HTML pages associated with a DSAME service and also for other web application specific information like classes and jars. Enter the URI prefix specified during DSAME installation. The default is `/amserver`

8. In the Currently Selected Settings window, review the configuration information that you’ve entered. If you need to make changes, click Back. Otherwise, click Next to proceed.

9. In the Ready to Install window, 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 window, click Details for a detailed summary of the configuration information that was processed during Installation. Then click Exit to end the program.

To Configure the CDSSO Component

1. Edit `AMConfig.properties` file of the installed CDSSO component, which is found in the *DSAME_root*`\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 DSAME services. For example:

   ```
   com.iplanet.services.cdsso.CDCURL =
   http(s)://DSAME_host:DSAME_port/services/cdcservlet
   ```

2. Edit `CDSSO.properties` file of the installed CDSSO component, which is found in the *DSAME_root*`\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 DSAME Web Agents to Work with the CDSSO Component

You can configure DSAME 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 `AMConfig.properties` file. Change the `com.iplanet.am.policy.agents.url.authLoginUrl` property to point to the agent's domain's cross-domain single sign-on service URL. For example:

   ```
   com.iplanet.am.policy.agents.url.authLoginUrl =
   http://CDSSO_host:CDSSO_port/CDSSO_URI/cdsso
   ```

2. Add the cross-domain single sign-on service URL to the agent's not-enforced list.

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 DSAME deployment to increase the availability and performance of the DSAME servers and services. You can set up DSAME directory servers in single-supplier or multi-supplier configurations. You can also configure load-balancers such as iPlanet Directory Access Router to work with DSAME.

Replication Considerations

Configure your directory servers for replication before you install DSAME. 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 DSAME database.

When you install DSAME for replication purposes, in each instance of Directory Server and in each instance of DSAME, 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 DSAME deployment. For example, authentication server host names or IP addresses must be the same. This precludes using geographically separated replicated DSAME 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 iPlanet Directory Server. You can access these guides on the Internet at:

`http://docs.iplanet.com/docs/manuals/directory.html`

Configuring DSAME to Support Directory Replication

You can configure DSAME 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 DSAME to Work With Directory Replication,” on page 203 of this manual.

Figure 10-1 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 10-1 Single-Supplier Replication.

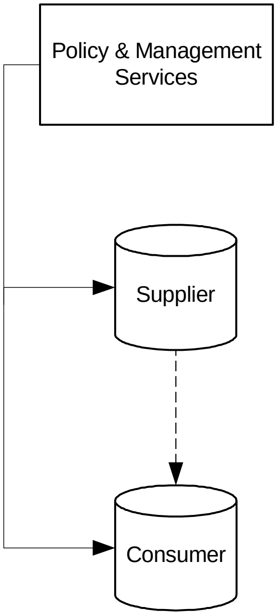


Figure 10-2 illustrates a multi-supplier configuration using multiple instances of DSAME. This configuration provides failover protection as well as high availability, resulting in further enhanced server performance.

Figure 10-2 Multi-Supplier Configuration. Also known as Multi-Master Replication (MMR)

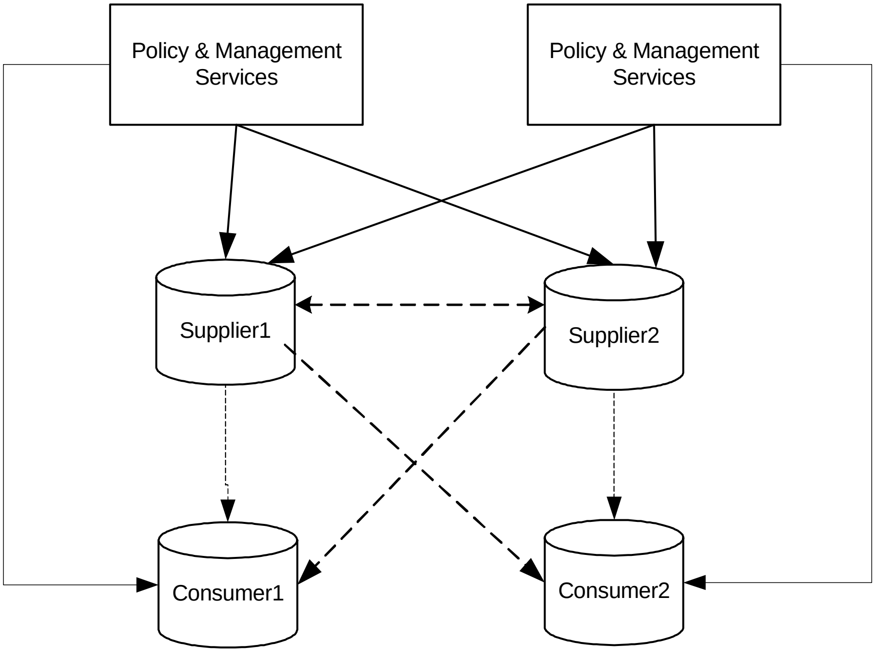
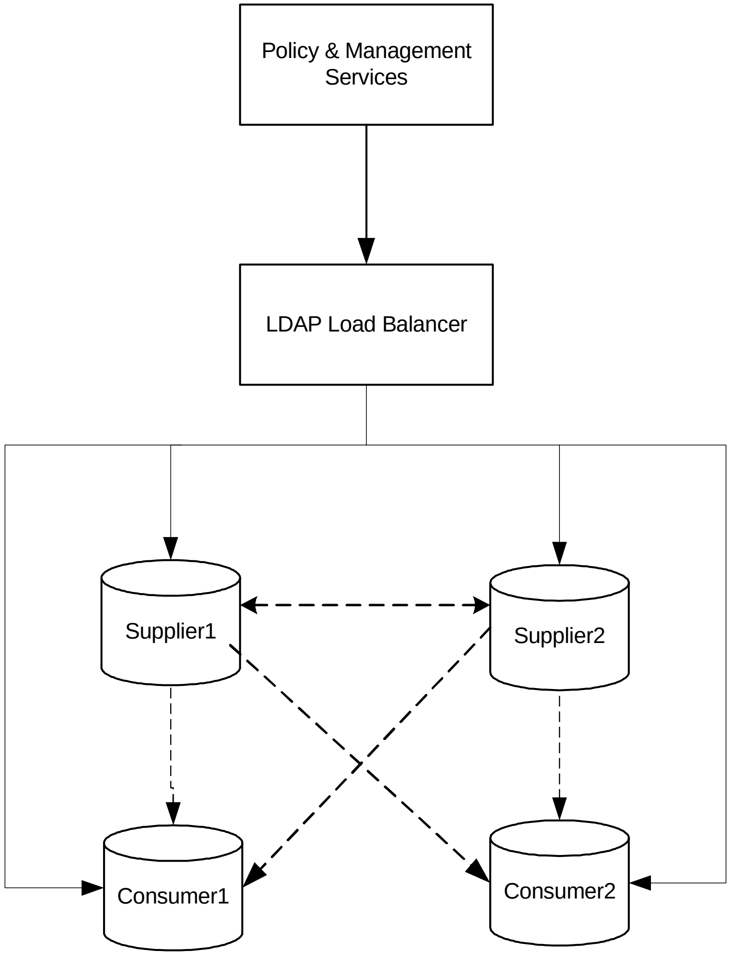


Figure 10-3 illustrates a multi-supplier configuration that includes iPlanet Access Router. This configuration takes full advantage of DSAME support for failover, high availability, and managed load-balancing.

Figure 10-3 Multi-Supplier Replication With Load-Balancer.



To Configure DSAME to Work With Directory Replication

Use the following steps to configure replication at the root or top level of the DSAME directory tree. 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 DSAME with user data from an existing, pre-5.1 Directory Server, you must migrate the user data and make Directory Tree Information (DIT) changes before proceeding. Follow the detailed instructions in Chapter 5, "Using an Existing Directory Server" of this manual. Then skip to step 5.

4. If you are deploying DSAME and Directory Server for the first time, or if you simply do not plan to use existing user data with DSAME, then run the DSAME installation program to install the DSAME 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 "Support for Directory Replication and High Availability," on page 199.

5. In the Web Server where DSAME Management and Policy services are installed, modify the following file:

   DSAME_root`\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:

      - `replica.enabled=true`
      - `com.iplanet.am.replica.retries`

        Specify the number of times DSAME 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 DSAME should allow to elapse between retries.

6. In each DSAME 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 DSAME 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**, enter 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**, enter the host name and port number for your secondary or (supplier) directory. Example: `supplier1.madisonparc.com:399`

   d. Click Submit.

7. In the file *DSAME_root*`\config\ums\serverconfig.xml` specify the host name and port number of the consumer directory you installed in step1. Example:

```
<iPlanetDataAccessLayer>
         <ServerGroup name="default" minConnPool="1"
              maxConnPool="10">
                 <Server name="Server1"
                     host="consumer1.madisonparc.com" port="389"
                        type="SIMPLE" />
```

8. Restart DSAME. Use one of the following methods:

   - In a DOS prompt window, enter the following commands:

     `cd` *DSAME_root*`\bin`

     `amserver stop`

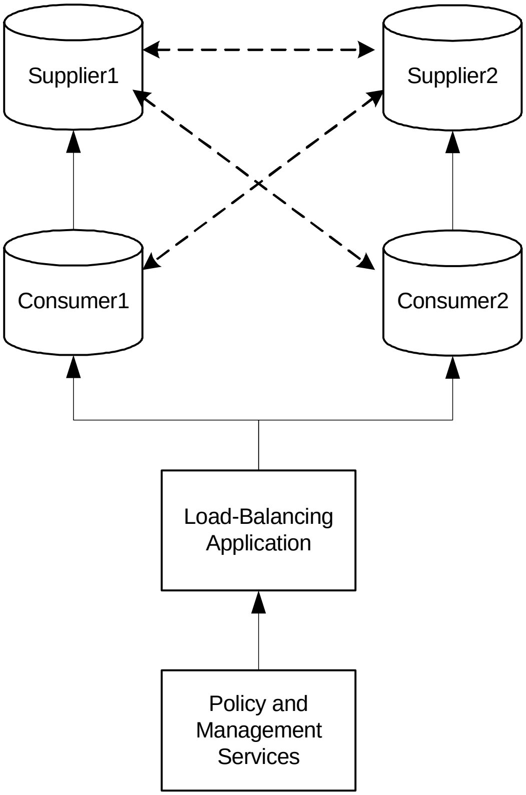
     `amserver start`

   - From the Start menu, select Programs > Administrative Tools > Services. In the Services window, right-click the icon for DSAME-*hostname*. From the menu, choose Restart.

Configuring a Load-Balancer to Work With DSAME

You can configure load-balancer such as iPlanet Directory Access Router to work with DSAME. iPlanet 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 10-4 Multi-Master Replication With Managed Load-Balancer.



Using a load-balancer adds a layer of high availability and directory failover protection beyond the basic level that comes with DSAME. For example, when you configure iPlanet Directory Access Router, you can specify what percentage of the load gets redistributed to each of your servers when one server becomes unavailable. iPlanet Directory Access Router continues to manage request traffic, and begins rejecting client queries when all back-end LDAP servers become unavailable.

By comparison, the DSAME high availability feature cannot be configured or managed as precisely. But when you add a load-balancer such as iPlanet Directory Access Router, DSAME seamlessly directs all requests to the application for total management.

If you choose to install a load-balancer, you must configure DSAME to recognize the application.

To Configure DSAME 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 *iPlanet 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 following file:

   DSAME_root`\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 DSAME 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 DSAME 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**, enter the host name and port number for your primary (consumer) Directory Server using the form:

  iPlanet_DAR_host.domain_name.com:port_number

- In the second field named **LDAP Server and Port**, enter nothing.

d. Click Submit.

4. In the file: *DSAME_root*`\config\ums\serverconfig.xml` specify the host name and port number of the consumer directory you installed in step1. Example:

```
<iPlanetDataAccessLayer>
        <ServerGroup name="default" minConnPool="1"
             maxConnPool="10">
                <Server name="Server1
                    host="iDAR_hostname.madisonparc.com"port="389"
                       type="SIMPLE" />
```

5. Restart DSAME. Use one of the following methods:

- In a DOS prompt window, enter the following commands:

  `cd` *DSAME_root*`\bin`

  `amserver stop`

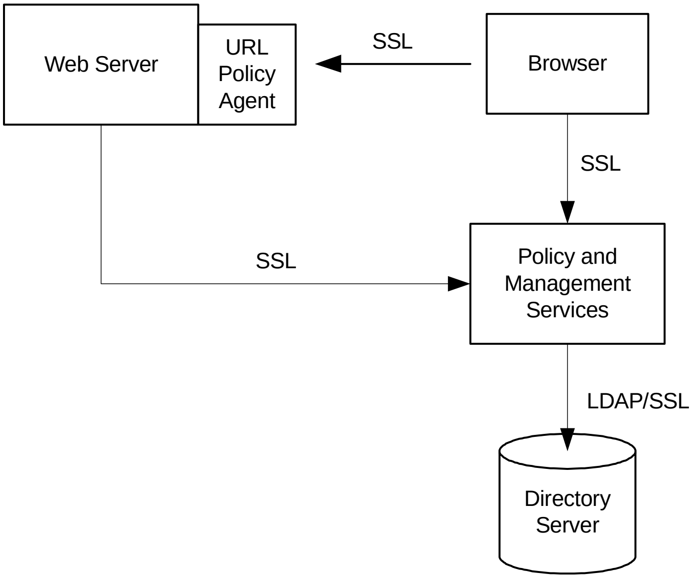
  `amserver start`

- From the Start menu, select Programs > Administrative Tools > Services. In the Services window, right-click the icon for DSAME-*hostname*. From the menu, choose Restart.

Secure Sockets Layer (SSL)

You can use the Secure Sockets Layer (SSL) protocol to provide secure connections between Directory Server and the DSAME services you use in your enterprise. The SSL protocol consists of rules governing server authentication, client authentication, and encrypted communication between servers and clients. When you enable SSL to work with DSAME, the requests and transactions between Directory Server and the DSAME console are encrypted and protected from intrusion by unauthorized entities.

Figure 10-5 How SSL Works in DSAME.



Enabling SSL for DSAME is a two-step process:

- Step 1: Enable LDAP Over SSL
- Step 2: Enable DSAME to Run in SSL Mode

This section explains how to enable SSL for DSAME services and URL access agents. It references the following resources for SSL information, which are appended to this manual for your convenience:

- *iPlanet Directory Server Administrator's Guide*

  Chapter 11, "Managing SSL"

- *iPlanet Web Server Administrator's Guide*

  Chapter 5, "Securing Your Web Browser"

For comprehensive information on SSL and on determining your SSL needs, see Chapter 7, "Designing a Secure Directory" in *iPlanet Directory Server Deployment Guide*. This guide comes with iPlanet Directory Server, and is also available on the Internet at
`http://docs.iplanet.com/docs/manuals/directory.html`

Step 1: Enable LDAP Over SSL

1. Install a Server Certificate in Directory Server.

   Follow the detailed instructions in “Obtaining and Installing Server Certificates,” on page 277 of this manual to perform the following steps. Or access the iPlanet Directory Server documentation on the Internet at `http://docs.iplanet.com/docs/manuals/directory.html`

   - Step 1: Generate a Certificate Request
   - Step 2: Send the Certificate Request
   - Step 3: Install the Certificate (on Directory Server)
   - Step 4: Trust the Certificate Authority (Install the Root CA Certificate)
   - Step 5: Confirm That Your New Certificates Are Installed

2. Activate SSL in the Directory Server.

   Follow the detailed instructions in “Activating SSL,” on page 282 of this manual.

3. In the Web Server that runs DSAME services is installed, in the Web Server console, create a trust database.

   Follow the detailed instructions “Creating a Trust Database,” on page 229.

4. In the Web Server that runs DSAME services, install the root CA Certificate for Directory Server’s server certificate. (This is the certificate you obtained in Step 2.) Follow the detailed instructions in “Requesting and Installing Other Server Certificates,” on page 233.

5. Edit the following DSAME configuration file:

   DSAME_root`\config\ums\serverconfig.xml`

   For the server corresponding to the Directory Server configured for SSL, provide the following values:

   port. Enter the SSL port number you specified in Step 2.

   type. Enter `SSL`.

   Example:

```
<?xml version="1.0" encoding="ISO-8859-1" standalone="yes"?>
<iPlanetDataAccessLayer>
          <ServerGroup name="default" minConnPool="1"
               maxConnPool="10">
```

```
<Server name="Server1"
    host="adam.red.madisonparc.com"
        port="636" type="SSL" />
<User name="User1" type="proxy">
    <DirDN>
        cn=puser,ou=People,o=isp
    </DirDN>
    <DirPassword>
        AQAA5Q9jwkb4pAJ2LGFYRDlqWxXxId+5v4nU
    </DirPassword>
</User>
```

6. Restart DSAME. Use one of the following methods:

   - At the command line, enter the following commands:

     `cd` *DSAME_root*`\bin`

     `amserver stop`

     `amserver start`

   - From the Start menu, select Programs > Administrative Tools > Services. In the Services window, right-click the icon for DSAME-*hostname*. From the menu, choose Restart.

7. If the Directory Server is not yet running, you are prompted for the internal key. Enter the key (password) you specified when creating the trust database in Step 3.

When DSAME starts up, its connection to Directory Server will be secured with SSL.

Step 2: Enable DSAME to Run in SSL Mode

When you enable DSAME to run in SSL mode, requests and transactions between the DSAME console and other SSL-configured Web Servers are encrypted and protected from intrusion by unauthorized entities.

1. Login to DSAME as Super Administrator.

2. In Service Name column, choose DSAME Platform.

3. In the Server List box:

   a. Remove this DSAME server from the list. First select its name in the list, and then click Remove.

   b. Change Protocol to `https` (instead of `http`).

   c. To add the same server with `https`, click Add.

4. Edit the following DSAME configuration file:
   DSAME_root`\bin\AMConfig.properties`

   Modify values for the following to reflect the HTTPS protocol and new port number (if the port number was changed):

   - `com.iplanet.am.server.protocol`
   - `com.iplanet.am.server.port`
   - `com.iplanet.am.profile.port`
   - `com.iplanet.am.naming.url`
   - `com.iplanet.am.notification.url`

5. In the Web Server that runs DSAME services, using the Web Server console, obtain and install a server certificate if one is not already installed.

NOTE In the following substeps, the following warning message may display:

“Warning: Manual edits not loaded,”

In this case, click the Apply link in the upper right corner of the console, and then click Load Configuration Files

   a. To obtain a server certificate, follow the detailed instructions for “Requesting Other Server Certificates,” on page 234.

   b. To install the server certificate, follow the detailed instructions for “Installing Other Server Certificates,” on page 236.

6. In the Web Server console, select the Web Server that runs DSAME services, and then click Manage.

   a. In the Web Server instance, choose Preferences.

   b. Click Edit Sockets.

   c. In the Security field for the default DSAME port, enter `On`.

   d. Click OK to save the change.

   e. Click Apply.

f. To save changes to Web Server configuration files, click Apply Changes.

7. Restart DSAME. Use one of the following methods:

- In a DOS prompt window, enter the following commands:

  `cd` *DSAME_root*`\bin`

  ```
  amserver stop
  ```

  ```
  amserver start
  ```

- From the Start menu, select Programs > Administrative Tools > Services. In the Services window, right-click the icon for DSAME-*hostname*. From the menu, choose Restart.

Part 4

Appendixes

Appendix A

DSAME ObjectClasses and Attributes

This appendix includes the following topics:

- Using DSAME Object Classes as Markers
- Using Alternative Naming Attributes
- DITs That Cannot Be Managed by DSAME
- Object Class and Attribute Descriptions

Using DSAME Object Classes as Markers

iPlanet Directory Server Access Management Edition (DSAME) defines the following entry types for its user and service management:

- Organization
- Container (Organizational Unit)
- People Container
- Static Group
- Filtered Group
- Assignable Group
- User
- Group Container

The DSAME entry types are manageable entities that are identified by DSAME *marker* object classes in the directory entries. Each entry type represents an abstract object managed by DSAME. An entry type in DSAME does not necessarily match the same type in iDS. For example, an DSAME organization or container (also known as an *organizational unit* in Directory Server) may not be organization or organizational unit in iDS.

When you add a DSAME marker object class to a Directory Server entry, you enable DSAME to manage this entry. For example, if you mark an entry in iDS with the DSAME organization object class `iplanet-am-managed-org`, DSAME will manage this entry as DSAME organization entry.

Using Alternative Naming Attributes

There is a limitation in marking the Directory Server entries with DSAME object classes. You cannot mark two Directory Server entries that have different naming attributes that are not the same as the DSAME entry type. For example, you cannot mark as organizations both `ou=iplanet.com` (which uses the naming attribute of `ou`) and `dc=engineering` (which uses the naming attribute of `dc`).

However, you can mark different entries with the same naming attribute for different DSAME entry types. For example, you can mark entry `ou=Group` as an DSAME container, and also mark entry `ou=People` as an DSAME people container. In this case, both use `ou` as their naming attributes, but are used for different entry types.

DITs That Cannot Be Managed by DSAME

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

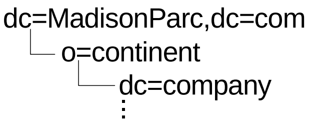
The limitations of DSAME entry types fall into three categories:

- Only One Type of Entry Can be Marked as an Organization

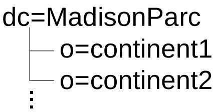
- People Containers Must be Parent Entries for Users
- Only One Organization Description is Allowed in the DSAME XML

Only One Type of Entry Can be Marked as an Organization

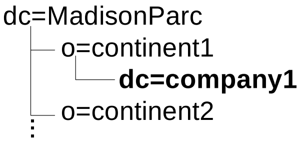
By adding the DSAME `iplanet-am-managed-org` auxiliary class to any entry, DSAME will manage this entry as if it is an organization. But there is a limitation: only one type of entry may be marked as an organization in DSAME. For example, if you have an entry `o=sun`, and another entry `dc=ibm` in your 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.



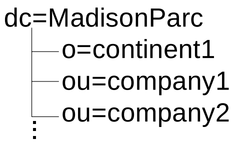
There is one exception to this rule. The entry at the DSAME root suffix does not count as one entry. So in the following example, the DIT structure can indeed be managed by DSAME:



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. See "Organization," on page 222.

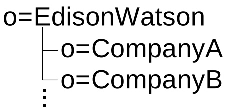
People Containers Must be Parent Entries for Users

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`. See "People Container," on page 223.

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.

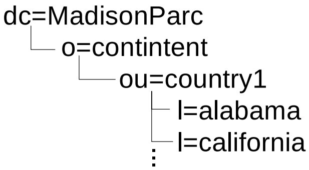


The organization description is defined at the root level (`o=Edison-Watson`), and not at the organization level. By default, the UI for both CompanyA and CompanyB must be identical. Also, all services globally define attributes to be of the subschema type `user`. So if CompanyA has attributes for its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

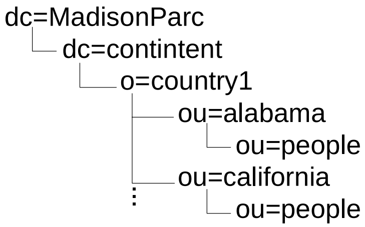
As a workaround, you can modify the ACIs to work for user display. However, this workaround will not address the attributes in Search and Create windows.

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:



Object Class and Attribute Descriptions

Organization

Object Class
`iplanet-am-managed-org`

Description
This entry type is used to manage DSAME organization entries. An DSAME DIT always starts with an organization. It usually maps to an organization or organizational unit in a Directory Server DIT.

Can Contain
suborganizations, people containers, containers (organizational units), roles, groups, group containers.

Other Required Object Class
`inetDomain`

Attributes
`inetDomainStatus :Active`

Container (Organizational Unit)

Object Class

`iplanet-am-managed-org-unit`

Description

This is referred to as a container in DSAME; it is usually mapped to an organizational unit in Directory Server. A container is functionally the same as an organization.

Can Contain

sub-organizations, people containers, containers, roles, groups.

People Container

Object Class

`iplanet-am-managed-people-container`

Description

A people container in DSAME is an organizational unit which is a parent for user entries. User entries can only be managed under a people container.

Can Contain

sub-people containers, users

Static Group

Object Classes

`iplanet-am-managed-static-group`

Description

This type of entry is usually mapped to a static group in Directory Server.

Can Contain

filtered or static sub-groups

Other Required Object Class

`iplanet-am-managed-group`

`iplanet-am-groupofuniquenames`

Attributes

`iplanet-am-group-subscribable`

Set to true if the group is subscribable by user otherwise false.

Assignable Dynamic Group

Object Classes

`iplanet-am-assignable-group`

Description

This type of entry is usually mapped to a filtered group in Directory Server. It describes a special group containing filtered uids. Each user in the group has to have the member-of attribute set to the group.

Can Contain

filtered or assignable groups

Other Required Object Class

`iplanet-am-managed-managed-group`

Attributes

`iplanet-am-group-subscribable`

Set to true if the group is subscribable by user, otherwise false.

Filtered Group

Object Class

`iplanet-am-managed-group`

Description

This entry type is usually mapped to a filtered group in Directory Server.

Can Contain

sub-groups

Other Required Object Class

`iplanet-am-managed-filtered-group`

User

Object Class

`iplanet-am-managed-person`

Description

A user entry in DSAME is a leaf node. It represents a user in an organization manageable by DSAME. It is always mapped to a user entry in Directory Server.

Other Required Object Classes

`inetOrgPerson`

`iPlanetPreferences`

`iplanet-am-user-service`

Other Optional Object Classes

`iplanet-am-logging-service`

`iplanet-am-platform-service`

`iplanet-am-session-service`

`iplanet-am-web-agent-service` (only for URL access)

Attributes

`inetUserStatus`

Set to `Active` if the user is able to login, or `InActive` if they are disabled. If this attribute is not present then they are active.

`iplanet-am-modifiable-by`

Set to the DN of the role of the admin who can create and delete this user.

`iplanet-am-static-group-dn`

Set to the DN of the role of the admin for the static group. This allows the administrator to manage this user.

Appendix B

Securing Your Web Server

This appendix is excerpted from the iPlanet Web Server Administrator's Guide. For your convenience, Chapter 5 of the Guide is reproduced here in its entirety. To view the full online manual on the Internet, go to `http://docs.iplanet.com/docs/manuals/enterprise.html`

This chapter describes how to activate the various security features designed to safeguard your data, deny intruders access, and allow access to those you want. iPlanet Web Server 6.0 incorporates the security architecture of all iPlanet servers: it's built on industry standards and public protocols for maximum interoperability and consistency.

Before reading this chapter you should be familiar with the basic concepts of public-key cryptography. These concepts include encryption and decryption; public and private keys; digital certificates; and the encryption protocols. For more information, see *Introduction to SSL* located at:

`http://docs.iplanet.com/docs/manuals/security/sslin/index.html`

The process of securing your web server will be explained in detail in the following sections:

- Requiring Authentication
- Creating a Trust Database
- Requesting and Installing a VeriSign Certificate
- Requesting and Installing Other Server Certificates
- Migrating Certificates When You Upgrade
- Managing Certificates
- Installing and Managing CRLs and CKLs
- Setting Security Preferences

- Using External Encryption Modules
- Setting Client Security Requirements
- Setting Stronger Ciphers
- Considering Additional Security Issues

Requiring Authentication

Authentication is the process of confirming an identity. In the context of network interactions, authentication is the confident identification of one party by another party. Certificates are one way of supporting authentication.

Using Certificates for Authentication

A certificate consists of digital data that specifies the name of an individual, company, or other entity, and certifies that the public key, included in the certificate, belongs to that entity. Both clients and servers can have certificates.

A certificate is issued and digitally signed by a Certificate Authority, or CA. The CA can be a company that sells certificates over the Internet, or it can be a department responsible for issuing certificates for your company's intranet or extranet. You decide which CAs you trust enough to serve as verifiers of other people's identities.

In addition to a public key and the name of the entity identified by the certificate, a certificate also includes an expiration date, the name of the CA that issued the certificate, and the "digital signature" of the issuing CA. For more information regarding the content and format of a certificate, see *Introduction to SSL*

NOTE A server certificate must be installed before encryption can be activated.

Server Authentication

Server authentication refers to the confident identification of a server by a client; that is, identification of the organization assumed to be responsible for the server at a particular network address.

Client Authentication

Client authentication refers to the confident identification of a client by a server; that is, identification of the person assumed to be using the client software. Clients can have multiple certificates, much like a person might have several different pieces of identification.

Virtual Server Certificates

You can have a different certificate database per virtual server. Each virtual server database can contain multiple certificates. Virtual servers can also have different certificates within each instance.

Creating a Trust Database

Before requesting a server certificate, you must create a trust database. In iPlanet Web Server the Administration Server and each server instance can have its own trust database. The trust database should only be created on your local machine.

When you create the trust database, you specify a password that will be used for a key-pair file. You will also need this password to start a server using encrypted communications. For a list of guidelines to consider when changing a password, see "Changing Passwords or PINs", on page 217.

In the trust database you create and store the public and private keys, referred to as your key-pair file. The key-pair file is used for SSL encryption. You will use the key-pair file when you request and install your server certificate. The certificate is stored in the trust database after installation. The key-pair file is stored encrypted in the following directory:

```
server_root/alias/<serverid-hostname>-key3.db
```

The Administration Server can only have one trust database. Each server instance can have its own trust database. Virtual servers are covered by the trust database created for their server instance.

Creating a Trust Database

To create a trust database, perform the following steps:

1. Access either the Administration Server or the Server Manager and choose the Security tab.

   For the Server Manager you must first select the server instance from the drop-down list.

2. Click on the Create Database link.
3. Enter a password for the database.
4. Repeat.
5. Click OK.
6. For the Server Manager, click Apply, and then Restart for changes to take effect.

Using password.conf

By default, the web server prompts the administrator for the key database password before starting up. If you want to be able to restart an unattended web server, you need to save the password in a `password.conf` file. Only do this if your system is adequately protected so that this file and the key databases are not compromised.

Normally, you cannot start an Unix SSL-enabled server with the `/etc/rc.local` or the `etc/inittab` files because the server requires a password before starting. Although you can start an SSL-enabled server automatically if you keep the password in plain text in a file, this is not recommended. The server's `password.conf` file should be owned by root or the user who installed the server, with only the owner having read and write access to them.

On Unix, leaving the SSL-enabled server's password in the `password.conf` file is a large security risk. Anyone who can access the file has access to the SSL-enabled server's password. Consider the security risks before keeping the SSL-enabled server's password in the `password.conf` file.

On NT, if you have an NTFS file system, you should protect the directory that contains the `password.conf` file by restricting its access, even if you do not use the file. The directory should have read / write permissions for the administration server user and the web server user. Protecting the directory prevents others from creating a false `password.conf` file. You cannot protect directories or files on FAT file systems by restricting access to them.

Start an SSL-Enabled Server Automatically

If security risks are not a concern for you, follow these steps to start your SSL-enabled server automatically:

1. Make sure SSL is on.

2. Create a new `password.conf` file in the `config` subdirectory of the server instance.

   - If you are using the internal PKCS#11 software encryption module that comes with the server, enter the following information:

     ```
     internal:your_password
     ```

   - If you are using a different PKCS#11 module (for hardware encryption or hardware accelerators), specify the name of the PKCS#11 module, followed with the password. For example:

     ```
     nFast:your_password
     ```

3. Stop and restart your server for the new setting to take effect.

You will always be prompted to supply a password when starting the web server, even after the `password.conf` file has been created.

Requesting and Installing a VeriSign Certificate

VeriSign is iPlanet Web Server's preferred certificate authority. VeriSign's VICE protocol simplifies the certificate request process. VeriSign has the advantage of being able to return their certificate directly to your server.

After creating a certificate trust database for your server, you can request a certificate and submit it to a Certificate Authority (CA). If your company has its own internal CA, request your certificate from them. If you plan to purchase your certificate from a commercial CA, choose a CA and ask for the specific format of the information they require. A list of available certificate authorities including links to their sites, is available on the Request a Certificate page. For more information on what CAs may require, a list of Certificate Authorities is available through both Server Administrator, and Server Manager Security Pages under Request a Certificate.

The Administration Server can have only one server certificate. Each server instance can have its own server certificate. You can select a server instance certificate for each virtual server.

Requesting a VeriSign Certificate

To request a VeriSign Certificate, perform the following steps:

1. Access either the Administration Server or the Server Manager and choose the Security tab.

   For the Server Manager you must first select the server instance from the drop-down list.
2. Click the Request VeriSign Certificate link.
3. Review the steps required.
4. Click Get Certificate.
5. Follow the VeriSign procedure.

Installing a VeriSign Certificate

If you request and receive approval for a VeriSign certificate, it should appear in the drop-down list of the Install VeriSign Certificate page in one to three days. To install a VeriSign Certificate, perform the following steps:

1. Access either the Administration Server or the Server Manager and choose the Security tab.

   For the Server Manager you must first select the server instance from the drop-down list.
2. Click the Install VeriSign Certificate link.
3. Choose internal (software) from the drop-down list for cryptographic module, unless you will use an external encryption module.
4. Enter your Key Pair File Password or PIN.
5. Select the Transaction ID to Retrieve from the drop-down list.
6. You will usually want the last one.
7. Click Install.
8. For the Server Manager, click Apply, and then Restart for changes to take effect.

Requesting and Installing Other Server Certificates

Besides VeriSign, you can request and install certificates from other certificate authorities. A list of CAs is available through both Server Administrator, and Server Manager Security Pages under Request a Certificate. Your company or organization may provide its own internal certificates. This section describes how you would request and install these other types of server certificates.

Required CA Information

Before you begin the request process, make sure you know what information your CA requires. Whether you are requesting a server certificate from a commercial CA or an internal CA, you need to provide the following information:

- **Common Name** must be the fully qualified hostname used in DNS lookups (for example, *www.iplanet.com*). This is the hostname in the URL that a browser uses to connect to your site. If these two names don't match, a client is notified that the certificate name doesn't match the site name, creating doubt about the authenticity of your certificate. Some CAs might have different requirements, so it's important to check with them.
- You can also enter wildcard and regular expressions in this field if you are requesting a certificate from an internal CA. Most vendors would not approve a certificate request with a wildcard or regular expression entered for common name.
- **Email Address** is your business email address. This is used for correspondence between you and the CA.
- **Organization** is the official, legal name of your company, educational institution, partnership, and so on. Most CAs require that you verify this information with legal documents (such as a copy of a business license).
- **Organizational Unit** is an optional field that describes an organization within your company. This can also be used to note a less formal company name (without the *Inc.*, *Corp.*, and so on).
- **Locality** is an optional field that usually describes the city, principality, or country for the organization.
- **State or Province** is usually required, but can be optional for some CAs. Note that most CAs won't accept abbreviations, but check with them to be sure.

- **Country** is a required, two-character abbreviation of your country name (in ISO format). The country code for the United States is US.

All this information is combined as a series of attribute-value pairs called the distinguished name (DN), which uniquely identifies the subject of the certificate.

If you are purchasing your certificate from a commercial CA, you must contact the CA to find out what additional information they require before they issue a certificate. Most CAs require that you prove your identity. For example, they want to verify your company name and who is authorized by the company to administer the server, and they might ask whether you have the legal right to use the information you provide.

Some commercial CAs offer certificates with greater detail and veracity to organizations or individuals who provide more thorough identification. For example, you might be able to purchase a certificate stating that the CA has not only verified that you are the rightful administrator of the www.iplanet.com computer, but that you are a company that has been in business for three years, and have no outstanding customer litigation.

Requesting Other Server Certificates

To request a certificate, perform the following steps:

1. Access either the Administration Server or the Server Manager and choose the Security tab.

   For the Server Manager you must first select the server instance from the drop-down list.

2. Click the Request a Certificate link.

3. Select if this is a new certificate or a certificate renewal.

   Many certificates expire after a set period of time, such as six months or a year. Some CAs will automatically send you a renewal.

4. Perform the following steps to specify how you want to submit the request for the certificate:

   - If the CA expects to receive the request in an email message, check CA Email and enter the email address of the CA. For a list of CAs, click List of available certificate authorities.

- If you are requesting the certificate from an internal CA that is using Netscape Certificate Server, click CA URL and enter the URL for the Certificate Server. This URL should point to the certificate server's program that handles certificate requests. A sample URL might be: `https://CA.mozilla.com:444/cms`.

5. Select the cryptographic module for the key-pair file you want to use when requesting the certificate from the drop-down list.

6. Enter the password for your key-pair file.

   This is the password you specified when you created the trust database, unless you selected a cryptographic module other than the internal module. The server uses the password to get your private key and encrypt a message to the CA. The server then sends both your *public key* and the encrypted message to the CA. The CA uses the public key to decrypt your message.

7. Enter your identification information.

   The format of this information varies by CA. For a general description of these fields, a list of Certificate Authorities is available through both Server Administrator, and Server Manager Security Pages under Request a Certificate. Note that most of this information usually isn't required for a certificate renewal.

8. Double-check your work to ensure accuracy.

   The more accurate the information, the faster your certificate is likely to be approved. If your request is going to a certificate server, you'll be prompted to verify the form information before the request is submitted.

9. Click OK.

10. For the Server Manager, click Apply, and then Restart for changes to take effect.

The server generates a certificate request that contains your information. The request has a digital signature created with your private key. The CA uses a digital signature to verify that the request wasn't tampered with during routing from your server machine to the CA. In the rare event that the request is tampered with, the CA will usually contact you by phone.

If you choose to email the request, the server composes an email message containing the request and sends the message to the CA. Typically, the certificate is then returned to you via email. If instead you specified a URL to a certificate server, your server uses the URL to submit the request to the Certificate Server. You might get a response via email or other means depending on the CA.

The CA will notify you if it agrees to issue you a certificate. In most cases, the CA will send your certificate via email. If your organization is using a certificate server, you may be able to search for the certificate by using the certificate server's forms.

NOTE Not everyone who requests a certificate from a commercial CA is given one. Many CAs require you to prove your identity before issuing you a certificate. Also, it can take anywhere from one day to two months to get approval. You are responsible for promptly providing all the necessary information to the CA.

Once you receive the certificate, you can install it. In the meantime, you can still use your server without SSL.

Installing Other Server Certificates

When you receive your certificate back from the CA, it will be encrypted with your public key so that only you can decrypt it. Only by entering the correct password for your trust database, can you decrypt and install your certificate.

There are three types of certificates:

- Your own server's certificate to present to clients
- A CA's own certificate for use in a certificate chain
- A trusted CA's certificate

A certificate chain is a hierarchical series of certificates signed by successive certificate authorities. A CA certificate identifies a certificate authority (CA) and is used to sign certificates issued by that authority. A CA certificate can in turn be signed by the CA certificate of a parent CA, and so on, up to a root CA.

NOTE If your CA doesn't automatically send you their certificate, you should request it. Many CAs include their certificate in the email with your certificate, and your server installs both certificates at the same time.

When you receive a certificate from the CA, it will be encrypted with your public key so that only you can decrypt it. The server will use the key-pair file password you specify to decrypt the certificate when you install it. You can either save the email somewhere accessible to the server, or copy the text of the email and be ready to paste the text into the Install Certificate form, as described here.

Installing a Certificate

To install a certificate, perform the following steps:

1. Access either the Administration Server or the Server Manager and choose the Security tab.

   For the Server Manager you must first select the server instance from the drop-down list.

2. Click the Install Certificate link.
3. Check the type of certificate you are installing:
   - This Server is for a single certificate associated only with your server.
   - Server Certificate Chain is for a CA's certificate to include in a certificate chain.
   - Trusted Certificate Authority (CA) is for a certificate of a CA that you want to accept as a trusted CA for client authentication.
4. Select the Cryptographic Module from the drop-down list.
5. Enter the Key-Pair File Password.
6. Leave the a name for the certificate field blank if it will be the only one used for this server instance, unless:
   - Multiple certificates will be used for virtual servers
   - Enter a certificate name unique within the server instance
   - Cryptographic modules other than internal are used
7. Enter a certificate name unique across all server instances within a single cryptographic module

   If a name is entered, it will be displayed in the Manage Certificates list, and should be descriptive. For example, "United States Postal Service CA" is the name of a CA, and "VeriSign Class 2 Primary CA" describes both a CA and the type of certificate. When no certificate name is entered, the default value is applied.

8. Select either:

   - Message is in this file and enter the full pathname to the saved email
   - Message text (with headers) and paste the email text

     If you copy and paste the text, be sure to include the headers “Begin Certificate” and “End Certificate”—including the beginning and ending hyphens.

9. Click OK.

10. Select either:

    - Add Certificate if you are installing a new certificate.
    - Replace Certificate if you are installing a certificate renewal.

11. For the Server Manager, click Apply, and then Restart for changes to take effect.

The certificate is stored in the server’s certificate database. The filename will be `<alias>-cert7.db`. For example:

`https-`*`serverid-hostname`*-cert7.db

Migrating Certificates When You Upgrade

If you are upgrading from iPlanet Web Server 4.x, your files, including your trust and certificate databases, will be updated automatically.

If you are upgrading from an Enterprise Server 3.x, you will need to migrate your trust and certificate databases. Make sure that iPlanet Web Server 6.0 Administration Server user has read and write permissions on the old 3.x database files. The files are `<alias>-cert.db` and `<alias>-key.db`, located in the `<3.`*x*`_server_root>/alias` directory.

Key-pair files and certificates are migrated only if your server has security enabled. You can also migrate keys and certificates by themselves using the Security tabs in the Administration Server page and the Server Manager page.

In previous versions, a certificate and key-pair file was referred to by an alias which could be used by multiple server instances. The Administration Server managed all the aliases and their constituent certificates. In iPlanet Web Server 6.0, the Administration Server and each server instance has its own certificate and key-pair file, referred to as a trust database instead of an alias.

You manage the trust database and its constituent certificates, including the server certificate and all the included Certificate Authorities, from the Administration Server for its self, and from the Server Manager for server instances. The certificate and key-pair database files are now named after the server instance that uses them. If in the previous version, multiple server instances shared the same alias, when migrated the certificate and key-pair file are renamed for the new server instance.

The entire trust database associated with the server instance is migrated. All the Certificate Authorities listed in your previous database are migrated to the iPlanet Web Server 6.0 database. If duplicate CAs occur, use the previous CA until it expires. Do not attempt to delete duplicate CAs.

Migrating a Certificate

To migrate a certificate, perform the following steps:

1. From your local machine, access either the Administration Server or the Server Manager and choose the Security tab.

   For the Server Manager you must first select the server instance from the drop-down list.

2. Choose:

   - Migrate 3.X Certificates link from the Administration Server
   - Migrate Certificate link from the Server Manager.

3. Enter the 3.6 Server Root.
4. Enter the Alias.
5. Enter the Password.
6. Click OK.
7. For the Server Manager, click Apply, and then Restart for changes to take effect.

Using the Built-in Root Certificate Module

The dynamically loadable root certificate module included with iPlanet Web Server 6.0 contains the root certificates for many CAs, including VeriSign. The root certificate module allows you to upgrade your root certificates to newer versions in a much easier way than before. In the past, you were required to delete the old root certificates one at a time, then install the new ones one at a time. To install well-known CA certificates, you can now simply update the root certificate module file to a newer version as it becomes available through future versions of iPlanet Web Server, or in Service Packs.

Because the root certificate is implemented as a PKCS#11 cryptographic module, you can never delete the root certificates it contains, and the option to delete will not be offered when managing these certificates. To remove the root certificates from your server instances, you can disable the root certificate module by deleting the following in the server's `alias` file:

- `libnssckbi.so` (on most Unix platforms)
- `libnssckbi.sl` (on HP-UX)
- `nssckbi.dll` (on NT)

If you later wish to restore the root certificate module, you can copy the extension from `bin/https/lib` (Unix and HP) or `bin\https\bin` (NT) back into the `alias` subdirectory.

You can modify the trust information of the root certificates. The trust information is written to the certificate database for the server instance being edited, not back to the root certificate module itself.

Managing Certificates

You can view, delete, or edit the trust settings of the various certificates installed on your server. This includes your own certificate and certificates from CAs.

To manage certificate lists, perform the following steps:

1. Access either the Administration Server or the Server Manager and choose the Security tab.

   For the Server Manager you must first select the server instance from the drop-down list.

2. Click the Manage Certificates link.

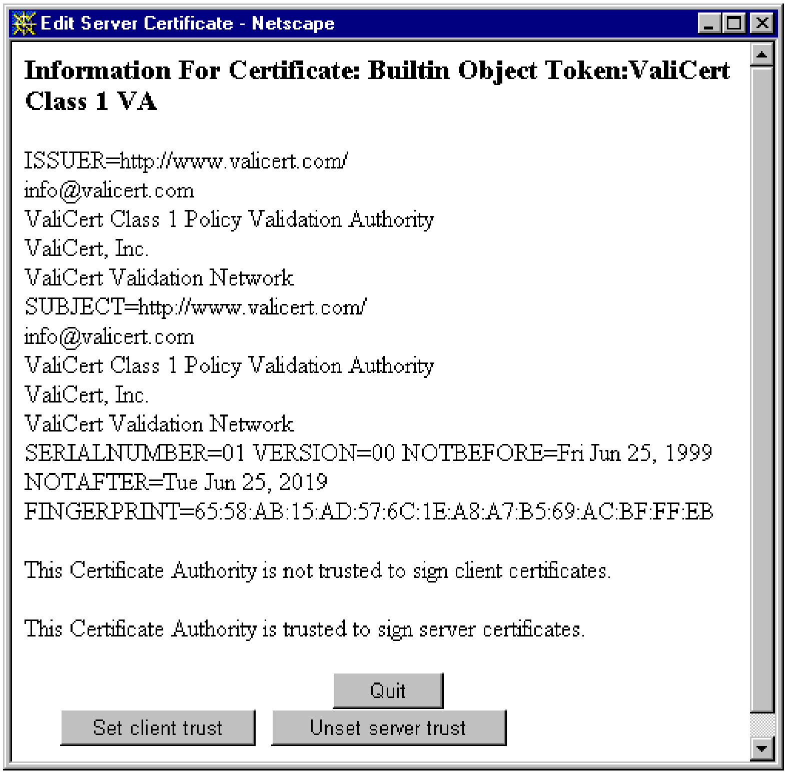
   - If you are managing a certificate for a default configuration using the internal cryptographic module, a list of all installed certificates with their type and expiration date is displayed. All certificates are stored in the directory *`server_root/`*`alias.`

- If you are using an external cryptographic module, such as a hardware accelerator, you will first need to enter your password for each specific module and click OK. The certificate list will update to include certificates in the module.

3. Click the Certificate Name you wish to manage.

   An Edit Server Certificate page appears with management options for that type of certificate. Only CA certificates will allow you to set or unset client trust. Some external cryptographic modules will not allow certificates to be deleted.

Figure B-1 Edit Server Certificate



Information For Certificate: Builtin Object Token:ValiCert Class 1 VA

ISSUER=http://www.valicert.com/
info@valicert.com
ValiCert Class 1 Policy Validation Authority
ValiCert, Inc.
ValiCert Validation Network
SUBJECT=http://www.valicert.com/
info@valicert.com
ValiCert Class 1 Policy Validation Authority
ValiCert, Inc.
ValiCert Validation Network
SERIALNUMBER=01 VERSION=00 NOTBEFORE=Fri Jun 25, 1999
NOTAFTER=Tue Jun 25, 2019
FINGERPRINT=65:58:AB:15:AD:57:6C:1E:A8:A7:B5:69:AC:BF:FF:EB

This Certificate Authority is not trusted to sign client certificates.

This Certificate Authority is trusted to sign server certificates.

4. In the Edit Server Certificate window you may select:

   - Delete Certificate or Quit for certificates obtained internally
   - Set client trust, Unset server trust, or Quit for CA certificates

5. Click OK.
6. For the Server Manager, click Apply, and then Restart for changes to take effect.

Certificate information includes the owner and who issued it.

Trust settings allow you to set client trust or unset server trust. For LDAP server certificates the server must be trusted.

Installing and Managing CRLs and CKLs

Certificate revocation lists (CRLs) and compromised key lists (CKLs) make known any certificates and keys that either client or server users should no longer trust. If data in a certificate changes, for example, a user changes offices or leaves the organization before the certificate expires, the certificate is revoked, and its data appears in a CRL. If a key is tampered with or otherwise compromised, the key and its data appear in a CKL. Both CRLs and CKLs are produced and periodically updated by a CA.

Installing a CRL or CKL

To obtain a CRL or CKL from a CA, perform the following steps:

1. Obtain the CA’s URL for downloading CRLs or CKLs.
2. Enter the URL in your browser to access the site.
3. Follow the CA's instructions for downloading the CRL or CKL to a local directory.
4. Access either the Administration Server or the Server Manager and choose the Security tab.

   For the Server Manager you must first select the server instance from the drop-down list.
5. Click the Install CRL/CKLs link.
6. Select either:
   - Certificate Revocation List
   - Compromised Key List
7. Enter the full path name to the associated file.

8. Click OK.

   - If you selected Certificate Revocation List, the Add Certificate Revocation List page will appear listing CRL information.
   - If you selected Compromised Key List, the Add Compromised Key List page will appear listing CKL information.

NOTE If a CRL or CKL list already exists in the database, a Replace Certificate Revocation List or Replace Compromised Key List page will appear.

9. Click Add.
10. Click OK.
11. For the Server Manager, click Apply, and then Restart for changes to take effect.

Managing CRLs and CKLs

To manage CRLs and CKLs, perform the following steps:

1. Access either the Administration Server or the Server Manager and choose the Security tab.

   For the Server Manager you must first select the server instance from the drop-down list.

2. Click the Manage CRL/CKLs link.

   The Manage Certificate Revocation Lists /Compromised Key Lists page appears with all installed Server CRLs and CKLs listed along with their expiration dates.

3. Select a Certificate Name from either the Server CRLs or Server CKLs list.
4. Choose:

   - Delete CRL
   - Delete CKL

5. For the Server Manager, click Apply, and then Restart for changes to take effect.

Setting Security Preferences

Once you have a certificate, you can begin securing your server. Several security elements are provided by iPlanet Web Server.

Encryption is the process of transforming information so it is unintelligible to anyone but the intended recipient. Decryption is the process of transforming encrypted information so that it is intelligible again. iPlanet Web Server 6.0 includes supports SSL and TLS encryption protocols.

A cipher is a cryptographic algorithm (a mathematical function), used for encryption or decryption. SSL and TLS protocols contain numerous cipher suites. Some ciphers are stronger and more secure than others. Generally speaking, the more bits a cipher uses, the harder it is to decrypt the data.

In any two-way encryption process, both parties must use the same ciphers. Because a number of ciphers are available, you need to enable your server for those most commonly used.

During a secure connection, the client and the server agree to use the strongest cipher they can both have for communication. You can choose ciphers from the SSL2, SSL3, and TLS protocols.

NOTE Improvements to security and performance were made after SSL version 2.0; you should not use SSL 2 unless you have clients that are not capable of using SSL 3. Client certificates are not guaranteed to work with SSL 2 ciphers.

The encryption process alone isn't enough to secure your server's confidential information. A key must be used with the encrypting cipher to produce the actual encrypted result, or to decrypt previously encrypted information. The encryption process uses two keys to achieve this result: a public key and a private key. Information encrypted with a public key can be decrypted only with the associated private key. The public key is published as part of a certificate; only the associated private key is safeguarded.

For description of the various cipher suites, and more information about keys and certificates, see *Introduction to SSL.*

To specify which ciphers your server can use, check them in the list. Unless you have a compelling reason not to use a specific cipher, you should check them all. However, you may not wish to enabling ciphers with less than optimal encryption.

CAUTION Do not select “No Encryption, only MD5 message authentication”. If no other ciphers are available on the client side, the server will default to this setting and no encryption will occur.

SSL and TLS Protocols

iPlanet Web Server 6.0 supports the Secure Sockets Layer (SSL) and the Transport Layer Security (TLS) protocols for encrypted communication. SSL and TLS are application independent, and higher level protocols can be layered transparently on them.

SSL and TLS protocols support a variety of ciphers used to authenticate the server and client to each other, transmit certificates, and establish session keys. Clients and servers may support different cipher suites, or sets of ciphers, depending on factors such as which protocol they support, company policies on encryption strength, and government restrictions on export of encrypted software. Among other functions, the SSL and TLS handshake protocols determine how the server and client negotiate which cipher suites they will use to communicate.

Using SSL to Communicate with LDAP

You should require your Administration Server to communicate with LDAP using SSL. To enable SSL on your Administration Server, perform the following steps:

1. Access the Administration Server and choose the Global Settings tab.
2. Click the Configure Directory Service link.
3. Select Yes to use Secure Sockets Layer (SSL) for connections.
4. Click Save Changes.
5. Click OK to change your port to the standard port for LDAP over SSL.

Enabling Security for Connection Groups

You can secure your server’s connection groups by:

- Turning the security on
- Selecting a server certificate for a connection group

- Selecting ciphers

Turning Security On

You must turn security on before you can configure the other security settings for your connection group. You can turn security on when you create a new listen socket, or when you edit an existing listen socket.

Turning Security On When Creating a Listen Socket

To turn security on when creating a new listen socket, perform the following steps:

1. Access the Server Manager and select the server instance the listen socket will be created in from the drop-down list.
2. Select the Preferences tab, if not already displayed.
3. Choose the Add Listen Socket link.

   The Create a Listen Socket page is displayed.
4. Enter the required information and select a default virtual server.
5. Turn Security on using the drop-down list.
6. Click OK
7. Click Apply, and then Restart for changes to take effect.

NOTE You will need to use the Edit Listen Sockets link to configure the security settings after a listen socket is created.

Turning Security On When Editing a Listen Socket

You can also turn security on when editing a listen socket from either the Administration Server or the Server Manager. To turn security on when editing a listen socket, perform the following steps:

1. Access either the Administration Server or the Server Manager and choose the Security tab.

   For the Server Manager you must first select the server instance from the drop-down list.
2. Select the Preferences tab, if not already displayed.
3. Choose the Edit Listen Sockets link.

   The Listen Sockets Table page is displayed.

4. Use the drop-down Action list to select Edit, if not already displayed, for the connection group you want to secure.

5. Use the drop-down list in the Security column to turn security on for the connection group.

6. Click OK.

   The Attributes link will now be displayed in the Security column.

7. For the Server Manager, click Apply, and then Restart for changes to take effect.

Selecting a Server Certificate for a Connection Group

You can configure connection groups in either the Administration Server or the Server Manager to use server certificates you have requested and installed.

NOTE You must have at least one certificate is installed.

To select a server certificate for your connection group to use, perform the following steps:

1. Access either the Administration Server or the Server Manager and choose the Preferences tab.

   For the Server Manager you must first select the server instance from the drop-down list.

2. Click the Edit Listen Sockets link.

   The Listen Socket Table page appears.

3. Use the drop-down Action list to select Edit, if not already displayed, for the connection group you are selecting a certificate for.

4. Use the drop-down list to turn Security on for that connection group, if it is off.

5. Click the Attributes link.

   The Security Settings of Listen Socket page appears.

NOTE If you have an external module installed, the Manage Server Certificates page will appear requiring the external module’s password before you can continue.

6. Select a server certificate from the drop-down CertificateName list for the connection group.

   The list contains all internal and external certificates installed.

7. Click OK

8. For the Server Manager, click Apply, and then Restart for changes to take effect.

Selecting Ciphers

To protect the security of your web server, you should enable SSL. You can enable the SSL 2.0, SSL 3.0, and TLS encryption protocols and select the various cipher suites. SSL and TLS can be enabled on the connection group for the Administration Server. Enabling SSL and TLS on a connection group for the Server Manager will set those security preferences for all virtual servers associated with that connection group.

If you wish to have unsecured virtual servers, they must all be configured to the same connection group with security turned off.

The default settings allow the most commonly used ciphers. Unless you have a compelling reason why you don't want to use a specific cipher suite, you should allow them all. For more information regarding specific ciphers, see *Introduction to SSL*

NOTE You must have at least one certificate installed.

To enable SSL and TLS, perform the following steps:

1. Access either the Administration Server or the Server Manager and choose the Preferences tab.

   For the Server Manager you must first select the server instance from the drop-down list.

2. Click the Edit Listen Sockets link.

   The Listen Socket Table page appears.

3. Use the drop-down Action list to select Edit, if not already displayed, for the connection group you are enabling security for.

4. Use the drop-down list to turn Security on for that connection group, if it is off.

5. Click OK.

   The Attributes link now appears.

6. Click the Attributes link.

   The Security Settings of Listen Socket page appears.

NOTE If you have an external module installed, the Manage Server Certificates page will appear requiring the external module's password before you can continue.

7. Select either:

   - Cipher Default
   - SSL2
   - SSL3 /TLS

8. (Optional) If you selected SSL2 or SSL3/TLS, in the Security Features window either:

   - Accept Allow and the default ciphers
   - Accept Allow and check only desired ciphers, or uncheck unwanted ciphers
   - Uncheck Allow to disable this protocol and all its ciphers

NOTE Check both TLS and SSL3 for Netscape Navigator 6.0. Use the TLS Rollback option for Microsoft Internet Explorer 5.0 and 5.5. TLS must also be enabled on the browser seeking access to your server. For TLS Rollback also check TLS, and make sure both SSL3 and SSL2 are disabled.

9. Click OK to close the Security Features window.

10. Click OK

11. For the Server Manager, click Apply, and then Restart for changes to take effect.

NOTE When you apply changes after turning on security for a connection group, the `magnus.conf` file is automatically modified to show security on, and all virtual servers associated with the connection group are automatically assigned the default security parameters.

Once you have enabled SSL on a server, its URLs use `https` instead of `http`. URLs that point to documents on an SSL-enabled server have this format:

`https://servername.[domain.[dom]]:[port#]`

For example, `https://admin.iplanet.com:443`.

If you use the default secure http port number (443), you don't have to enter the port number in the URL.

Configuring Security Globally

Installing an SSL-enabled server creates directive entries in the `magnus.conf` file (the server's main configuration file) for global security parameters. Security must be set to 'on' for virtual server security settings to work. SSL properties for virtual servers can be found on a per-server basis in the `SSLPARAMS` element of the `server.xml` file.

To set values for your SSL configuration file directives, perform the following steps:

1. Access the Server Manager and select the server instance of the virtual server from the drop-down list.
2. Select the Preferences tab, if not already selected.
3. Choose the Edit Listen Sockets link.
4. Turn Security On for the listen socket you will set values for, if it isn't already on.
5. Click OK.
6. Go to the Magnus Editor link.
7. Select SSL Settings from the drop-down list and click Manage.
8. Enter the values for:
   - SSLSessionTimeout
   - SSLCacheEntires
   - SSL3SessionTimeout
9. Click OK
10. Click Apply, and then Restart for changes to take effect.

These SSL Configuration File Directives are described below:

SSLSessionTimeout

The `SSLSessionTimeout` directive controls SSL2 session caching.

Syntax

```
    SSLSessionTimeout seconds
```

`seconds` is the number of seconds until a cached SSL session becomes invalid. The default value is 100. If the `SSLSessionTimeout` directive is specified, the value of seconds is silently constrained to be between 5 and 100 seconds.

SSLCacheEntries

Specifies the number of SSL sessions that can be cached.

SSL3SessionTimeout

The SSL3SessionTimeout directive controls SSL3 and TLS session caching.

Syntax

```
SSL3SessionTimeout seconds
```

`seconds` is the number of seconds until a cached SSL3 session becomes invalid. The default value is 86400 (24 hours). If the `SSL3SessionTimeout` directive is specified, the value of seconds is silently constrained to be between 5 and 86400 seconds.

NOTE A single connection group on a listen socket must have the same SSLPARAMS; multiple groups can have different SSLPARAMS.

Using External Encryption Modules

iPlanet Web Server 6.0 supports the following methods of using external cryptographic modules such as smart cards or token rings:

- PKCS#11
- FIPS-140

You will need to add the PKCS #11 module before activating the FIPS-140 encryption standard.

Installing the PKCS#11Module

iPlanet Web Server supports Public Key Cryptography Standard (PKCS) #11, which defines the interface used for communication between SSL and PKCS#11 modules. PKCS#11 modules are used for standards-based connectivity to SSL hardware accelerators. Imported certificates and keys for external hardware accelerators are stored in the `secmod.db` file, which is generated when the PKCs#11 module is installed.

Using modutil to Install a PKCS#11 Module

You can install PKCS#11 modules in the form of `.jar` files or object files using the `modutil` tool.

To install the PKCS#11 module using `modutil`, perform the following steps:

1. Make sure all servers, including the Administration server, are turned off.
2. Go to the `server_root/alias directory` containing the databases.
3. Add `server_root/bin/https/admin/bin` to your PATH.
4. Locate `modutil` in `server_root/bin/https/admin/bin`.
5. Set the environment. For example:
    - On Unix: `setenv`
    - `LD_LIBRARY_PATH server_root/bin/https/lib:${LD_LIBRARY_PATH}`
    - On IBM-AIX: `LIBPATH`
    - On HP-UX: `SHLIB_PATH`
    - On NT, add it to the `PATH`

      `LD_LIBRARY_PATH server_root/bin/https/bin`

      You can find the PATH for your machine listed under: `server_root/https-admin/start`.
6. Enter the command: `modutil`.

    The options will be listed.
7. Perform the actions required.

    For example, to add the PCKS#11 module in Unix you would enter:

    `modutil -add` (the name of PCKS#11 file) `-libfile` (your `libfile` for PCKS#11) `-nocertdb -dbdir .` (your db directory)

Using pk12util

The `pk12util` allows you to export certificates and keys from your internal database and to import them into an internal or external PKCS#11 module. You can always export certificates and keys to your internal database, but most external tokens will not allow you to export certificates and keys. By default, `pk12util` uses certificate and key databases named `cert7.db` and `key3.db`.

Exporting with pk12util

To export a certificate and key from an internal database, perform the following steps:

1. Go to the `server_root/alias directory` containing the databases.
2. Add `server_root/bin/https/admin/bin` to your PATH.
3. Locate `pk12util` in `server_root/bin/https/admin/bin`.
4. Set the environment. For example:
    - On Unix: `setenv`
    - `LD_LIBRARY_PATH/server_root/bin/https/lib:${LD_LIBRARY_PATH}`
    - On IBM-AIX: `LIBPATH`
    - On HP-UX: `SHLIB_PATH`
    - On NT, add it to the `PATH`

      `LD_LIBRARY_PATH server_root/bin/https/bin`

      You can find the PATH for your machine listed under: `server_root/https-admin/start`.
5. Enter the command: `pk12util`.

    The options will be listed.
6. Perform the actions required.

    For example, in Unix you would enter:

    ```
    pk12util -o certpk12 -n Server-Cert [-d /server/alias] [-P
    https-test-host]
    ```
7. Enter the database password.
8. Enter `pkcs12` password.

Importing with pk12util

To import a certificate and key into an internal or external PKCS#11 module, perform the following steps:

1. Go to the `server_root/alias directory` containing the databases.
2. Add `server_root/bin/https/admin/bin` to your PATH.
3. Locate `pk12util` in `server_root/bin/https/admin/bin`.
4. Set the environment. For example:
   - On Unix: `setenv`
   - `LD_LIBRARY_PATH/server_root/bin/https/lib:${LD_LIBRARY_PATH}`
   - On IBM-AIX: `LIBPATH`
   - On HP-UX: `SHLIB_PATH`
   - On NT, add it to the `PATH`

     `LD_LIBRARY_PATH server_root/bin/https/bin`

     You can find the PATH for your machine listed under: `server_root/https-admin/start`.
5. Enter the command: `pk12util`.

   The options will be listed.
6. Perform the actions required.

   For example, in Unix you would enter:

   ```
   pk12util -i pk12_sunspot [-d certdir][-h “nCipher”][-P
   https-jones.redplanet.com-jones-]
   ```

   -P must follow the -h and be the last argument.

   Enter the exact token name including capital letters and spaces between quote marks.
7. Enter the database password.
8. Enter `pkcs12` password.Starting the Server with an External Certificate

If you install a certificate for your server into an external PKCS#11 module (for example, a hardware accelerator), the server will not be able to start using that certificate until you edit the `server.xml`, or specify the certificate name as described below.

The server always tries to start with the certificate named “Server-Cert.” However, certificates in external PKCS#11 modules include one of the module’s token names in their identifier. For example, a server certificate installed on an external smartcard reader called “smartcard0” would be named “smartcard0:Server-Cert.”

To start a server with a certificate installed in an external module, you’ll need to specify the certificate name for the connection group it runs on.

Selecting the Certificate Name for a Connection Group

To select the certificate name for the connection group, perform the following steps:

1. Access either the Administration Server or the Server Manager and choose the Preferences tab.

   For the Server Manager you must first select the server instance from the drop-down list.

2. Select the Preferences tab, if not already selected.
3. Click the Edit Listen Sockets link.

   The Listen Socket Table page appears.

4. Use the drop-down Action list to select Edit, if not already displayed, for the connection group you are enabling security for.
5. Use the drop-down list to turn Security on for that connection group, if it is off.
6. Click OK.

   The Attributes link now appears.

7. Click the Attributes link.

   The Security Settings of Listen Socket page appears.

8. Use the drop-down CertificateName list to select the external server certificate.
9. Click OK
10. For the Server Manager, click Apply, and then Restart for changes to take effect.

You could also tell the server to start with that server certificate instead, by manually editing the `server.xml` file. Change the `servercertnickname` attribute in the SSLPARAMS to:

```
$TOKENNAME:Server-Cert
```

To find what value to use for `$TOKENNAME`, go to the server's Security tab and select the Manage Certificates link. When you log in to the external module where Server-Cert is stored, its certificates are displayed in the list in the `$TOKENNAME:$NICKNAME` form.

NOTE If you did not create a trust database, one will be created for you when you request or install a certificate for an external PKCS#11 module. The default database created has no password and cannot be accessed. Your external module will work, but you will not be able to request and install server certificates. If a default database has been created without a password, use the Security tab Create Database page to set the password.

FIPS-140 Standard

PKCS#11 APIs enable communication with software or hardware modules that perform cryptographic operations. Once PKCS#11 is installed on your server, you can configure iPlanet Web Server to be Federal Information Processing Standards (FIPS)-140 compliant. These libraries are included only in SSL version 3.0.

To enable FIPS-140, perform the following steps:

1. Install the plug-in following the FIPS-140 instructions.
2. Access either the Administration Server or the Server Manager and choose the Preferences tab.

   For the Server Manager you must first select the server instance from the drop-down list.
3. Click the Edit Listen Sockets link.

   The Listen Socket Table page appears.
4. Use the drop-down Action list to select Edit, if not already displayed, for the connection group you are enabling FIPS-140 on.
5. Use the drop-down list to turn Security on for that connection group, if it is off.
6. Click OK.

   The Attributes link now appears.
7. Click the Attributes link.
8. The Security Settings of Listen Socket page appears.

9. Click the SSL3/TLS link.

   The Security Feature window appears.

10. Check Allow: SSL version 3, if it is not already checked.

11. Select the appropriate FIPS-140 cipher suite:

    - (FIPS) DES with 56 bit encryption and SHA message authentication
    - (FIPS) Triple DES with 168 bit encryption and SHA message authentication

12. Click OK to close the Security Features window.

13. Click OK

14. For the Server Manager, click Apply, and then Restart for changes to take effect.

Setting Client Security Requirements

After you have performed all of the steps to secure your servers, you can set additional security requirements for your clients.

Requiring Client Authentication

You can enable the connection groups for your Administration Server and each server instance to require client authentication. When client authentication is enabled, the client's certificate is required before the server will send a response to a query.

iPlanet Web Server supports authenticating client certificates by matching the CA in the client certificate with a CA trusted for signing client certificates. You can view a list of CAs trusted for signing client certificates in the Manage Certificates page under Security in the Administration Server. There are four types of CAs:

- Untrusted CA (will not be matched)
- Trusted Server CA (will not be matched)
- Trusted Client CA (will be matched)
- Trusted Client/Server CA (will be matched)

You can configure the web server to refuse any client that doesn't have a client certificate from a trusted CA. To accept or reject trusted CAs, you must have set client trust for the CA. For more information, see "Managing Certificates," on page 188.

iPlanet Web Server will log an error, reject the certificate, and return a message to the client if the certificate has expired. You can also view which certificates have expired in the Administration Servers Manage Certificates page.

You can configure your server to gather information from the client certificate and match it with a user entry in an LDAP directory. This ensures that the client has a valid certificate and an entry in the LDAP directory. It can also ensure that the client certificate matches the one in the LDAP directory. To learn how to do this, see "Mapping Client Certificates to LDAP" on page 281.

You can combine client certificates with access control, so that in addition to being from a trusted CA, the user associated with the certificate must match the access control rules (ACLs). For more information, see "Using Access Control Files," on page 161.

You can also process information from client certificates. For more information, see the *NSAPI Programmer's Guide.*

To Require Client Authentication

To require client authentication, perform the following steps:

1. Access either the Administration Server or the Server Manager and choose the Preferences tab.

   For the Server Manager you must first select the server instance from the drop-down list.

2. Click the Edit Listen Sockets link.

   The Listen Socket Table page appears.

3. Use the drop-down Action list to select Edit, if not already displayed, for the connection group you are requiring client authentication for.

4. Use the drop-down list to turn Security on for that connection group, if it is off.

5. Click the Attributes link.

   The Security Settings of Listen Socket page appears.

6. Click Off for Client Auth to turn it on.

7. Click OK.

8. For the Server Manager, click Apply, and then Restart for changes to take effect.

NOTE Currently, there is a single certificate trust database per web server instance. All the secure virtual servers running under that server instance share the same list of trusted client CAs. If two virtual servers require different trusted CAs, then these virtual servers should be run in different server instances with separate trust databases.

Mapping Client Certificates to LDAP

This section describes the process iPlanet Web Server uses to map a client certificate to an entry in an LDAP directory.

When the server gets a request from a client, it asks for the client's certificate before proceeding. Some clients send the client certificate to the server along with the request.

NOTE Before mapping client certificates to LDAP, you also need to set up the required ACLs; for more information, see Chapter 8, "Controlling Access to Your Server."

The server tries to match the CA to the list of trusted CAs in the Administration Server. If there isn't a match, iPlanet Web Server ends the connection. If there is a match, the server continues processing the request.

After verifying the certificate is from a trusted CA, the server maps the certificate to an LDAP entry by:

- Mapping the issuer and subject DN from the client certificate to a branch point in the LDAP directory.
- Searching the LDAP directory for an entry that matches the information about the subject (end-user) of the client certificate.
- (Optional) Verifying the client certificate with one in the LDAP entry that corresponds to the DN.

The server uses a certificate mapping file called `certmap.conf` to determine how to do the LDAP search. The mapping file tells the server what values to take from the client certificate (such as the end-user's name, email address, and so on). The server uses these values to search for a user entry in the LDAP directory, but first the server needs to determine where in the LDAP directory it needs to start its search. The certificate mapping file also tells the server where to start.

Once the server knows where to start its search and what it needs to search for (step 1), it performs the search in the LDAP directory (step 2). If it finds no matching entry or more than one matching entry, and the mapping is *not* set to verify the certificate, the search fails. For a complete list of the expected search result behavior, see the following Table 5-1 table. Note that you can specify the expected behavior in the ACL; for example, you can specify that iPlanet Web Server accepts only you if the certificate match fails. For more information regarding how to set the ACL preferences, see "Using Access Control Files," on page 161.

Table B-1 LDAP Search Results

LDAP Search Result	Certificate Verification ON	Certificate Verification OFF
No entry found	Authentication fails	Authentication fails
Exactly one entry found	Authentication fails	Authentication succeeds
More than one entry found	Authentication fails	Authorization fails

After the server finds a matching entry and certificate in the LDAP directory, it can use that information to process the transaction. For example, some servers use certificate-to-LDAP mapping to determine access to a server.

Using the certmap.conf File

Certificate mapping determines how a server looks up a user entry in the LDAP directory. You can use `certmap.conf` to configure how a certificate, designated by name, is mapped to an LDAP entry. You edit this file and add entries to match the organization of your LDAP directory and to list the certificates you want your users to have. Users can be authenticated based on userid, email, or any other value used in the `subjectDN`. Specifically, the mapping file defines the following information:

- Where in the LDAP tree the server should begin its search
- What certificate attributes the server should use as search criteria when searching for the entry in the LDAP directory
- Whether or not the server goes through an additional verification process

The certificate mapping file is located in the following location:

```
server_root/userdb/certmap.conf
```

The file contains one or more named mappings, each applying to a different CA. A mapping has the following syntax:

```
certmap <name> <issuerDN>

<name>:<property> [<value>]
```

The first line specifies a name for the entry and the attributes that form the distinguished name found in the CA certificate. The name is arbitrary; you can define it to be whatever you want. However, `issuerDN` must exactly match the issuer DN of the CA who issued the client certificate. For example, the following two `issuerDN` lines differ only in the spaces separating the attributes, but the server treats these two entries as different:

```
certmap iplanet1 ou=iPlanet Certificate Authority,o=iPlanet,c=US
certmap iplanet2 ou=iPlanet Certificate Authority,o=iPlanet, c=US
```

TIP If you are using iPlanet Directory Server and experiencing problems in matching the `issuerDN`, check the Directory Server error logs for useful information.

The second and subsequent lines in the named mapping match properties with values. The `certmap.conf` file has six default properties (you can use the certificate API to customize your own properties):

- `DNComps` is a list of comma-separated attributes used to determine where in the LDAP directory the server should start searching for entries that match the user's information (that is, the owner of the client certificate). The server gathers values for these attributes from the client certificate and uses the values to form an LDAP DN, which then determines where the server starts its search in the LDAP directory. For example, if you set `DNComps` to use the `o` and `c` attributes of the DN, the server starts the search from the `o=<org>, c=<country>` entry in the LDAP directory, where `<org>` and `<country>` are replaced with values from the DN in the certificate.

  Note the following situations:

  - If there isn't a `DNComps` entry in the mapping, the server uses either the `CmapLdapAttr` setting or the entire subject DN in the client certificate (that is, the end-user's information).
  - If the `DNComps` entry is present but has no value, the server searches the entire LDAP tree for entries matching the filter.

- FilterComps is a list of comma-separated attributes used to create a filter by gathering information from the user's DN in the client certificate. The server uses the values for these attributes to form the search criteria used to match entries in the LDAP directory. If the server finds one or more entries in the LDAP directory that match the user's information gathered from the certificate, the search is successful and the server optionally performs a verification.

  For example, if FilterComps is set to use the email and userid attributes (FilterComps=e,uid), the server searches the directory for an entry whose values for email and userid match the end user's information gathered from the client certificate. Email addresses and userids are good filters because they are usually unique entries in the directory. The filter needs to be specific enough to match one and only one entry in the LDAP database.

  For a list of the x509v3 certificate attributes, see the following table:

Table B-2 Attributes for x509v3 Certificates

Attribute	Description
c	Country
o	Organization
cn	Common name
l	Location
st	State
ou	Organizational unit
uid	Unix/Linux userid
email	Email address

  The attribute names for the filters need to be attribute names from the certificate, not from the LDAP directory. For example, some certificates have an e attribute for the user's email address; whereas LDAP calls that attribute mail.

- verifycert tells the server whether it should compare the client's certificate with the certificate found in the LDAP directory. It takes two values: on, and off. You should only use this property if your LDAP directory contains certificates. This feature is useful to ensure your end-users have a valid, unrevoked certificate.

- `CmapLdapAttr` is a name for the attribute in the LDAP directory that contains subject DNs from all certificates belonging to the user. The default for this property is `certSubjectDN`. This attribute isn't a standard LDAP attribute, so to use this property, you have to extend the LDAP schema. For more information, see *Introduction to SSL*.

  If this property exists in the `certmap.conf` file, the server searches the entire LDAP directory for an entry whose attribute (named with this property) matches the subject's full DN (taken from the certificate). If the search doesn't find any entries, the server retries the search using the `DNComps` and `FilterComps` mappings.

  This approach to matching a certificate to an LDAP entry is useful when it's difficult to match entries using `DNComps` and `FilterComps`.

- `Library` is a property whose value is a pathname to a shared library or DLL. You only need to use this property if you create your own properties using the certificate API. For more information, see the *NSAPI Programmer's Guide.*

- `InitFn` is a property whose value is the name of an init function from a custom library. You only need to use this property if you create your own properties using the certificate API.

For more information on these properties, refer to the examples described in "Sample Mappings," on page 212.

Creating Custom Properties

You can use the client certificate API to create your own properties. For information on programming and using the client certificate API, see the *NSAPI Programmer's Guide.*

Once you have a custom mapping, you reference the mapping as follows:

```
<name>:library <path_to_shared_library>
<name>:InitFn <name_of_init_function>
```

For example:

```
certmap default1 o=Netscape Communications, c=US
default1:library /usr/netscape/enterprise/userdb/plugin.so
default1:InitFn plugin_init_fn
default1:DNComps  ou o c
default1:FilterComps l
default1:verifycert on
```

Sample Mappings

The `certmap.conf` file should have at least one entry. The following examples illustrate the different ways you can use the `certmap.conf` file.

Example #1

This example represents a `certmap.conf` file with only one "default" mapping:

```
certmap default default
default:DNComps ou, o, c
default:FilterComps e, uid
default:verifycert on
```

Using this example, the server starts its search at the LDAP branch point containing the entry `ou=<orgunit>, o=<org>, c=<country>` where the text in <> is replaced with the values from the subject's DN in the client certificate.

The server then uses the values for email address and userid from the certificate to search for a match in the LDAP directory. When it finds an entry, the server verifies the certificate by comparing the one the client sent to the one stored in the directory.

Example #2

The following example file has two mappings: one for default and another for the US Postal Service:

```
certmap default default
default:DNComps
default:FilterComps e, uid

certmap usps ou=United States Postal Service, o=usps, c=US
usps:DNComps ou,o,c
usps:FilterComps e
usps:verifycert on
```

When the server gets a certificate from anyone other than the US Postal Service, it uses the default mapping, which starts at the top of the LDAP tree and searches for an entry matching the client's email and userid. If the certificate is from the US Postal Service, the server starts its search at the LDAP branch containing the organizational unit and searches for matching email addresses. Also note that if the certificate is from the USPS, the server verifies the certificate; other certificates are not verified.

CAUTION The issuer DN (that is, the CA's information) in the certificate must be identical to the issuer DN listed in the first line of the mapping. In the previous example, a certificate from an issuer DN that is o=United States Postal Service,c=US won't match because there isn't a space between the o and the c attributes.

Example #3

The following example uses the CmapLdapAttr property to search the LDAP database for an attribute called certSubjectDN whose value exactly matches the entire subject DN taken from the client certificate.

```
certmap myco ou=My Company Inc, o=myco, c=US
myco:CmapLdapAttr certSubjectDN
myco:DNComps  o, c
myco:FilterComps mail, uid
myco:verifycert on
```

If the client certificate subject is:

```
uid=Walt Whitman, o=LeavesOfGrass Inc, c=US
```

the server first searches for entries that contain the following information:

```
certSubjectDN=uid=Walt Whitman, o=LeavesOfGrass Inc, c=US
```

If one or more matching entries are found, the server proceeds to verify the entries. If no matching entries are found, the server will use DNComps and FilterComps to search for matching entries. In this example, the server would search for uid=Walt Whitman in all entries under o=LeavesOfGrass Inc, c=US.

NOTE This example assumes the LDAP directory contains entries with the attribute certSubjectDN.

Setting Stronger Ciphers

The Stronger Ciphers option presents a choice of 168, 128, or 56-bit secret key size for access, or no restriction. You can specify a file to be served when the restriction is not met. If no file is specified, iPlanet Web Server returns a "Forbidden" status.

If you select a key size for access that is not consistent with the current cipher settings under Security Preferences, iPlanet Web Server displays a popup dialog warning that you need to enable ciphers with larger secret key sizes.

The implementation of the key size restriction is now based on an NSAPI `PathCheck` directive in `obj.conf`, rather than Service `fn=key-toosmall`. This directive is:

```
PathCheck fn="ssl-check" [secret-keysize=<nbits>]
[bong-file=<filename>]
```

where `<nbits>` is the minimum number of bits required in the secret key, and `<filename>` is the name of a file (not a URI) to be served if the restriction is not met.

`PathCheck` returns `REQ_NOACTION` if SSL is not enabled, or if the `secret-keysize` parameter is not specified. If the secret key size for the current session is less than the specified `secret-keysize`, the function returns `REQ_ABORTED` with a status of `PROTOCOL_FORBIDDEN` if `bong-file` is not specified, or else `REQ_PROCEED`, and the “path” variable is set to the `bong-file <filename>`. Also, when a key size restriction is not met, the SSL session cache entry for the current session is invalidated, so that a full SSL handshake will occur the next time the same client connects to the server.

NOTE The Stronger Ciphers form removes any Service `fn=key-toosmall` directives that it finds in an object when it adds a `PathCheck fn=ssl-check`.

To Set Stronger Ciphers, perform the following steps:

1. Access the Server Manager and select the server instance from the drop-down list.
2. Click the Virtual Server Class tab.
3. Select a class from the drop-down list and click Manage.
4. The Class Manger page appears.
5. Choose the Content Mgmt tab.
6. Select Stronger Ciphers.
7. Choose to edit:
   - from the drop down list

  - by clicking Browse
  - by clicking Wildcard

8. Select the secret key size restriction:
   - 168 bit or larger
   - 128 bit or larger
   - 56 bit or larger
   - No restrictions
9. Enter the file location of the message to reject access.
10. Click OK.
11. Click Apply.
12. Select hard start / restart or dynamically apply

For more information, see *Introduction to SSL*.

Considering Additional Security Issues

There are other security risks besides someone trying to break your encryption. Networks face risks from external and internal hackers, using a variety of tactics to gain access to your server and the information on it.

So in addition to enabling encryption on your server, you should take extra security precautions. For example, put the server machine into a secure room, and don’t allow individuals you don’t trust to upload programs to your server.

The following sections describe the most important things you can do to make your server more secure:

- Limit Physical Access
- Limit Administration Access
- Choosing Solid Passwords
- Changing Passwords or PINs
- Limiting Other Applications on the Server
- Preventing Clients from Caching SSL Files
- Limiting Ports

- Knowing Your Server's Limits
- Making Additional Changes to Protect Servers

Limit Physical Access

This simple security measure is often forgotten. Keep the server machine in a locked room that only authorized people can enter. This prevents anyone from hacking the server machine itself.

Also, protect your machine's administrative (root) password, if you have one.

Limit Administration Access

If you use remote configuration, be sure to set access control to allow administration from only a few users and computers. If you want your Administration Server to provide end-user access to the LDAP server or local directory information, consider maintaining two Administration Servers and using cluster management, so that the SSL-enabled Administration Server acts as the master server, and the other Administration Server is available for end-users' access.

For more information regarding clusters, see "About Clusters," on page 131.

You should also turn on encryption for the Administration Server. If you don't use an SSL connection for administration, then you should be cautious when performing remote server administration over an unsecure network. Anyone could intercept your administrative password and reconfigure your servers.

Choosing Solid Passwords

You use a number of passwords with your server: the administrative password, the private key password, database passwords, and so on. Your administrative password is the most important password of all, since anyone with that password can configure any and all servers on your computer. Your private key password is next most important. If someone gets your private key and your private key password, they can create a fake server that appears to be yours, or intercept and change communications to and from your server.

A good password is one you'll remember but others won't guess. For example, you could remember *MCi12!mo* as "My Child is 12 months old!" A bad password is your child's name or birthdate.

Creating Hard-to-Crack Passwords

There are some simple guidelines that will help you create a stronger password.

It is not necessary to incorporate all of the following rules in one password, but the more of the rules you use, the better your chances of making your password hard to crack:

- Passwords should be 6-14 characters long. (Mac passwords cannot be longer than 8 characters)
- Do not use the “illegal” characters: *, ", or spaces
- Do not use dictionary words (any language)
- Do not make common letter substitutions, like replacing E with 3, or L with 1
- Include characters from as many of these classes as possible:
    - Uppercase letters
    - Lowercase letters
    - Numbers
    - Symbols

Changing Passwords or PINs

It’s a good practice to change your trust database / key pair file password or PIN periodically. If your Administration Server is SSL enabled, this password is required when starting the server. Changing your password periodically adds an extra level of server protection.

You should only change this password on your local machine. For a list of guidelines to consider when changing a password, see “Creating Hard-to-Crack Passwords,” on page 217.

Changing Passwords

To change your trust database / key-pair file password for the Administration Server or an server instance, perform the following steps:

1. Access either the Administration Server or the Server Manager and choose the Security tab.

   For the Server Manager you must first select the server instance from the drop-down list.

2. Select the Change Password link.
3. Select the security token on which you want to change the password from the drop-down list.

   By default this is 'internal' for the internal key database. If you have PKCS#11 modules installed, you will see all the tokens listed. Click the Change Password link.
4. Enter your current password.
5. Enter your new password
6. Enter it again.
7. Click OK.
8. For the Server Manager, click Apply, and then Restart for changes to take effect

Make sure your key-pair file is protected. The Administration Server stores key-pair files in the directory *server_root*/alias. Consider making the files and directory readable only to iPlanet servers installed on your computer.

It's also important to know if the file is stored on backup tapes or is otherwise available for someone to intercept. If so, you must protect your backups as completely as your server.

Limiting Other Applications on the Server

Carefully consider all applications that run on the same machine as the server. It's possible to circumvent your server's security by exploiting holes in other programs running on your server. Disable all unnecessary programs and services. For example, the Unix sendmail daemon is difficult to configure securely and it can be programmed to run other possibly detrimental programs on the server machine.

Unix and Linux

Carefully choose the processes started from inittab and rc scripts. Don't run telnet or rlogin from the server machine. You also shouldn't have rdist on the server machine (this can distribute files but it can also be used to update files on the server machine).

Windows NT

Carefully consider which drives and directories you share with other machines. Also, consider which users have accounts or Guest privileges.

Similarly, be careful about what programs you put on your server, or allow other people to install on your server. Other people's programs might have security holes. Worst of all, someone might upload a malicious program designed specifically to subvert your security. Always examine programs carefully before you allow them on your server.

Preventing Clients from Caching SSL Files

You can prevent pre-encrypted files from being cached by a client by adding the following line inside the `<HEAD>` section of a file in HTML:

```
<meta http-equiv="pragma" content="no-cache">
```

Limiting Ports

Disable any ports not used on the machine. Use routers or firewall configurations to prevent incoming connections to anything other than the absolute minimum set of ports. This means that the only way to get a shell on the machine is to physically use the server's machine, which should be in a restricted area already.

Knowing Your Server's Limits

The server offers secure connections between the server and the client. It can't control the security of information once the client has it, nor can it control access to the server machine itself and its directories and files.

Being aware of these limitations helps you understand what situations to avoid. For example, you might acquire credit card numbers over an SSL connection, but are those numbers stored in a secure file on the server machine? What happens to those numbers after the SSL connection is terminated? You should be responsible for securing any information clients send to you through SSL.

Making Additional Changes to Protect Servers

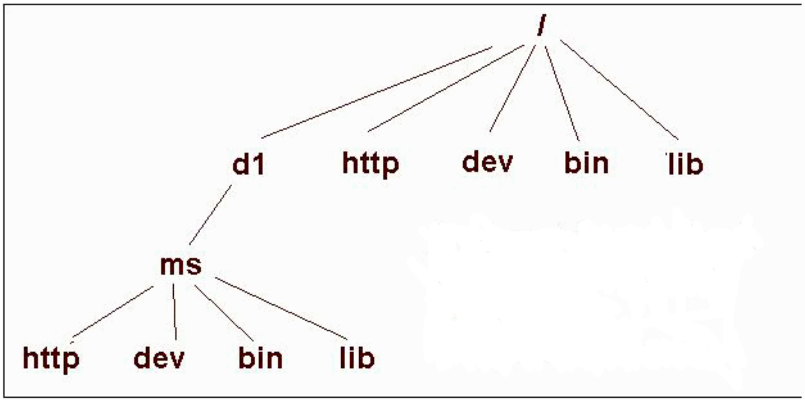
If you want to have both protected and unprotected servers, you should operate the unprotected server on a different machine from the protected one. If your resources are limited and you must run an unprotected server on the same machine as your protected server, do the following.

- Assign proper port numbers. Make sure that the protected server and the unprotected server are assigned different port numbers. The registered default port numbers are:
    - 443 for the protected server
    - 80 for the unprotected server
- For Unix or Linux, enable the `chroot` feature for the document root directory. The unprotected server should have references to its document root redirected using `chroot`.

`chroot` allows you to create a second root directory to limit the server to specific directories. You'd use this feature to safeguard an unprotected server. For example, you could say that the root directory is `/d1/ms`. Then any time the web server tries to access the root directory, it really gets `/d1/ms`. If it tries to access `/dev`, it gets `/d1/ms/dev` and so on. This allows you to run the web server on your Unix/Linux system, without giving it access to all the files under the actual root directory.

However, if you use `chroot`, you need to set up the full directory structure required by iPlanet Web Server under the alternative root directory, as shown in the following illustration:

Figure B-2 Example of `chroot` Directory Structure



Specifying chroot for a Virtual Server Class

You can specify the `chroot` directory for a virtual server class by performing the following steps:

1. Access the Server Manager and select the server instance from the drop-down list.
2. Select the Virtual Server Class tab.
3. Click the Edit Classes link.
4. Make sure the Option is set to Edit for the class in which you wish to specify `chroot`.
5. Click the Advanced button for that class.

   The Virtual Servers CGI Settings page appears.
6. Enter the full pathname in the Chroot field.
7. Click OK.
8. Click Apply.
9. Choose Load Configuration Files to dynamically apply.

Specifying chroot for a Virtual Server

You can specify the `chroot` directory for a specific virtual server by performing the following steps:

1. Access the Server Manager and select the server instance from the drop-down list.
2. Select the Virtual Server Class tab.
3. Click on the link for the virtual server you wish to specify the `chroot` directory for from the Tree View of the Server.
4. Select the Settings tab.

   The Settings page appears.
5. Enter the full pathname in the Set to field next to Chroot Directory.
6. Click OK.
7. Click Apply.
8. Choose Load Configuration Files to dynamically apply.

You can also specify the `chroot` directory for a virtual server using the Class Manager Virtual Servers tab and the CGI Settings link.

For more information regarding how to specify a `chroot` directory for a virtual server, see the *Programmer's Guide for iPlanet Web Server*.

Appendix C

Managing SSL

This appendix is excerpted from the iPlanet Directory Server Administrator's Guide. For your convenience, Chapter 11 of the Guide is reproduced here in its entirety. To view the full online manual on the Internet, go to `http://docs.iplanet.com/docs/manuals/directory.html`

To provide secure communications over the network, iPlanet Directory Server Access Management Edition includes the LDAPS communications protocol. LDAPS is the standard LDAP protocol, but it runs on top of the Secure Sockets Layer (SSL).

This chapter describes how to use SSL with your Directory Server in the following sections:

- Introduction to SSL in the Directory Server
- Obtaining and Installing Server Certificates
- Activating SSL
- Setting Security Preferences
- Using Certificate-Based Authentication
- Configuring LDAP Clients to Use SSL

Introduction to SSL in the Directory Server

You can use SSL to secure communications between LDAP clients and the Directory Server, or between Directory Servers that are bound by a replication agreement, or between a database link and a remote database. You can use SSL with simple authentication (bind DN and password), or with certificate-based authentication.

Using SSL with simple authentication guarantees confidentiality and data integrity. The benefits of using a certificate to authenticate to the Directory Server instead of a bind DN and password include:

- Improved efficiency

  When you are using applications that prompt you once for your certificate database password, and then use that certificate for all subsequent bind or authentication operations, it is more efficient than continuously providing a bind DN and password.

- Improved security

  The use of certificate-based authentication is more secure than non-certificate bind operations. This is because certificate-based authentication uses public-key cryptography. As a result, bind credentials cannot be intercepted across the network.

Directory Server is capable of simultaneous SSL and non-SSL communications. This means that you do not have to choose between SSL or non-SSL communications for your Directory Server; you can use both at the same time.

NOTE If you are running Directory Server on a UNIX platform, enabling SSL will also enable support the StartTLS extended operation. The StartTLS extended operation provides security on a regular LDAP connection.

Enabling SSL: Summary of Steps

To use LDAPS, you must do the following:

1. Obtain and install a certificate for your Directory Server, and configure the Directory Server to trust the certification authority's certificate.

   For information, see "Obtaining and Installing Server Certificates," on page 161.

2. Turn on SSL in your directory.

   For information, see "Activating SSL," on page 166.

3. Configure the administration server to connect to an SSL-enabled Directory Server.

   For information, see *Managing Servers with iPlanet Console*.

4. Optionally, ensure that each user of the Directory Server obtains and installs a personal certificate for all clients that will authenticate with SSL.

   For information, see "Configuring LDAP Clients to Use SSL," on page 171.

If you are using FORTEZZA, please read Chapter 12, "Managing FORTEZZA," for information before you attempt to set up SSL.

For a complete description of SSL, internet security, and certificates, see *Managing Servers with iPlanet Console*.

Obtaining and Installing Server Certificates

This section describes the process of creating a certificate database, obtaining and installing a certificate for use with your Directory Server, and configuring Directory Server to trust the certification authority's (CA) certificate.

This process is a necessary first step before you can turn on SSL in your directory. If you have already completed these tasks, see "Activating SSL," on page 166. If you are using FORTEZZA with your directory server, see Chapter 12, "Managing FORTEZZA."

Obtaining and installing certificates consists of the following steps:

- Step 1: Generate a Certificate Request
- Step 2: Send the Certificate Request
- Step 3: Install the Certificate
- Step 4: Trust the Certificate Authority
- Step 5: Confirm That Your New Certificates Are Installed

You will use the Certificate Request Wizard to generate a certificate request (Step 1) and send it to a Certificate Authority (Step 2). You then use the Certificate Install Wizard to install the certificate (Step 3), and to trust the Certificate Authority's certificate (Step 4).

These wizards automate the process of creating a certificate database, and of installing the key-pair.

Step 1: Generate a Certificate Request

To generate a certificate request and send it to a CA:

1. On the Directory Server Console, select the Tasks tab and click Manage Certificates.

   The Manage Certificates window is displayed.

2. Select the Server Certs tab, and click the Request button.

   The Certificate Request Wizard is displayed.

3. Click Next.

4. Enter the Requester Information in the blank text fields, then click Next.

   Enter the following information:

   Server Name. Enter the fully qualified hostname of the Directory Server as it is used in DNS lookups, for example, `dir.siroe.com`.

   Organization. Enter the legal name of your company or institution. Most CAs require you to verify this information with legal documents such as a copy of a business license.

   Organizational Unit. (Optional). Enter a descriptive name for your organization within your company.

   Locality. (Optional). Enter your company's city name.

   State or Province. Enter the full name of your company's state or province (no abbreviations).

   Country. Select the two-character abbreviation for your country's name (ISO format). The country code for the United States is US. The *iPlanet Directory Server Schema Reference* contains a complete list of ISO Country Codes.

5. Enter the password that will be used to protect the private key, and click Next.

   The Next field is greyed out until you supply a password. When you click Next, the Request Submission dialog box is displayed.

6. Select Copy to Clipboard or Save to File to save the certificate request information that you must send to the Certificate Authority.

7. Click Done to dismiss the Certificate Request Wizard.

Once you have generated the request, you are ready to send it to the CA.

Step 2: Send the Certificate Request

Follow these steps to send the certificate information to the CA:

1. Use your email program to create a new email message.
2. Copy the certificate request information from the clipboard or the saved file into the body of the message.

   The content will look similar to the following example:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBrjCCARcCAQAwbjELMAkGA1UEBhMCVXMxEzARBgNVBAgTCkNBTElGT1JOSUExLD
AqBgVBAoTI25ldHNjYXBlIGNvbW11bmljYXRpb25zIGNvcnBvcmF0aW9uMRwwGgYDV
QQDExNtZWxsb24ubmV0c2NhcGUuY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQK
BgQCwAbskGh6SKYOgHy+UCSLnm3ok3X3u83Us7ug0EfgSLR0f+K41eNqqWRftGR83e
mqPLDOf0ZLTLjVGJaH4Jn4l1gG+JDf/n/zMyahxtV7+mT8GOFFigFfuxJaxMjr2j7I
vELlxQ4IfZgWwqCm4qQecv3G+N9YdbjveMVXW0v4XwIDAQABoAAwDQYJKoZIhvcNAQ
EEBQADgYEAZyZAm8UmP9PQYwNy4Pmypk79t2nvzKbwKVb97G+MT/gw1pLRsI1uBoKi
nMfLgKp1Q38K5Py2VGW1E47K7/rhm3yVQrIiwV+Z8Lcc=
-----END NEW CERTIFICATE REQUEST-----
```

3. Send the email message to the CA.

Once you have emailed your request, you must wait for the CA to respond with your certificate. Response time for your request varies. For example, if your CA is internal to your company, it may only take a day or two to respond to your request. If your selected CA is external to your company, it could take several weeks to respond to your request.

When the CA sends a response, be sure to save the information in a text file. You will need the data when you install the certificate.

You should also back up the certificate data in a safe location. If your system ever loses the certificate data, you can reinstall the certificate using your backup file.

Once you receive your certificate, you are ready to install it in your server's certificate database.

Step 3: Install the Certificate

To install a server certificate:

1. On the Directory Server Console, select the Tasks tab and click Manage Certificates.

   The Manage Certificates window is displayed.

2. Select the Server Certs tab, and click Install.

   The Certificate Install Wizard is displayed.

3. Choose one of the following options for the certificate location, then click Next.

   In this file. Enter the absolute path to the certificate in this field.

   In the following encoded text block. Copy the text from the CAs email or from the text file you created and paste it in this field. For example:

```
-----BEGIN CERTIFICATE-----
MIICMjCCAZugAwIBAgICCEEwDQYJKoZIhvcNAQEFBQAwfDELMAkGA1UEBhMCVVMx
IzAhBgNVBAoTGlBhbG9va2FWaWxsZSBXaWRnZXRzLCBJbmMuMR0wGwYDVQQLExRX
aWRnZXQgTWFrZXJzICdSJyBVczEpMCcGA1UEAxMgVGVzdCBUZXN0IFRlc3QgVGVz
dCBUZXN0IFRlc3QgQ0EwHhcNOTgwMzEyMDIzMzU3WhcNOTgwMzI2MDIzMzU3WjBP
MQswCQYDVQQGEwJVUzEoMCYGA1UEChMfTmV0c2NhcGUgRGlyZWN0b3J5IFB1Ymxp
Y2F0aW9uczEWMBQGA1UEAxMNZHVgh49dq2itLmNvbTBaMA0GCSqGSIb3DQEBAQUA
A0kAMEYCQQCksMR/aLGdfp4m0OiGcgijG5KgOsyRNvwGYW7kfW+8mmijDtZRjYNj
jcgpF3VnlsbxbclX9LVjjNLC57u37XZdAgEDozYwNDARBglghkgBhvhCAQEEBAMC
APAwHwYDVR0jBBgwFoAU67URjwCaGqZuUpSpdLxlzweJKiMwDQYJKoZIhvcNAQEF
BQADgYEAJ+BVem3vBOP/BveNdLGfjlb9hucgmaMcQa98A/db8qimKT/ue9UGOJqL
bwbMKBBopsD56p2yV3PLJIsBgrcuSoBCuFFnxBnqSiTS/7YiYgCWqWaUAExJFmD6
6hBLseqkSWulk+hXHN7L/NrViO+7zNtKcaZLlFPf7d7j2MgX4Bo=
-----END CERTIFICATE-----
```

4. Check that the certificate information displayed is correct, and click Next.

5. Specify a name for the certificate, and click Next.

6. Verify the certificate by providing the password that protects the private key.

   This password is the same as the one you provided in “Step 1: Generate a Certificate Request,” on page 161.

Now that you have installed your certificate, you need to configure your server to trust the Certificate Authority from which you obtained the server’s certificate.

Step 4: Trust the Certificate Authority

Configuring your Directory Server to trust the certificate authority consists of obtaining your CA’s certificate and installing it into your server’s certificate database. This process differs depending on the certificate authority you use. Some commercial CAs provide a website that allows you to automatically download the certificate. Others will email it to you upon request.

Once you have the CA certificate, you can use the Certificate Install Wizard to configure the Directory Server to trust the Certificate Authority.

1. On the Directory Server Console, select the Tasks tab and click Manage Certificates.

   The Manage Certificates window is displayed.

2. Go to the CA Certs tab, and click Install.

   The Certificate Install Wizard is displayed.

3. If you saved the CA's certificate to a file, enter the path in the field provided. If you received the CA's certificate via email, copy and paste the certificate including the headers into the text field provided. Click Next.

4. Check that the certificate information that is displayed is correct, and click Next.

5. Specify a name for the certificate, and click Next.

6. Select the purpose of trusting this Certificate Authority (you can select both):

   Accepting connections from clients (Client Authentication). The server checks that the client's certificate has been issued by a trusted Certificate Authority.

   Accepting connections to other servers (Server Authentication). This server checks that the directory to which it is making a connection (for example, for replication updates) has a certificate that has been issued by a trusted Certificate Authority.

7. Click Done to dismiss the wizard.

Once you have installed your certificate and trusted the CA's certificate, you are ready to activate SSL. However, you should first make sure that the certificates have been installed correctly.

Step 5: Confirm That Your New Certificates Are Installed

1. On the Directory Server Console, select the Tasks tab and click Manage Certificates.

   The Manage Certificates window is displayed.

2. Select the Server Certs tab.

   A list of all the installed certificates for the server is displayed.

3. Scroll through the list. You should find the certificates you installed.

   Your server is now ready for SSL activation.

Activating SSL

Most of the time, you want your server to run with SSL enabled. If you temporarily disable SSL, make sure you re-enable it before processing transactions that require confidentiality, authentication, or data integrity.

Before you can activate SSL, you must create a certificate database, obtain and install a server certificate and trust the CA's certificate as described in "Obtaining and Installing Server Certificates," on page 161.

To activate SSL communications:

1. Set the secure port you want the server to use for SSL communications. See "Changing Directory Server Port Numbers," on page 37 for information.

   The encrypted port number that you specify must not be the same port number you use for normal LDAP communications. By default, the standard port number is 389 and the secure port is 636.

2. On the Directory Server Console, select the Configuration tab and then select the topmost entry in the navigation tree in the left pane.

3. Select the Encryption tab in the right pane.

   The tab displays the current server encryption settings.

4. Indicate that you want encryption enabled by selecting the "Enable SSL for this Server" checkbox.

5. Check the "Use this Cipher Family" checkbox.

6. Select the certificate that you want to use from the drop-down menu.

7. Click Cipher Settings.

   The Cipher Preference dialog box is displayed.

8. Select the checkbox next to the cipher you want to use, and click OK to dismiss the Cipher Preference dialog box.

   For more information about specific ciphers, see "Setting Security Preferences," on page 167.

9. Set your preferences for client authentication.

   Do not allow client authentication. With this option, the server will ignore the client's certificate. This does not mean that the bind will fail.

   Allow client authentication. This is the default setting. With this option, authentication is performed on the client's request. For more information about certificate-based authentication, see "Using Certificate-Based Authentication," on page 169.

   Require client authentication. With this option, the server requests authentication from the client.

NOTE	If you are using certificate-based authentication with replication, then you must configure the consumer server to either allow or require client authentication.

10. If you want iPlanet Console to use SSL during communications with Directory Server, select Use SSL in iPlanet Console.

11. Click Save.

12. Restart the Directory Server.

    See "Starting the Server with SSL Enabled," on page 38 for more information.

Setting Security Preferences

You can choose the type of ciphers you want to use for SSL communications. A *cipher* is the algorithm used in encryption. Some ciphers are more secure or *stronger* than others. Generally speaking, the more bits a cipher uses during encryption, the more difficult it is to decrypt the key. For a more complete discussion of algorithms and their strength, see *Managing Servers with iPlanet Console.*

When a client initiates an SSL connection with a server, the client tells the server what ciphers it prefers to use to encrypt information. In any two-way encryption process, both parties must use the same ciphers. There are a number of ciphers available. Your server needs to be able to use the ciphers that will be used by client applications connecting to the server.

iPlanet Directory Server Access Management Edition provides the following SSL 3.0 ciphers:

- RC4 cipher with 40-bit encryption and MD5 message authentication.

- RC2 cipher with 40-bit encryption and MD5 message authentication.
- No encryption, only MD5 message authentication.
- DES with 56-bit encryption and SHA message authentication.
- RC4 cipher with 128-bit encryption and MD5 message authentication.
- Triple DES with 168-bit encryption and SHA message authentication.
- FIPS DES with 56-bit encryption and SHA message authentication. This cipher meets the FIPS 140-1 U.S. government standard for implementations of cryptographic modules.
- FIPS Triple DES with 168-bit encryption and SHA message authentication. This cipher meets the FIPS 140-1 US government standard for implementations of cryptographic modules.

In addition, the directory server also provides FORTEZZA ciphers. For information on using FORTEZZA with the Directory Server, see Chapter 12, “Managing FORTEZZA.”.

To select the ciphers you want the server to use:

1. Make sure SSL is enabled for your server.

   For information, see “Activating SSL,” on page 166.

2. On the Directory Server Console, select the Configuration tab and then select the topmost entry in the navigation tree in the left pane.

3. Select the Encryption tab in the right pane.

   This displays the current server encryption settings.

4. Click Cipher Settings.

   The Cipher Preference dialog box is displayed.

5. In the Cipher Preference dialog box, specify which ciphers you want your server to use by selecting them from the list, and click OK.

   Unless you have a security reason to not use a specific cipher, you should select all of the ciphers, except for `none,MD5`.

6. On the Encryption tab, click Save.

CAUTION Avoid selecting the `none,MD5` cipher because the server will use this option if no other ciphers are available on the client. It is not secure because encryption doesn’t occur.

In order to continue using the iPlanet Console with SSL, you must select at least one of the following ciphers:

- RC4 cipher with 40-bit encryption and MD5 message authentication.
- No encryption, only MD5 message authentication.
- DES with 56-bit encryption and SHA message authentication.
- RC4 cipher with 128-bit encryption and MD5 message authentication.
- Triple DES with 168-bit encryption and SHA message authentication.

Using Certificate-Based Authentication

Directory Server allows you to use certificate-based authentication for the command-line tools (which are LDAP clients) and for replication communications. Certificate-based authentication can occur between:

- An LDAP client connecting to the Directory Server
- A Directory Server connecting to another Directory Server (replication or chaining)

Setting up Certificate-Based Authentication

To set up certificate-based authentication, you must:

1. Create a certificate database for the client and the server, or for both servers involved in replication.

   On the Directory Server, the certificate database creation automatically takes place when you install a certificate. For information on creating a certificate database for a client, see “Configuring LDAP Clients to Use SSL,” on page 171.

2. Obtain and install a certificate on both the client and the server, or on both servers involved in replication.

3. Enable SSL on the server, or on both servers involved in replication.

   For information on enabling SSL, refer to “Activating SSL,” on page 166.

NOTE If iPlanet Console connects to Directory Server over SSL, selecting "Require client authentication" disables communication. This is because although iPlanet Console supports SSL, it does not have a certificate to use for client authentication.

4. Map the certificate's distinguished name to a distinguished name known by your directory.

   This allows you to set access control for the client when it binds using this certificate. This mapping process is described in *Managing Servers with iPlanet Console.*

Allowing/Requiring Client Authentication

If you have configured iPlanet Console to connect to your Directory Server using SSL *and* your Directory Server *requires* client authentication, you can no longer use iPlanet Console to manage any of your iPlanet servers. You will have to use the appropriate command-line utilities instead.

However, if at a later date you wish to change your directory configuration to no longer *require* but *allow* client authentication, so that you can use iPlanet Console, you must follow these steps:

1. Stop Directory Server.

   For information on stopping and starting the server from the command line, see "Starting/Stopping the Server From the Command Line," on page 35.

2. Modify the `cn=encryption,cn=config` entry by changing the value of the nsSSLClientAuth attribute from **required** to **allowed**.

   For information on modifying entries from the command line, see Chapter2, "Creating Directory Entries."

3. Start Directory Server.

   You can now start iPlanet Console.

Configuring LDAP Clients to Use SSL

If you want all the users of your Directory Server to use SSL or certificate-based authentication when they connect using LDAP client applications, you must make sure they perform the following tasks:

- Create a certificate database.
- Trust the Certificate Authority (CA) that issues the server certificate.

These operations are sufficient if you want to ensure that LDAP clients recognize the server's certificate. However, if you also want LDAP clients to use their own certificate to authenticate to the directory, make sure that all your directory users obtain and install a personal certificate.

NOTE Some client applications do not verify that the server has a trusted certificate.

The following procedure describes how to use Netscape Communicator 4.7 to perform these tasks.

1. To create a certificate, it is sufficient to start Netscape Communicator 4.7.

If it does not already exist, the certificate database will be created.

2. Use Communicator to connect to your Certificate Authority.

If you are using an internally deployed iPlanet Certificate Server, you will go to a URL of the form:

`https://`*hostname*`:444`

Some Certificate Authorities provide a link that allows you to download the CA's certificate.

3. Trust the Certificate Authority.

This task differs depending on the CA. In some cases, such as if you are connecting to a iPlanet Certificate Server, Communicator will automatically prompt you to see if you want to trust the CA.

These steps are sufficient to ensure that your client applications will accept connections to take place with the Directory Server, because the clients recognize that the Directory Server's certificate has been issued by a trusted CA.

However, if you also want the Directory Server to authenticate clients using the clients' certificate, you must perform the following additional steps:

4. On the client system, obtain a client certificate from the CA.

5. On your client system, install your client certificate.

   Regardless of how you receive your certificate (either in email or on a web page), there should be a link that you click to install the certificate. Click it and step through the dialog boxes that Communicator presents to you.

   Make sure you record the certificate information that is sent to you in a file. In particular, you must know the subject DN of the certificate because you must configure the server to map it to an entry in the directory. Your client certificate will be similar to:

```
-----BEGIN CERTIFICATE-----
MIICMjCCAZugAwIBAgICCEEwDQYJKoZIhvcNAQEFBQAwfDELMAkGA1UEBhMCVVMx
IzAhBgNVBAoTGlBhbG9va2FWaWxsZSBXaWRnZXRzLCBJbmMuMR0wGwYDVQQLExRX
aWRnZXQgTWFrZXJzICdSJyBVczEpMCcGA1UEAxMgVGVzdCBUZXN0IFRlc3QgVGVz
dCBUZXN0IFRlc3QgQ0EwHhcNOTgwMzEyMDIzMzU3WhcNOTgwMzI2MDIzMzU3WjBP
MQswCQYDVQQGEwJVUzEoMCYGA1UEChMfTmV0c2NhcGUgRGlyZWN0b3J5IFB1Ymxp
Y2F0aW9uczEWMBQGA1UEAxMNZHVgh49dq2itLmNvbTBaMA0GCSqGSIb3DQEBAQUA
A0kAMEYCQQCksMR/aLGdfp4m0OiGcgijG5KgOsyRNvwGYW7kfW+8mmijDtZRjYNj
jcgpF3VnlsbxbclX9LVjjNLC57u37XZdAgEDozYwNDARBglghkgBhvhCAQEEBAMC
APAwHwYDVR0jBBgwFoAU67URjwCaGqZuUpSpdLxlzweJKiMwDQYJKoZIhvcNAQEF
BQADgYEAJ+BVem3vBOP/BveNdLGfjlb9hucgmaMcQa98A/db8qimKT/ue9UGOJqL
bwbMKBBopsD56p2yV3PLJIsBgrcuSoBCuFFnxBnqSiTS/7YiYgCWqWaUAExJFmD6
6hBLseqkSWulk+hXHN7L/NrViO+7zNtKcaZLlFPf7d7j2MgX4Bo=
-----END CERTIFICATE-----
```

6. You must convert the client certificate into binary format using the `certutil` utility. To do this:

   a. Download the `certutil` utility from `http://www.iplanet.com`

      On the iPlanet home page, search for **certutil**. Download the most recent PKCS package. It will contain the `certutil` utility.

   b. Run `certutil` as follows:

      `certutil -L -d` *cert7.db_path* `-n` *user_cert_name* `-r >` *user_cert.bin*

      where *cert7.db_path* is the location of your certificate database, *user_cert_name* is the name you gave to your certificate when you installed it, and *user_cert.bin* is the name you must specify for the output file that will contain the binary certificate.

7. On the server, map the subject DN of the certificate that you obtained to the appropriate directory entry by editing the `certmap.conf` file.

   This procedure is described in *Managing Servers with iPlanet Console*. Make sure that the `verifyCert` parameter is set to **on** in the `certmap.conf` file.

NOTE	Note that if this parameter is not set to **on**, Directory Server simply searches for an entry in the directory that matches the information in the `certmap.conf` file. If the search is successful, it grants access without actually checking the value of the `userCertificate` attribute.

8. On the Directory Server, you must modify the directory entry for the user who owns the client certificate to add the `userCertificate` attribute.

   a. Select the Directory tab, and navigate to the user entry.

   b. Double click the user entry, and use the Property Editor to add the `userCertificate` attribute, with the `binary` subtype.

      When you add this attribute, instead of an editable field, the server provides a Set Value button.

   c. Click Set Value.

      A file selector is displayed. Use it to select the binary file you created in Step 6.

   For information on using the Directory Server Console to edit entries, refer to “Modifying Directory Entries,” on page 45.

You can now use SSL with your LDAP clients. For information on how to use SSL with `ldapmodify`, `ldapdelete` and `ldapsearch`, refer to *iPlanet Directory Server Configuration, Command, and File Reference*.

Index