Administration Guide

iPlanet™ Directory Server
Access Management Edition

Version 5.1

May 2002

Contents

About This Guide

This *Administration Guide* offers an explanation on how to manage the iPlanet™ Directory Server Access Management Edition (DSAME) enterprises and how to administer the graphical user interface procedures. This preface contains the following sections:

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

NOTE Sun™ ONE Identity Server was previously known as iPlanet Directory Server Access Management Edition (DSAME). The product was renamed shortly before the launch of the product.

The late renaming of this 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 referenced as DSAME within the product GUI and within the product documentation. For this release, please consider Directory Server Access Management Edition 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 “second” manual in the documentation series provided with iPlanet Directory Server Access Management Edition. 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. It’s

recommended that you understand directory server technologies, including Lightweight Directory Access Protocol (LDAP), and have some experience with Java and eXtensible Markup Language (XML). Particularly, you should be familiar with iPlanet Directory Server and the documentation provided with that product.

iPlanet Directory Server Access Management Edition Documentation Set

The Directory Server Access Management Edition documentation set contains the following titles:

- *Installation and Configuration Guide* describes iPlanet DSAME and provides details on how to plan and install the iPlanet DSAME on Solaris systems.
- *Administration Guide* (this guide) documents how to manage user and service data and customize the DSAME console.
- *Programmer's Guide* documents how to customize an iPlanet Directory Server Access Management Edition system for your organization.
- The *Release Notes* file gathers an assortment of information, including a description of what is new in this release, last minute installation notes, 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. Updated documents will be marked with the revision date.

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

Organization of This Guide

The Administration Guide (this guide) has two parts:

- Part 1, "DSAME Console Guide," explains the DSAME console and how to manage and configure user data, organization services and enterprise policies. It also includes procedures on how to navigate the graphical user interface and create DSAME objects.

- Part 2, “Attribute Reference Guide,” explains each of the attributes contained within the default DSAME services. Information included is an attribute definition, default values and attribute type.

The table below lists and briefly describes the content of the *Administration Guide*.

Table 1 *Administration Guide* Chapters

Chapter	Description
About This Guide	An outline of the DSAME documentation set and a description of the Administration Guide.
Part 1, “DSAME Console Guide”	
Chapter 1, “Product Overview“	A brief explanation of DSAME concepts.
Chapter 2, “Service Management”	Managing and configuring DSAME services using the graphical user interface.
Chapter 3, “Policy Management”	Managing and configuring DSAME policies using the graphical user interface.
Chapter 4, “User Management”	Managing and configuring DSAME objects using the graphical user interface.
Chapter 5, “Authentication Options	A description of the DSAME authentication options and associated procedures.
Part 2, “Attribute Reference Guide”	
Chapter 6, “Administration Attributes”	Definitions of DSAME’s administration attributes.
Chapter 7, “Anonymous Authentication Attributes”	Definitions of DSAME’s attributes associated with anonymous authentication.
Chapter 8, “Certificate Authentication Attributes”	Definitions of DSAME’s attributes associated with certificate-based authentication.
Chapter 9, “Core Authentication Attributes”	Definitions of DSAME’s attributes associated with the core authentication service.
Chapter 10, “LDAP Authentication Attributes”	Definitions of DSAME’s attributes associated with LDAP authentication.
Chapter 11, “Membership Authentication Attributes”	Definitions of DSAME’s attributes associated with membership authentication.
Chapter 12, “RADIUS Authentication Attributes”	Definitions of DSAME’s attributes associated with RADIUS authentication.
Chapter 13, “SafeWord Authentication Attributes”	Definitions of DSAME’s attributes associated with SafeWord authentication

Table 1 *Administration Guide* Chapters *(Continued)*

Chapter	Description
Chapter 14, “Unix Authentication Attributes”	Definitions of DSAME’s attributes associated with Unix authentication
Chapter 15, “Logging Attributes”	Definitions of DSAME’s logging service attributes.
Chapter 16, “Naming Attributes”	Definitions of DSAME’s naming service attributes.
Chapter 17, “Platform Attributes	Definitions of DSAME’s platform service attributes.
Chapter 18, “Session Attributes”	Definitions of DSAME’s session service attributes.
Chapter 19, “URL Policy Agent Attributes”	Definitions of the attributes associated with the URL Policy Agent.
Chapter 20, “User Attributes”	Definitions of DSAME’s user attributes.
Index	Alphabetical index of the Administration Guide.

Documentation Conventions Used in This Guide

In the iPlanet Directory Server Access Management Edition documentation, 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 you have installed and running on a dedicated Web Server.
- *Web Server that runs DSAME* refers to the dedicated Web Server where the DSAME is installed.
- *Directory Server* refers to an installed instance of iPlanet Directory Server or Netscape™ Directory Server.
- *DSAME_root* is a variable placeholder for the home directory where you have installed iPlanet Directory Server Access Management Edition.
- *Directory_Server_root* is a variable placeholder for the home directory where you have installed iPlanet Directory Server.
- *Web_Server_root* is a variable placeholder for the home directory where you have installed iPlanet Web 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, iPlanet Web Server, iPlanet Proxy Server, and iPlanet Certificate Management System 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`

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 Certificate Management System Documentation

You can find the iPlanet Certificate Management System documentation at the following site:

http://docs.iplanet.com/docs/manuals/cms.html

iPlanet Proxy Server Documentation

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

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

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

DSAME Console Guide

This is part one of the iPlanet Directory Server Access Management Edition (DSAME) Administration Guide, the DSAME Console Guide. It discusses the DSAME graphical user interface and how to navigate through it. This section contains the following chapters:

- Product Overview
- Service Management
- Policy Management
- User Management
- Authentication Options

Chapter 1

Product Overview

This chapter provides an overview of the features of iPlanet Directory Server Access Management Edition (DSAME). It contains the following sections:

- Directory Server Access Management Edition
- Features of DSAME
- Installing DSAME
- The DSAME Console

Directory Server Access Management Edition

iPlanet DSAME is a set of tools used to leverage the management and security potential of Directory Server, iPlanet's Lightweight Directory Access Protocol-based (LDAP) data store. DSAME integrates Directory Server with a user authentication and single sign-on function which increases data security. It also allows administrators to initiate user entry management based on *roles*, an entry grouping mechanism which appears as an attribute in a user entry. Lastly, developers can define and manage the configuration parameters of a multitude of default and custom-made services. All three of these functions are accessed through a customizable graphical user interface, the web-based DSAME console.

Features of DSAME

DSAME is built on top of an installation of iPlanet Directory Server, version 5.1. The concept is to give directory administrators a more consistent and intuitive interface to work from as well as features used to extend the capabilities of Directory Server.

Service Management

Configuration parameters for default and custom-made business services can be specified with DSAME's service management component. Using XML and the DTD defined within the DSAME framework, service developers can define the parameters of a corporate service (such as a mail service, a billing service or a logging service) and manage the service's parameters or *attributes*. In addition, DSAME allows service administrators to define the value of these attributes.

Policy Management

DSAME also provides a component to define, modify or remove the rules that control access to business resources. Collectively, these rules are referred to as *policy*. Policies can be role-based or organization-based and can offer privileges or define constraints.

Authentication

DSAME provides a plug-in solution for user authentication. The criteria needed to authenticate a particular user is based on the authentication service configured for each organization in the DSAME enterprise. Before being allowed access to a DSAME session, a user must pass through authentication successfully.

Single Sign-On

Once the user is authenticated, DSAME's API for Single Sign-On (SSO) takes over. Each time the authenticated user tries to access a protected page, the SSO API determines whether the user has the permissions required based on their authentication credentials. If the user is valid, access to the page is given without additional authentication. If not, the user will be prompted to authenticate again.

URL Policy Agents

The URL Policy Agent is installed onto a Web Server. It is a specific instance of the DSAME policy component. This agent serves as an additional authentication step when a user sends a request for a web resource that lives on the protected web server. This authentication is in addition to any user authentication check which the resource must do. The agent protects the web server; the resource is protected by the authentication plug-in.

User Management

The user management component allows for the creation and management of user-related objects. User, role, group, people container, organization, sub-organization and organizational unit objects can be defined, modified or deleted using either the DSAME console or the command line interface.

DSAME Console

This HTML-based console provides a graphical user interface for businesses to manage the DSAME enterprise. The console has default administrators with varying degrees of privileges used to create and manage the services, policies and users. (Additional administrators can be created based on roles.) The administrators are defined within the Directory Server when installed with DSAME. These administrators are the:

- Top Level Administrator with read and write access to all entries within the DSAME enterprise.
- Top Level Help Desk Administrator with read access of all entries within the DSAME enterprise.
- Organization Administrator with read and write access to all entries within its organization.
- Organization Help Desk Administrator with read access of all entries within its organization.
- Organizational Unit Administrator with read and write access to all organizational unit entries.
- Organizational Unit Help Desk Administrator with read access of all organizational unit entries.

- People Container Administrator with read and write access to all users within its people container.
- Group Administrator with read and write access to all members of its group.

Installing DSAME

The goal of DSAME is to provide an interface for managing user objects, policies and services for organizations using iPlanet Directory Server. When the DSAME installer is run, an instance of Directory Server is installed. This instance serves as the data store for DSAME. In addition, three modules are integrated into the Directory Server: the Policy module, the Management module, and the URL Policy Agent module.

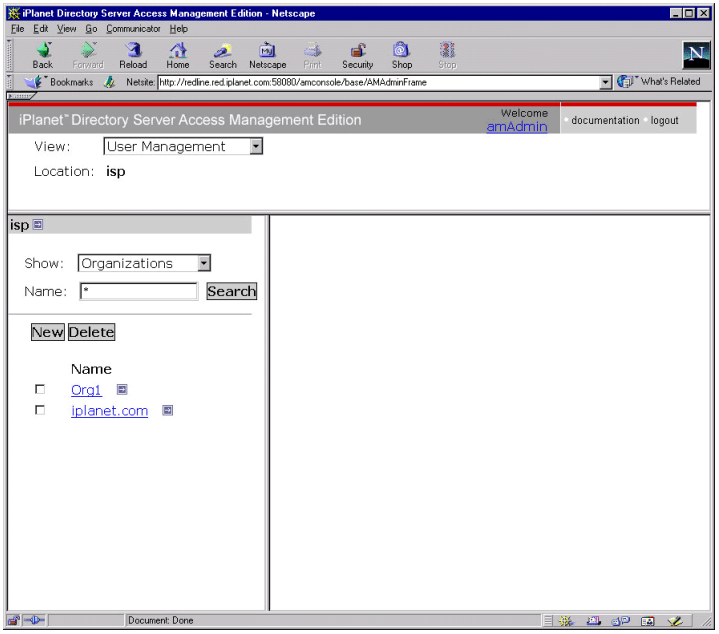
The Policy module consists of the logging module, Single Sign-On (SSO) SDK and the Authentication SPI. The Management module provides policy, user and service management functions through either the DSAME console or the command line interface. The URL Policy Agent validates a user's SSO and web resource access. All of these functions can be accessed through a web browser using the DSAME console.

NOTE The DSAME installer can install the three DSAME modules into an existing Directory Server. For information on how this is done, please see the iPlanet Directory Server Access Management Edition Installation and Deployment Guide.

The DSAME Console

The DSAME console is divided into three sections: the location pane, the navigator pane and the data pane. By using all three panes the administrator is able to navigate the directory, perform user and service configurations and create policies.

Figure 1-1 The DSAME Console



Location Pane

The Location pane runs along the top of the console. The uppermost *View* menu allows the administrator to switch between the three different management views:

- Service Management as discussed in Chapter 2
- Policy Management as discussed in Chapter 3
- User Management as discussed in Chapter 4

The *Location* field provides a trail to the administrator's position in the directory tree. This path is used for navigational purposes.

The *Currently Logged In* field displays the name of the user that is currently running the console with a link to their user profile.

The *Documentation* link opens a browser window containing an HTML version of Part 2 of this documentation, the Attribute Reference Guide.

The *Logout* link allows the user to log out of the DSAME.

Navigation Pane

The Navigation pane is the left portion of the console. The *Directory Object* portion (within the grey box) displays the name of the directory object that is currently open and its *Properties* link. (Most objects displayed in the Navigation pane will have a corresponding *Properties* link. Selecting this link will render the object's attributes in the Data frame to the right.) The Show menu lists the directories under the selected directory object. Depending on the number of sub-directories, a paging mechanism is provided.

Data Pane

The Data pane is the right portion of the console. This is where all object attributes and their values are displayed and configured and where entries are selected for their respective group, role or organization.

Chapter 2

Service Management

This chapter describes the service management features of iPlanet Directory Server Access Management Edition (DSAME). The Service Management interface provides a way to view, manage and configure all DSAME services and their values (both default and customized) in addition to configuring DSAME console display settings. This chapter contains the following sections:

- Definition of a Service
- DSAME Services Defined
- Attribute Types
- Service Management

Definition of a Service

A service is a group of attributes defined under a common name. The attributes define the parameters that the service provides to an organization. For instance, in developing a payroll service, a developer might decide to include attributes that define an employee name, an hourly rate and a tax exemption. When the service is registered to an organization, that organization can use these attributes in the configuration of its entries.

DSAME defines services using Extensible Markup Language (XML). The Service Management Services Document Type Definition (`sms.dtd`) defines the structure of a service XML file. This file can be found in the following directory:

DSAME_root`/SUNWam/web-apps/services/dtd/`

For more information on defining a DSAME service, see the *iPlanet Directory Server Access Management Edition Programmer's Guide.*

DSAME Services Defined

The default services provided with DSAME are defined by XML files located in the following directory:

DSAME_root/SUNWam/web-apps/services/WEB-INF/config/xml

Some of these services, when configured through the Service Management interface, define values for the DSAME application. Others are registered to a specific organization configured within DSAME and are used to define default values for the organization.

Administration

The Administration service allows for the configuration of the DSAME Administration Console at both the application level (similar to a *Preferences* or *Options* menu for the DSAME application) as well as at a configured organization level (*Preferences* or *Options* specific to a configured organization).

Authentication

There are six authentication services including a base service. This allows the administrator the opportunity to choose the method with which each defined organization would have their user's authorization verified.

Core

The Core service is the general configuration base for the DSAME authentication services. It must be registered and configured to use any of the specific services. It allows the administrator to define default values that will be picked up for those not specifically set in the Anonymous, Certificate-based, LDAP, Membership and RADIUS, SafeWord and Unix services.

Anonymous

This service allows for log in without specifying a user name and password. Anonymous connections have limited access to the server and are customized by the administrator.

Certificate-based

This service allows login through a personal digital certificate (PDC). iPlanet Certificate Management System (CMS) can be installed as a Certificate Authority. For more information on CMS, see the documentation set located at `http://docs.iplanet.com/docs/manuals/cms.html`

LDAP

This service allows for authentication using LDAP bind, an operation which associates a password with a particular LDAP entry.

Membership (Self-Registration)

This service allows a new user to self-register for authentication with a login and password.

RADIUS

This service allows for authenticating users using an external Remote Authentication Dial-In User Service (RADIUS) server.

SafeWord

This service allows for authenticating users using a SafeWord server.

NOTE For this release, the SafeWord authentication service is only supported on the Solaris 8 platform.

Unix

This service allows for authenticating users using a Unix server.

NOTE For this release, the Unix authentication service is not supported on the Windows 2000 platform.

Logging

The Logging service is where the administrator configures values for the DSAME application logging function. Examples include log file size and log file location.

Naming

The Naming service is used to get and set URLs, plug-ins and configurations as well as request notifications for various other DSAME services such as session, authentication and logging.

Platform

The Platform service is where additional servers can be added to the DSAME configuration as well as other options applied at the top level of the DSAME application.

Session

The Session service defines values for an authenticated user session such as maximum session time and maximum idle time.

URL Policy Agent

The URL Policy Agent is configured by navigating to the Policy Management window in the graphical user interface. It defines user privileges to web resources, allowing an administrator to allow or deny access to `http` and `https`-based URLs.

User

Default user preferences are defined through the user service. (These include time zone, locale and DN starting view).

Attribute Types

The attributes that make up a DSAME service are classified as one of the following types: *Dynamic*, *Policy*, *User*, *Organization* or *Global*. Using these types to subdivide the attributes in each service allows for a more consistent arrangement of the service schema and easier management of the service parameters.

Dynamic Attributes

A dynamic attribute can be assigned to a DSAME configured role or organization. When the role is assigned to a user or a user is created in an organization, the dynamic attribute then becomes a characteristic of the user. For example, a role is created for an organization's employees. This role might contain the organization's address and a fax number, two things that remain static for all employees. When the role is assigned to each employee, these dynamic attributes are inherited by them.

Policy Attributes

Policy attributes are privilege attributes. Policy attributes are configured through the Policy Management interface as discussed in Chapter 3, "Policy Management." Once a policy is configured, they may be assigned to roles or organizations. That is the only difference between dynamic and policy attributes; dynamic attributes are assigned directly to a role or an organization and policy attributes are used to configure policies and then applied to a role or an organization. DSAME currently has only one service which uses policy attributes, the URL Policy Agent. These specific policy attributes deny or allow users access to web resources.

User Attributes

These attributes are assigned directly to each user. They are not inherited from a role or an organization and, typically, are different for each user. Examples of user attributes include `userid`, `employee number` and `password`. User attributes can be added or removed from the User service by modifying the `dpUser.xml` file. For more information, see the *iPlanet Directory Server Access Management Edition Programmer's Guide*.

Organization Attributes

Organization attributes are assigned to organizations only. In that respect, they work as dynamic attributes. They differ from dynamic attributes, though, as they are not inherited by entries in the subtrees. Additionally, no object classes are associated with organization attributes. Attributes listed in the authentication services are defined as organization attributes because authentication is done at the organization level rather than at a subtree or user level.

Global Attributes

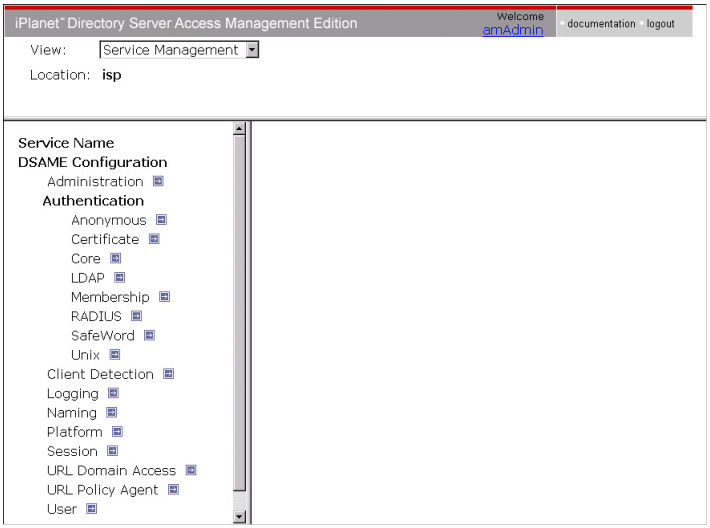
Global attributes are applied across the DSAME configuration. They can not be applied to users, roles or organizations as the goal of global attributes is to customize the DSAME application. There is only one instance of a global attribute in the DSAME configuration. There are no object classes associated with global attributes. Examples of global attributes include log file size, log file location, port number or a server URL that DSAME can use to access data.

Service Management

Services are configured and managed through the Service Management window. Organization-specific services which are not covered by the DSAME default service packages can be written using XML (based on the DSAME services document type definition or DTD) and added into the interface under the Other Configuration heading. Instructions on how this is done can be found in the *iPlanet Directory Server Access Management Edition Programmer's Guide.* Part 2, "Attribute Reference Guide" describes the default services and the definitions of their corresponding attributes.

The Service Management View is for displaying service configurations on a global level. In other words, it is a view of the default configurations of all available services in DSAME, whether registered or not. When a service is registered and activated by an organization, the initial default data assigned to the service is that which is displayed under the service's Service Management page. Figure 2-1 is a screenshot of the graphical user interface.

Figure 2-1 Service Management View



Access the Service Management view by choosing Service Management in the View menu. The navigation pane will display a list of all defined DSAME services. To set the global default values for a service, select the Properties arrow next to the name of the service. The attributes for the service will be displayed in the data pane.

Chapter 3

Policy Management

This chapter describes the policy service management features of iPlanet Directory Server Access Management Edition (DSAME). The Policy Management interface provides a way to view, manage and configure all DSAME policies. This chapter contains the following sections:

- The Policy Service
- The URL Policy Agent
- Hierarchy Of Enforcement
- Policy Management

The Policy Service

Every business has a need to protect its resources. This is done by configuring and managing rules that define who can do what to which resource. The DSAME Policy Service allows an organization to set up these rules or *policies.*

Each DSAME service that is written to enforce policies must have a *policy schema.* A policy schema is a set of rules and all their possible values. In DSAME, a policy schema is defined in an XML document that describes the full range of policy options available for a given service. From the policy schema, an administrator can create named policies, in the Policy Management view, to apply at different levels (role or organization). These named policies, once created, are then assigned to a specific role or organization within the User Management view.

DSAME ships with one policy service, the URL Policy Agent, and one sample mail service. For more information on the sample mail service and writing new policy schema, see the *iPlanet Directory Server Access Management Edition Programmer's Guide*.

The URL Policy Agent

A URL Policy Agent is a plug-in that enforces web access rules. The URL Policy Agent plugs into the iPlanet Web Server and performs two functions:

1. It validates a user's sign on.
2. It enforces the user's URL access.

Validating a User's Sign On

Once a user has logged in to DSAME, each request to the server will contain a user identification token which, in effect, proves that they have been successfully authenticated. The token is unique for a user on a given server. Once the URL Policy Agent intercepts a user's request, it looks for this token to verify that it represents an authenticated user. If the user is represented properly, the request is passed forward and subjected to the user's URL policy enforcement. If the user is not verified, the user is redirected to the Authentication page. (Similarly, if there is no user identification token at all, the user is redirected to the Authentication page.)

Enforcing URL Access

Once a user's identification is verified, the URL Policy Agent checks the user's URL access policies to find out the user's level of access. The URL being requested can be assigned to one of three attributes that are inherited by every entity in an organization's hierarchy when the URL Policy Agent service is registered. These three attributes are *Allow*, *Deny* or *Not Enforced*.

- Allow

  `iplanet-am-web-agent-access-allow-list` is the attribute that contains all the URLs that an authenticated user is allowed to access.

- Deny

  `iplanet-am-web-agent-access-deny-list` is the attribute that contains all the URLs that an authenticated user is not allowed to access.

- Not Enforced

  `iplanet-am-web-agent-access-not-enforced-list` is the attribute that contains all the URLs that are not subjected to URL policy enforcement. However, user authentication is still required to ensure the value of this attribute.

The values of these three attributes are obtained from the aggregation of a user's roles.

Hierarchy Of Enforcement

In the enforcement of policy, deny privileges takes precedence over allow privileges. An empty Deny list will allow only those resources that are allowed by the Allow list. An empty Allow list will not allow access to any resources except those in the Not Enforced list. If the URL access policy cannot be resolved between the Deny and Allow lists, access will not be allowed to the resource.

The following URLs are default values of the Not Enforced option located in the `AMConfig.properties` file. No authentication is required for this option (named `com.iplanet.am.policy.agents.url.notenforcedlist.local`):

- `http://<host>:<port>/amserver/console*`
- `http://<host>:<port>/amserver/login*`
- `http://<host>:<port>/amserver/images*`
- `http://<host>:<port>/amserver/admin*`
- `http://<host>:<port>/amserver/docs*`
- `http://<host>:<port>/amserver/logout`
- `http://<host>:<port>/amserver/index.html`
- `http://<host>:<port>/amserver/namingservice`
- `http://<host>:<port>/amserver/loggingservice`
- `http://<host>:<port>/amserver/sessionservice`
- `http://<host>:<port>/amserver/profileservice`

- `http://<host>:<port>/amagent/html/URLAccessDenied.html`

Allowing all users access to these URLs makes user authentication possible. Any edits made to the `AMConfig.properties` file require a server restart of the agent.

How the URL Policy Agent Works

Below is a description of how the URL Policy Agent works.

1. Upon initialization, the URL Policy Agent reads the Not Enforced list from the `AMConfig.properties` file. Because access to the `/login` screen is not enforced, the user is able to view the login page.
2. After successful user authentication, the user's URL access is Not Enforced until the user's URL Policy values are found.
3. DSAME applies the Deny URLs to the user's URL access.
4. DSAME applies the Allow URLs to the user's URL access.
5. The user's policy profile is complete for this authentication session.

Policy Management

Policies are configured using the Policy Management interface. This interface provides a means for:

- The Top Level Administrator to view, create, delete and modify policies for a specific service that can be used across all organizations.
- An organization's or sub-organization's administrator to view, create, delete and modify policies for specific use by the organization.

In general, policy is created at the organization (or sub-organization) level to be used throughout the organization's tree. In order to create a named policy, the specific policy service must first be registered to the organization under which the policy will be created.

Registering Policy Services

Registering a policy service is the same as registering any type of service; it is done within the User Management interface.

1. Navigate to User Management by choosing View User Management.

   When the DSAME console opens, the default interface is User Management.

2. Choose the organization for which you would like to create policy.

   If logged in as the Top Level Administrator, make sure that the location of the User Management interface is the top level organization where all configured organizations are visible. The default top level organization is `o=isp`.

3. Choose Services from the Show menu.

   If the organization already has registered services, they will be displayed in the navigation pane.

4. Click Register in the navigation pane.

   A listing of services not yet registered to this organization are displayed in the data pane.

5. Select URL Policy Agent checkbox from Register Services.

   The URL Policy Agent service is now registered to the chosen organization.

NOTE Sub-organizations must register their policy services independently of their parent organization. In other words, the sub-organization `o=suborg,o=iplanet,o=isp` will not inherit the policy service from its parent `o=iplanet,o=isp`.

Creating Named Policies

Policies are created through the Policy Management interface. Once a named policy is created, it can be assigned to roles or organizations via the User Management interface.

1. Navigate to Policy Management by choosing View Policy Management.

   Policies can only be created under an organization if that organization has first registered the URL Policy Agent service. See Registering Policy Services above.

2. Choose the organization for which you would like to create a policy.

   Ensure that the location of the Policy Management window is correct for your organization. The default top level organization is `o=isp`.

3. Choose Policies from the Show menu.

   By default, Organizations is visible in the Show menu. All sub-organizations configured, if any, will be visible below it. If creating policies for a sub-organization, choose the sub-organization and then choose Policies from the Show menu.

4. Click New in the navigation pane.

   The New Policy window in the data pane opens. Service URL Policy Agent is selected by default as it is the only policy service available. To add other policy services, see the *iPlanet Directory Server Access Management Edition Programmer's Guide*.

5. Type a name for the policy and click Create.

   The new policy rule window opens under the policy name created.

6. Choose an action for the URL Policy Service.

   The choices Allow, Deny or Not Enforced are explained in "Enforcing URL Access," on page 36.

7. Type a resource in the Resource field and press Add Rule for the URL Policy Service.

   Currently, the only resources that can be enforced are `http://` and `https://` addresses. Wild cards are also supported.

8. Repeat Step 6 and Step 7 to add additional actions to the URL policy.

9. Click Save to complete the named policy's configuration.

   Actions that have already been added to a policy can be deleted by checking the Select box next to the action and pressing Delete.

Assigning Named Policies

Once a policy has been named and created, it can be assigned to the organization or role. This is done using the User Management interface. Assigning a policy at the organization level makes its attributes available to all entries in the organization. Assigning policy to a role makes its attributes available to all users who contain the role attribute.

Assigning Named Policies to an Organization

1. Navigate to User Management by choosing View User Management.

   When the DSAME console opens, the default window is User Management.

2. Choose the organization for which you would like to assign a named policy.

   Ensure that the location of User Management is correct for your organization. The default top level organization is `o=isp`.

3. Choose Policies from the Show menu.

   If the organization already has policies assigned to it, they are displayed in the navigation pane. If the Assign Policies interface is not visible, click Assign and all unassigned policies will be displayed in the data pane.

4. Select the box (or boxes) next to the unassigned policy (or policies) and click Assign.

   The chosen policy (or policies) will be displayed in the navigation pane. The policy is now assigned to the organization.

Assigning Named Policies to a Role

1. Navigate to User Management by choosing View User Management.

   When the DSAME console opens, the default window is User Management.

2. Choose Organizations from the Show menu.

   If the role to which you would like to assign a named policy is in the top level organization, choose Roles from the Show menu and skip to Step 4. (The default top level organization is `o=isp`.)

3. Choose Roles from the Show menu.

   All configured roles for the organization are displayed in the navigation pane.

4. Select the role to which you would like to apply a policy.

   The chosen role displays in the Location field in the uppermost window.

5. Choose Policies from the Show menu.

   If the role already has policies assigned to it, they are displayed in the navigation pane.

6. Click Assign to see a list of all unassigned policies.

7. Choose the box (or boxes) next to the unassigned policy (or policies) and click Assign.

   The chosen policy (or policies) displays in the navigation pane. The policy is now assigned to the role.

NOTE If multiple named policies are assigned to a role or organization, the values for allow and deny will be aggregated. If a priority is desired, the policy schema (XML) can be modified.

Chapter 4

User Management

This chapter describes the user management features of iPlanet Directory Server Access Management Edition (DSAME). The User Management interface provides a way to view, manage and configure all DSAME objects and identities. This chapter contains the following sections:

- The User Management Interface
- Managing DSAME Objects
- Properties Function

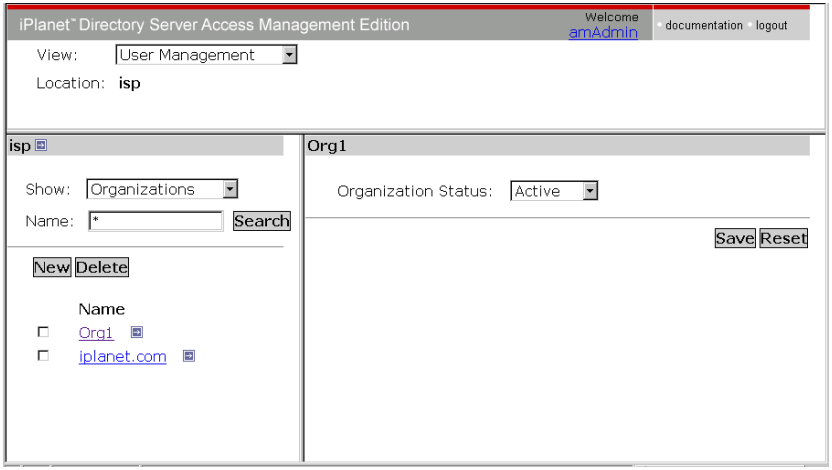
The User Management Interface

There are two types of user management views. Depending on the roles of the user logging in, they might gain access to the User Management View or the User Profile View.

User Management View

When a user with an administrative role authenticates to the DSAME, their default view is the User Management View. In this view the administrator can perform all user-based administrative tasks. This can include, but is not limited to, creating objects and identities, configuring services and assigning policies.

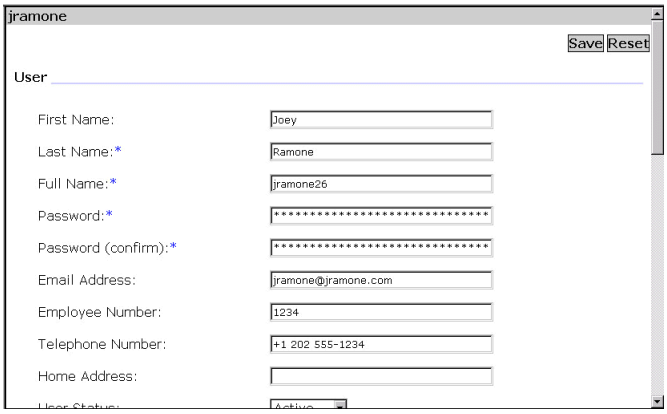
Figure 4-1 User Management View with Organization Properties Displayed



User Profile View

When a user without an administrative role authenticates to the DSAME, the default view is their own User Profile. In this view the user can modify the values of the attributes particular to their personal profile. This can include, but is not limited to, name, home address and password. The attributes displayed in the User Profile View can be extended. For more information on adding customized attributes for objects and identities, see the *iPlanet Directory Server Access Management Edition Programmer's Guide.*

Figure 4-2 User Profile View



Managing DSAME Objects

The User Management interface contains all the components needed to view and manage the DSAME objects (organization, configured enterprise organizations and their corresponding groups, roles, users, policies and containers). This section explains the object types and details on how to configure them.

Organizations

This object represents the top level of a hierarchical structure used by an enterprise to manage its departments and resources. Upon installation, DSAME dynamically creates a top-level organization (default `o=isp`) to manage the DSAME enterprise configurations. Additional organizations can be created after installation to manage separate enterprises. All created organizations fall beneath the top-level organization.

Create an Organization

1. Choose Organizations from the Show menu in User Management.

   All created organizations display in the navigation pane.

2. Click New in the navigation pane.

   The Create Organization template displays in the data pane.

3. Enter a value for the name of the Organization in the New Organization template.
4. Choose a status of `active` or `inactive`.

   The default is `active`. This can be changed at any time during the life of the organization by selecting the Properties icon. Choosing `inactive` disables log in to the organization.
5. Click Create.

   The new organization displays in the navigation pane.

Delete an Organization

1. Choose Organizations from the Show menu in User Management.

   All created organizations display in the navigation pane.
2. Select the checkbox next to the name of the Organization to be deleted.
3. Click Delete.

NOTE There is no warning message when performing a delete. All entries within the organization will be deleted.

Containers

The container entry is used when, due to object class and attribute differences, it is not possible to use an organization entry. It is important to remember that the DSAME container entry and the DSAME organization entry are not necessarily equivalent to the LDAP object classes `organizationalUnit` and `organization`. They are abstract DSAME entries. Ideally, the organization entry will be used instead of the container entry.

Create a Container

1. Navigate to the navigation pane of the Organization or Container where the new Container will be created.

   Use the Show menu in the navigation pane and the Location path in the location pane.
2. Click New.

   A Container template displays in the data pane.

3. Enter the name of the Container to be created.
4. Click Create.

Delete a Container

1. Navigate to the navigation pane of the Organization or Container which contains the Container to be deleted.

   Use the Show menu in the navigation pane and the Location path in the location pane.
2. Choose Containers from the Show menu.
3. Select the checkbox next to the name of the Container to be deleted.
4. Click Delete.

NOTE Deleting a container will delete all objects that exist in that Container. This includes all objects and sub Containers.

People Containers

A People Container is the default LDAP organizational unit to which all users are assigned when they are created within an organization. People Containers can be found at the organization level and at the People Container level as a sub People Container. They can only contain other People Containers and users. Additional People Containers can be added into the organization, if desired.

NOTE The display of People Containers is optional. To view People Containers you must select Show People Containers in the DSAME Administration service. For more information, see “Show People Containers,” on page 78.

Create a People Container

1. Navigate to the navigation pane of the Organization or People Container where the new People Container will be created.

   Use the Show menu in the navigation pane and the Location path in the location pane.

2. Click New.

   A People Container template displays in the data pane.

3. Enter the name of the People Container to be created.

4. Click Create.

Delete a People Container

1. Navigate to the navigation pane of the organization or People Container which contains the People Container to be deleted.

   Use the Show menu in the navigation pane and the Location path in the location pane.

2. Choose People Containers from the Show menu.

3. Select the checkbox next to the name of the People Container to be deleted.

4. Click Delete.

NOTE Deleting a People Container will delete all objects that exist in that People Container. This includes all users and sub People Containers.

Group Containers

A Group Container is used to manage groups. It can only contain groups and other group containers. The group container Groups is dynamically assigned as the parent entry for all managed groups. Additional group containers can be added, if desired.

Create a Group Container

1. Navigate to the navigation pane of the Organization or the Group Container which contains the Group Container to be created.

   Use the Show menu in the navigation pane and the Location path in the location pane.

2. Choose Group Containers from the Show menu.

   The default Groups was created during the organization's creation.

3. Click New.

4. Type a value in the Name field and press Create.

The new Group Container displays in the navigation pane.

Delete a Group Container

1. Navigate to the navigation pane of the Organization which contains the Group Container to be deleted.

   Use the Show menu in the navigation pane and the Location path in the location pane.

2. Choose Group Containers from the Show menu.

   The default Groups and all created Group Containers display in the navigation pane.

3. Select the checkbox next to the Group Container to be deleted.

4. Click Delete Selected.

Roles

This grouping represents a selection of privileged operations. By applying the role to a user or a service, the principal can perform the operations. For example, by confining certain privileges to an Employee role or a Manager role and applying the role to a user, the user's accessibility is confined to the privileges granted it by the role.

Create a Role

1. Navigate to the navigation pane of the Organization where the role will be created.

   Choose Organizations from the Show menu in User Management and select the organization from the navigation pane. The Location path displays the default top-level organization and chosen organization.

2. Choose Roles from the Show menu.

   The default roles created when an organization is configured display in the navigation pane:

   - Organization Admin Role
   - Organization Help Desk Admin Role
   - People Admin

For descriptions of these roles, see “Dynamic Admin Roles ACIs,” on page 82 of the Attribute Reference section.

3. Click New in the navigation pane.

   The Create Role template appears in the data pane.

4. Enter a name for the role.

5. Enter a description of the role.

6. Choose the role type from the Type menu.

   The role can be either an Administrative role or a Service role. The role type is used by the DSAME console to figure out where to start the user in the DIT. An administrative role notifies the console that the possessor of the role has administrative privileges; the service role notifies the console that the possessor is an end user.

7. Choose a default set of ACIs to apply to the role from the Access Permission menu.

   The default ACIs are permissions to access entries within the organization. They are discussed in the section “Default Role Permissions (ACIs),” on page 80. No permissions can also be chosen. (The default ACIs shown are in no particular order.)

8. Click Create.

Delete a Role

1. Navigate to the organization that contains the role for deletion.

   Choose Organizations from the Show menu in User Management and select the organization from the navigation pane. The Location path displays the default top-level organization and chosen organization.

2. Choose Roles from the Show menu.

3. Select the checkbox next to the name of the role.

4. Click Delete.

Add Users to a Role

1. Navigate to the Organization that contains the role to modify.

   Choose Organizations from the Show menu in User Management and select the organization from the navigation pane. The Location path displays the default top-level organization and chosen organization.

2. Choose Roles from the Show menu.
3. Select the role to modify.
4. Choose Users from the Show menu.
5. Click Add.

   A search window appears in the data pane.
6. Enter a user id.

   Search criteria can also be entered (including first name, last name or active/inactive) if specific user id information is not available.
7. Choose the users from the names returned by selecting the checkbox next to the user name.
8. Click Save.

Remove Users from a Role

1. Navigate to the Organization that contains the role to modify.

   Choose Organizations from the Show menu in User Management and select the organization from the navigation pane. The Location path displays the default top-level organization and chosen organization.
2. Choose Roles from the Show menu.
3. Select the role to modify.
4. Choose Users from the Show menu.
5. Select the checkbox of the users for removal.
6. Click Delete.

Services

Activating a service for an organization is a two step process. In the first step you need to register the service with the organization. After a service is registered, a template configured specifically for that organization must be created. For additional information, see Chapter 2, “Service Management.”

NOTE A new service must first be imported into the DSAME through the command line's `amadmin`. Information on importing a service's XML schema can be found in the *iPlanet Directory Server Access Management Edition Programmer's Guide.*

Register a Service

1. Navigate to the Organization where you will add services.

   Choose Organizations from the Show menu in User Management and select the organization from the navigation pane. The Location path displays the default top-level organization and chosen organization.

2. Choose Services from the Show menu.

3. Click Register.

   The data pane will display a list of services available to register to this organization.

4. Select the checkbox next to the services to be added.

5. Click Register.

Create a Template for a Service

1. Navigate to the organization or role where the registered service exists.

   Choose Organizations from the Show menu in User Management and select the organization from the navigation pane. The Location path displays the default top-level organization and chosen organization.

2. Choose Services from the Show menu

3. Click the properties icon next to the name of the service to be activated.

   The data pane displays the message *No Template Available For This Service.*

4. Click Create.

   The data pane displays the default attributes and values for this service.

5. Accept or modify the default values and click Save.

   A template is created for this service for the parent organization or role.

Unregister a Service

1. Navigate to the organization where you will remove services.

   Choose Organizations from the Show menu in User Management and select the organization from the navigation pane. The Location path displays the default top-level organization and chosen organization.

2. Choose Services from the Show menu.
3. Select the checkboxes for the services to remove.
4. Click Unregister.

Policies

Policies define rules to help protect an organization's web resources. They can be assigned to organizations and roles only. Policies cannot be created, deleted or viewed in User Management; they can only be assigned. See Chapter 3, "Policy Management for information on how to configure policies.

Assign a Policy

1. Navigate to the Organization or Role where the policy will be added.

   Use the Show menu in the navigation pane and the Location path in the location pane.

2. Choose Policies in the Show menu.
3. Click Assign.

   A list of registered policies displays in the data pane.

4. Select the checkbox for the policy to assign.
5. Click Assign.

Unassign a Policy

1. Navigate to the organization or role where the policy exists.

   Use the Show menu in the navigation pane and the Location path in the location pane.

2. Choose Policies in the Show menu.
3. Select the checkbox next to the policy to be deleted.

4. Click Unassign.

NOTE These procedures assign and unassign policy from roles and organizations; they do not delete the policy. In order to delete a named policy from the DSAME, navigate to Policy Management, select the named policy's checkbox and click Delete.

Users

Users represent the identity of a person. They are created within an organization's default People Container. If Show People Containers in the Administration service of the organization is disabled, users are visible at the organization level. If Show People Containers is enabled, users are visible within the organization's default People Container. (People Containers are discussed on page 47.)

Create a User

1. Navigate to the Organization or People Container where the user should be created.

   Use the Show menu in the navigation pane and the Location path in the location pane.

2. Choose Users from the Show menu.
3. Click New.
4. Enter values for the required attributes and any optional fields.

   Information on the user profile attributes can be found in "User Profile Attributes," on page 153.

5. Click Create.

Delete a User

1. Navigate to the Organization or People Container where the user exists.

   Use the Show menu in the navigation pane and the Location path in the location pane.

2. Choose Users from the Show menu.
3. Select the checkbox next to the name of the user to be deleted.
4. Click Delete.

Managed Groups

This grouping represents a collection of users with a common function, feature or interest. Typically, this grouping has no privileges associated with it. They can exist at two levels, within an organization and within other managed groups as a sub group. Users can be added to Managed Groups either statically or dynamically (filtered).

Membership By Subscription. A group created by subscription creates a group based on the option chosen in "Managed Group Type" on page 79. If the Managed Group Type value is `static`, group members are added to a group entry using the `groupOfNames` or `groupOfUniqueNames` object class. If the Managed Group Type value is `dynamic`, a LDAP filter is used to search and return only user entries that contain the `memberof` attribute.

Membership By Filter. A filtered group is one that is created through the use of a LDAP filter. All entries are funneled through the filter and dynamically assigned to the group. The filter would look for any attribute in an entry and return those that contain the attribute.

Create a Managed Group

1. Navigate to the Organization or Managed Group where the group will be created.

   Use the Show menu in the navigation pane and the Location path in the location pane. Managed groups are listed underneath Group Containers.

2. Choose Managed Groups from the Show menu.

3. Click New.

4. Select the group type from within the data pane.

   a. If a static subscription group is to be created, select Membership By Subscription.

      I. Enter a name for the group in the Name field.

      II. Add users to the group by selecting Add.

      Adding users to the group is optional. They can be added after the group is created.

      III. Enter a user id to search for a user entry or configure a LDAP filter.

      IV. Choose the users from the names returned by selecting the checkbox next to the user name and pressing Create.

V. Select Users Can Subscribe to this Group to allow users to subscribe to the group themselves.

VI. Click Create.

b. If a dynamic (LDAP filtered) group is to be created, select Membership By Filter and click Save.

I. Enter a name for the group in the Name field.

II. Construct the LDAP search filter.

The fields used to construct the filter use either an OR or AND operator. All the fields listed in the UI are used. If a field is left blank it will match all possible entries for that particular attribute.

III. Click Create.

Delete a Managed Group

1. Navigate to the Organization or Managed Group where the group exists.

   Use the Show menu in the navigation pane and the Location path in the location pane. Managed groups are listed underneath Group Containers.

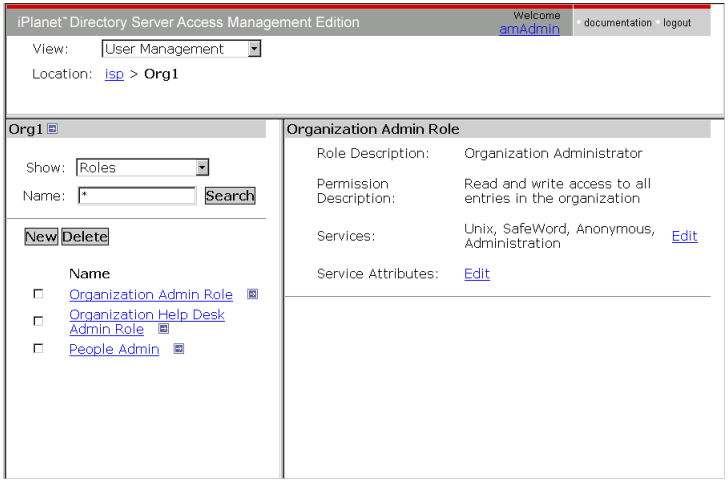
2. Choose Managed Groups from the Show menu.
3. Select the checkbox next to the name of the group to be deleted.
4. Click Delete.

Role Profile View

A Role Based Profile allows for customizing the services available to a role, and the access level for the service attributes, on a per-role basis. Using a Role Based Profile, an administrator can customize the Service and End User pages, and create service administrators who only have access to specific services. For example, an administrator can deny write-access to one or more attributes in the user services for a given role, and a user possessing this role will not be able to modify these attributes. A policy administrator role can be created by granting access to all policy services, but denying access to other services. An administrator possessing the policy administrator role will then be able to create and assign policies, but will be denied from performing user management tasks.

To display the Role Profile page, click on the Properties button associated with a given role in the Show Roles page, as shown in Figure 4-3.

Figure 4-3 Role Profile View

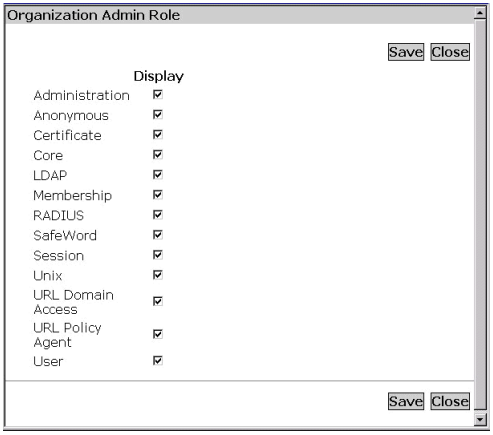


Customize Service Access

1. In the Role Profile page, click Edit in the Services listing. The Service Access page is displayed, as shown in Figure 4-4.
2. Choose a service that is to be granted to the role by clicking on the service name in the Display column. By default, a role has access to all services.
3. Click Save.

NOTE When access to a service is denied (not checked), the service will not be displayed in the Console for the user possessing the role. Additionally, it is not possible to register or unregister a user, assign the service to a user, or create, delete, view or modify the Service template.

Figure 4-4 Service Access Page

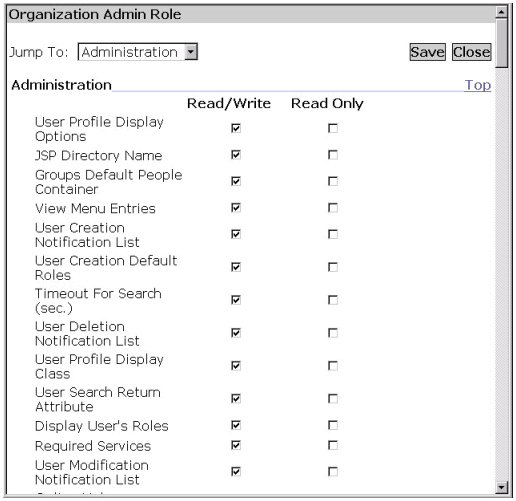


Customize Attribute Access

1. In the Role Profile page, click Edit in the Service Attribute listing. The Attribute Access page is displayed, as shown in Figure 4-5.
2. Use the Jump menu to display the attributes for a particular service.
3. Assign an access level to an attribute by selecting the Read / Write or Read Only check boxes.
4. Click Save.

NOTE If neither the Read / Write or Read Only options are selected for a given attribute, read and write access to that attribute is denied.

Figure 4-5 Attribute Access Page



For more information on specific Service attributes, see Part 2 of this manual, the *Attribute Reference Guide.*

Properties Function

To view or modify an entry's properties, click the arrow next to the object's name. It's attributes and corresponding values are displayed in the data pane. Different objects display different properties.

- Organizations properties allow status modification between active and inactive.
- Role properties include role and permission descriptions and the services registered to the role. ACI details can be viewed by selecting Show Access Permissions.
- User properties include, but are not limited to, basic user information such as first name, last name, home address, telephone number and password.
- The Groups configurable attribute, aside from the naming attribute, is allowing or disallowing the user to self-subscribe themselves to the group.
- Containers do not have any configurable attributes excepting the naming attribute.

- Policy properties are a listing of the URLs being affected by the policy.
- Service properties include any of the attribute listed in Part 2, “Attribute Reference Guide” depending on the service.

See the *iPlanet Directory Server Access Management Edition Programmer’s Guide* for information on how to extend an entry’s properties.

Chapter 5

Authentication Options

iPlanet Directory Server Access Management Edition (DSAME) provides a framework for authentication, a process which verifies the identities of users accessing applications within an enterprise. Authentication is implemented through plug-ins that validate the user's identity. (This plug-in architecture is described more fully in the *iPlanet Directory Server Access Management Edition Programmer's Guide*.) The DSAME console is used to set the default values, to register authentication services, to create an organization's authentication template and to enable the service. This chapter provides an overview of the authentication services and instructions for registering them. It contains the following sections:

- The Core Authentication Service
- Anonymous Authentication
- Certificate-based Authentication
- LDAP Directory Authentication
- Membership Authentication
- RADIUS Server Authentication
- SafeWord Authentication
- Unix Authentication

The Core Authentication Service

Seven different authentication services are provided with DSAME as well as a Core authentication service. The Core authentication service provides overall configuration for the authentication service. Before registering and enabling Anonymous, Certificate-based, LDAP, Membership or RADIUS authentication, Core authentication must be registered and enabled. Chapter 9, “Core Authentication Attributes” contains a detailed listing of the Core attributes.

To Register and Enable the Core Service

1. Navigate to the navigation pane of the Organization for which the Core service is to be registered.

   Use the Show menu in the navigation pane and the Location path in the location pane.

2. Choose Services from the Show menu.

3. Click Register in the navigation pane.

   A list of available services displays in the data pane.

4. Select the checkbox for Core Authentication and click Register.

   The Core Authentication service will appear in the navigation pane assuring the administrator that it has been registered.

5. Click the Core Authentication Properties arrow.

   The message *No template available for this service* appears in the data pane.

6. Click Create.

   The Core attributes appear in the data pane. Modify the attributes as necessary. An explanation of the Core attributes can be found in Chapter 9, “Core Authentication Attributes” or by clicking the Documentation link in the upper right hand corner of the DSAME console.

7. Click Register.

   The Core service has been enabled.

Anonymous Authentication

When this method is enabled, a user can log in to DSAME as an *anonymous* user. Granting anonymous access means that it can be accessed without providing a user name or password. Anonymous access can be limited to specific types of access (for example, access for read or access for search) or to specific subtrees or individual entries within the directory.

To Register and Enable Anonymous Authentication

You must log in to DSAME as the Organization Administrator or Super Administrator.

1. Navigate to the navigation pane of the Organization for which Anonymous Authentication is to be registered.

   Use the Show menu in the navigation pane and the Location path in the location pane.

2. Choose Services from the Show menu.

   The Core service, if already registered, displays in the navigation pane. If it is not already registered, it can be done concurrently with the Anonymous Authentication service.

3. Click Register in the navigation pane.

   A list of available services displays in the data pane.

4. Select the checkbox for Anonymous Authentication and click Register.

   The Anonymous Authentication service will appear in the navigation pane assuring the administrator that it has been registered.

5. Click the Anonymous Authentication Properties arrow.

   The message *No template available for this service* appears in the data pane.

6. Click Create.

   The Anonymous Authentication attributes appear in the data pane. Modify the attributes as necessary. An explanation of these attributes can be found in Chapter 7, “Anonymous Authentication Attributes” or by clicking the Documentation link in the upper right hand corner of the DSAME console.

7. Click Save.

   The Anonymous Authentication service has been enabled.

Logging In Using Anonymous Authentication

In order to log in using Anonymous Authentication, the Core Authentication service attribute “Authentication Menu,” on page 102 must be modified to define Anonymous Authentication. This ensures that when the user logs in using `http://<hostname>:<port>/amserver/login`, they will see the Anonymous Authentication login window.

NOTE The Default Anonymous User Name attribute value in the Anonymous Authentication service is anonymous. This is the name users use to log in. A default Anonymous User must be created within the organization. The user id should be identical to the user name specified in the Anonymous Authentication attributes.

Certificate-based Authentication

Certificate-based Authentication involves using a personal digital certificate (PDC) to identify and authenticate a user. A PDC can be configured to require a match against a PDC stored in Directory Server, and verification against a Certificate Revocation List.

There are a number of things that need to be accomplished before registering the Certificate-based Authentication service to an organization. First, the iPlanet Web Server that is installed with the DSAME needs to be secured and configured for Certificate-based Authentication. Before enabling the Certificate-based service, see Appendix C, Securing Your Web Server in the *iPlanet Directory Server Access Management Edition Installation and Configuration Guide* for these initial Web Server configuration steps.

NOTE Each user that will authenticate using the certificate-based service must request a PDC for their browser. Instructions are different depending upon the browser used. See your browser’s documentation for more information.

To Register and Enable Certificate-based Authentication

You must log in to DSAME as the Organization Administrator or Super Administrator.

1. Navigate to the navigation pane of the Organization for which Certificate-based Authentication is to be registered.

   Use the Show menu in the navigation pane and the Location path in the location pane.

2. Choose Services from the Show menu.

   The Core service, if already registered, displays in the navigation pane. If it is not already registered, it can be done concurrently with the Certificate-based Authentication service.

3. Click Register in the navigation pane.

   A list of available services displays in the data pane.

4. Select the checkbox for Certificate-based Authentication and click Register.

   The Certificate-based Authentication service will appear in the navigation pane assuring the administrator that it has been registered.

5. Click the Certificate-based Authentication Properties arrow.

   The message *No template available for this service* appears in the data pane.

6. Click Create.

   The Certificate-based Authentication attributes appear in the data pane. Modify the attributes as necessary. An explanation of these attributes can be found in Chapter 8, “Certificate Authentication Attributes” or by clicking the Documentation link in the upper right hand corner of the DSAME console.

7. Click Save.

Logging In Using Certificate-based Authentication

In order to log in using Certificate-based Authentication, the Core Authentication service attribute “Authentication Menu,” on page 102 must be modified to define Certificate-based Authentication. This ensures that when the user logs in using `http://<hostname>:<port>/amserver/login`, they will see the Certificate-based Authentication login window.

LDAP Directory Authentication

With the LDAP Authentication service, when a user logs in, he or she is required to bind to the LDAP Directory Server with a specific user DN and password. If the user provides a user id and password that are in the Directory Server, the user is allowed access to, and is set up with, a valid DSAME session. LDAP Authentication is enabled by default when DSAME is installed. The following instructions are provided in the event that the service is disabled.

To Register and Enable LDAP Authentication

You must log in to DSAME as the Organization Administrator or Super Administrator.

1. Navigate to the navigation pane of the Organization for which LDAP Authentication is to be registered.

   Use the Show menu in the navigation pane and the Location path in the location pane.

2. Choose Services from the Show menu.

   The Core service, if already registered, displays in the navigation pane. If it is not already registered, it can be done concurrently with the LDAP Authentication service.

3. Click Register in the navigation pane.

   A list of available services displays in the data pane.

4. Select the checkbox for LDAP Authentication and click Register.

   The LDAP Authentication service will appear in the navigation pane assuring the administrator that it has been registered.

5. Click the LDAP Authentication Properties arrow.

   The message *No template available for this service* appears in the data pane.

6. Click Create.

   The LDAP Authentication attributes appear in the data pane. Modify the attributes as necessary. An explanation of these attributes can be found in Chapter 10, “LDAP Authentication Attributes” or by clicking the Documentation link in the upper right hand corner of the DSAME console.

7. Click Save.

   The LDAP Authentication service has been enabled.

Logging In Using LDAP Authentication

In order to log in using LDAP Authentication, the Core Authentication service attribute “Authentication Menu,” on page 102 must be modified to define LDAP Authentication. This ensures that when the user logs in using `http://<hostname>:<port>/amserver/login`, they will see the LDAP Authentication login window.

Enabling LDAP Authentication Failover

The LDAP authentication attributes include a value field for both a primary and a secondary Directory Server. DSAME will look to the second server for authentication if the primary server becomes unavailable. For more information, see the LDAP attributes “Primary LDAP Server and Port,” on page 114 and “Secondary LDAP Server and Port,” on page 114.

Membership Authentication

Membership authentication is implemented similarly to personalized sites such as `my.netscape.com`, or `mysun.sun.com`. When this service is enabled, a user creates an account and personalizes it without the aid of an administrator. With this new account, the user can access it as a registered user. The user can also access the viewer interface, saved on the iPlanet user profile database as authorization data and user preferences.

To Register and Enable Membership Authentication

You must log in to DSAME as the Organization Administrator or Super Administrator.

1. Navigate to the navigation pane of the Organization for which Membership Authentication is to be registered.

   Use the Show menu in the navigation pane and the Location path in the location pane.

2. Choose Services from the Show menu.

   The Core service, if already registered, displays in the navigation pane. If it is not already registered, it can be done concurrently with the Membership Authentication service.

3. Click Register in the navigation pane.

   A list of available services displays in the data pane.

4. Select the checkbox for Membership Authentication and click Register.

   The Membership Authentication service will appear in the navigation pane assuring the administrator that it has been registered.

5. Click the Membership Authentication Properties arrow.

   The message *No template available for this service* appears in the data pane.

6. Click Create.

   The Membership Authentication attributes appear in the data pane. Modify the attributes as necessary. An explanation of these attributes can be found in Chapter 11, “Membership Authentication Attributes” or by selecting the Documentation link in the upper right hand corner of the DSAME console.

7. Click Save.

   The Membership Authentication service has been enabled.

Logging In Using Membership Authentication

In order to log in using Membership Authentication, the Core Authentication service attribute “Authentication Menu,” on page 102 must be modified to define Membership Authentication. This ensures that when the user logs in using `http://<hostname>:<port>/amserver/login`, they will see the Membership Authentication login window.

RADIUS Server Authentication

DSAME can be configured to work with a RADIUS server that is already installed. This is useful if there is a legacy RADIUS server being used for authentication in your enterprise. Enabling the RADIUS authentication service is a two-step process.

1. Configure the RADIUS server.

   For detailed instructions, see the RADIUS server documentation.

2. Register and enable the RADIUS authentication service.

NOTE A user must be created in the DSAME organization using the RADIUS server that matches each user specified when the RADIUS server user file was modified.

To Register and Enable RADIUS Authentication

You must log in to DSAME as the Organization Administrator or Super Administrator.

1. Navigate to the navigation pane of the Organization for which RADIUS Authentication is to be registered.

   Use the Show menu in the navigation pane and the Location path in the location pane.

2. Choose Services from the Show menu.

   The Core service, if already registered, displays in the navigation pane. If it is not already registered, it can be done concurrently with the RADIUS Authentication service.

3. Click Register in the navigation pane.

   A list of available services displays in the data pane.

4. Select the checkbox for RADIUS Authentication and click Register.

   The RADIUS Authentication service will appear in the navigation pane assuring the administrator that it has been registered.

5. Click the RADIUS Authentication Properties arrow.

   The message *No template available for this service* appears in the data pane.

6. Click Create.

   The RADIUS Authentication attributes appear in the data pane. Modify the attributes as necessary. An explanation of these attributes can be found in Chapter 12, “RADIUS Authentication Attributes” or by selecting the Documentation link in the upper right hand corner of the DSAME Administration Console.

7. Click Save.

   The RADIUS Authentication service has been enabled.

Logging In Using RADIUS Authentication

In order to log in using RADIUS Authentication, the Core Authentication service attribute “Authentication Menu,” on page 102 must be modified to define RADIUS Authentication. This ensures that when the user logs in using `http://<hostname>:<port>/amserver/login`, they will see the RADIUS Authentication login window.

SafeWord Authentication

DSAME can be configured to handle SafeWord Authentication requests to Secure Computing’s SafeWord authentication server. DSAME provides the client portion of SafeWord authentication. The SafeWord server may exist on the system on which DSAME is installed, or on a separate system.

NOTE For this release, the SafeWord Authentication service is only supported on the Solaris 8 platform.

To Register and Enable SafeWord Authentication

You must log in to DSAME as the Organization Administrator or Super Administrator.

1. Navigate to the navigation pane of the Organization for which SafeWord Authentication is to be registered.

   Use the Show menu in the navigation pane and the Location path in the location pane.

2. Choose Services from the Show menu.

   The Core service, if already registered, displays in the navigation pane. If it is not already registered, it can be done concurrently with the SafeWord Authentication service.

3. Click Register in the navigation pane.

   A list of available services displays in the data pane.

4. Select the checkbox for SafeWord Authentication and click Register.

   The SafeWord Authentication service will appear in the navigation pane, assuring the administrator that it has been registered.

5. Click the SafeWord Authentication Properties arrow.

   The message *No template available for this service* appears in the data pane.

6. Click Create.

   The SafeWord Authentication attributes appear in the data pane. Modify the attributes as necessary. An explanation of these attributes can be found in Chapter 13, “SafeWord Authentication Attributes,” or by clicking the Documentation link on the upper righthand corner of the DSAME Console.

7. Click Save.

   The SafeWord Authentication service has been enabled.

Unix Authentication

DSAME can be configured to process authentication requests against Unix userids and passwords known to the (Solaris) system on which DSAME is installed. While there is only one organizational attribute, and a few global attributes for Unix authentication, there are some system-oriented considerations.

In order to authenticate locally-administered userids (see `admintool` (1M)), root access is required. If DSAME is installed to run as `nobody`, or a userid other than root, then the `<install_dir>/SUNWam/bin/doUnix` process must still execute as root. The `passwd` entry in the `/etc/nsswitch.conf` file determines whether the `/etc/passwd` and `/etc/shadow` files, or NIS are consulted for authentication.

Unix Authentication makes use of an authentication “helper”, which is a separate process from the main DSAME process. Upon startup, this helper listens on a port for configuration information. There is only one Unix helper per DSAME server to serve all of its organizations.

To Register and Enable Unix Authentication

You must log in to the DSAME as Super Administrator for the following steps.

1. Navigate to the Navigation pane and select the Service Management View.
2. Click on the Unix Authentication Properties arrow in the Service Name list.

   Several Global and one Organization attributes are displayed. Because one Unix helper serves all of the DSAME server's organizations, most of the Unix attributes are global. An explanation of these attributes can be found in Chapter 14, “Unix Authentication Attributes,” or by clicking the Documentation link in the upper righthand corner of the DSAME console.
3. Click Save to save the new values for the attributes.

You may log in to the DSAME as the Organization Administrator to enable Unix Authentication for an organization.

4. Navigate to the navigation pane of the Organization for which Unix Authentication is to be registered.

   Use the Show menu in the navigation pane and the Location path in the location pane.
5. Choose Services from the Show menu.

The Core service, if already registered, displays in the Navigation pane. If it is not already registered, it can be done concurrently with the Unix Authentication service.

6. Click Register in the navigation pane.

   A list of available services displays in the data pane.

7. Select the checkbox for Unix Authentication and click Register.

   The Unix Authentication service will appear in the Navigation pane, assuring the administrator that it has been registered.

8. Click the Unix Authentication Properties arrow.

   The message *No template available for this service* appears in the date pane.

9. Click Create.

   The Unix Authentication organization attribute appears in the data pane. Modify the Authentication Level attribute as necessary. An explanation of this attribute can be found in Chapter 14, “Unix Authentication Attributes,” or by clicking the Documentation link in the upper righthand corner of the DSAME console.

10. Click Save.

    The Unix Authentication service has been enabled.

Part 2

Attribute Reference Guide

This is the Attribute Reference Guide, part two of the iPlanet Directory Server Access Management Edition (DSAME) Administration Guide. It discusses the configured attributes within DSAME's default services. This part contains the following chapters:

- Administration Attributes
- Anonymous Authentication Attributes
- Certificate Authentication Attributes
- Core Authentication Attributes
- LDAP Authentication Attributes
- Membership Authentication Attributes
- RADIUS Authentication Attributes
- SafeWord Authentication Attributes
- Unix Authentication Attributes
- Logging Attributes
- Naming Attributes
- Platform Attributes
- Session Attributes
- URL Policy Agent Attributes
- User Attributes

Chapter 6

Administration Attributes

The Administration Service consists of global and organization attributes. The values applied to the global attributes are applied across the iPlanet Directory Server Access Management Edition (DSAME) configuration and are inherited by every configured organization. They can not be applied directly to roles or organizations as the goal of global attributes is to customize the DSAME application. Values applied to the organization attributes are default values for each organization configured and can be changed when the service is registered to the organization. The organization attributes are not inherited by entries of the organization. The Administration Attributes are divided into:

- Global Attributes
- Organization Attributes

Global Attributes

The global attributes in the Administration Service are:

- Show People Containers
- Display Containers In Menu
- Show Group Containers
- Managed Group Type
- Attribute Uniqueness Enabled
- Default Role Permissions (ACIs)
- Domain Component Tree Enabled
- Admin Groups Enabled

- Compliance User Deletion Enabled
- Dynamic Admin Roles ACIs
- User Profile Service Classes

Show People Containers

This attribute specifies whether to display People Containers in the DSAME console. If this option is selected, the menu choice People Containers displays in the Show menu for Organizations, Containers and Group Containers. People Containers will be seen at the top-level only for a flat DIT.

People containers are organizational units containing user profiles.It is recommended that you use a single people container in your DIT and leverage the flexibility of roles to manage access and services. The default behavior of the DSAME console is therefore to hide the People Container. However, if you have multiple people containers in your DIT, select Show People Containers to display People Containers as managed objects in the DSAME console.

Display Containers In Menu

This attribute specifies whether to display any containers in the Show menu of the DSAME console. The default value is `false`. An administrator can optionally chose either:

- `false` (checkbox not selected) — Containers are not listed among the choices on the Show menu at the top level for organizations and other containers.
- `true` (checkbox selected) — Containers are listed among the choices on the Show menu at the top level and for organizations and other containers.

Show Group Containers

This attribute specifies whether to show Group Containers in the DSAME console. If this option is selected, the menu choice Group Containers displays in the Show menu for organizations, containers, and group containers. Group containers are organizational units for groups.

Managed Group Type

This option specifies whether subscription groups created through the DSAME Console are static or dynamic. The console will either create and display subscription groups that are static or dynamic, not both. (Filtered groups are always supported regardless of the value given to this attribute.) The default value is dynamic.

- A static group explicitly lists each group member using the `groupOfNames` or `groupOfUniqueNames` object class. The group entry contains the `uniqueMember` attribute for each member of the group. Members of static groups are manually added; the user entry itself remains unchanged. Static groups are suitable for groups with few members.
- A dynamic group uses a `memberOf` attribute in the entry of each group member. Members of dynamic groups are generated through the use of an LDAP filter which searches and returns all entries which contain the `memberOf` attribute. Dynamic groups are suitable for groups that have a very large membership.
- A filtered group uses an LDAP filter to search and return members that meet the requirement of the filter. For instance, the filter can generate members with a specific uid (`uid=g*`) or email address (`email=*@sun.com`). In these examples, the LDAP filter would return all users whose uid begins with `g` or whose email address ends with `sun.com`, respectively. Filtered groups can only be created within the User Management view by choosing Membership by Filter. See “Managed Groups,” on page 55 for more information.

An administrator can select one of the following:

- `Dynamic` — Groups created through the Membership By Subscription option will be dynamic.
- `Static` — Groups created through the Membership By Subscription option will be static.

NOTE The Managed Group Type option is only available when DSAME is installed using the default mode.

Attribute Uniqueness Enabled

When this attribute is selected as `true`, attribute uniqueness is enabled and verified for every user creation. The default is `false`.

Default Role Permissions (ACIs)

This attribute defines a list of default access control instructions (ACIs) or *permissions* that are used to grant administrator privileges when creating new roles. One of these ACIs is selected depending on the level of privilege desired. DSAME ships with two default role permissions:

Organization Help Desk Admin

The Organization Help Desk Administrator has read access to all entries in the configured organization and write access to the `userPassword` attribute.

NOTE Roles are defined using the format `aci_name | aci_desc | dn:aci ## dn:aci ## dn:aci` where:

- *aci_name* is the name of the ACI.
- *aci_desc* is a description of the access these ACIs allow. For maximum usability, assume the reader of this description does not understand ACIs or other directory concepts.

aci_name and *aci_desc* are i18n keys contained in the `amAdminUserMsgs.properties` file. The values displayed in the console come from the `.properties` file, and the keys are used to retrieve those values.

- *dn:aci* represents pairs of DNs and ACIs separated by ##. DSAME sets each ACI in the associated DN entry. This format also supports tags that can be substituted for values that would otherwise have to be specified literally in an ACI: ROLENAME, ORGANIZATION, GROUPNAME and PCNAME. Using these tags lets you define roles flexible enough to be used as defaults. When a role is created based on one of the default roles, tags in the ACI resolve to values taken from the DN of the new role.

Organization Admin

The Organization Administrator has read and write access to all entries in the configured organization.

Domain Component Tree Enabled

The Domain Component tree (DC tree) is an iPlanet-specific DIT structure used by many iPlanet components to map between DNS names and organizations' entries.

When this option is enabled, the DC tree entry for an organization is created, provided that the DNS name of the organization is entered at the time the organization is created. The DNS name field will appear in the Organization Create page. This option is only applicable to top level organizations, and will not be displayed for suborganizations.

Any status change made to the `inetdomainstatus` attribute through the DSAME SDK in the organization tree will update the corresponding DC tree entry status. (Updates to status that are not made through the DSAME SDK will not be synchronized.) For example, if a new organization, `sun`, is created with the DNS name attribute sun.com, the following entry will be created in the DC tree:

`dc=sun,dc=com,o=internet,<`*root suffix*`>`

The DC tree may optionally have its own root suffix configured by setting `com.iplanet.am.domaincomponent` in `AMCONFIG.properties`. By default, this is set to the DMSAME root. If a different suffix is desired, this suffix must be created using LDAP commands. The ACIs for administrators that create organizations required modification so that they have unrestricted access to the new DC tree root.

Admin Groups Enabled

This option specifies whether to create the DomainAdministrators and DomainHelpDeskAdministrators groups. If selected (`true`), these groups are created and associated with the Organization Admin Role and Organization Help Desk Admin Role, respectively. Once created, adding or removing a user to one of these associated roles automatically adds or removes the user from the corresponding group. This behavior, however, does not work in reverse. Adding or removing a user to one of these groups will not add or remove the user in their associated roles.

The DomainAdministrators and DomainHelpDeskAdministrators groups are only created in organizations that are created after this option is enabled.

NOTE This option does not apply to suborganizations, with the exception of the `root org`. At the `root org`, the ServiceAdministrators and ServiceHelpDesk Administrators groups are created and associated with the Top-level Admin and Top-level Help Desk Admin roles, respectively. The same behavior applies.

Compliance User Deletion Enabled

This option specifies whether a user's entry will be deleted, or just marked as deleted, from the directory. When a user's entry is deleted and this option is selected (`true`), the user's entry will still exist in the directory, but will be marked as deleted. User entries that are marked for deletion are not returned during Directory Server searches. If this option is not selected, the user's entry will be deleted from the directory.

Dynamic Admin Roles ACIs

This attribute defines the access control instructions for the administrator roles that are created dynamically when a group, organization, container or people container is configured using DSAME. These roles are used for granting administrative privileges for the specific grouping of entries created. The default ACIs can be modified only under this attribute listing.

CAUTION Administrators at the Organization and People Container level have a wider scope of access than do group administrators. But, by default, when a user is added to a group administrator role, that user can change the password of anyone in the group. This would include any organization or people container administrator who is a member of that group.

Top-level Admin

The Top-level Administrator has read and write access to all entries in the top level organization. In other words, this Top-level Admin role has privileges for every configuration principal within the DSAME application.

Organization Admin

The Organization Administrator has read and write access to all entries in an organization. When an organization is created, the Organization Admin role is automatically generated with the necessary privileges to manage the organization.

Organization Help Desk Admin

The Organization Help Desk Administrator has read access to all entries in an organization and write access to the `userPassword` attribute.

NOTE When a sub-organization is created, remember that the administration roles are created in the sub-organization, not in the parent organization.

Container Admin

The Container Admin role has read and write access to all entries in an LDAP organizational unit. In DSAME, the LDAP organizational unit is often referred to as a container.

Container Help Desk Admin

The Container Help Desk Admin role has read access to all entries in an organizational unit and write access to the `userPassword` attribute in user entries only in this organizational unit.

Group Admin

The Group Administrator has read and write access to all members of a specific group, and can create new users, assign users to the groups they manage, and delete the users the that they have created.

When a group is created, the Group Administrator role is automatically generated with the necessary privileges to manage the group. The role is not automatically assigned to a group member. It must be assigned by the group's creator, or anyone that has access to the Group Administrator Role.

People Container Admin

By default, any user entry in an newly created organization is a member of that organization's People Container. The People Container Administrator has read and write access to all entries in the organization's People Container. Keep in mind that the this role DOES NOT have read and write access to the attributes that contain role and group DNs therefore, they cannot modify the attributes of, or remove a user from, a role or a group.

NOTE Other containers can be configured with DSAME to hold user entries, group entries or even other containers. To apply an Administrator role to a container created after the organization has already been configured, the Container Admin Role or Container Help Desk Admin defaults would be used.

User Profile Service Classes

This attribute lists the services that will have a custom display in the User Profile page. The default display generated by the Administration Console may not be sufficient for some services. This attribute creates a custom display for any service, giving full control over what and how the service information is displayed. The syntax is as follows:

<s*ervice name*> | <*relative url*>

NOTE Services that are listed in this attribute will not display in the User Create pages. Any data configuration for a custom service display must be performed the User Profile pages.

Organization Attributes

The organization attributes in the administration service are:

- Groups Default People Container
- Groups People Container List
- Display User's Roles
- User Profile Display Class
- Display User's Groups

- User Group Self Subscription
- User Profile Display Options
- User Creation Default Roles
- View Menu Entries
- Maximum Results Returned From Search
- Timeout For Search (sec.)
- JSP Directory Name
- Online Help Documents
- Required Services
- User Search Key
- User Search Return Attribute
- User Creation Notification List
- User Deletion Notification List
- User Modification Notification List
- Unique Attribute List

Groups Default People Container

This field specifies the default People Container where users will be placed when they are created. There is no default value. A valid value is the DN of a people container. See the note under Groups People Container List attribute for the People Container fallback order.

Groups People Container List

This field specifies a list of People Containers from which a Group Administrator can choose when creating a new user. This list can be used if there are multiple People Containers in the directory tree. (If no People Containers are specified in this list or in the Groups Default People Container field, users are created in the default DSAME people container, `ou=people`.) There is no default value for this field. The syntax for this attribute is as follows:

<group name>|<dn of people container>

For a Group Administrator to have access to the relevant People Container, this attribute must be set before creating the group.

NOTE When a user is created, this attribute is checked for a container in which to place the entry. If the attribute is empty, the Groups Default People Container attribute is checked for a container. If the latter attribute is empty, the entry is created under `ou=People`.

Display User's Roles

This option specifies whether to display a list of roles assigned to a user as part of their user profile page. If the value is `false` (not selected), the user profile page shows the user's roles only for administrators. The default value is `false`.

User Profile Display Class

This attribute specifies the java class used by the Administration Console when it displays the User Profile pages.

Display User's Groups

This option specifies whether to display a list of groups assigned to a user as part of their user profile page. If the value is `false` (not selected), the user profile page shows the user's groups only for administrators. The default value is `false`.

User Group Self Subscription

This option specifies whether users can add themselves to groups that are open to subscription. If the value is false, the user profile page allows the user's group membership to be modified only by an administrator. The default value is `false`.

NOTE This option applies only when the Display User's Groups option is selected.

User Profile Display Options

This menu specifies which service attributes will be displayed in the user profile page. An administrator can select from the following:

- `UserOnly` — Display viewable User schema attributes for services assigned to the user.

  User service attribute values are viewable by the user when the attribute contains the keyword Display. See the *iPlanet Directory Server Access Management Edition Programmer's Guide* for details.

- `Combined` — Display viewable User and Dynamic schema attributes for services assinged to the user.

User Creation Default Roles

This listing defines roles that will be assigned to newly created users automatically. There is no default value. An administrator can input the DN of one or more roles.

NOTE This field only takes a full Distinguished Name address, not a role name.

View Menu Entries

This field lists the Java classes of services that will be displayed in the View menu at the top of the DSAME console. The syntax is `i18N key | java class name.` (The i18N key is used for the localized name of the entry in the View menu.)

Maximum Results Returned From Search

This field defines the maximum number of results returned from a search. The default value is 100.

CAUTION Do not set this value above 500. The search will be refused.

Timeout For Search (sec.)

This field defines the amount of time (in number of seconds) that a search will continue before timing out. It is used to stop potentially long searches. After the maximum search time is reached, an error is returned. The default is 5 seconds.

JSP Directory Name

This field specifies the name of the directory that contains the `.jsp` files used to construct the Administration Console, to give an organization a different appearance (customization). The `.jsp` files need to be copied into the directory that is specified in this field.

Online Help Documents

This field lists the online help links that will be created on the main DSAME help page. This allows other applications to add their online help links in the DSAME page. The format for this attribute is as follows:

linki18nkey | *html page to load when clicked* | *i18n properties file*

For example:

```
DSAME Help | /dpAdminHelp.html | amAdminModuleMsgs
```

Required Services

This field lists the services that are dynamically added to the users' entries when they are created. Administrators can choose which services are added at the time of creation.

This attribute is not used by the console, but by the DSAME SDK. Users that are dynamically created will be assigned the services listed in this attribute.

User Search Key

This attribute defines the attribute name that is to be searched upon when performing a simple search in the Navigation page. The default value for this attribute is cn. For example, if this attribute uses the default:

If you enter `j*` in the Name field in the Navigation frame, users whose names begins with “j” or “J” will be displayed.

User Search Return Attribute

This attribute defines the attribute name used when displaying the users returned from a simple search. The default of this attribute is cn, and the full name of the user will be displayed.

User Creation Notification List

This field defines a list of email addresses that will be sent notification when a new user is created.

User Deletion Notification List

This field defines a list of email addresses that will be sent notification when a new user is deleted.

User Modification Notification List

This field defines a list of attributes and email addresses associated with the attribute. When a user modification occurs on an attribute defined in the list, the email address associated with the attribute will be sent notification. Each attribute can have a different set of addresses associated to it.

NOTE The attribute name is the same as it appears in the Directory Server schema, and not as the display name in the Administration Console.

Unique Attribute List

This attribute is a list of attributes defined in the iPlanet Directory Server schema. When the Attribute Uniqueness Enabled attribute is selected as `true`, each parent organization of the user that is being created is checked to see if the Unique Attribute List attribute is configured. If it is configured, a search is executed

starting from that organization for the entire subtree, to determine if any users exist with any of the attribute values contained in the list. If such an entry exists, an error is returned. If such an entry does not exist, the next suborganization is checked. Once all suborganizations have been checked, the user is created.

Anonymous Authentication Attributes

The Anonymous Authentication attributes are organization attributes. The values applied to them under Service Management become the default values for the Anonymous Authentication template. A template is created for each organization when the organization registers for the service. The default values can be changed after registration by the organization's administrator. Organization attributes are not inherited by entries in the subtrees of the organization. The Anonymous Authentication attributes are:

- Authentication Level
- Valid Anonymous User List
- Default Anonymous User Name

Authentication Level

The authentication level is set separately for each method of authentication. The value indicates how much to trust an authentication. Once a user has authenticated, this value is stored in the SSO token for the session. When the SSO token is presented to an application the user wants to access, the application uses the stored value to determine whether the level is sufficient to grant the user access. (The value in this attribute is not specifically used by DSAME but by any external application that may chose to use it.) If the authentication level stored in an SSO token does not meet the minimum value required, the application can prompt the user to authenticate again through a service with a higher authentication level. The default value is `0`, the lowest authentication level.

NOTE If no authentication level is specified, the SSO token stores the value specified in the Core Authentication attribute Default Auth Level. See "Default Auth Level," on page 107 for details.

Valid Anonymous User List

This field contains a list of user IDs that have permission to login without providing credentials. If a user's login name matches a user ID in this list, access is granted and the session is assigned to the specified user ID. If the user's login name does not match a user ID in this list, anonymous access is still granted, but the session is assigned to the user ID specified in the Default Anonymous User Name field.

NOTE In order to login with a user ID defined in Valid Anonymous User List, the user must use the following URL:

```
http://<hostname>:<port>/<DEPLOY_URI>/login?module=
Anonymous&org=<org_name>&username=<user_id>
```

Default Anonymous User Name

This field defines the user ID that a session is assigned to if the login name does not match a user ID in the Valid Anonymous User List field. The default value is anonymous. An Anonymous user must also be created in the organization.

NOTE In order to login using the anonymous authentication service, the user defined in Default Anonymous User Name must use the following URL:

```
http://<hostname>:<port>/<DEPLOY_URI>/login?module=
Anonymous&org=<org_name>
```

Certificate Authentication Attributes

The Certificate Authentication attributes are organization attributes. The values applied to them under Service Management become the default values for the Certificate Authentication template. A template is created for each organization when the organization registers for a service. The default values can be changed after registration by the organization's administrator. Organization attributes are not inherited by entries in the subtrees of the organization. The Certificate Authentication attributes are:

- Match Certificate in LDAP
- Attribute In Cert To Use To Search LDAP
- Match Certificate to CRL
- Attribute In Cert To Use To Search CRL
- LDAP Server and Port
- LDAP Start Search DN
- LDAP Access Authentication Type
- LDAP Server Principal User
- LDAP Server Principal Password
- LDAP Attribute for Profile ID
- SSL On For LDAP Access
- Field in Cert to Use to Access User Profile
- Alternate Attribute Name To Use To Access User Profile
- Authentication Level

Match Certificate in LDAP

This option specifies whether to check if the user certificate presented at login is stored in the LDAP Server. If no match is found, the user is denied access. If a match is found and no other validation is required, the user is granted access. The default is that the Certificate Authentication service does not check for the user certificate.

NOTE A certificate stored in the Directory Server is not necessarily valid; it may be on the certificate revocation list. See "Match Certificate to CRL," on page 94.

Attribute In Cert To Use To Search LDAP

This field specifies the attribute of the certificate's `SubjectDN` value that will be used to search LDAP for certificates. The actual value will be used for the search. The default is `CN`.

Match Certificate to CRL

This option specifies whether to compare the user certificate against the Certificate Revocation List (CRL) in the LDAP Server. This check is performed against a user certificate after a matching user profile is found (see "Match Certificate in LDAP," on page 94). If the certificate is on the CRL, the user is denied access; if not, the user is allowed to proceed. This attribute is, by default, not enabled.

NOTE Certificates should be revoked when the owner of the certificate has changed status and no longer has the right to use the certificate or when the private key of a certificate owner has been compromised.

Attribute In Cert To Use To Search CRL

This field specifies the attribute of the received certificate's `subjectDN` value that will be used to search LDAP for revoked certificates. The actual value will be used for the search. The default is `CN`.

LDAP Server and Port

This field specifies the name and port number of the LDAP server where the certificates are stored. The default value is the host name and port specified when DSAME was installed. The host name and port of any LDAP Server where the certificates are stored can be used. The format is *host_name:port*.

LDAP Start Search DN

This field specifies the DN of the node where the search for the user's certificate should start. There is no default value. The field will recognize any valid DN.

LDAP Access Authentication Type

This menu specifies whether the name and password of the principal user are required for LDAP access and whether those values are sent as plain or encrypted text. The user ID of the principal user is specified in the LDAP Server Principal User field. The default value is none. The valid values are:

- `none` — Access to LDAP does not require the name or password of the principal user.
- `simple` — Access to LDAP requires a user name and password. These values are sent to LDAP in plain text.
- `CRAM-MD5` — Access to LDAP requires a user name and password. These values are sent to LDAP in encrypted text.

LDAP Server Principal User

This field accepts the DN of the principal user (usually Directory Manager) for the LDAP server where the certificates are stored. There is no default value for this field which will recognize any valid DN. The principal user must be authorized to read, and search certificate information stored in the Directory Server.

LDAP Server Principal Password

This field carries the LDAP password associated with the user specified in the LDAP Server Principal User field. There is no default value for this field which will recognize the valid LDAP password for the specified principal user.

NOTE This value is stored as readable text in the directory.

LDAP Attribute for Profile ID

This field specifies the attribute in the Directory Server entry that matches the certificate whose value should be used to identify the correct user profile. There is no default value for this field which will recognize any valid attribute in a user entry (cn, sn, and so on) that can be used as the user ID.

SSL On For LDAP Access

This option specifies whether to use SSL to access the LDAP server. The default is that the Certificate Authentication service does not use SSL for LDAP access.

Field in Cert to Use to Access User Profile

This menu specifies which field in the certificate should be used to search for a matching user profile. For example, if you choose `email address`, the certificate authentication service will search for the user profile that matches the attribute `emailAddr` in the user certificate. The user logging in then uses the matched profile. The default field is `subject CN`. The list contains:

- email address
- issuer DN
- issuer CN
- issuer O
- serial number
- subject CN
- subject DN

- subject O
- subject UID
- other

Alternate Attribute Name To Use To Access User Profile

If the value of the Field in Cert to Use to Access User Profile attribute is set to `other`, then this field specifies the attribute that will be selected from the received certificate's `subjectDN` value. The authentication service will then search the user profile that matches the value of that attribute.

Authentication Level

The authentication level is set separately for each method of authentication. The value indicates how much to trust an authentication. Once a user has authenticated, this value is stored in the SSO token for the session. When the SSO token is presented to an application the user wants to access, the application uses the stored value to determine whether the level is sufficient to grant the user access. (The value in this attribute is not specifically used by DSAME but by any external application that may chose to use it.) If the authentication level stored in an SSO token does not meet the minimum value required, the application can prompt the user to authenticate again through a service with a higher authentication level. The default value is `0`, the lowest authentication level.

NOTE If no authentication level is specified, the SSO token stores the value specified in the Core Authentication attribute Default Auth Level. See "Default Auth Level," on page 107 for details.

Core Authentication Attributes

The Core Authentication service is the basic service for the Anonymous, Certificate, LDAP, Membership, Safeword, Unix and RADIUS authentication services as well as any custom authentication service created with the Authentication SPI. Core authentication must be configured as a service for each organization that wishes to use any form of authentication. The Core Authentication attributes consist of global and organization attributes.The values applied to the global attributes are applied across the iPlanet Access Management Edition (DSAME) configuration and are inherited by every configured organization. (They can not be applied directly to roles or organizations as the goal of global attributes is to customize the DSAME application.) The values applied to the organization attributes under Service Management become the default values for the Core Authentication template. A template is created for each organization when the organization registers for the core service. The default values can be changed after registration by the organization's administrator. Organization attributes are not inherited by entries in the organization. The Core Authentication attributes are separated into:

- Global Attributes
- Organization Attributes

Global Attributes

The organization attributes in the Core Authentication service are:

- Pluggable Auth Module Classes
- Pluggable Auth Page Generator Classes
- LDAP Connection Pool Size
- LDAP Connection Default Pool Size

Pluggable Auth Module Classes

This field specifies the Java classes of the authentication services available to any organization configured within the DSAME platform. By default, this includes LDAP, SafeWord, Anonymous, Application, Membership, Unix, Certification, and RADIUS. DSAME also includes a public SPI that can be used to add other authentication services. To define new services, this field must take a text string specifying the full class name (including package name) of each new authentication service.

Pluggable Auth Page Generator Classes

This attribute specifies the default authentication page generator class, which generates HTML. If a different format page generator is added, its full classname must be specified.

LDAP Connection Pool Size

This attribute specifies the minimum and maximum connection pool to be used on a specific server and port. This attribute is for LDAP and Membership authentication services only. The format is as follows:

```
server:port:min:max
```

NOTE This connection pool is different than the SDK connection pool configured in `serverconfig.xml`.

LDAP Connection Default Pool Size

This attribute sets the default minimum and maximum connection pool to be used with all LDAP authentication module configurations. If an entry for the host and port exists in the LDAP Connection Pool Size attribute, the minimum and maximum settings will be used from LDAP Connection Default Pool Size.

Organization Attributes

The organization attributes in the Core Authentication service are:

- Authentication Menu
- Dynamic User Profile Creation
- Organization URL Mapping
- Admin Authenticator
- Dynamic User Profile Creation Default Roles
- Authentication Chaining Modules
- Authentication Chaining Enabled
- Persistent Cookie Mode
- Persistent Cookie Max Time (seconds)
- Non Interactive Modules
- User's Default Redirect URL
- User Based Auth
- People Container For All Users
- Alias Search Attribute Name
- Default Auth Level
- User Naming Attribute
- Pluggable Auth Page Generator Class
- Default Auth Locale
- Login Failure Lockout Mode
- Login Failure Lockout Duration (minutes)
- Login Failure Lockout Count
- Login Failure Lockout Interval (minutes)
- Email Address to Send Lockout Notification
- Warn User After N Failure
- Lockout Attribute Name
- Lockout Attribute Value

Authentication Menu

This list specifies the default authentication services available to the organization. Each administrator can choose the type of authentication for their specific organization. If one service is chosen, that module's login page is immediately displayed. If multiple services are selected, a list of possible authentication modules is presented to the users at login. (Multiple services provide flexibility, but users must be sure that their login setting is appropriate for the selected authentication module.) The default authentication is LDAP. The authentication services included with DSAME are:

- Anonymous
- Cert
- LDAP
- Membership
- RADIUS
- SafeWord
- Unix

NOTE Currently, the SafeWord authentication service is only supported on the Solaris platform.

The Administrator must create and notify the core and authentication module templates in a created organization for that organization to function properly.

Dynamic User Profile Creation

This option specifies whether to create a profile dynamically when a user authenticates successfully but no user profile is found. (User profiles would be created in the location specified in "People Container For All Users," on page 106.) If security considerations require a controlled user population, do not enable this feature. By default, dynamic user profile creation is not enabled.

Organization URL Mapping

This list determines a user's login organization based on the *host:URI* portion of the URL used for login. When a user logs in, the authentication service takes the *host:URI* portion of the URL and checks it against strings in this list. Each organization has its own URL mapping list for matching. The first match found sets the organization for the user. For example, if the value of Organization URL Mapping is `engr` and a user logs in using the URL:

`http://`*`hostname:port`*`/amserver/login?module=<authModuleName>&org=engr`

The login organization of the user is determined to be `engr`. If this value is not specified, the user's organization is assumed to be the default organization specified during DSAME installation. (This option can also be used to map simple URLs for hosted environments; for instance, `http://`*`orgname`*`.com/amserver/login`, can be mapped to more difficult URLs like that listed above. This simplifies the login URL that a user must remember.)

NOTE The Organization URL Mapping value must be unique across all organizations in the DSAME platform. Therefore, this value should be configured at the organization level (in User Management view after the service has been registered) only. At root level (in Service Management view), this field should be left empty.

Admin Authenticator

This menu specifies the authentication service for administrators only. An administrator is a user who needs access to the DSAME console. This attribute can be used if the authentication method for administrators needs to be different from the method for end users. The default value is `LDAP`. The only authentication choices are Cert, SafeWord, RADIUS, and Unix.

Dynamic User Profile Creation Default Roles

This field specifies the roles assigned to a new user whose profiles are created through the feature "Dynamic User Profile Creation," on page 102". There is no default value. The administrator must specify the DNs of the roles that will be assigned to the new user.

NOTE The role specified must be under the organization for which authentication is being configured.

Authentication Chaining Modules

This field specifies additional services a user must authenticate past in order to login. For example, if the Authentication Menu attribute is set to LDAP and the Authentication Chaining Module attribute is set to RADIUS, a user must authenticate through LDAP and then RADIUS to login. There is no default value. Two or more of the following services can be specified in the order you would like them to be implemented:

- Anonymous
- Cert
- LDAP
- Membership
- RADIUS
- SafeWord
- Unix

NOTE The Authentication Chaining field is case sensitive. Type the module names exactly as shown above, using single spaces to delimit the module names.

Authentication Chaining Enabled

This option activates authentication chaining as described in “Authentication Chaining Modules,” on page 104. If authentication chaining is enabled but no modules are specified in the Authentication Chaining Modules field, the authentication attempt will pass. The default value is that authentication chaining is not enabled.

Persistent Cookie Mode

This option determines whether users can restart the browser and still return to their authenticated session. User sessions can be retained by enabling Persistent Cookie Mode. When Persistent Cookie Mode is enabled, a user session does not expire until its persistent cookie expires. The expiration time is specified in Persistent Cookie Max Time (seconds). The default value is that Persistent Cookie Mode is not enabled and the authentication service uses only memory cookies.

NOTE A persistent cookie must be explicitly requested by the client using the `iDSPCookie=yes` parameter in the login URL. Once the persistent cookie has been set, the `iDSPCookie` parameter expires.

Persistent Cookie Max Time (seconds)

This field specifies the interval after which a persistent cookie expires. (Persistent Cookie Mode must be enabled by selecting its checkbox.) The interval begins when the user's session has been successfully authenticated. The default value is `2147483` (time in seconds). The field will take any integer value between `0` and `2147483`.

Non Interactive Modules

This field specifies the authentication services that can be used in addition to those defined in "Authentication Menu," on page 102. These modules do not appear in the authentication menu presented to users, but a user can choose to use a non-interactive authentication service by directly entering the URL for the service.

For example, if `Cert` is one of the selected non-interactive authentication services, a user can login to DSAME using the following URL:

`http://`*`hostname:port`*`/<DEPLOY_URI>/login?module=Cert`

If a user tries to login to DSAME using an authentication service not listed in either Authentication Menu or Non-Interactive Modules, the Authentication Module Denied page displays. The default non-interactive module value is `Cert`. The administrator can select one or more services from the list:

- Anonymous
- Cert
- LDAP

- Membership
- RADIUS
- SafeWord
- Unix

NOTE Currently, the SafeWord authentication service is only supported on the Solaris platform.

User's Default Redirect URL

This field specifies the URL to which users are redirected after successful authentication. The default value is the DSAME console URL, `amconsole/base/AMAdminFrame`. The field will take any valid URL.

User Based Auth

This option allows different authentication services to be configured for individual users within an organization. When logging on to the DSAME server, a user is first presented with a screen to submit their user ID. Their user profile is then retrieved and the individual authentication method assigned to them is called. By default, user-based authentication is not enabled.

People Container For All Users

After successful authentication by a user, their profile is retrieved. The value in this field specifies where to search for the profile. Generally, this value will be the DN of the default People Container. All user entries added to an organization are automatically added to the organization's default People Container. The default value is `ou=People`, and generally, this is completed with the organization name(s) and root suffix. The field will take a valid DN for any organizational unit.

NOTE Authentication searches for a user profile by:

- Searching under the default People Container, then
- Searching under the default organization, then
- Searching for the user in the default organization using the Alias Search Attribute Name attribute.

The final search is for SSO cases where the user name used to authenticate may not be the naming attribute in the profile. For example, user may authenticate using Safeword ID of `jn10191`, but their profile is `uid=jamie`.

Alias Search Attribute Name

After successful authentication by a user, their profile is retrieved. This field specifies a second LDAP attribute to search from if a search on the first LDAP attribute, specified in "User Naming Attribute," on page 108, fails to locate a matching user profile. Primarily, this attribute will be used when the user identification returned from an authentication module is not the same as that specified in User Naming Attribute. For example, a RADIUS server might return `abc1234` but the user name is `abc`. There is no default value for this attribute. The field will take any valid LDAP attribute (for example, `cn`).

Default Auth Level

The authentication level value indicates how much to trust authentications. Once a user has authenticated, this value is stored in the SSO token for the session. When the SSO token is presented to an application the user wants to access, the application can use the stored value to determine whether the level is sufficient to grant the user access. If the authentication level stored in an SSO token does not meet the minimum value required, the application can prompt the user to authenticate again through a service with a higher authentication level.

The authentication level should be set within the organization's specific authentication template. The Default Auth Level value described here will apply only when no authentication level has been specified in the Authentication Level field for a specific organization's authentication template. The Default Auth Level default value is `0`, the lowest authentication level. (The value in this attribute is not used by DSAME but by any external application that may chose to use it.)

User Naming Attribute

After successful authentication by a user, their profile is retrieved. The value of this attribute specifies the LDAP attribute to use for the search. By default, DSAME assumes that user entries are identified by the `uid` attribute. If your Directory Server uses a different attribute (such as `givenname`) specify the attribute name in this field.

Pluggable Auth Page Generator Class

This field specifies the Java class that generates the login page for users. The default class specified is `com.iplanet.authentication.spi.HTMLLoginWorker`. The default can be overridden by specifying another value which includes the full name (including package name) of the Java class that will generate the default login page.

Default Auth Locale

This field specifies the default language subtype to be used by the authentication service. The default value is `en_US`. A listing of valid language subtypes can be found in Table 9-1.

NOTE In order to use a different locale, all authentication templates for that locale must first be created. A new directory must then be created for these templates. See the iPlanet Directory Server Access Management Edition Programmer's Guide for more information.

Table 9-1 Supported Language Locales

Language Tag	Language
af	Afrikaans
be	Byelorussian
bg	Bulgarian
ca	Catalan
cs	Czechoslovakian
da	Danish

Table 9-1 Supported Language Locales *(Continued)*

Language Tag	Language
de	German
el	Greek
en	English
es	Spanish
eu	Basque
fi	Finnish
fo	Faroese
fr	French
ga	Irish
gl	Galician
hr	Croatian
hu	Hungarian
id	Indonesian
is	Icelandic
it	Italian
ja	Japanese
ko	Korean
nl	Dutch
no	Norwegian
pl	Polish
pt	Portuguese
ro	Romanian
ru	Russian
sk	Slovakian
sl	Slovenian
sq	Albanian
sr	Serbian
sv	Swedish
tr	Turkish

Table 9-1 Supported Language Locales *(Continued)*

Language Tag	Language
uk	Ukrainian
zh	Chinese

Login Failure Lockout Mode

This feature specifies whether to disallow a user to re-authenticate (lockout) if that user has initially failed to authenticate. Selecting this attribute will enable the lockout. By default, the lockout feature is not enabled.

Login Failure Lockout Duration (minutes)

This attribute defines (in minutes) the duration that a user will not be allowed to attempt to re-authenticate, if a lockout has occurred.

If this attribute value is set to 0, and Login Failure Lockout Mode is enabled, the user will be locked out by setting the Lockout Attribute Name in their entry to Lockout Attribute Value.

Login Failure Lockout Count

This attribute defines the number of attempts that a user may try to authenticate, within the time interval defined in Login Failure Lockout Interval (minutes), before being locked out.

For example, if Login Failure Lockout Count is set to 5, and Login Failure Lockout Interval (minutes) is set to 5, then a user has five chanced within five minutes to authenticate before being locked out.

Login Failure Lockout Interval (minutes)

This attribute defines (in minutes) the amount of time in which the number of authentication attempts (as defined in Login Failure Lockout Count) can be completed, before a user is locked out.

For example, if Login Failure Lockout Count is set to 5, and Login Failure Lockout Interval (minutes) is set to 5, then a user has five chanced within five minutes to authenticate before being locked out.

Email Address to Send Lockout Notification

This attribute specifies an email address that will receive notification if a user lockout occurs.

Warn User After N Failure

This attribute specifies the number of authentication failures that can occur before DSAME sends a warning message that the user will be locked out.

Lockout Attribute Name

This attribute contains the `ientuserstaus` value that is set in the Lockout Attribute Value attribute. If a user is locked out, and the Login Failure Lockout Duration (minutes) variable is set to 0, `inetuserstatus` will be set to inactive, prohibiting the user from attempting to authenticate.

Lockout Attribute Value

This attribute specifies the `inetuserstatus` value (contained in Lockout Attribute Name) of the user status as either active or inactive. If a user is locked out, and the Login Failure Lockout Duration (minutes) variable is set to 0, `inetuserstatus` will be set to inactive, prohibiting the user from attempting to authenticate.

LDAP Authentication Attributes

The LDAP Authentication attributes are organization attributes. The values applied to them under Service Management become the default values for the LDAP Authentication template. A template is created for each organization when the organization registers for a service. The default values can be changed after registration by the organization's administrator. Organization attributes are not inherited by entries in the organization. The LDAP Authentication attributes are:

- Primary LDAP Server and Port
- Secondary LDAP Server and Port
- DN to Start User Search
- DN for Root User Bind
- Password for Root User Bind
- User Entry Naming Attribute
- User Entry Search Attributes
- User Search Filter
- Search Scope
- Enable SSL to LDAP Server
- Return User DN To Auth
- Authentication Level

Primary LDAP Server and Port

This field specifies the host name and port number of the primary LDAP server specified during DSAME installation. This is the first server contacted for LDAP authentication. The format is `hostname:port`. (If there is no port number, assume `389`.) Multiple entries must be prefixed by the local server name.

Secondary LDAP Server and Port

This field specifies the host name and port number of a secondary LDAP server available to the DSAME platform. If the primary LDAP server does not respond to a request for authentication, this server would then be contacted. If this server goes down, DSAME will switch back to the primary server. The format is also `hostname:port`. Multiple entries must be prefixed by the local server name.

CAUTION When authenticating users from a Directory Server that is remote from the DSAME enterprise, it is important that both the Primary and Secondary LDAP Server Ports have values. The value for one Directory Server location can be used for both fields.

DN to Start User Search

This field specifies the DN of the node where the search for a user would start. (For performance reasons, this DN should be as specific as possible.) The default value is the root of the directory tree. Any valid DN will be recognized. Multiple entries must be prefixed by the local server name.

NOTE If multiple users match the same search, authentication will fail.

DN for Root User Bind

This field specifies the DN of the user that will be used to bind to the Directory Server specified in the Primary LDAP Server and Port field as administrator. The authentication service needs to bind as this DN in order to search for a matching user DN based on the user login ID. There is no default value. Any valid DN will be recognized.

Password for Root User Bind

This field carries the password for the administrator profile specified in the DN for Root User Bind field. There is no default value. Only the administrator's valid LDAP password will be recognized.

User Entry Naming Attribute

After successful authentication by a user, the user's profile is retrieved. The value of this attribute is used to perform the search. The field specifies the LDAP attribute to use. By default, DSAME assumes that user entries are identified by the `uid` attribute. If your Directory Server uses a different attribute (such as `givenname`) specify the attribute name in this field.

NOTE The user search filter will be a combination of the Search Filter attribute and the User Entry Naming Attribute.

User Entry Search Attributes

This field lists the attributes to be used to form the search filter for a user that is to be authenticated, and allows the user to authenticate with more than one attribute in the user's entry. For example, if this field is set to `uid`, `employeenumber` and `mail`, the user could authenticate with any of these names.

User Search Filter

This field specifies an attribute to be used to find the user under the DN to Start User Search field. It works with the User Entry Naming Attribute. There is no default value. Any valid user entry attribute will be recognized.

Search Scope

This menu indicates the number of levels in the Directory Server that will be searched for a matching user profile. The search begins from the node specified in the attribute “DN to Start User Search,” on page 114. The default value is `SUBTREE`. One of the following choices can be selected from the list:

- OBJECT — Searches only the specified node
- ONELEVEL — Searches at the level of the specified node and one level down
- SUBTREE — Search all entries at and below the specified node

Enable SSL to LDAP Server

This option enables SSL access to the Directory Server specified in the Primary and Secondary LDAP Server and Port field. By default, the box is not checked and the SSL protocol will not be used to access the Directory Server.

Return User DN To Auth

When the DSAME directory is the same as the directory configured for LDAP, this option may be enabled. If enabled, this option allows the LDAP authentication module to return the DN instead of the `userId`, and no search is necessary. Normally, an authentication module returns only the `userId`, and the authentication service searches for the user in the local DSAME LDAP.

Authentication Level

The authentication level is set separately for each method of authentication. The value indicates how much to trust an authentication. Once a user has authenticated, this value is stored in the SSO token for the session. When the SSO token is presented to an application the user wants to access, the application uses the stored value to determine whether the level is sufficient to grant the user access. (The value in this attribute is not specifically used by DSAME but by any external application that may chose to use it.) If the authentication level stored in an SSO token does not meet the minimum value required, the application can prompt the user to authenticate again through a service with a higher authentication level. The default value is `0`, the lowest authentication level.

NOTE If no authentication level is specified, the SSO token stores the value specified in the Core Authentication attribute Default Auth Level. See “Default Auth Level,” on page 107 for details.

Membership Authentication Attributes

The Membership Authentication attributes are organization attributes. The values applied to them under Service Management become the default values for the Membership Authentication template. A template is created for each organization when the organization registers for a service. The default values can be changed after registration by the organization's administrator. Organization attributes are not inherited by entries in the subtrees of the organization. The Membership Authentication attributes are:

- Minimum Password Length
- Default User Roles
- User Status After Registration
- Primary LDAP Server and Port
- Secondary LDAP Server and Port
- DN to Start User Search
- DN for Root User Bind
- Password for Root User Bind
- User Naming Attribute
- User Entry Search Attributes
- User Search Filter
- Search Scope
- Enable SSL to LDAP Server
- Return User DN To Auth
- Authentication Level

Minimum Password Length

This field specifies the minimum number of characters required for a password set during self-registration. The default value is 8.

If this value is changed, it should also be changed in the registration and error text in the following files:

<*install_dir*>/SUNWam/web-apps/services/WEB-INF/config/auth/default/invalidPassword.html

<*install_dir*>/SUNWam/web-apps/services/WEB-INF/config/auth/default/register.html

<*install_dir*>/locale/amAuthMembership.properties *(*PasswordMinChars *entry)*

Default User Roles

This field specifies the roles assigned to new users whose profiles are created through self-registration. There is no default value. The administrator must specify the DNs of the roles that will be assigned to the new user.

NOTE The role specified must be under the organization for which authentication is being configured.

User Status After Registration

This menu specifies whether services are immediately made available to a user who has self-registered. The default value is Active and services are available to the new user. By selecting Inactive, the administrator chooses to make no services available to a new user.

Primary LDAP Server and Port

This field specifies the host name and port number of the primary Directory Server. This is the first server searched for membership authentication. The default value is the Directory Server URL specified during DSAME installation. The format is `hostname:port`. If you use multiple entries, the entries must be prefixed by the local sever name.

Secondary LDAP Server and Port

This field specifies the host name and port number of the secondary Directory Server. If the primary server does not respond to a request for authentication, this server would then be contacted. There is no default value for this field. The format is `hostname:port`.If you use multiple entries, the entries must be prefixed by the local sever name.

DN to Start User Search

This field specifies the DN of the node where the search for a user would start. (For performance reasons, this DN should be as specific as possible.) The default value is the root of the directory tree. Any valid DN will be recognized. If you use multiple entries, the entries must be prefixed by the local server name.

NOTE If multiple users match the same search, authentication will fail.

DN for Root User Bind

This field specifies the DN of the user that will be used to bind to the Directory Server specified in the Primary LDAP Server and Port field as administrator. The authentication service needs to bind as this DN in order to search for a matching user DN based on the user login ID. There is no default value. Any valid DN will be recognized.

Password for Root User Bind

This field carries the password for the administrator profile specified in the DN for Root User Bind field. There is no default value. Only the administrator's valid LDAP password will be recognized.

User Naming Attribute

This field specifies the attribute used for the naming convention of user entries. By default, DSAME assumes that user entries are identified by the `uid` attribute. If your Directory Server uses a different attribute (such as `givenname`) specify the attribute name in this field.

User Entry Search Attributes

This field lists the attributes to be used to form the search filter for a user that is to be authenticated, and allows the user to authenticate with more than one attribute in the user's entry. For example, if this field is set to `uid`, `employeenumber` and `mail`, the user could authenticate with any of these names.

User Search Filter

This field specifies an attribute to be used to find the user under the DN to Start User Search field. It works with the User Naming Attribute. There is no default value. Any valid user entry attribute will be recognized.

Search Scope

This menu indicates the number of levels in the Directory Server that will be searched for a matching user profile. The search begins from the node specified in the attribute "DN to Start User Search," on page 121. The default value is `SUBTREE`. One of the following choices can be selected from the list:

- OBJECT — Searches only the specified node

- ONELEVEL — Searches at the level of the specified node and one level down
- SUBTREE — Search all entries at and below the specified node

Enable SSL to LDAP Server

This option enables SSL access to the Directory Server specified in the Primary and Secondary LDAP Authentication Server field. By default, the box is not checked and the SSL protocol will not be used to access the Directory Server.

Return User DN To Auth

When the DSAME directory is the same as the directory configured for LDAP, this option may be enabled. If enabled, this option allows the LDAP authentication module to return the DN instead of the `userId`, and no search is necessary. Normally, an authentication module returns only the `userId`, and the authentication service searches for the user in the local DSAME LDAP.

Authentication Level

The authentication level is set separately for each method of authentication. The value indicates how much to trust an authentication. Once a user has authenticated, this value is stored in the SSO token for the session. When the SSO token is presented to an application the user wants to access, the application uses the stored value to determine whether the level is sufficient to grant the user access. (The value in this attribute is not specifically used by DSAME but by any external application that may chose to use it.) If the authentication level stored in an SSO token does not meet the minimum value required, the application can prompt the user to authenticate again through a service with a higher authentication level. The default value is `0`, the lowest authentication level.

NOTE If no authentication level is specified, the SSO token stores the value specified in the Core Authentication attribute Default Auth Level. See “Default Auth Level,” on page 107 for details.

RADIUS Authentication Attributes

The RADIUS Authentication attributes are organization attributes. The values applied to them under Service Management become the default values for the RADIUS Authentication template. A template is created for each organization when the organization registers for a service. The default values can be changed after registration by the organization's administrator. Organization attributes are not inherited by entries in the organization. The RADIUS Authentication attributes are:

- RADIUS Server 1
- RADIUS Server 2
- RADIUS Shared Secret
- RADIUS Server's Port
- Authentication Level
- Timeout (Seconds)

RADIUS Server 1

This field displays the IP address or host name of the primary RADIUS server. The default IP address is `127.0.0.1`. The field will recognize any valid IP address or host name. Multiple entries must be prefixed by the local server name.

RADIUS Server 2

This field displays the IP address or host name of the secondary RADIUS server. It is a failover server which will be contacted if the primary server could not be contacted. The default IP address is `127.0.0.1`. Multiple entries must be prefixed by the local server name.

RADIUS Shared Secret

This field carries the shared secret for RADIUS authentication. The shared secret should have the same qualifications as a well-chosen password. There is no default value for this field.

RADIUS Server's Port

This field specifies the port on which the RADIUS server is listening. The default value is `1645`.

Authentication Level

The authentication level is set separately for each method of authentication. The value indicates how much to trust an authentication. Once a user has authenticated, this value is stored in the SSO token for the session. When the SSO token is presented to an application the user wants to access, the application uses the stored value to determine whether the level is sufficient to grant the user access. (The value in this attribute is not specifically used by DSAME but by any external application that may chose to use it.) If the authentication level stored in an SSO token does not meet the minimum value required, the application can prompt the user to authenticate again through a service with a higher authentication level. The default value is `0`, the lowest authentication level.

NOTE If no authentication level is specified, the SSO token stores the value specified in the Core Authentication attribute Default Auth Level. See "Default Auth Level," on page 107 for details.

Timeout (Seconds)

This field specifies the time interval in seconds to wait for the RADIUS server to respond before a timeout. The default value is 3 seconds. It will recognize any number specifying the timeout in seconds.

Timeout (Seconds)

SafeWord Authentication Attributes

The SafeWord Authentication Attributes are organization attributes. The values applied to them under Service Management become the default values for the SafeWord Authentication template. A template is created for each organization when the organization registers for a service. The default values can be changed after registration by the organization's administrator. Organization attributes are not inherited by entries in the subtrees of the organization. The SafeWord Authentication attributes are:

- SafeWord Server Specification
- SafeWord System Name
- SafeWord Server Verification Files Path
- SafeWord Logging Level
- SafeWord Log Path
- SafeWord Module Authentication Level

SafeWord Server Specification

This field specifies the SafeWord server name and port. Port 7482 is set as the default.

SafeWord System Name

This field specifies the system name configured in the SafeWord server. The default system name is `STANDARD`.

SafeWord Server Verification Files Path

This field specifies the directory into which the SafeWord client library places its verification files. The default is as follows:

```
/var/opt/SUNWam/auth/safeword/serverVerification
```

If a different directory is specified in this field, the directory must exist before attempting SafeWord authentication.

SafeWord Logging Level

This attribute specifies the logging level for the SafeWord client. The default is 0.

SafeWord Log Path

This attribute specifies the directory path and log file name for SafeWord client logging. The default path is as follows:

```
/var/opt/SUNWam/auth/safeword/safe.log
```

If a different path or filename is specified, they must exist before attempting SafeWord authentication.

SafeWord Module Authentication Level

The authentication level is set separately for each method of authentication. The value indicates how much to trust an authentication. Once a user has authenticated, this value is stored in the SSO token for the session. When the SSO token is presented to an application the user wants to access, the application uses the stored value to determine whether the level is sufficient to grant the user access. (The value in this attribute is not specifically used by DSAME but by any external application that may chose to use it.) If the authentication level stored in an SSO token does not meet the minimum value required, the application can prompt the user to authenticate again through a service with a higher authentication level. The default value is `0`, the lowest authentication level.

NOTE If no authentication level is specified, the SSO token stores the value specified in the Core Authentication attribute Default Auth Level. See “Default Auth Level,” on page 107 for details.

Unix Authentication Attributes

The Unix Authentication Service consists of global and organization attributes. The values applied to the global attributes are applied across the iPlanet Directory Server Access Management Edition (DSAME) configuration, and are inherited by every configured organization. They can not be applied directly to roles or organizations, as the goal of global attributes is to customize the DSAME application. Values applied to the organization attributes are default values for each organization configured and can be changed when the service is registered to the organization. The organization attributes are not inherited by entries of the organization. The Unix Authentication Attributes are divided into:

- Global Attributes
- Organization Attribute

Global Attributes

The global attributes in the Unix Authentication service are:

- Unix Helper Configuration Port
- Unix Helper Authentication Port
- Unix Helper Timeout (Minutes)
- Unix Helper Threads

Unix Helper Configuration Port

This attribute specifies the port to which the Unix Helper ‘listens’ upon startup for the configuration information contained in the Unix Helper Authentication Port, Unix Helper Timeout (Minutes), and Unix Helper Threads attributes. The default is 8946.

Unix Helper Authentication Port

This attribute specifies the port to which the Unix Helper ‘listens’ for authentication requests after configuration. The default port is 7946.

Unix Helper Timeout (Minutes)

This attribute specifies the number of minutes that users have to complete authentication. If users surpass the allotted time, authentication automatically fails. The default time is set to 3 minutes.

Unix Helper Threads

This attribute specifies the maximum number of permitted simultaneous Unix authentication sessions. If the maximum is reached at a given moment, subsequent authentication attempts are not allowed until a session is freed up. The default is set to 5.

Organization Attribute

The organization attribute for the Unix Authentication service is:

Unix Module Authentication Level

The authentication level is set separately for each method of authentication. The value indicates how much to trust an authentication. Once a user has authenticated, this value is stored in the SSO token for the session. When the SSO token is presented to an application the user wants to access, the application uses the stored value to determine whether the level is sufficient to grant the user

access. (The value in this attribute is not specifically used by DSAME but by any external application that may chose to use it.) If the authentication level stored in an SSO token does not meet the minimum value required, the application can prompt the user to authenticate again through a service with a higher authentication level. The default value is `0`, the lowest authentication level.

NOTE If no authentication level is specified, the SSO token stores the value specified in the Core Authentication attribute Default Auth Level. See “Default Auth Level,” on page 107 for details.

Logging Attributes

The Logging Attributes are global attributes. The values applied to them are applied across the iPlanet Directory Server Access Management Edition (DSAME) configuration and are inherited by every configured organization. (They can not be applied directly to roles or organizations as the goal of global attributes is to customize the DSAME application.) The Logging Attributes are:

- Max Log Size
- Number of History Files
- Log Location
- Logging Type
- Database User Name
- Database User Password
- Database Driver Name

Max Log Size

This attribute accepts a value for the maximum size (in bytes) of a DSAME log file. A number up to one million can be input in the value field. The default value is `1000000`.

Number of History Files

This attribute has a value equal to the number of backup log files that will be retained for historical analysis. Any integer can be input depending on the partition size and available disk space of the local system. The default value is 3.

Log Location

The file-based logging function needs a location where log files can be stored. This field accepts a full directory path to that location. The default location is `/DSAMEServer_root/SUNWam/logs/`. If a non-default directory is being used, this directory must have write permission to the user under which DSAME is running.

NOTE Any changes in logging attribute values require a restart of the DSAME server before the changes are activated.

Logging Type

This attribute allows you to specify either File, for flat file logging, or JDBC for database logging.

Database User Name

This attribute accepts the name of the user that will connect to the database when the Logging Type attribute is set to JDBC.

Database User Password

This attribute accepts the database user password when the Logging Type attribute is set to JDBC.

Database Driver Name

This attribute allows the user to specify the driver that is to be used for the logging implementation class.

Chapter 16

Naming Attributes

The Naming Attributes are global attributes. The values applied to them are carried across the iPlanet Directory Server Access Management Edition (DSAME) configuration and inherited by every configured organization. (They can not be applied directly to roles or organizations as the goal of global attributes is to customize the DSAME application.)

The Naming Service allows clients to find the correct service URL if the platform is running more than one DSAME server. When a naming URL is found, the naming service will decode the session of the user and dynamically replace the protocol, host, and port with the parameters from the session. This ensures that the URL returned for the service is for the host that the user session was created on. The Naming Attributes are:

- Profile Service URL
- Session Service URL
- Logging Service URL

Profile Service URL

This field takes a value equal to

`http://<hostname>:<port>/<DEPLOY_URI>/profileservice`

This syntax allows for dynamic substitution of the profile URL based on the specific session parameters.

Session Service URL

This field takes a value equal to

`%protocol://%host:%port/<DEPLOY_URI>/sessionservice`

This syntax allows for dynamic substitution of the session URL based on the specific session parameters.

Logging Service URL

This field takes a value equal to

`%protocol://%host:%port/<DEPLOY_URI>/loggingservice`

This syntax allows for dynamic substitution of the logging URL based on the specific session parameters.

Chapter 17

Platform Attributes

The Platform Attributes are global attributes. The values applied to them are carried across the iPlanet Directory Server Access Management Edition (DSAME) configuration and inherited by every configured organization. (They can not be applied directly to roles or organizations as the goal of global attributes is to customize the DSAME application.) The Platform Attributes are:

- Server List
- Platform Locale
- Cookie Domains
- Login Service URL
- Logout Service URL
- Available Locales
-

Server List

The naming service reads this attribute at initialization time. This list contains the DSAME session servers in a single DSAME configuration. For example, if two DSAME servers are installed and should work as one, they must both be included in this list. If the host specified in a request for a service URL is not in this list, the naming service will reject the request. The first value in the list specifies the host name and port of the server specified during installation. Additional servers can be added using the format `protocol://<server_domain>:<port>`.

Platform Locale

The platform locale value is the default language subtype that DSAME was installed with. The authentication, logging and administration services are administered in the language of this value. The default is `en_US`. See Table 9-1 on page 108 for a listing of all supported language subtypes.

Cookie Domains

This is the list of domains that will be returned in the cookie header when setting a cookie to the user's browser during authentication. If empty, no cookie domain will be set. In other words, the DSAME session cookie will only be forwarded to the DSAME server itself and no other servers in the domain. If SSO is required with other servers in the domain, this attribute must be set with the cookie domain. If you had two interfaces in different domains on one DSAME server then you would need to set both cookie domains in this attribute. If a load balancer is used, the cookie domain must be that of the load balancer's domain, not the servers behind the load balancer. The default value for this field is the domain of the installed DSAME server.

Login Service URL

This field specifies the URL of the login page. The default value for this attribute is `http://<hostname>:<port>/amserver/login`.

Logout Service URL

This field specifies the URL of the logout page. The default value for this attribute is `http://<hostname>:<port>/amserver/logout`.

Available Locales

This attribute stores all available locales configured for the platform. Consider an application that lets the user choose their locale. This application would get this attribute from the platform profile and present the list of locales to the user. The user would choose a locale and the application would set this in the user entry `preferredLocale`.

Chapter 18

Session Attributes

The Session Attributes are dynamic attributes. The values applied to these attributes are applied to either a role or an organization. If the role is assigned to a user or a user is assigned to the organization, these attributes, by default, are inherited by the user. The Session Attributes are:

- Max Session Time (Minutes)
- Max Idle Time (Minutes)
- Max Caching Time (Minutes)

Default session values are set in Service Management for all DSAME registered organizations. These values can be set differently for separate organizations by registering the session service to the specific organization, creating a template and inputting a value other than the default value.

Max Session Time (Minutes)

This attribute accepts a value in minutes to express the maximum time before the session expires and the user must reauthenticate to regain access. A value of 1 or higher will be accepted. The default value is `120`. (To balance the requirements of security and convenience, consider setting the Max Session Time interval to a higher value and setting the Max Idle Time interval to a relatively low value.)

Max Idle Time (Minutes)

This attribute accepts a value (in minutes) equal to the maximum amount of time without activity before a session expires and the user must reauthenticate to regain access. A value of 1 or higher will be accepted. The default value is `30`. (To balance the requirements of security and convenience, consider setting the Max Session Time interval to a higher value and setting the Max Idle Time interval to a relatively low value.)

Max Caching Time (Minutes)

This attribute accepts a value (in minutes) equal to the maximum interval before the client contacts DSAME to refresh cached session information. A value of 0 or higher will be accepted. The default value is `3`.

URL Policy Agent Attributes

URL Policy Agent attributes are policy attributes. Policy attributes are privilege attributes. They deny or allow users access to web resources. They are configured through the Policy Management view. When a policy is created, policy attributes may be assigned to organizations via Show Policies in the User Management view.

Policy attributes list resources that are assigned the same action. When you specify an action for a resource, you effectively specify which attribute will list the resource as one of its values. The URL Policy Agent attributes are:

- URL Policy Agent Action: Allow
- URL Policy Agent Action: Deny
- URL Policy Agent Action: Not Enforced
- Additional Information

URL Policy Agent Action: Allow

This attribute lists the URLs that a user is allowed to access. If the URL that an authenticated user wants to access matches a URL listed here and the request is not explicitly denied by another rule, access is granted. The default value is * (all). The field will take any URL that a user should be allowed to access.

The Allow list is checked after the Not Enforced list and the Deny list. If a matching URL is not found after the Allow list is checked, the access request is denied.

URL Policy Agent Action: Deny

This attribute lists the URLs a user is not allowed to access. If the URL that an authenticated user wants to access matches an URL listed here, access is denied. The default value is `/config`, denying access to the configuration files. The field will take any URL to which a user should be denied access. (The Deny list is checked after the Not Enforced list.)

URL Policy Agent Action: Not Enforced

This attributes lists URLs that can be accessed by any user who is in the organization or assigned the role to which this policy applies. The following URLs are default values of the Not Enforced attribute:

- `http://<host>:<port>/amserver/console*`
- `http://<host>:<port>/amserver/login*`
- `http://<host>:<port>/amserver/images*`
- `http://<host>:<port>/amserver/admin*`
- `http://<host>:<port>/amserver/docs*`
- `http://<host>:<port>/amserver/logout`
- `http://<host>:<port>/amserver/index.html`
- `http://<host>:<port>/amserver/namingservice`
- `http://<host>:<port>/amserver/loggingservice`
- `http://<host>:<port>/amserver/sessionservice`
- `http://<host>:<port>/amserver/profileservice`
- `http://<host>:<port>/amagent/html/URLAccessDenied.html`

Allowing all users access to these URLs makes user authentication possible.

Additional Information

Below is additional information specific to policy attributes.

Hierarchy Of Enforcement

In the enforcement of policy, the first URL list checked is Not Enforced, followed by the Deny list and, lastly, the Allow list. Deny privileges takes precedence over allow privileges. An empty Deny list will allow only those resources that are allowed by the Allow list. An empty Allow list will not allow access to any resources except those in the Not Enforced list. By default, the Allow list would contain the "*" entry, allowing access to all resources. However, as the Deny list takes precedence over the Allow list, anything in the Deny list will not be accessible. If the URL access policy cannot be resolved between the Deny and Allow lists, access will not be allowed to the resource.

Configuring Policy Attributes

The Allow and Deny attributes support the use of the asterisk (*) wildcard to represent one or more characters. Use the wildcard to specify resources so that rules can be more flexible. You can use one or more wildcards anywhere in the resource name. For example:

- `http://www.madisonparc.com/*`
- `*.madisonparc.com`
- `*/accessAll`
- `http://www.madisonparc.com/*/engr*`

If you specify part of an URL without using the wildcard character, the rule applies only to resources that are an exact match. For example, the following URL:

```
http://www.madisonparc.com/*
```

matches any URL that begins `http://www.madisonparc.com/`

However, the following URL:

```
http://www.madisonparc.com/
```

matches only `http://www.madisonparc.com/`

NOTE The Not Enforced list is the first list checked by the Policy Manager. Do not use the asterisk wildcard alone in this field. No URL access policy will be enforced and all users will have access to all web pages.

Chapter 20

User Attributes

There are two places which house user attributes: the Service Management and User Management windows. The Service Management window contains default attributes for registered organizations. The User Management window contains user entry attributes.

- Service Management Attributes
- User Profile Attributes
- Unique User IDs

Service Management Attributes

The User Attributes in the Service Management window are dynamic attributes. The values applied to dynamic attributes are assigned to a role or an organization that is configured in DSAME. When the role is assigned to a user or a user is assigned to the organization, the dynamic attributes become a characteristic of the user. The User Attributes are divided into:

- User Preferred Language
- User Preferred Timezone
- Inherited Locale
- Admin DN Starting View
- Default User Status
- User Auth Modules

Default user values are set in Service Management for all DSAME registered organizations. These values can be set differently for separate organizations by registering the user service to the specific organization, creating a template and inputting a value other than the default value.

User Preferred Language

This field specifies the user's choice for the text language displayed in the DSAME console. The default value is `en`. This value maps a set of localization keys to the user session so that onscreen text appears in a language appropriate for the user.

User Preferred Timezone

This field specifies the time zone in which the user accesses the DSAME console. There is no default value.

Inherited Locale

This field specifies the locale for the user. The default value is `en_US`. Any value from Table 9-1 on page 108 can be used.

Admin DN Starting View

If this user is a DSAME administrator, this field specifies the node that would be the starting point displayed in the DSAME console when this user logs in. There is no default value. A valid DN for which the user has, at the least, read access can be used.

CAUTION If the Top Level Administrator wishes to assign a user the administration privileges to two different groups, the Admin DN Starting View should be specified as the DN of the level above BOTH groups. This holds true for any entries at the same level such as organizations, groups, or People Containers. This action could result in the user being able to manage an organization, group, or People Container that is not specifically assigned to them. It is up to the Top Level Administrator to decide on the ACI model and where to define the DN Starting View.

Default User Status

This option indicates the default status for any newly created user. This status is superseded by the User Entry status. Only active users can authenticate through DSAME. The default value is `Active`. Either of the following can be selected from the pull-down menu:

- `Active` – The user can authenticate through DSAME.
- `Inactive` – The user cannot authenticate through DSAME, but the user profile remains stored in the directory.

The individual user status is set by registering the User service, choosing the value, applying it to a role and adding the role to the user's profile.

User Auth Modules

This option specifies individual user authentication modules to be accessed when the "User Based Auth" option is chosen in Core Authentication. The user will be presented with the configured authentication module(s) after entering the user id. The administrator can select one or more authentication services (from Anonymous, Certification, LDAP, Membership, RADIUS, SafeWord, and Unix) for the user to authenticate through.

NOTE Currently, the SafeWord authentication service is supported only on the Solaris platform. The Unix authentication service is not supported on Windows 2000.

User Profile Attributes

The User Profile Attributes are default attributes for user profiles. These values are set in the User Profile view by an administrator or by the user when they log on. Administrators can add their own user attributes to the user profile or create a new service. For more information see iPlanet Directory Server Access Management Edition Programmer's Guide.

NOTE DSAME does not enforce uniqueness for attributes within user entries. For example, `userA` and `userB` are both created in the same organization. For both, the email address attribute can be set `jimb@madisonparc.com`. The administrator can configure iPlanet Directory Server's attribute uniqueness plug-in to help enforce unique attribute values. For more information, see Unique User IDs at the end of this chapter or the iPlanet Directory Server Administrator's Guide.

Home Address

This field can take the home address of the user.

User Status

This option indicates whether the user is allowed to authenticate through DSAME. Only active users can authenticate through DSAME. The default value is `Active`. Either of the following can be selected from the pull-down menu:

- `Active` – The user can authenticate through DSAME.
- `Inactive` – The user cannot authenticate through DSAME, but the user profile remains stored in the directory.

NOTE Changing the user status to `Inactive` only affects authentication through DSAME. The Directory Server uses the `nsAccountLock` attribute to determine user account status. User accounts inactivated for DSAME authentication can still perform tasks that do not require DSAME. To inactivate a user account in the directory, and not just for DSAME authentication, set the value of `nsAccountLock` to `false`. If delegated administrators at your site will be inactivating users on a regular basis, consider adding the `nsAccountLock` attribute to the iDSAME User Profile page. See the *iPlanet Directory Server Access Management Edition Programmer's Guide* for details.

First Name

This field takes the first name of the user. (The First Name value and the Last Name value identify the user in the Currently Logged In field in the upper right corner of the DSAME console.)

Last Name

This field takes the last name of the user. (The First Name value and the Last Name value identify the user in the Currently Logged In field in the upper right corner of the DSAME console.)

Full Name

This field takes the full name of the user.

Password

This field takes the password for the name specified in the UserId field.

Confirm Password

Password type attributes automatically set this field.

Email Address

This field takes the email address of the user.

Employee Number

This field takes the employee number of the user.

Telephone Number

This field takes the telephone number of the user.

Roles For This User

This field takes the valid DN for the roles that are applied to the user.

Groups for this User

This field takes the DN of the groups of which this user is a member.

Account Expiration Date

If this attribute is present, the authentication service will check the date disallow login if the user's account life is less than the current date. The format for this attribute is as follows:

```
(mm/dd/yy hh:mm)
```

NOTE There is no error checking on syntax for this attribute. If incorrect, the user will not be able to login until it is corrected.

Unique User IDs

In order to enforce uid uniqueness within the DSAME application, the plug-in, available in iPlanet Directory Server, must be configured as follows:

```
dn: cn=uid uniqueness,cn=plugins,cn=config
objectClass: top
objectClass: nsSlapdPlugin
objectClass: extensibleObject
cn: uid uniqueness
nsslapd-pluginPath: /ids908/lib/uid-plugin.so
nsslapd-pluginInitfunc: NSUniqueAttr_Init
```

```
nsslapd-pluginType: preoperation
nsslapd-pluginEnabled: on
nsslapd-pluginarg0: attribute=uid
nsslapd-pluginarg1: markerObjectClass=nsManagedDomain
nsslapd-plugin-depends-on-type: database
nsslapd-pluginId: NSUniqueAttr
nsslapd-pluginVersion: 5.1
nsslapd-pluginVendor: Sun | Netscape Alliance
nsslapd-pluginDescription: Enforce unique attribute values
```

It is recommended that the `nsManagedDomain` object class is used to mark the organization in which uid uniqueness is desired. The plug-in is not enabled by default.

To configure the uniqueness of uids per organization, either add the DN for each organization in the plug-in entry or use the marker object class option and add `nsManagedDomain` to each top level organization entry.

```
nsslapd-pluginEnabled: on
nsslapd-pluginarg0: attribute=uid
nsslapd-pluginarg1: markerObjectClass=nsManagedDomain
```

Index

A

C

D

E

F

G

H

L

M

N

O

P

R

S

T

U

V

W